Discrete Mathematics and Theoretical Computer Science **4**, 2001, 291–300

Simple Equational Specifications of Rational Arithmetic

Lawrence S. Moss

Department of Mathematics, Indiana University, Bloomington IN 47405 USA

received June 16, 2000, *revised October 11, 2001*, *accepted October 15, 2001.*

We exhibit an initial specification of the rational numbers equipped with addition, subtraction, multiplication, greatest integer function, and absolute value. Our specification uses only the sort of rational numbers. It uses one hidden function; that function is unary. But it does not use an error constant, or extra (hidden) sorts, or conditional equations. All of our work is elementary and self-contained.

Keywords: equational specification, hidden function symbols, rational numbers

1 Introduction

This paper is a comment on the use of hidden functions in a well-studied example in the field of abstract data types. We are concerned with the rational numbers, considered as an algebra Q with the constants 0 and 1 and the operations of addition, subtraction, and multiplication, greatest integer function $\lfloor x \rfloor$ and absolute value function $|x|$. To specify Q using initial algebra semantics means coming up with a possibly bigger signature Σ, writing a finite set E of equations in Σ, and then showing that the initial Σ–model of E is an expansion of Q.

This particular example of rational arithmetic (without $\lfloor x \rfloor$ and $|x|$) seems to have been important historically, and a number of sources mention it. It is problematic because one cannot take a specification of the integers and add an inverse function $inv(x)$. (The natural equation to add would be $x \times \mathtt{inv}(x) = \mathtt{1}$. But there is no way to equip the rationals with such an operation; there is no inverse of 0.) It is well-known that Q can be specified in some version of *many-sorted* equational logic. For example, Ehrig and Mahr [4] has a specification using "hidden" sorts of integers and booleans and also an error constant. This raises the issue of whether the error constant is necessary, and indeed it also raises the same issue about the use of more than one sort. It is also not hard to give a specification avoiding the error constant and using conditional equations and two sorts (see [5]). But then this raises the same question about conditional equations.

Ehrig and Mahr were also of the opinion (see p. 150 of [4]) that "Similar to other examples ..., there seems to be also in this example no way around hidden function symbols." It is not clear whether they mean that hidden *sorts* were needed, but one senses that they were. Meseguer's review [5] of [4] interprets their comment by saying, "the authors conclude in 6.10 that there is no way around heavily using hidden functions and error constants to get the rational numbers." Again, it is not clear what would constitute a "heavy" use, but one senses that it would be the use of an additional sort. For it had been known from the work of Thatcher et al. [6] (following earlier results of Majster) that there are examples where hidden sorts are indeed necessary. And since rational arithmetic was not easily specifiable without hidden sorts, one might think that it was *impossible* to do so.

The goal of this note is to clear up the situation with regard to Q. Neither extra sorts nor error constants are needed to specify Q. Moreover, one can get by with just one hidden function, and that function can be taken to be unary. The key to our work is a recent result of Calkin and Wilf [2] which shows that there is a bijection $g : N \to Q^+$ which is definable by a very simple set of equations.

We should mention that the fact that Q has a finite specification with no hidden sorts follows immediately from the main theorem of Bergstra and Tucker [1]. Indeed, [1] has the stronger result that a minimal computable algebra has a specification which may be taken to a finite complete rewriting system. We shall have more to say on the "complete rewriting system" part at the very end of our note. For now, here is an explanation of how Bergstra and Tucker's theorem implies that Q has an equational specification. Since the rationals are countable, there are functions α, β, and γ such that $\langle Q,0,1,+,-,\times\rangle \cong \langle N,0,1,\alpha,\beta,\gamma\rangle$. Moreover, α, β, and γ may be taken to be primitive recursive. Now "minimal" means that every element of the carrier set should be the denotation of some term. This is not the case with $\langle Q,0,1,+,-,\times\rangle$, so not with $\langle N,0,1,\alpha,\beta,\gamma\rangle$ either. But if we add to our signature a symbol $\mathtt{s}$ and interpret it by the successor function s on N, then $N' = \langle N,0,1,\alpha,\beta,\gamma,s\rangle$ is minimal (and computable). So by the main theorem of [1], there is a bigger signature (but without new sorts) and a set of equations in it specifying Q'.

However, if one follows the method of [1], the specification of N' that one would get would be large. (The exact size would depend on the exact build up of α, β, γ as primitive recursive functions. My guess is that the actual specification would be too large for many people to ever write explicitly.) Our purpose is to exhibit small specifications which can be understood from first principles. These should be interesting to people who have worked in the area, and it would be suitable for classroom or textbook presentation.

The easiest way to get a one-sorted specification of Q is to begin with a specification for Z (any one will do, for example the laws of commutative rings with 1). Then add a function symbol $\mathtt{f}$ of arity 4, with the equation:

$$\mathtt{f}(w,x,y,z) \times (1+w^2+x^2+y^2+z^2) \quad = \quad 1.$$

The intended semantics is $f(w,x,y,z) = (1+w^2+x^2+y^2+z^2)^{-1}$. The point is that this f is total function on the rationals, and moreover, for every natural number $n \geq 1$, there are natural numbers w, x, y, and z so that $f(w,x,y,z) = 1/n$. This uses the classical result of Lagrange that every natural number is the sum of four squares. It is not hard to check that this gives a specification of Q. We omit the details here since similar ones will be presented in Section 2 for a different set of equations below. The reason that we want to consider a different specification is that there does not seem to be a way to add other interesting functions, such as absolute value or greatest integer, on top of this specification. Another reason is that I could not see a way to reduce the arity of f. Perhaps a unary function like $f(x) = (1+x+x^2)^{-1}$ would work, but the matter is open. (As Ignacio Viglizzo pointed out to me, $f(x) = (1+x^2)^{-1}$ does not work because the smallest subring of Q closed under this operation does not contain $1/3$.)

Our results are summarized in the table below. Each line represents a specification. The result that $\langle Q,0,1,+,-,\times,\lfloor\ \rfloor\rangle$ can be specified with one hidden symbol which is unary is probably the most important of this paper.

Structure	Hidden symbols	Number of Hidden Equations
$\langle Q,0,1,+,-,\times\rangle$	one 4-ary	1
$\langle Q,0,1,+,-,\times\rangle$	two unary	21
$\langle Q,0,1,+,-,\times,\lfloor\ \rfloor\rangle$	one unary	18
$\langle Q,0,1,+,-,\times,\lfloor\ \rfloor,\vert\ \vert\rangle$	one unary	18

2 A Specification of $\langle Q,0,1,+,-,\times,\lfloor\ \rfloor\rangle$

We begin with the following result:

Proposition 1 *There is a unique $f : Z \to Z$ so that for all $n \in Z$:*

$$\begin{array}{lcl} f(4n) & = & 1 \\ f(1+4n) & = & f(n) \\ f(2+4n) & = & f(n)+f(1+n) \\ f(3+4n) & = & f(1+n) \end{array}$$

Moreover,

1. *For all $n \in Z$, $f(n) \geq 1$.*

2. *For all a, $\gcd(f(a), f(1+a)) = 1$.*

3. *If a and b are positive integers such that $\gcd(a,b) = 1$, then there is some $c \geq 0$ so that $f(c) = a$ and $f(1+c) = b$.*

Proof For the uniqueness, note that for all integers n, $|1+4n| > n$ and $|2+4n| > n+1$. This implies that for all n except 0, the values of the left sides of the recursion equations for f are always greater in absolute value than those on the right. This, together with the fact that $f(0) = 1$, means that f is specified uniquely on all integers.

Parts (1) and (2) are an easy induction on n. For (3), we argue by induction on $\max(a,b)$. If $a = b = 1$, we take $c = 0$. In case $a > b > 1$, we consider $a-b$ and b. Clearly $\gcd(a-b,b) = 1$. (This is just the argument behind the Euclidean algorithm for the gcd.) And $\max(a-b,b) < \max(a,b)$. By our induction hypothesis, let c be so that $f(c) = a-b$ and $f(1+c) = b$. Then $f(2+4c) = a$ and $f(3+4c) = b$. In case $1 < a < b$, we consider $b-a$ and b. Again, $\gcd(a,b-a) = 1$, and $\max(b-a,a) < \max(a,b)$. By our induction hypothesis, let c be so that $f(c) = a$ and $f(1+c) = b-a$. Then $f(1+4c) = a$ and $f(2+4c) = b$. ⊣

Our f is not the only function with the properties of Proposition 1, of course. For our purposes, the only facts we need are those of the proposition, together with the facts that some natural functions related to f are equationally specifiable. We turn to these matters shortly.

But first, we should mention that this function f is based on a function from Calkin and Wilf's article [2]. That paper considers the following simpler version which we call f_0: $f_0(0) = 1$, $f_0(2n+1) = f_0(n)$, and $f_0(2n+2) = f_0(n) + f_0(n+1)$. Then [2] shows that for all $n \geq 0$, $f_0(n)$ and $f_0(n+1)$ are relatively prime, and that for all relatively prime a and b there is a *unique* n so that $f_0(n) = a$ and $f_0(n+1) = b$.

In other words, if we define $g : N \to Q^+$ by $g(n) = f_0(n)/f_0(n+1)$, then g is a bijection. This leads to a rather explicit proof of Cantor's theorem that the rationals are countable.

The problem for us about f_0 is that the equation $f_0(2n+2) = f_0(n) + f_0(n+1)$ implies that $f_0(-1) = 0$. We needed to modify f_0 to obtain a function on Z all of whose values are positive. We lose the uniqueness assertion, but this is not a big problem.

Returning to our development, we extend f to a function which we also call f in the following way: $f(x) = f(\lfloor x \rfloor)$. (Here $\lfloor x \rfloor$ is the greatest integer $\leq x$; for example $\lfloor -1/2 \rfloor = -1$.) This is one natural way to extend f. There are other ways, and they would lead to other sets of equations. We chose this way because the details are the simplest that we could find, and because the resulting set of equations is the smallest. Once again, we use $f(x) = f(\lfloor x \rfloor)$. This determines $f : Q \to Q$. Next, let $g : Q \to Q$ be given by $g(x) = f(x)/f(1+x)$. Then again $g(x) = g(\lfloor x \rfloor)$. The point about g is that for every positive rational number m/n in lowest terms, there is some natural number a so that $g(a) = m/n$.

We need the following equations involving g and $\lfloor x \rfloor$:

$$
\begin{array}{lcllcl}
\lfloor g(4n) \rfloor & = & h(n) & \lfloor -g(4n) \rfloor & = & -1 \\
\lfloor g(1+4n) \rfloor & = & 0 & \lfloor -g(1+4n) \rfloor & = & -1 \\
\lfloor g(2+4n) \rfloor & = & 1 + \lfloor g(n) \rfloor & \lfloor -g(2+4n) \rfloor & = & -1 + \lfloor -g(n) \rfloor \\
\lfloor g(3+4n) \rfloor & = & f(1+n) & \lfloor -g(3+4n) \rfloor & = & -f(1+n)
\end{array}
$$

Note that here n is an integer. We can obtain equations valid for all rational x by replacing n by $\lfloor x \rfloor$ throughout. The function $h : Z \to Z$ which figures into g is given by

$$
\begin{array}{lcl}
h(4n) & = & 1 \\
h(1+4n) & = & h(n) \\
h(2+4n) & = & 0 \\
h(3+4n) & = & h(1+n)
\end{array}
$$

As with g, h extends naturally to a function on Q by $h(x) = h(\lfloor x \rfloor)$. The point is that for all n, $h(n) = 1$ iff $f(n) = 1$, and $h(n) = 0$ iff $f(n) > 1$. So $\lfloor g(4n) \rfloor = 0$ iff $h(1+4n) = 0$, and $\lfloor g(4n) \rfloor = 1$ iff $h(1+4n) = 1$. It follows that for all $x \in Q$, $\lfloor g(4n) \rfloor = h(1+4n) = h(n)$. As we have seen, the extended h is equationally specifiable.

2.1 The specification

We take our signature Σ to consist of the symbols $\mathtt{0}$, $\mathtt{1}$, $\mathtt{+}$, $-$, $\times$, $\lfloor$, $\mathtt{f}$, $\mathtt{g}$, $\mathtt{h}$, where $\mathtt{0}$ and $\mathtt{1}$ are 0-ary (i.e., constants); $-$, $\lfloor$, $\mathtt{f}$, $\mathtt{g}$, and $\mathtt{h}$ are 1-ary; and $+$ and $\times$ are binary. As we have already been doing, we use a different font to distinguish syntax from semantics. Our set E of equations is listed in the box below. Of course, the main example of a Σ-algebra satisfying E is

$$\mathcal{Q} \quad = \quad \langle Q, 0, 1, +, -, \times, \lfloor\ \rfloor, f, g, h \rangle,$$

where all of the interpretations shown are the ones we have already considered. That is, henceforth $\mathcal{Q}$ denotes the rationals equipped with all of the functions above.

Here are a few comments on our notation and equations: In general, we omit the parentheses on $\lfloor(x)$, and we sometimes omit other parentheses for readability. We use 2 as an abbreviation for $1+1$, and similarly for 3 and 4. Further, $4\lfloor x$ abbreviates $4 \times \lfloor x$. In the invariance equation (3), we do not need

The set E of equations for $\langle Q, 0, 1, +, -, \times, \lfloor\ \rfloor\rangle$ using hidden functions $\mathtt{f}$, $\mathtt{g}$, and $\mathtt{h}$

1. The equational laws of commutative rings with 1.
2. Concerning $\lfloor$: $\lfloor 0 = 0$, $\lfloor(\mathtt{1}+x) = \mathtt{1}+\lfloor x$, and $\lfloor(-\mathtt{1}+x) = -\mathtt{1}+\lfloor x$.
3. The laws that $\lfloor$ is invariant for $\mathtt{f}$ and $\mathtt{h}$: $\mathtt{f}x = \mathtt{f}\lfloor x$ and $\mathtt{h}x = \mathtt{h}\lfloor x$.
4. The connection of $\mathtt{g}$ and $\mathtt{f}$: $\mathtt{g}(x) \times \mathtt{f}(\mathtt{1}+x) = \mathtt{f}(x)$.
5. The recursion equations for $\mathtt{f}$, $\mathtt{h}$, $\lfloor\mathtt{g}$ and $\lfloor-\mathtt{g}$:

$$
\begin{array}{lcllcl}
\mathtt{f}(\mathtt{4}\lfloor x) & = & \mathtt{1} & \mathtt{h}(\mathtt{4}\lfloor x) & = & \mathtt{1} \\
\mathtt{f}(\mathtt{1}+\mathtt{4}\lfloor x) & = & \mathtt{f}(x) & \mathtt{h}(\mathtt{1}+\mathtt{4}\lfloor x) & = & \mathtt{h}(x) \\
\mathtt{f}(\mathtt{2}+\mathtt{4}\lfloor x) & = & \mathtt{f}(x)+\mathtt{f}(\mathtt{1}+x) & \mathtt{h}(\mathtt{2}+\mathtt{4}\lfloor x) & = & \mathtt{0} \\
\mathtt{f}(\mathtt{3}+\mathtt{4}\lfloor x) & = & \mathtt{f}(\mathtt{1}+x) & \mathtt{h}(\mathtt{3}+\mathtt{4}\lfloor x) & = & \mathtt{h}(\mathtt{1}+x) \\
 & & & & & \\
\lfloor\mathtt{g}(\mathtt{4}\lfloor x) & = & \mathtt{h}(x) & \lfloor-\mathtt{g}(\mathtt{4}\lfloor x) & = & -\mathtt{1} \\
\lfloor\mathtt{g}(\mathtt{1}+\mathtt{4}\lfloor x) & = & 0 & \lfloor-\mathtt{g}(\mathtt{1}+\mathtt{4}\lfloor x) & = & -\mathtt{1} \\
\lfloor\mathtt{g}(\mathtt{2}+\mathtt{4}\lfloor x) & = & \mathtt{1}+\lfloor\mathtt{g}(x) & \lfloor-\mathtt{g}(\mathtt{2}+\mathtt{4}\lfloor x) & = & -\mathtt{1}+\lfloor-\mathtt{g}(x) \\
\lfloor\mathtt{g}(\mathtt{3}+\mathtt{4}\lfloor x) & = & \mathtt{f}(\mathtt{1}+x) & \lfloor-\mathtt{g}(\mathtt{3}+\mathtt{4}\lfloor x) & = & -\mathtt{f}(\mathtt{1}+x)
\end{array}
$$

$\mathtt{g}x = \mathtt{g}\lfloor x$; the ground instances of this turn out to be derivable. For the same reason, we do not need $\lfloor\lfloor x = \lfloor x$ in (2). Concerning (5), note that earlier we had the same laws but for integers n. The important point is that since $f(x) = f(\lfloor x \rfloor)$ for all x, the laws in (5) are valid in Q.

Finally, notice that E has $2+1+16 = 19$ equations that use the hidden symbols.

2.2 Proof of correctness

As usual, we let T_Σ be the set of (ground) Σ-terms, and T_Σ/E the quotient of T_Σ by the smallest Σ-congruence including the substitution instances of E. Let $\varepsilon : T_\Sigma \to Q$ be the unique Σ-homomorphism. We write $E \vdash t = u$ to mean that $t = u$ is derivable from E in equational logic. (This is the logical system whose axioms are the substitution instances of the equations in $E \cup \{x = x\}$ and whose rules of inference correspond to the symmetric and transitive properties of equality and to the substitution of equals for equals in functions.) We shall only be interested in this when t and u are ground terms, and then it also means that $[t] = [u]$ in T_Σ/E.

We prove that $T_\Sigma/E \cong Q$. The idea is that every term is provably equal, mod E, to a special kind of term which we call *normal*. To state the definition, and for our future work, we associate with each integer n a term $\mathtt{n}$ in the following way. For $n = 0$, we set $\mathtt{n}$ to be $\mathtt{0}$; for $n = 1+\cdots+1$, we set $\mathtt{n}$ to be $\mathtt{1}+\cdots+\mathtt{1}$; and for $n = -(1+\cdots+1)$, we use $-(\mathtt{1}+\cdots+\mathtt{1})$. Now we can say that our normal terms are 0, $\mathtt{g}(\mathtt{n})$ for $n \geq 1$, and $-\mathtt{g}(\mathtt{n})$ for $n \in Z$.

Lemma 2 *Let a, b, and $c \in Z$.*

1. *If $a+b=c$, then $E \vdash \mathtt{a}+\mathtt{b}=\mathtt{c}$, and similarly for $\times$ and $-$.*

2. $E \vdash \mathtt{a} = \lfloor \mathtt{a}$.

3. *If $f(a)=b$, then $E \vdash \mathtt{f}(\mathtt{a}) = \mathtt{b}$, and similarly for h and* $\mathtt{h}$.

Proof Part (1) is an easy consequence of the initiality of Z among commutative rings with 1. Part (2) is an easy induction on $|a|$, as is (3). In addition, (3) uses the invariance laws for $\lfloor$ with $\mathtt{f}$ and $\mathtt{h}$, and also parts (1) and (2). It is essentially an elaboration of the proof of Proposition 1. $\dashv$

Lemma 3 *If $t \in T_\Sigma$ is such that $E \vdash t \times \mathtt{f}(\mathtt{1}+\mathtt{n}) = \mathtt{f}(\mathtt{n})$, then $E \vdash t = \mathtt{g}(\mathtt{n})$.*

Proof Let $m = 1+4(1+n)$, so that $f(m)=1$, $f(1+m) = f(1+n)$, and $g(m) = 1/f(1+n)$. Then $E \vdash \mathtt{g}(\mathtt{m}) \times \mathtt{f}(\mathtt{1}+\mathtt{m}) = \mathtt{1}$. And by Lemma 2(3), $E \vdash \mathtt{f}(\mathtt{1}+\mathtt{n}) = \mathtt{f}(\mathtt{1}+\mathtt{m})$. From these facts and the commutative, associative, and unit laws, we deduce according to E that

$$\begin{array}{lll} t & = & t \times \mathtt{1} \\ & = & t \times \mathtt{f}(\mathtt{1}+\mathtt{m}) \times \mathtt{g}(\mathtt{m}) \\ & = & t \times \mathtt{f}(\mathtt{1}+\mathtt{n}) \times \mathtt{g}(\mathtt{m}) \\ & = & \mathtt{f}(\mathtt{n}) \times \mathtt{g}(\mathtt{m}) \\ & = & \mathtt{g}(\mathtt{n}) \times \mathtt{f}(\mathtt{1}+\mathtt{n}) \times \mathtt{g}(\mathtt{m}) \\ & = & \mathtt{g}(\mathtt{n}) \times \mathtt{f}(\mathtt{1}+\mathtt{m}) \times \mathtt{g}(\mathtt{m}) \\ & = & \mathtt{g}(\mathtt{n}) \end{array}$$

$\dashv$

Lemma 4 *Let $a,b \in Z$. Then*

1. $E \vdash \mathtt{ga} = \mathtt{g}\lfloor\mathtt{a}$.

2. *If $\lfloor g(a) \rfloor = b$, then $E \vdash \lfloor \mathtt{ga} = \mathtt{b}$, and if $\lfloor -g(a) \rfloor = b$, then $E \vdash \lfloor -\mathtt{ga} = \mathtt{b}$.*

Proof The first part is an easy calculation using Lemma 3, and the second is an induction on $|a|$ using the first and Lemma 2(3). $\dashv$

Lemma 5 *Let a, b, and $c \in Z$.*

1. *If $g(a) = g(b)$, then $E \vdash \mathtt{g}(\mathtt{a}) = \mathtt{g}(\mathtt{b})$.*

2. *If $g(a) = b$, then $E \vdash \mathtt{g}(\mathtt{a}) = \mathtt{b}$.*

3. *If $g(a)+g(b) = g(c)$, then $E \vdash \mathtt{g}(\mathtt{a}) + \mathtt{g}(\mathtt{b}) = \mathtt{g}(\mathtt{c})$.*

4. *If $g(a)-g(b) = g(c)$, then $E \vdash \mathtt{g}(\mathtt{a}) + (-\mathtt{g}(\mathtt{b})) = \mathtt{g}(\mathtt{c})$.*

5. *If $g(a)\times g(b) = g(c)$, then $E \vdash \mathtt{g}(\mathtt{a}) \times \mathtt{g}(\mathtt{b}) = \mathtt{g}(\mathtt{c})$.*

Proof For part (1), note that since $f(a)$ and $f(1+a)$ are relatively prime, and similarly for $f(b)$ and

$f(1+b)$, we have $f(a) = f(b)$ and $f(1+a) = f(1+b)$. Now our result follows easily from Lemma 3.

Part (2) is similar. If $g(a)$ is the natural number b, then $f(a) = b$ and $f(1+a) = 1$. Then since $E \vdash \mathtt{b} \times \mathtt{f(1+a)} = \mathtt{f(a)}$, we see that $E \vdash \mathtt{g(a)} = \mathtt{b}$.

We also use Lemma 3 to check part (3). We know that

$$\frac{f(a)f(1+b)+f(1+a)f(b)}{f(1+a)f(1+b)} \quad = \quad \frac{f(c)}{f(1+c)}\ .$$

Moreover, the second fraction is reduced. Let m be such that $m \cdot f(c) = f(a)f(1+b)+f(1+a)f(b)$ and $m \cdot f(1+c) = f(1+a)f(1+b)$. Let n be such that $f(n) = 1$ and $f(1+n) = m$. So $g(n) = 1/m$. Using Lemma 2, parts (1) and (3), we see that

$$E \vdash \mathtt{f(1+n)} \times \mathtt{f(c)} \quad = \quad (\mathtt{f(a)} \times \mathtt{f(1+b)}) + (\mathtt{f(1+a)} \times \mathtt{f(b)}),$$

and also that $E \vdash \mathtt{f(n)} = \mathtt{1}$ and that $E \vdash \mathtt{f(1+n)} \times \mathtt{f(1+c)} = \mathtt{f(1+a)} \times \mathtt{f(1+b)}$. So modulo E,

$$\begin{array}{rl}
 & (\mathtt{g(a)+g(b)}) \times \mathtt{f(1+c)} \\
= & (\mathtt{g(a)+g(b)}) \times \mathtt{f(1+c)} \times \mathtt{f(1+n)} \times \mathtt{g(n)} \\
= & (\mathtt{g(a)+g(b)}) \times \mathtt{f(1+a)} \times \mathtt{f(1+b)} \times \mathtt{g(n)} \\
= & (\mathtt{g(a)f(1+a)f(1+b)+g(b)f(1+a)f(1+b)}) \times \mathtt{g(n)} \\
= & (\mathtt{f(a)f(1+b)+f(1+a)f(b)}) \times \mathtt{g(n)} \\
= & \mathtt{f(c)} \times \mathtt{f(1+n)} \times \mathtt{g(n)} \\
= & \mathtt{f(c)} \times \mathtt{f(n)} \\
= & \mathtt{f(c)}
\end{array}$$

(We have omitted some $\times$ signs for readability.) Part (4) is similar, and (5) is the easiest to check. $\dashv$

In the next lemma, recall that the *normal* terms are $\mathtt{0}$ and also $\mathtt{g}n$ and $-\mathtt{g}n$ for $n \in Z$.

Lemma 6 *For every $t \in T_\Sigma$ there is some normal $u \in T_\Sigma$ such that $E \vdash t = u$.*

Proof By induction on t. Obviously $\mathtt{0}$ is normal, and as for $\mathtt{1}$, $E \vdash \mathtt{1} = \mathtt{g(0)}$ by a calculation involving Lemma 3. Assuming the lemma for t and u, we easily get it for $t+u$, $-t$ and $t \times u$. The routine details use Lemma 5.

Concerning $\lfloor t$, we argue as follows: By induction hypothesis, t is normal. If $E \vdash t = \mathtt{0}$, then $E \vdash \lfloor t = \lfloor \mathtt{0} = \mathtt{0}$. Suppose, for example, that $E \vdash t = -\mathtt{g(n)}$. Then $E \vdash \lfloor t = \lfloor -\mathtt{g(n)}$. Now $\lfloor -g(n) \rfloor$ is some natural number b, and by Lemma 5(2), $E \vdash \lfloor -\mathtt{g(n)} = \mathtt{b}$. If $b = 0$, then $\mathtt{b}$ is normal and we are done. Otherwise, let a be so that $g(a) = b$. Then by Lemma 5(2) we see that $E \vdash \lfloor t = \lfloor -\mathtt{g(n)} = \mathtt{g(a)}$.

The argument for $\mathtt{f}(t)$ is similar: If $E \vdash t = \mathtt{0}$, then $E \vdash \mathtt{f}(t) = \mathtt{f(0)} = \mathtt{1} = \mathtt{g(0)}$. Suppose again that $E \vdash t = -\mathtt{g(n)}$. Then $E \vdash \mathtt{f}(t) = \mathtt{f(-g(n))} = \mathtt{f}\lfloor -\mathtt{g(n)}$. This uses the invariance law for $\lfloor$ and $\mathtt{f}$. Now $\lfloor -g(n) \rfloor$ is some natural number b, and by Lemma 5(2), $E \vdash \lfloor -\mathtt{g(n)} = \mathtt{b}$. Let a and c be natural numbers such that $c = f(b)$ and $g(a) = c$, so that $E \vdash \mathtt{f(b)} = \mathtt{c} = \mathtt{g(a)}$. Then $E \vdash \mathtt{f}(t) = \mathtt{g(a)}$.

The same argument works for $\mathtt{h}(t)$. For $\mathtt{g}(t)$, the argument is slightly easier: as soon as we know $E \vdash \lfloor -\mathtt{g(n)} = \mathtt{b}$, we then have $E \vdash \mathtt{g}\lfloor -\mathtt{g(n)} = \mathtt{g(b)}$. This last term is normal. $\dashv$

Theorem 7 $T_\Sigma/E \;\cong\; Q$.

Proof Let $\varphi : T_\Sigma/E \to Q$ be the unique Σ-homomorphism, by initiality. Explicitly, $\varphi([t]) = \varepsilon(t)$. Then φ

is surjective, since $\varphi(\mathtt{0}) = 0$, and for every positive rational r there is some n so that $\varepsilon(\mathtt{g}(\mathtt{n})) = g(n) = r$ (and hence also $\varepsilon(-\mathtt{g}(\mathtt{n})) = -r$).

We conclude by showing that φ is injective. Let $\varepsilon(t) = \varepsilon(u)$. We assume first that this number is positive, say $\varepsilon(t) = g(n)$. Then there are normal terms t' and u' so that $E \vdash t = t'$ and $E \vdash u = u'$. Since $\varepsilon(t') = \varepsilon(t) = g(n) > 0$, t' must be of the form $\mathtt{g}(\mathtt{m})$ for some m. Similarly, u' must be of the form $\mathtt{g}(\mathtt{p})$ for some p. But now $g(m) = g(n) = g(p)$. So by Lemma 5(1), we see that $E \vdash \mathtt{g}(\mathtt{m}) = \mathtt{g}(\mathtt{n}) = \mathtt{g}(\mathtt{p})$. And from this we see that $E \vdash t = \mathtt{g}(\mathtt{n}) = t'$. This concludes the argument when $\varepsilon(t) > 0$. Of course, the same reasoning applies when $\varepsilon(t) < 0$. If $\varepsilon(t) = 0 = \varepsilon(t')$, then again we have normal u and u' as above. We have $\varepsilon(u) = \varepsilon(t)$ and $\varepsilon(u') = \varepsilon(t')$. By normality, u and u' must both be the term $\mathtt{0}$. And so $E \vdash t = \mathtt{0} = t'$. $\dashv$

2.3 One hidden function

We promised at the outset to get things down to one hidden function symbol which is unary. Currently we have three hidden symbols, $\mathtt{f}$, $\mathtt{g}$, and $\mathtt{h}$. To combine them into one, say $\mathtt{i}$, we first describe the intended semantic function i. On integers, i is given by $i(3n) = f(n)$, $i(1+3n) = g(n)$, and $i(2+3n) = h(n)$. Then we extend this to all rationals by $i(x) = i(\lfloor x \rfloor)$. Let $Q^* = \langle Q, 0, 1, +, -, \times, i \rangle$.

Let Σ be our old signature, and let $\Sigma^* = (\Sigma \setminus \{\mathtt{f},\mathtt{g},\mathtt{h}\}) \cup \{\mathtt{i}\}$. There is a translation $t \mapsto t^*$ of T_Σ to T_{Σ^*} given as follows: $x^* = x$ for variables, $\mathtt{0}^* = \mathtt{0}$, $\mathtt{1}^* = \mathtt{1}$, $(\lfloor t)^* = \lfloor t^*$, $(t+u)^* = t^* + u^*$, and similarly for $-$ and $\times$, $(\mathtt{f}t)^* = \mathtt{i}(\mathtt{3}\lfloor t^*)$, $(\mathtt{g}t)^* = \mathtt{i}(\mathtt{1}+\mathtt{3}\lfloor t^*)$, $(\mathtt{h}t)^* = \mathtt{i}(\mathtt{2}+\mathtt{3}\lfloor t^*)$. For example, $\mathtt{n}^* = \mathtt{n}$ for all $n \in Z$. And the translations of the normal terms of T_Σ are just those of the form $\mathtt{i}(\mathtt{1}+\mathtt{3n})$, where $n \in Z$. We get a set E^* of Σ^*-equations by

$$E^* \quad = \quad \{t^* = u^* : t = u \text{ is an axiom of } E\}.$$

Theorem 8 $T_{\Sigma^*}/E^* \cong Q^*$.

Proof The translation map commutes with substitution in the appropriate sense. Using this, we prove by an easy induction on derivations that if $E \vdash t = u$, then $E^* \vdash t^* = u^*$.

The crux of the proof is the analog of Lemma 6: for every term $t \in T_{\Sigma^*}$ there is some normal $u \in T_\Sigma$ such that $E^* \vdash t = u^*$. Just as in Theorem 7, this implies that $T_{\Sigma^*}/E^* \cong Q^*$.

We argue by induction on t. The only interesting case is for $\mathtt{i}$. Assuming that $E^* \vdash t = u^*$, we consider $\mathtt{i}(t)$. Since the case that u is $\mathtt{0}$ is easy, we consider only the case when u is $\mathtt{gn}$. Then $E^* \vdash \mathtt{i}(t) = \mathtt{i}\lfloor t = \mathtt{i}\lfloor(\mathtt{gn})^* = \mathtt{i}(\lfloor \mathtt{gn})^*$. Let $m = \lfloor g(n) \rfloor$, so $E \vdash \lfloor \mathtt{gn} = \mathtt{m}$ by Lemma 4(2). Thus $E^* \vdash \mathtt{i}(t) = \mathtt{i}(\mathtt{m})$. Now we argue by cases on m. If m is of the form $3p$ or $2+3p$ for some positive integer p, then $\mathtt{im}$ is $(\mathtt{fp})^*$ or $(\mathtt{hp})^*$. Both situations are similar. In the first, let q be such that $g(q) = f(p)$. Then $E \vdash \mathtt{fp} = \mathtt{gq}$, and so $E^* \vdash \mathtt{i}(t) = (\mathtt{gq})^*$. If m is of the form $1+2p$, then $\mathtt{i}(\mathtt{m})$ is $(\mathtt{gp})^*$. So $E^* \vdash \mathtt{i}(t) = (\mathtt{gp})^*$. $\dashv$

At this point, E^* has 19 equations involving $\mathtt{i}$. The translations of $\mathtt{f}\lfloor x = \mathtt{f}x$ and $\mathtt{h}\lfloor x = \mathtt{h}x$ can be replaced by $\mathtt{i}\lfloor x = \mathtt{i}x$. So we are left with a specification with $\mathtt{i}$ as the one and only hidden function symbol, and 18 equations using $\mathtt{i}$.

2.4 Additional remarks

More operations We also promised to specify Q with the absolute value function $|x|$. Here we would add $|\mathtt{0}| = \mathtt{0}$, $|\mathtt{g}(x)| = \mathtt{g}(x)$, and $|-\mathtt{g}(x)| = \mathtt{g}(x)$.

We could also consider a function *inv* on Q defined by $inv(0) = 0$ and $inv(m/n) = n/m$. We specify this using $\mathtt{inv}(\mathtt{0}) = \mathtt{0}$, $\mathtt{inv}(\mathtt{g}x) \times \mathtt{g}x = \mathtt{1}$, and $\mathtt{inv}(-\mathtt{g}x) \times (-\mathtt{g}x) = \mathtt{1}$.

Fewer operations Suppose one wants to drop $\lfloor x \rfloor$ and specify the ring $\langle Q, 0, 1, +, -, \times \rangle$ with as few hidden symbols as possible. Our work gives this with two hidden unary symbols, $\lfloor$ and $\mathtt{i}$. Since $\lfloor$ is hidden, we now have $18 + 3 = 21$ hidden equations. We do not know how to specify this structure with just one unary hidden symbol, though we believe that this should be possible. As we mentioned early on, one 4-ary symbol suffices.

Rewriting Specifications of Q We conclude with a remark on rewriting presentations for Q, as studied in Contejean et al [3]. Their paper is really about getting a rewriting presentation suitable for efficient computation. Our work does not address that important issue. In any case, the paper gives a three-sorted presentation of rational arithmetic using a *complete rewrite system*. The three sorts are the natural numbers, the non-zero natural numbers, and the rationals. Moreover, the addition and multiplication on the natural number sort are associative and commutative. A complete rewrite system obtained by the methods of [1] should be neither associative nor commutative. It is still open to get a rewrite presentation with addition and multiplication on the rational number sort being associative and commutative.

Our approach cannot directly give a complete rewrite system for two reasons. First and foremost, the connection law $\mathtt{g}(x) \times \mathtt{f}(\mathtt{1}+x) = \mathtt{f}(x)$ leads to a non-confluent system. The same is true of the distributive law, which we have used in a few places. (However, [3] show how to use a positional notation for integers to get around this.) We believe it is likely that our work could be combined with that of [3] to get a *two*-sorted presentation of rational arithmetic, again with addition and multiplication on integers to be associative and commutative.

References

[1] Bergstra, J. A. and J. V. Tucker, “Equational specifications, complete term rewriting systems, and computable and semicomputable algebras”, *JACM* 42 (1995), no. 6, 1194–1230.

[2] Calkin, Neil and Herbert S. Wilf, “Recounting the Rationals”, American Mathematical Monthly 107 (2000), no. 4, 360–363.

[3] Contejean, Evelyne, Claude Marché, and Landy Rabehasaina, “Rewrite systems for natural, integral, and rational arithmetic. *Rewriting techniques and applications* 1997, 98–112, LNCS 1232, Springer, Berlin, 1997.

[4] Ehrig, H. and B. Mahr, *Fundamentals of Algebraic Specifications I: Equations and Initial Semantics*. EATCS Monographs on Theoretical Computer Science Vol. 6, Springer-Verlag, Berlin, 1985.

[5] Meseguer, José, Review of [4], *Mathematical Reviews* 87k:68103, American Mathematical Society, 1987.

[6] Thatcher, James W., Eric G. Wagner, and Jesse B. Wright, “Data type specification: parameterization and the power of specification techniques.” *Tenth Annual ACM Symposium on Theory of Computing*, ACM, New York, 1978, 119–132.