The University of Manchester

MATH61202

MSc Pure Mathematics and Mathematical Logic

Quantifier Elimination for some Expansions of Divisible Ordered Abelian Groups.

Author:

Supervisor:

May 16, 2017

Contents

1 Introduction.

The aim of this project is to establish several results used by Hieronymi in 'When is Scalar Multiplication Decidable?' [3]. In the first half (sections 2 and 3) continued fractions are introduced and two results are given. The first result is a way of uniquely representing any natural number based on the continued fraction of some fixed irrational number. The second result is a way of uniquely representing any real number based on the continued fraction of some fixed irrational number.

In the second half (sections 4 and 5) the primary concern is the decidability of the first order theory of $(\mathbb{R}; <, +, \mathbb{Z})$. To establish this quantifier elimination is proved for an axiomatisation of the first order theory of $(\mathbb{Q}; <, +, -, 0, 1, (\lambda_q)_{q\in\mathbb{Q}}, \lfloor\ \rfloor)$, which is then used to establish decidability of the first order theory of $(\mathbb{R}; <, +, \mathbb{Z})$ by interpreting the elementary substructure $(\mathbb{Q}; <, +, \mathbb{Z})$.

Two shorter sections follow these at the end. The first (section 6) proves the undecidability of $(\mathbb{R}; <, +, \times, \mathbb{Z})$, using a theorem of Tarski. The second (section 7) looks at some of the results in Hieronymi [3] and gives an overview of how all of the results presented in the project will be used to prove these results in an upcoming dissertation. All of these are either used by Hieronymi, or otherwise provide the starting point for results in [3], where further expansions are considered. Results from [2] and [4] are also built upon by Hieronymi in [3]. The remainder of this introduction will outline the contents of each section in more depth one by one.

Section 2 involves a treatment of basic results about continued fractions. Several sequences associated with them are defined, and a way of assigning a unique continued fraction to a real number is established (in particular see algorithm 2.3.1). The continued fraction for a real number is then used as the foundation of two results in section 3.

Section 3 features two main results. The first is a result about unique representations of natural numbers based on the continued fraction of some fixed irrational number (as produced in section 2). In particular this utilises the sequence of denominators from the continued fraction (see definition 2.1.4). The precise statement is given in theorem 3.1.2. Secondly a way of uniquely representing real numbers is developed. These representations are also based on the continued fraction of some fixed irrational number, but utilise the sequence of differences from the continued fraction (see definition 2.4.1). The precise statement is given in theorem 3.2.1. In both cases uniqueness of the representations depends on conditions placed on coefficients used.

In sections 4 and 5 quantifier elimination is used to prove that the first order theories of the two structures $(\mathbb{Q}; <, +, \mathbb{Z})$ and $(\mathbb{R}; <, +, \mathbb{Z})$ are decidable. Throughout these sections the main source is Miller [7]. The strategy is as follows.

In section 4 a set of formulas $T_{\mathfrak{Q}}$ in the language $\{<, +, -, 0, 1, (\lambda_q)_{q\in\mathbb{Q}}, \lfloor\ \rfloor\}$ will be given (see axioms 4.1.3). These formulas will then be shown to axiomatise the structure $\mathfrak{Q} = (\mathbb{Q}; <, +, -, 0, 1, (\lambda_q)_{\mathbb{Q}}, \lfloor\ \rfloor)$. Informally the formulas will say that $\mathfrak{Q}$ is a divisible ordered abelian group, and that the image of $\lfloor\ \rfloor$ forms a subgroup with least positive element 1 such that every element $q \in \mathbb{Q}$ lies between $\lfloor q \rfloor$ and $\lfloor q \rfloor + 1$.

This will be done by using an embedding test to prove that $T_{\mathfrak{Q}}$ admits quantifier elimination. The reason we work in this language is that it allows us to exploit the fact that if an ordered abelian group is a $\mathbb{Q}$-vector space, then it is divisible (see lemma 4.1.4). By including axioms that force this $\mathbb{Q}$-vector space structure, we are able to use universal axioms to force divisibility. An embedding test specific to universal theories can then be used. Such a test will be proved as a consequence of the Shoenfield-Blum

embedding test (see theorem 4.2.3). With quantifier elimination established, we will be ready to prove $T_{\mathfrak{Q}}$ really does axiomatise $\mathfrak{Q}$ by showing that $\mathfrak{Q}$ embeds into every model of $T_{\mathfrak{Q}}$. Combining this with the fact that $\mathfrak{Q}$ is a model of $T_{\mathfrak{Q}}$, we also get as a consequence that $T_{\mathfrak{Q}}$ is a complete theory (see proposition 4.3.9), which will be used in section 5.

In section 5 we will harvest the results from section 4 to get decidability for the structures $(\mathbb{Q}; <, +, \mathbb{Z})$ and $(\mathbb{R}; <, +, \mathbb{Z})$. Firstly $T_{\mathfrak{Q}}$ is shown to be recursive. In section 4 it was shown that $T_{\mathfrak{Q}}$ is satisfiable, and complete, which gives us that $T_{\mathfrak{Q}}$ is decidable from the recursivity (see lemma 5.1.2 and propositions 5.1.4 and 5.1.5). With this we go on to prove decidability for the structures $(\mathbb{Q}; <, +, \mathbb{Z})$ and $(\mathbb{R}; <, +, \mathbb{Z})$. This is done by recursively interpreting the structure $(\mathbb{Q}; <, +, \mathbb{Z})$ in $\mathfrak{Q}$. For the real case we introduce the structure $\mathfrak{R} = (\mathbb{R}; <, +, -, 0, 1, (\lambda_q)_{q\in\mathbb{Q}}, \lfloor\ \rfloor)$. It is easily seen that $\mathfrak{R} \models T_{\mathfrak{Q}}$, and is an therefore an elementary extension of $\mathfrak{Q}$ by the fact $T_{\mathfrak{Q}}$ admits quantifier elimination (since $\mathfrak{Q}$ embeds into $\mathfrak{R}$ as a substructure). Then as $\mathfrak{R}$ recursively defines the structure $(\mathbb{R}; <, +, \mathbb{Z})$ (this is almost identical to the rational case) this structure is also decidable.

In section 6 it is shown that including multiplication to give the field structure of $\mathbb{R}$ kills the first order decidability of the structure $(\mathbb{R}; <, +, \mathbb{Z})$. This is done by straightforward application of a theorem of Tarski, and recursively interpreting $\bar{\omega} = (\omega; <, +, \times, 0, S)$, which is already known to be undecidable, in the structure $(\mathbb{R}; <, +, \times, \mathbb{Z})$.

Finally, in section 7, the link between all of the results are discussed, and the motivation behind them is given. An overview of some results proved by Hieronymi [3] are given. These will be covered in a dissertation expanding this project. The results are, in a loose sense, about which structures 'in-between' $(\mathbb{R}; <, +, \mathbb{Z})$ and $(\mathbb{R}; <, +, \times, \mathbb{Z})$ have decidable first order theory.

2 Continued Fractions.

This section will cover definitions and results about continued fractions which will be used in section 3. Most importantly a way of associating a unique continued fraction to a real number is given. Several sequences derived from these continued fractions will also play a large part in section 3.

After defining what a continued fraction is, a class of continued fractions will be introduced which will be shown to always converge with a real limit. An algorithm is given which produces, for any real number as input, a unique continued fraction in this class converging to that real number (the sense in which a continued fraction 'converges' will be stated clearly, see lemma 2.2.3 and the following comment). The main source used is Stein [9], the material can also be found in Rockett and Szusz [8].

2.1 Continued fractions.

Definition 2.1.1. A continued fraction is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}.$$

We call the a_i partial quotients.

In order to condense notation, I will write continued fractions in the form $[a_0; a_1, a_2, \ldots]$. Sometimes these will terminate, i.e. we will have $[a_0; a_1, \ldots, a_n]$. However in most uses later, especially in section 3, only continued fractions which do not terminate will be of interest.

Definition 2.1.2. We will call a continued fraction infinite if it does not terminate, i.e. when there are infinitely many (ignoring repetition) partial quotients. Otherwise, if a continued fraction is of the form $[a_0; a_1, \ldots, a_m]$ for some natural m, we call it finite.

Definition 2.1.3. Given a continued fraction, we define the sequence $(c_n)_{n\geq 0}$ of convergents by $c_0 = a_0, c_1 = [a_0; a_1], c_2 = [a_0; a_1, a_2]$ and so on up to $c_k = [a_0; a_1, a_2, \ldots, a_k]$. Of course in the case of finite continued fractions we only define finitely many terms.

Definition 2.1.4. We define two more sequences, the numerators and the denominators of a continued fraction, respectively p_n and q_n for $n \geq -1$ as follows. Set $p_{-1} = 1$, $p_0 = a_0$, and $q_{-1} = 0$, $q_0 = 1$, and then define further entries by the following two recursion relations, making use of the partial quotients from the continued fraction, $p_{k+1} = a_{k+1}p_k + p_{k-1}$ and $q_{k+1} = a_{k+1}q_k + q_{k-1}$ for $k \geq 0$.

Note that immediately we get $p_0/q_0 = a_0 = c_0$, and

$$\frac{p_1}{q_1} = \frac{a_1p_0 + p_{-1}}{a_1q_0 + q_{-1}} = \frac{a_1a_0 + 1}{a_1} = a_0 + \frac{1}{a_1} = c_1.$$

In the following proposition we will show that this extends, that is we have $c_k = p_k/q_k$ for all $k \geq 0$, using these observations as the base case in an induction on k.

Proposition 2.1.5. *For all $k \in \mathbb{N}$, $c_k = p_k/q_k$.*

Proof. We proceed by induction, having established the base case ($k = 0, 1$) in the comment above. Supposing that the statement holds for all natural numbers up to and including k, we show that $c_{k+1} = p_{k+1}/q_{k+1}$.

We can think of c_{k+1} as a continued fraction with just k partial quotients by taking the last two partial quotients and considering them together , that is by considering $\widetilde{a_k}$ given by $a_k + \frac{1}{a_{k+1}}$. Then we have

$$c_{k+1} = [a_0; a_1, \ldots, a_{k-1}, a_k, a_{k+1}] = [a_0; a_1, \ldots, a_{k-1}, \widetilde{a_k}] = \widetilde{c_k}.$$

Now the k-th convergent of this new continued fraction is, by induction hypothesis and the recursion relations satisfied (by construction)by the nu-

merators and denominators of the continued fraction, given by

$$\widetilde{c_k} = \frac{\widetilde{a_k}p_{k-1} + p_{k-2}}{\widetilde{a_k}q_{k-1} + q_{k-2}} = \frac{(a_k + \frac{1}{a_{k+1}})p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}})q_{k-1} + q_{k-2}}.$$

Importantly the p_{k-1}, p_{k-2}, q_{k-1}, and q_{k-2} coincide when considering c_{k+1} and $\widetilde{c_k}$. Further rearranging gives

$$\begin{aligned} c_{k+1} &= \frac{(a_k + \frac{1}{a_{k+1}})p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}})q_{k-1} + q_{k-2}} \\ &= \frac{(a_k p_{k-1} + p_{k-2}) + \frac{1}{a_{k+1}}p_{k-1}}{(a_k q_{k-1} + q_{k-2}) + \frac{1}{a_{k+1}}q_{k-1}} \\ &= \frac{p_k + \frac{1}{a_{k+1}}p_{k-1}}{q_k + \frac{1}{a_{k+1}}q_{k-1}} \cdot \frac{a_{k+1}}{a_{k+1}} \\ &= \frac{p_{k+1}}{q_{k+1}}, \end{aligned}$$

which is precisely what we wanted to show. □

Now that we have seen p_k/q_k agrees with c_k for all $k \geq 0$, we will largely dispense with referring to the c_k's, and instead refer just to p_k and q_k.

A useful property of the numerators and denominators of the convergents is given in the following lemma.

Lemma 2.1.6. *For $k \geq 0$ we have $p_k q_{k-1} - p_{k-1}q_k = (-1)^{k-1}$.*

Proof. Firstly $p_0 q_{-1} - p_{-1}q_0 = -1\ (= (-1)^{-1})$. We then proceed inductively, for $k \geq 0$ we have

$$\begin{aligned} p_{k+1}q_k - p_k q_{k+1} &= (a_{k+1}p_k + p_{k-1})q_k - p_k(a_{k+1}q_k + q_{k-1}) \\ &= -(p_k q_{k-1} - p_{k-1}q_k) \\ &= (-1)(-1)^{k-1} = (-1)^k. \end{aligned}$$

Where the third equality goes through by use of the induction hypothesis. Whence the statement holds for all $k \geq 0$. □

The usefulness of this lemma will become apparent in the following subsection where we restrict the partial quotients.

2.2 Regular continued fractions.

In this subsection we look at a class of continued fractions whose partial quotients are natural numbers. It will be seen that the sequence of convergents for such continued fractions always tends to a real limit.

Definition 2.2.1. We say that a continued fraction is a regular continued fraction if $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{N} \setminus \{0\}$ for $i \geq 1$.

From now on continued fraction will always be taken to mean regular continued fraction, unless specifically stated otherwise.

Remark 2.2.2. Once we have restricted ourself to regular continued fractions, lemma 2.1.6 tells us that p_k and q_k are coprime for $k \geq 0$, and hence that each convergent is a reduced fraction.

Lemma 2.2.3. *Let $(p_k/q_k)_{k\geq 0}$ be the sequence of convergents for an infinite regular continued fraction, then this sequence converges to a real limit t.*

Proof. We have, for $k \geq 1$, that

$$\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{p_k q_{k-1} - q_k p_{k-1}}{q_k q_{k-1}} = \frac{(-1)^{k-1}}{q_k q_{k-1}},$$

where the first equality is obvious and the second follows from lemma 2.1.6. Therefore we have

$$\frac{p_0}{q_0} + \sum_{k=1}^{\infty} (\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}}) = \frac{p_0}{q_0} + \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{q_k q_{k-1}},$$

but notice that since $q_0 = 1$ and $q_k = a_k q_{k-1} + q_{k-2}$, we get $q_k > q_{k-1}$ for $k \geq 1$. So we have that $1/q_k q_{k-1} < 1/k^2$, and it then follows that the series described converges. Hence the sequence of convergents converges, say with $\lim_{k\to\infty} p_k/q_k = t$. □

So now we have a way of associating real numbers to (regular) continued fractions. As shorthand we will often say that a continued fraction converges to or tends to some real number t to mean that t is the limit of its sequence of convergents.

Definition 2.2.4. Given a continued fraction $[a_0; a_1, a_2, \ldots]$, the k-th complete quotient is defined as the continued fraction $[a_k; a_{k+1}, a_{k+2}, \ldots]$. We will denote the k-th complete quotient ζ_k. Immediate from the definition, notice that $\zeta_k = a_k + 1/\zeta_{k+1}$.

So far we have associated a real number to each continued fraction. The following lemma will be used in the next subsection, where we go in the opposite direction and produce a continued fraction which converges to some given real limit t.

Lemma 2.2.5. *Given a continued fraction with convergents $(p_k/q_k)_{k\geq 0}$, we have*

$$t = \frac{p_k\zeta_{k+1} + p_{k-1}}{q_k\zeta_{k+1} + q_{k-1}}$$

for all $k \geq 0$.

Proof. For the base case $k = 0$, we have

$$\frac{p_0\zeta_1 + p_{-1}}{q_0\zeta_1 + q_{-1}} = \frac{a_0\zeta_1 + 1}{\zeta_1} = a_0 + 1/\zeta_1 = \zeta_0.$$

Next for the induction step, suppose the statement holds for k, then we show it also holds for $k + 1$.

$$\begin{aligned} t &= \frac{(a_{k+1} + \frac{1}{\zeta_{k+2}})p_k + p_{k-1}}{(a_{k+1} + \frac{1}{\zeta_{k+2}})q_k + q_{k-1}} \\ &= \frac{(a_{k+1}p_k + p_{k-1}) + (\frac{1}{\zeta_{k+2}})p_k}{(a_{k+1}q_k + q_{k-1}) + (\frac{1}{\zeta_{k+2}})q_k} \\ &= \frac{p_{k+1}\zeta_{k+2} + p_k}{q_{k+1}\zeta_{k+2} + q_k}. \end{aligned}$$

Here the first equality is by induction hypothesis and an immediate consequence of the definition of ζ_{k+1}, the second equality is by rearrangement, and the third equality is by the definition of the convergents along with multiplying through by ζ_{k+2}/ζ_{k+2}. Hence the statement holds for all $k \geq 0$ as required. □

2.3 Continued fraction for a real number.

The following algorithm produces, given some real number t, a continued fraction that converges to t. In section 3 this will be used to give ways of representing both natural numbers and real numbers based on the continued fraction converging to some fixed irrational number t.

Algorithm 2.3.1. We want to take as input a real number t, and produce a continued fraction that converges to t.

Step 1: Set $a_0 = \lfloor t \rfloor$. Then define $\delta_0 = t - a_0$. If $\delta_0 = 0$ then we stop and the process is finished with $[a_0]$ being the continued fraction for t. If not then we proceed as follows.

Further steps: Suppose we have iterated the algorithm and produced a_k and δ_k. Then set $a_{k+1} = \lfloor 1/\delta_k \rfloor$, and $\delta_{k+1} = 1/\delta_k - a_{k+1}$. If $\delta_{k+1} = 0$ we are done, otherwise we continue iterating.

Starting with $t \in \mathbb{R}$ the continued fraction produced by algorithm 2.3.1 is hereafter referred to as the continued fraction for t. The intuition behind algorithm 2.3.1 is to take the greatest integer not exceeding t (as a_0), then to make up as much of the rest of t as possible by taking the greatest integer not exceeding the reciprocal of the difference between t and this integer (as a_1). Repeating this to get progressively closer to t while conforming to the definition of a regular continued fraction by always taking natural numbers for the partial quotients.

Note that if t is rational then the process outlined will terminate and we will get a finite expression $[a_0; a_1, \ldots, a_n]$. On the other hand for irrational t if the algorithm were to terminate then clearly we would get a contradiction, since by multiplying through by denominators repeatedly we would get an expression for t as a quotient of two integers. The following proposition shows that algorithm 2.3.1 successfully produces a continued fraction which converges to t.

Proposition 2.3.2. *With p_k/q_k defined according to algorithm 2.3.1, we have $\lim_{k\to\infty}(t - p_k/q_k) = 0$.*

Proof. The key here is to use lemma 2.2.5. This gives us that

$$t = \frac{p_k\zeta_{k+1} + p_{k-1}}{q_k\zeta_{k+1} + q_{k-1}}$$

for all $k \geq 0$. Using this we get

$$\lim_{k\to\infty}(t - p_k/q_k) = \lim_{k\to\infty}(\frac{p_k\zeta_{k+1} + p_{k-1}}{q_k\zeta_{k+1} + q_{k-1}} - \frac{p_k}{q_k}).$$

Now with some straightforward rearranging we get

$$\frac{p_k\zeta_{k+1} + p_{k-1}}{q_k\zeta_{k+1} + q_{k-1}} - \frac{p_k}{q_k} = \frac{p_{k-1}q_k - p_kq_{k-1}}{q_k^2\zeta_{k+1} + q_kq_{k-1}},$$

and then applying lemma 2.1.6 we get

$$\lim_{k\to\infty}(t - p_k/q_k) = \lim_{k\to\infty}(\frac{(-1)^k}{q_k^2\zeta_{k+1} + q_kq_{k-1}}).$$

Note that this shows the convergents alternate between approximating t from below and above. Now taking the modulus (since we are looking to establish a null sequence this is valid) we have

$$\lim_{k\to\infty}|t - p_k/q_k| = \lim_{k\to\infty}(\frac{1}{q_k^2\zeta_{k+1} + q_kq_{k-1}}).$$

Lastly we note that $\zeta_{k+1} = 1/\delta_k \geq a_{k+1}$ by construction. This means we can bound the terms of our sequence as follows,

$$\frac{1}{q_k^2\zeta_{k+1} + q_kq_{k-1}} \leq \frac{1}{q_k^2a_{k+1} + q_kq_{k-1}} = \frac{1}{q_k(q_ka_{k+1} + q_{k-1})} = \frac{1}{q_kq_{k+1}}.$$

So since the last term gives a null sequence, we are done. Algorithm 2.3.1 takes input $t \in \mathbb{R}$ and has as output a regular continued fraction which is either equal to t (if the algorithm terminates) or whose convergents have limit t. □

2.4 The sequence of differences β_k.

The following sequence will be used in section 3 when we give representations of real numbers based on continued fractions.

Definition 2.4.1. We define the k-th difference of the continued fraction for some real number t to be $\beta_k \coloneqq q_k t - p_k$. As it is notationally useful to do so we start from $k = -1$, with $\beta_{-1} = -1$.

Remark 2.4.2. The differences of the continued fraction of t share the same recurrence relation as the numerators and the denominators since we have

$$\begin{aligned}\beta_{k+1} &= q_{k+1}t - p_{k+1} \\ &= (a_{k+1}q_k + q_{k-1})t - (a_{k+1}p_k + p_{k-1}) \\ &= a_{k+1}(q_k t - p_k) + (q_{k-1}t - p_{k-1}) \\ &= a_{k+1}\beta_k + \beta_{k-1}.\end{aligned}$$

3 Ostrowski Representations.

Now we present two results which using the definitions and results from section 2. In both cases we work with a fixed irrational number t, and the continued fraction for t, as produced by algorithm 2.3.1. With algorithm 3.1.3 we see that every natural number can be represented as a sum of denominators from the continued fraction of t. The first result then establishes conditions on the coefficients used, see theorem 3.1.2 for the precise statement. Theorem 3.2.1) gives a similar result for real numbers, using the sequence of differences from the continued fraction of t (definition 2.4.1) rather than the denominators, unique representations are available for all real numbers (again with important restrictions on the coefficients). In both cases the precise statement is taken from Hieronymi [3], however no proof is presented there. Theorem 3.1.2 follows the proof from [1]. Theorem 3.2.1 uses a proof adapted from Rockett and Szusz[8] (which gives a slightly different formulation).

3.1 Representations for $\mathbb{N}$.

Here we want to prove that under certain conditions on coefficients every natural number can be uniquely represented as a sum of the denominators from the continued fraction of some fixed irrational t. First a lemma that will be used in the proof.

Lemma 3.1.1. *Let $1 = u_0 < u_1 < u_2 < \dots$ be a strictly increasing sequence of integers. Then every natural number m has a unique representation of the form $\sum_{k=0}^{N} b_{k+1}u_k$ where $b_{N+1} \neq 0$ and for $k \geq 0$ the b_{k+1} are non-negative integers satisfying*

$$b_1u_0 + b_2u_1 + \cdots + b_{k+1}u_k < u_{k+1}.$$

Proof. For existence we defer to algorithm 3.1.3, which is an example of

the 'greedy algorithm' (see Allouche and Shallit [1] for a discussion in full generality).

Now for uniqueness. Suppose a natural number m has two distinct representations $b_1u_0 + \cdots + b_{N+1}u_N$ and $c_1u_0 + \cdots + c_{N+1}u_N$ (if the lengths are different, say with one having length $M < N$ then add $N - M$ terms to the end of the shorter representation, with 0 coefficients for each new term). We can choose N such that one of b_{N+1}, c_{N+1} is non-zero. Let $i \in \{0, \ldots, N\}$ be minimal such that $b_{i+1} \neq c_{i+1}$ (such an i exists by the assumption that the two representations are distinct). Without loss of generality we can assume $b_{i+1} > c_{i+1}$, however $(b_1u_0 + \cdots + b_{k+1}u_k) - (c_1u_0 + \cdots c_{k+1}u_k) = 0$, so we get

$$(b_{k+1} - c_{k+1})u_k = (c_1 - b_1)u_0 + \cdots + (c_k - b_k)u_{k-1} \leq c_1u_0 + \cdots + c_ku_{k-1} < u_k.$$

But $b_{k+1} - c_{k+1} \geq 1$, so we have $u_k \leq (b_{k+1} - c_{k+1})u_k < u_k$ which is obviously a contradiction. Hence such representations are unique as required. □

Theorem 3.1.2. *Let m be a natural number. Then there exists unique natural N such that $q_N \leq m < q_{N+1}$, and tuple $(b_1, \ldots, b_{N+1})$ of integers such that $m = \sum_{k=0}^{N} b_{k+1}q_k$ with*

- $0 \leq b_1 < a_1$,
- $0 \leq b_k \leq a_k$ *for* $k > 1$, *and*
- $b_{k+1} = a_{k+1}$ *implies* $b_k = 0$.

Proof. By lemma 3.1.1 it is sufficient to show that the three conditions on the coefficients b_k are equivalent to $b_1q_0 + b_2q_1 + \cdots + b_{k+1}q_k < q_{k+1}$.

Suppose the three conditions hold. We induct on k to show that the inequality holds.

If $k = 0$ then we have $b_1q_0 = b_1 < a_1 = q_1$ by the first condition.

If $k = 1$ then we have to show $b_1q_0 + b_2q_1 < q_2$. Well if $b_2 = a_2$ then $b_1 = 0$ and we get $a_2q_1 = q_2 - q_0 < q_2$ as expected. Meanwhile if $b_2 < a_2$ we have

$b_1q_0 + b_2q_1 < b_1 + b_2a_1 \leq a_1a_2 < a_1a_2 + 1 = q_2$. So the cases $k = 0$ and $k = 1$ are established.

Suppose that the inequality holds for $k < j$, then we want to show it holds for j. By the second condition we have $b_{j+1} \leq a_{j+1}$. If $b_{j+1} < a_{j+1}$ then $b_{j+1} \leq a_{j+1} - 1$, so

$$b_{j+1}q_j \leq (a_{j+1} - 1)q_j \leq q_{j+1} - q_{j-1} - q_j \leq q_{j+1} - q_j.$$

Combining this with the induction hypothesis that $b_1q_0 + \cdots + b_jq_{j-1} < q_j$, we get

$$b_1q_0 + \cdots + b_{j+1}q_j < q_j + b_{j+1}q_j \leq q_{j+1}.$$

On the other hand if $b_{j+1} = a_{j+1}$ we get $b_j = 0$ from the third condition, hence

$$b_jq_{j-1} + b_{j+1}q_j = a_{j+1}q_j = q_{j+1} - q_{j-1}.$$

But then by induction hypothesis we have $b_1q_0 + \cdots + b_{j-1}q_{j-2} < q_{j-1}$, whence $b_1q_0 + \cdots + b_{j+1}q_j < q_{j+1}$ as required.

Now for the opposite direction. We get the first condition out of the inequality since $b_1q_0 < q_1$ implies $b_1 < a_1$ (as $q_0 = 1$ and $q_1 = a_1$). For the second condition note that $b_{k+1}q_k < q_{k+1}$ is given by the inequality, so $b_{k+1}q_k < a_{k+1}q_k + q_{k-1}$. This gives $b_{k+1} < a_{k+1} + (q_{k-1}/q_k)$, then as $q_{k-1} \leq q_k$ we have $b_{k+1} < a_{k+1} + 1$, so $b_{k+1} \leq a_{k+1}$. For the third condition, $b_{k+1} = a_{k+1}$ and $b_k \neq 0$, imply

$$b_1q_0 + \cdots + b_kq_{k-1} + b_{k+1}q_k \geq q_{k-1} + a_{k+1}q_k = q_{k+1}.$$

So the conditions are equivalent, hence by lemma 3.1.1 any representation satisfying the conditions in the statement is unique. Existence is demonstrated in algorithm 3.1.3 next. □

The following algorithm gives the unique representation from theorem 3.1.2 of any natural number m based on the continued fraction of some fixed irrational t.

Algorithm 3.1.3. We have fixed irrational $t \in \mathbb{R}$. If $(q_k)_{k\in\mathbb{N}}$ is the sequence of denominators of the continued fraction for t we get $1 = q_0 \leq q_1 < q_2 < \ldots$ and so for any natural number m there must be indices N and $N+1$ such that $q_N \leq m < q_{N+1}$.

Step 1: Dividing m by q_N we get $m = \lfloor m/q_N \rfloor q_N + r_N$ where $0 \leq r_N < q_N$ is the remainder. If q_N divides m then we get $r_N = 0$ and we are done. Otherwise we let r_N take the role of m and we proceed to the next step.

Further steps: We then divide r_N by q_k for some $k < N$ with $q_k \leq r_N < q_{k+1}$, getting $r_N = \lfloor r_N/q_k \rfloor q_k + r_k$, at which point if $r_k = 0$ we stop, otherwise letting r_k take the role of m.

Repeating this process until a remainder 0 is obtained at some stage (note that the indices are strictly decreasing, and $q_0 = 1$, which divides any possible remainder r, hence the process will always terminate in finitely many steps).

At each stage the coefficient is chosen to be maximal and hence unique. Note that the coefficients obtained by the algorithm conform to the conditions given in the statement of theorem 3.1.2.

3.2 Representations for $\mathbb{R}$.

Now look at representations for real numbers instead of natural numbers. The representation is still grounded in the continued fraction of some fixed irrational number t, but this time uses the sequence of differences instead of the sequence of denominators. Again we have important restrictions on the coefficients, which are relied on for the uniqueness of the representations. At the end an algorithm is given to explain how such representations are produced (algorithm 3.2.2).

Theorem 3.2.1. *Let c be a real number such that $\frac{-1}{\zeta_1} \leq c < 1 - \frac{1}{\zeta_1}$. Then there is a unique sequence $(b_k)_{k\geq 1}$, $b_k \in \mathbb{N}$ such that $c = \sum_{k=0}^{\infty} b_{k+1}\beta_k$ with*

- $0 \leq b_1 < a_1$,
- $0 \leq b_k \leq a_k$ *for* $k > 1$,
- $b_{k+1} = a_{k+1}$ *implies* $b_k = 0$, *and*
- $b_k < a_k$ *for infinitely many odd* k.

Proof. First notice that the interval which we are assuming c lies in is $[-\beta_0, (a_1 - 1)\beta_0 - \beta_1)$. This is because by remark 2.4.2 we have

$$\frac{-1}{\zeta_1} = a_0 - t = -(q_0 t - p_0) = -\beta_0,$$

$$1 - \frac{1}{\zeta_1} = 1 - \beta_0 = -(0t - 1) - \beta_0 = -\beta_{-1} - \beta_0 = (a_1 - 1)\beta_0 - \beta_1.$$

First we should note that all such sums do lie in the interval. To see this notice that the signs of the differences alternate, with $\beta_k \geq 0$ for even k and $\beta_k \leq 0$ for odd k, so we can estimate any such sum as follows.

For the lower bound, we set the coefficients of all positive differences to 0, and take the highest possible coefficient for all negative differences. That is we consider $a_2\beta_1 + a_4\beta_3 + \ldots$, then cancel terms using the recurrence relation in the following way to get a non-strict lower bound

$$\sum_{k=1}^{\infty} a_{2k}\beta_{2k-1} = \sum_{k=1}^{\infty}(\beta_{2k} - \beta_{2k-2}) = -\beta_0.$$

Similarly for the upper bound we get

$$(a_1 - 1)\beta_0 + \sum_{k=1}^{\infty} a_{2k+1}\beta_{2k} = (a_1 - 1)\beta_0 + \sum_{k=1}^{\infty}(\beta_{2k+1} - \beta_{2k-1}) = (a_1 - 1)\beta_0 - \beta_1.$$

However as $b_k < a_k$ for infinitely many odd k, we have that $b_k < a_k$ for some $k > 1$, meaning that the upper bound is strict. (Note that this is true at

every stage, and is the reason we always have intervals open on the right and closed on the left. This contributes to uniqueness of representation in the same way as disallowing recurring 9's in decimal expansions.)

It can also be seen that such sums of β_k's fill the interval (if you aren't convinced, look at algorithm 3.2.2 below). Hence any real number c in the interval can be written as such a sum of the β_k's of the continued fraction for t. What remains to show is that the coefficients are unique.

To do this we outline a process of nested partitioning of the initial interval according to the range of values for the coefficients in the representation of c. Starting with b_1, a partitioning of the interval $[-\beta_0, (a_1-1)\beta_0-\beta_1)$ according to the a_1 different possible values of b_1 is given. Then at subsequent stages, we partition each of the subintervals produced in the previous stage according to the range of values the subsequent coefficient can take. At the k-th stage this will be a partitioning of each of the subintervals into a further $a_k + 1$ subintervals. As we will have a partitioning at each stage (i.e. none of the subintervals given at any step will have non-trivial intersection with another subinterval produced at that step), the coefficients will therefore be unique.

Step 1: The first partitioning goes as follows.

If $b_1 = 0$ then we use the same style of estimate before. The lower bound is not affected as we were already taking $b_1 = 0$. For the upper bound we get

$$\sum_{k=0}^{\infty} b_{k+1}\beta_k < a_3\beta_2 + a_5\beta_4 + \ldots = \sum_{k=0}^{\infty}(\beta_{2k+1} - \beta_{2k-1}) = -\beta_1.$$

So if $b_1 = 0$ we have $c \in [-\beta_0, -\beta_1)$.

If $0 < b_1 < a_1$ then we have that $b_2 < a_2$ by our initial restrictions on the coefficients since $b_2 = a_2$ implies $b_1 = 0$. So the lower bound of our estimation, with b_1 now being fixed, becomes

$$b_1\beta_0 + (a_2 - 1)\beta_1 + a_4\beta_3 + \ldots = (b_1 - 1)\beta_0 - \beta_1,$$

and the upper bound becomes

$$b_1\beta_0 + a_3\beta_2 + a_5\beta_4 + \ldots = b_1\beta_0 - \beta_1.$$

Putting the two cases together, we get the required partitioning of $[-\beta_0, (a_1 - 1)\beta_0 - \beta_1)$ into subintervals.

Further steps: For the subsequent steps we proceed in the same way as before, but the subinterval determined by the coefficients already calculated now acts as the starting interval. We do the second step as an example.

So supposing we have $c = b_1\beta_0 + \sum_{k=1}^{\infty} b_{k+1}\beta_k$, with b_1 fixed, we need to show that the choices for b_2 partition the estimates from the first step depending on b_1.

If $b_1 = 0$ then the upper and lower bounds on $b_1\beta_0 + \sum_{k=1}^{\infty} b_{k+1}\beta_k$ are $-\beta_0$ and $-\beta_1$ respectively. Then if $b_2 = 0$ we get a lower bound of

$$a_4\beta_3 + a_6\beta_5 + \ldots = -\beta_2,$$

which is indeed in $[-\beta_0, -\beta_1)$. We also get an upper bound of

$$a_3\beta_2 + a_5\beta_4 + \ldots = -\beta_1.$$

If instead $0 < b_2 \leq a_2$ then $b_3 < a_3$ and so the lower bound is given by

$$b_2\beta_1 + a_4\beta_3 + a_6\beta_5 + \ldots = b_2\beta_1 - \beta_2,$$

while the upper bound is given by

$$b_2\beta_1 + (a_3 - 1)\beta_2 + a_5\beta_4 + \ldots = (b_2 - 1)\beta_1 - \beta_2.$$

Notice here that since $\beta_1 \leq 0$, larger values of b_2 correspond to lower estimates of c. In this sense at at each stage we alternate between partitioning left to right or right to left.

If $0 < b_1 < a_1$ then $0 \leq b_2 < a_2$. Now if $b_2 = 0$ we get

$$b_1\beta_0 + a_4\beta_3 + a_6\beta_5 + \ldots = b_1\beta_0 - \beta_2,$$

as a lower bound, while for an upper bound we get

$$b_1\beta_0 + a_3\beta_2 + a_5\beta_4 + \ldots = b_1\beta_0 - \beta_1.$$

Finally if also $0 < b_2 < a_2$ then we have $b_3 < a_3$, so we get a lower bound of

$$b_1\beta_0 + b_2\beta_1 + a_4\beta_3 + a_6\beta_5 + \ldots = b_1\beta_0 + b_2\beta_1 - \beta_2,$$

and an upper bound of

$$b_1\beta_0 + b_2\beta_1 + (a_3 - 1)\beta_2 + a_5\beta_4 + \ldots = b_1\beta_0 + (b_2 - 1)\beta_1 - \beta_2.$$

Notice that for the lower bound, the lowest estimate is attained when $b_2 = a_2 - 1$ in which case

$$b_1\beta_0 + (a_2 - 1)\beta_1 - \beta_2 = b_1\beta_0 - \beta_1 + (a_2\beta_1 - \beta_2) = (b_1 - 1)\beta_0 - \beta_1$$

Thus we have a partitioning of the subinterval $[(b_1 - 1)\beta_0 - \beta_1, b_1\beta_0 - \beta_1)$ into further subintervals according to the value of b_2 as required.

All further stages follow identical procedures. □

Algorithm 3.2.2. Supposing that we have fixed a real number t and taken its continued fraction, to get the t-expansion of some suitable real number c we simply choose the coefficients b_k according to the subinterval which c lies in. So if $-\beta_0 \leq c < -\beta_1$ we take $b_1 = 0$, and so on choosing successive coefficients one at a time.

We call the representation $c = \sum_{k=0}^{\infty} b_{k+1}\beta_k$ obtained in this manner the t-expansion of c. Notice that $\beta_0 < 1$, so if we need to uniquely represent all real numbers then we can instead take $\sum_{k=-1}^{\infty} b_{k+1}\beta_k$, with b_0 taking any integer value. As all real numbers can be integer translated into the interval $\frac{-1}{\zeta_1} < c < 1 - \frac{1}{\zeta_1}$ this is sufficient since $\beta_{-1} = -1$.

4 Quantifier Elimination for $\mathfrak{Q}$.

In this section we work with the structure $\mathfrak{Q} = (\mathbb{Q}; <, +, -, 0, 1, (\lambda_q)_{q\in\mathbb{Q}}, \lfloor\ \rfloor)$. Here each λ_q is the usual scalar map $x \mapsto qx$ in $\mathbb{Q}$, and $\lfloor\ \rfloor$ maps elements of $\mathbb{Q}$ to the greatest integer less than or equal to them, i.e. is the expected floor function on $\mathbb{Q}$.

First a universal theory $T_{\mathfrak{Q}}$ in the language of $\mathfrak{Q}$ will be shown to admit quantifier elimination using a consequence of the Shoenfield-Blum test (see theorem 4.2.3 and theorem 4.3.7). The consequence of Shoenfield-Blum gives sufficient conditions for a universal theory to have quantifier elimination. It will then be shown that this set $T_{\mathfrak{Q}}$ axiomatises the structure $\mathfrak{Q}$.

The order of results may seem unintuitive at first, but establishing quantifier elimination will greatly simplify the proof that $T_{\mathfrak{Q}}$ axiomatises $\mathfrak{Q}$, and so is presented at the start. These results will all be put to use in section 5, where we will show that $\mathfrak{Q}$ defines $(\mathbb{Q}; <, +, \mathbb{Z})$, to prove decidability of the first order theory of the latter. The main sources are Miller [7] who establishes quantifer elimination for the theory $T_{\mathfrak{Q}}$. For the background model theoretic results employed both Marker [6] and Hodges [5] have been used, and for the quantifier elimination tests Tressl [10] is used.

4.1 Axiomatisation $T_{\mathfrak{Q}}$.

Definition 4.1.1. We say that an $\mathscr{L}$-theory U is axiomatised by an $\mathscr{L}$-theory T if $\mathrm{Ded}(T) = U$. We also say that an $\mathscr{L}$-structure $\mathcal{M}$ is axiomatised by an $\mathscr{L}$-theory T if $\mathrm{Th}(\mathcal{M})$ is axiomatised by the theory T.

Definition 4.1.2. We say that a theory T in a language $\mathscr{L}$ admits quantifier elimination if for every $\mathscr{L}$-formula $\varphi(x_1, ..., x_n)$ there is some quantifier free $\mathscr{L}$-formula $\chi(x_1, ..., x_n)$ such that $T \models \varphi \leftrightarrow \chi$.

Note that embeddings between models of theories with quantifier elimination are always elementary embeddings. This is because embeddings preserve all quantifier free formulas, so if every formula is equivalent modulo the theory to some quantifier free formula then it is preserved by an embedding.

Axioms 4.1.3. Let $\mathscr{L}$ be the language of $\mathfrak{Q}$, then we fix the following set of axioms $T_{\mathfrak{Q}}$:

(i) Axioms for ordered abelian groups;

  (a) the group axioms,

  (b) axioms for a linear order,

  (c) $\forall x \forall y \; x + y = y + x$,

  (d) $\forall x \forall y \forall z \; x < y \to x + z < y + z$,

(ii) $0 < 1$,

(iii) An axiom for each pair $(j, n) \in \mathbb{Z} \times \mathbb{N}$ stating that $\forall x \; n\lambda_{j/n}(x) = jx$,

(iv) $\forall x \forall y \; \lfloor \lfloor x \rfloor + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$,

(v) $\forall x \; 0 \leq x < 1 \to \lfloor x \rfloor = 0$,

(vi) $\lfloor 1 \rfloor = 1$,

(vii) $\forall x \; \lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

We will see shortly that $T_{\mathfrak{Q}}$ admits quantifier elimination. Since $\mathfrak{Q} \models T_{\mathfrak{Q}}$ we have that $\mathrm{Ded}(T_{\mathfrak{Q}}) \subseteq \mathrm{Th}(\mathfrak{Q})$, to show that $T_{\mathfrak{Q}}$ axiomatises $\mathfrak{Q}$ it will be sufficient to show that $\mathfrak{Q}$ embeds into every model of $T_{\mathfrak{Q}}$. By the comment above about embeddings this will give us that $\mathrm{Th}(\mathfrak{Q}) \subseteq \mathrm{Ded}(T_{\mathfrak{Q}})$, and hence that $\mathrm{Ded}(T_{\mathfrak{Q}}) = \mathrm{Th}(\mathfrak{Q})$ as required. We do this now using some results about ordered divisible abelian groups.

Lemma 4.1.4. *Let $(G, +, <)$ be an ordered abelian group. If G has $\mathbb{Q}$-vector space structure, then it is a divisible group.*

Proof. Suppose we have $\mathbb{Q}$-vector space structure on G, then we need to show that for all $g \in G$ and $n \in \mathbb{N}$ there is $h \in G$ such that $h + \cdots + h = g$ (where we have n summands). Well using the vector space structure we can just take $h = \frac{1}{n}g$. By the usual vector space axioms we get $h + \cdots + h = (\frac{1}{n} + \cdots + \frac{1}{n})g = g$. □

Lemma 4.1.4 will be essential in allowing us to use a variation of the Shoenfield-Blum test for quantifier elimination. By using axiom (iii) to force $\mathbb{Q}$-vector space structure for $T_{\mathfrak{Q}}$-models, we can axiomatise divisibility with universal formulas. Writing out the usual axiom for divisibility $\forall x \exists y(ny = x)$ would undermine this.

Remark 4.1.5. $T_{\mathfrak{Q}}$ is universal. That is, all formulas in $T_{\mathfrak{Q}}$ are of the form $\forall x_1, ...x_n \phi$ where ϕ is a quantifier free $\mathscr{L}$-formula (or are themselves quantifier free).

Proposition 4.1.6. *$\mathfrak{Q}$ embeds into every model of $T_{\mathfrak{Q}}$.*

Proof. Let $\mathcal{M} = (M; <', +', -', 0', 1', (\lambda_q)_{q \in \mathbb{Q}})$ be a model of $T_{\mathfrak{Q}}$. Notice that axiom (iii) just says that λ_q is to be interpreted as usual $\mathbb{Q}$-multiplication. So any model of $T_{\mathfrak{Q}}$ is an ordered abelian group with $\mathbb{Q}$-vector space structure.

We show that $\phi : \mathbb{Q} \to M$ given by $p \mapsto \lambda_p(1')$ is an embedding. From axiom (iii) we get that $0 \mapsto 0'$ and $1 \mapsto 1'$. Then by the usual properties of scalar multiplication we get

$$p_1 + p_2 \mapsto \lambda_{p_1+p_2}(1') = \lambda p_1(1') + \lambda_{p_2}(1') = \phi(p_1) +' \phi(p_2),$$

and $-p \mapsto \lambda_{-p}(1')$, while clearly $\lambda_{-p}(1') +' \lambda_p(1') = \lambda_0(1') = 0'$, whence $\phi(-p) = -'\phi(p)$.

For the order we have that $p_1 < p_2$ implies $\lambda_{p_1}(1') < \lambda_{p_2}(1')$ by axiom (ii) and the usual properties of ordered vector spaces. While if $p_1 \geq p_2$ we

get either $p_1 = p_2$ in which case $\lambda_{p_1}(1') = \lambda_{p_2}(1')$, or $p_2 < p_1$ in which case $\lambda_{p_2}(1') < \lambda_{p_1}(1')$. In both cases we clearly cannot have $\lambda_{p_1}(1') < \lambda_{p_2}(1')$, so we have $p_1 < p_2$ if and only if $\lambda_{p_1}(1') < \lambda_{p_2}(1')$.

Lastly note for any $p \in \mathbb{Q}$ we get

$$\begin{aligned}\lfloor \phi(p) \rfloor' &= \lfloor \phi(p - \lfloor p \rfloor) + \phi(\lfloor p \rfloor) \rfloor' \\ &= \lfloor \phi(p - \lfloor p \rfloor) + \lfloor \phi(\lfloor p \rfloor) \rfloor' \rfloor' \\ &= \lfloor \phi(p - \lfloor p \rfloor) \rfloor' + \lfloor \phi(\lfloor p \rfloor) \rfloor' \\ &= \lfloor \phi(\lfloor p \rfloor) \rfloor',\end{aligned}$$

but note that as $\lfloor p \rfloor \in \mathbb{Z}$, we can write $\lfloor p \rfloor = 1 + \cdots + 1$ and then we get that

$$\lfloor \phi(\lfloor p \rfloor) \rfloor' = \lfloor \phi(1 + \cdots + 1) \rfloor' = \lfloor 1' + \cdots + 1' \rfloor' = 1' + \cdots + 1' = \phi(\lfloor p \rfloor).$$

So putting this together, we at last have $\lfloor \phi(p) \rfloor' = \phi(\lfloor p \rfloor)$.

Therefore ϕ is indeed an embedding. □

4.2 Quantifier elimination tests

Definition 4.2.1. Let $\mathcal{M}, \mathcal{N}$ be $\mathscr{L}$-structures, with a common substructure $\mathcal{U}$. Then we write $\mathcal{M} \Rrightarrow_{\exists_1 \mathcal{U}} \mathcal{N}$ to mean the following:

For all quantifier free $\mathscr{L}$-formulas $\chi(y_1, \ldots, y_n, x)$ and n-tuples α from $\mathcal{U}$, the implication $\mathcal{M} \models \exists x \chi(\alpha, x) \Rightarrow \mathcal{N} \models \exists x \chi(\alpha, x)$ holds.

The following test for quantifier elimination is stated without proof, for a full proof see Tressl[10].

Proposition 4.2.2 (Shoenfield-Blum Test)**.** *Let T be an $\mathscr{L}$-theory without finite models. Then the following are equivalent:*

1. *T admits quantifier elimination.*
2. *If $\mathcal{B}, \mathcal{C} \models T$, and $\mathcal{A}$ is a finitely generated common substructure of $\mathcal{B}$ and $\mathcal{C}$, then $\mathcal{B} \Rrightarrow_{\exists_1 \mathcal{A}} \mathcal{C}$.*

In the following theorem the test for quantifier elimination which will be used on $T_{\mathfrak{Q}}$ is given. It is proved as a consequence of the Shoenfield-Blum test.

Theorem 4.2.3. *Let T be a universal $\mathscr{L}$-theory, and suppose for all models $\mathcal{M} \subsetneqq \mathcal{N}$ of T there is some $a \in N \setminus M$ and $\mathcal{M}' \succ \mathcal{M}$ such that $\mathcal{M}\langle a\rangle_{\mathcal{N}}$ embeds into $\mathcal{M}'$ over $\mathcal{M}$. Then T admits quantifier elimination.*

Proof. Suppose the conditions in the statement all hold. We want to show that the Shoenfield-Blum test goes through.

So let T be universal theory, with $\mathcal{B}, \mathcal{C} \models T$, and with $\mathcal{A}$ a finitely generated common substructure of the two. Now consider the collection of structures $\Psi = \{\mathcal{A}_0 : \mathcal{A} \leq \mathcal{A}_0 \leq \mathcal{B} \text{ and } \mathcal{A}_0 \Rrightarrow_{\exists_1 \mathcal{A}} \mathcal{C}\}$.

This collection is partially ordered under the substructure relation. We also have that any chain in Ψ has an upper bound in Ψ. Taking $\mathcal{A}^*$ to be the union of a chain, we just need to check that $\mathcal{A}^* \Rrightarrow_{\exists_1 \mathcal{A}} \mathcal{C}$. But this is clear since any witness for a formula from the union can be found in some structure which makes up the chain, and so there is a witness in $\mathcal{C}$ by assumption.

Now by Zorn's lemma Ψ contains a maximal element, say $\mathcal{A}_1$. As $\mathcal{A}_1 \in \Psi$ we have that $\mathcal{A}_1 \leq \mathcal{B}$. Then since $\mathcal{B}$ models T, which is universal, we have that $\mathcal{A}_1 \models T$. Note that this is where we utilise the assumption that T is universal.

Supposing that $\mathcal{A}_1 \subsetneqq \mathcal{B}$, we can bring in the assumptions from the statement. These tell us that there is some $\alpha \in B \setminus A_1$ and an elementary extension $\mathcal{A}_1' \succ \mathcal{A}_1$ such that there exists an embedding $\phi : \mathcal{A}_1\langle\alpha\rangle_{\mathcal{B}} \to \mathcal{A}_1'$ over $\mathcal{A}_1$.

So then we get that $\mathcal{A}_1\langle\alpha\rangle_{\mathcal{B}} \in \Psi$ since if $\mathcal{A}_1\langle\alpha\rangle_{\mathcal{B}} \models \exists x \chi(\bar{a}, x)$ we have a witness, say λ. This gives us that $\mathcal{A}_1' \models \chi(\bar{a}, \phi(\lambda))$, so that $\mathcal{A}_1' \models \exists x \chi(\bar{a}, x)$, and hence $\mathcal{A}_1 \models \exists x \chi(\bar{a}, x)$ by $\mathcal{A}_1 \prec \mathcal{A}_1'$. So as $\mathcal{A}_1 \in \Psi$ we get by transitivity of $\Rrightarrow_{\exists_1 \mathcal{A}}$ that $\mathcal{A}_1\langle\alpha\rangle_{\mathcal{B}} \in \Psi$, contradicting the maximality of $\mathcal{A}_1$. Hence we must have $\mathcal{A}_1 = \mathcal{B}$. Whence $\mathcal{B} \Rrightarrow_{\exists_1 \mathcal{A}} \mathcal{C}$, so by the Shoenfield-Blum test T admits quantifier elimination as required. □

4.3 $T_{\mathfrak{Q}}$ admits quantifier elimination.

We will use theorem 4.2.3 to prove that the theory $T_{\mathfrak{Q}}$ admits quantifier elimination, but before the proof we establish some results about $T_{\mathfrak{Q}}$-models which will be used.

Lemma 4.3.1. *Let $\mathcal{M} \models T_{\mathfrak{Q}}$, then for any $a \in M$ we have $a \in \lfloor M \rfloor$ if and only if $a = \lfloor a \rfloor$.*

Proof. The implication right to left is trivial. For left to right simply notice that since $a = \lfloor m \rfloor$ for some $m \in M$, we get $\lfloor a \rfloor = \lfloor \lfloor m \rfloor + 0 \rfloor$. But as $\mathcal{M}$ satisfies axiom (iv) we get $\lfloor a \rfloor = \lfloor m \rfloor = a$ as required. □

Lemma 4.3.2. *Let $\mathcal{M} \models T_{\mathfrak{Q}}$, then $\lfloor M \rfloor$ forms a subgroup of $(M, +)$.*

Proof. Note that $\lfloor 0 \rfloor = 0$ so $\lfloor M \rfloor \neq \emptyset$, and for $a, b \in \lfloor M \rfloor$ we have

$$a - b = \lfloor a \rfloor - b = \lfloor \lfloor a \rfloor - b \rfloor = \lfloor a - b \rfloor,$$

so $a - b \in \lfloor M \rfloor$. Hence $\lfloor M \rfloor$ forms a subgroup of $(M, +)$ as required. □

Lemma 4.3.3. *Let $\mathcal{M} \models T$, $a \in \lfloor M \rfloor$ and n a positive integer. Then there is unique $i \in \{0, \ldots, n-1\}$ such that $\frac{a+i}{n} \in \lfloor M \rfloor$.*

Proof. For uniqueness note that if we have $\frac{a+i_1}{n}, \frac{a+i_2}{n} \in \lfloor M \rfloor$ then by lemma 4.3.2 we get that both $\frac{i_1-i_2}{n}, \frac{i_2-i_1}{n} \in \lfloor M \rfloor$. Note that for one of these we can apply axiom (vii) and so using lemma 4.3.1 we get that $i_1 = i_2$.

Then for existence, consider different values of n. For $n = 1$, taking $i = 0$ is the only choice, and fortunately it works as we assume $a \in \lfloor M \rfloor$.

So now for $n \geq 2$ we can assume that $\frac{a}{n} \notin \lfloor M \rfloor$ since otherwise we are done. In this case we notice that

$$\begin{aligned} \lfloor n(a/n - \lfloor a/n \rfloor) \rfloor &= \lfloor a - n\lfloor a/n \rfloor \rfloor \\ &= \lfloor \lfloor a \rfloor - n\lfloor a/n \rfloor \rfloor \\ &= \lfloor a \rfloor + \lfloor -n\lfloor a/n \rfloor \rfloor \\ &= a - n\lfloor a/n \rfloor \neq 0. \end{aligned}$$

Where the inequality at the end is due to the assumption that $\frac{a}{n} \notin \lfloor M \rfloor$.

Then by considering axiom (vii) we get that $0 < a - n\lfloor \frac{a}{n} \rfloor < n$. Now $\lfloor M \rfloor \cap (0, n) = \{1, ..., n-1\}$ so for some $k \in \{1, ..., n-1\}$ we have $a = n\lfloor \frac{a}{n} \rfloor + k$. But then $\frac{a-k}{n} \in \lfloor M \rfloor$, hence $1 + \frac{a-k}{n} = \frac{a+(n-k)}{n} \in \lfloor M \rfloor$ by lemma 4.3.2 and axiom (vi). Since $0 < n - k < n$ we can take $i = n - k$ for $n \geq 2$. So we have existence and uniqueness, hence we are done. □

Definition 4.3.4. Let $G \leq H$ be ordered groups. We say that $h_1, h_2 \in H$ realise the same cut in G if for all $g \in G$ we have $g < h_1$ if and only if $g < h_2$.

Definition 4.3.5. A map between ordered structures will be called an order embedding if it is both order preserving and order reflective.

Proposition 4.3.6. *Let $(G, <, +)$ be a divisible ordered abelian group with proper extensions H_1 and H_2 (which are also divisible ordered abelian groups). Let $h_1 \in H_1 \setminus G$ and $h_2 \in H_2 \setminus G$. Then the map $\phi : G \oplus \mathbb{Q}h_1 \to G \oplus \mathbb{Q}h_2$ given by $\phi(g + qh_1) = g + qh_2$ is an order embedding if h_1 and h_2 realise the same cut in G.*

Proof. We want to show that for any $g_1, g_2 \in G$, $h_1 \in H_1$, and $q_1, q_2 \in \mathbb{Q}$ we have $g_1 + q_1h_1 < g_2 + q_2h_1$ if and only if $g_1 + q_1h_2 < g_2 + q_2h_2$.

If $q_1 \neq q_2$ then we can rearrange in the following way,

$$\begin{aligned} g_1 + q_1h_1 < g_2 + q_2h_1 &\Leftrightarrow \frac{g_1 - g_2}{q_2 - q_1} < h_1 \\ &\Leftrightarrow \frac{g_1 - g_2}{q_2 - q_1} < h_2 \\ &\Leftrightarrow g_1 + q_1h_2 < g_2 + q_2h_2. \end{aligned}$$

Whereas if $q_1 = q_2$ we have,

$$\begin{aligned} g_1 + q_1h_1 < g_2 + q_2h_1 &\Leftrightarrow g_1 < g_2 \\ &\Leftrightarrow g_1 + q_1h_2 < g_2 + q_2h_2. \end{aligned}$$

So we are done. □

Theorem 4.3.7. *$T_{\mathfrak{Q}}$ admits quantifier elimination.*

Proof. We apply theorem 4.2.3. Let $\mathcal{M} \lneqq \mathcal{N}$ be models of $T_{\mathfrak{Q}}$. To establish quantifier elimination we produce $\alpha \in N \setminus M$ and an extension $\mathcal{M}' \succ \mathcal{M}$ such that $\mathcal{M}\langle\alpha\rangle_{\mathcal{N}}$ embeds into $\mathcal{M}'$ over M. We consider two cases according to whether or not $\lfloor N \rfloor$ is contained in $\lfloor M \rfloor$. In both cases we will choose some suitable $\alpha \in N$, then produce a type over M, and give an embedding over M between $\mathcal{M}\langle\alpha\rangle_{\mathcal{N}}$ and an elementary extension of $\mathcal{M}$ which contains a realisation of this type.

Case 1:
For the first case, suppose $\lfloor N \rfloor = \lfloor M \rfloor$ (note that as $\mathcal{M} \leq \mathcal{N}$ we must have $\lfloor M \rfloor \subseteq \lfloor N \rfloor$, so we are adding the assumption that $\lfloor N \rfloor \subseteq \lfloor M \rfloor$). Then for any $\alpha \in N \setminus M$ we have $\lfloor m + q\alpha \rfloor \in M$ for all $m \in M$ and $q \in \mathbb{Q}$. Hence for such α we have $\lfloor M \oplus \mathbb{Q}\alpha \rfloor \subseteq M \subseteq M \oplus \mathbb{Q}\alpha$, and so $|\mathcal{M}\langle\alpha\rangle_{\mathcal{N}}| = M \oplus \mathbb{Q}\alpha$.

Now to produce a suitable extension $\mathcal{M}' \succ \mathcal{M}$ we take any $\alpha \in N \setminus M$ and an extension $\mathcal{M}'$ containing some α' which realises the same cut in M as α does. The sets of parameters $\alpha_L = \{m \in M : \mathcal{N} \models m < \alpha\}$ and $\alpha_R = \{m \in M : \mathcal{N} \models \alpha < m\}$, are clearly contained in M. We define a partial $\mathcal{M}$-type using these, by $\{m < x : m \in \alpha_L\} \cup \{m > x : m \in \alpha_R\}$. To verify that this is a partial type, we check that it is finitely realisable in $\mathcal{M}$. Taking a finite subset, we clearly get an open interval by taking the formulas corresponding to the most restrictive m from both α_L and α_R (or possibly just an upper or lower bound, but this case is of course even easier to deal with). Now suppose the interval we get is (m_1, m_2), then $m_1 + \frac{1}{2}(m_2 - m_1) \in M$ satisfies all of the formulas in the finite collection. Extending to a maximally consistent set of formulas we get an $\mathcal{M}$-type over M, which is hence realised in some extension $\mathcal{M}' \succ \mathcal{M}$, say by $\alpha' \in M'$. Note that as $\alpha \notin M$ we have $\alpha_L \cup \alpha_R = M$, hence $\alpha' \notin M$ also.

We can now use proposition 4.3.6. As we have two extensions $\mathcal{N}$ and $\mathcal{M}'$, both containing elements realising the same cut in the ground structure

$\mathcal{M}$, the map $\phi : M \oplus \mathbb{Q}\alpha \to M \oplus \mathbb{Q}\alpha'$ given by $m + q\alpha \mapsto m +' q\alpha'$ is an order embedding (also note that ϕ is well defined since the domain is a direct sum). Checking addition, constants, and scalar multiplication are all straightforward, so the details for the floor function are given.

For the floor function we need to check that for any $m \in M$ and $q \in \mathbb{Q}$ we have $\phi(\lfloor m + q\alpha \rfloor) = \lfloor m +' q\alpha' \rfloor'$. By our assumption that $\lfloor N \rfloor = \lfloor M \rfloor$ we have that $\lfloor m + q\alpha \rfloor \in \lfloor M \rfloor \subset M$, so $\phi(\lfloor m + q\alpha \rfloor) = \lfloor m + q\alpha \rfloor$. Since $\mathcal{N}$ satisfies $T_{\mathfrak{Q}}$ we know

$$\lfloor m + q\alpha \rfloor \leq m + q\alpha < \lfloor m + q\alpha \rfloor + 1,$$

so as ϕ is an order embedding we get

$$\lfloor m + q\alpha \rfloor \leq' m +' q\alpha' <' \lfloor m + q\alpha \rfloor +' 1.$$

This gives us that

$$0 \leq' (m +' q\alpha') -' \lfloor m + q\alpha \rfloor <' 1,$$

and hence $\lfloor (m+q\alpha') -' \lfloor m+q\alpha \rfloor \rfloor' = 0$. It is easily seen that in any $T_{\mathfrak{Q}}$-model $\lfloor x - \lfloor y \rfloor \rfloor = \lfloor x \rfloor - \lfloor y \rfloor$. As $\mathcal{M}' \succ \mathcal{M}$ we have $\lfloor M \rfloor \subseteq \lfloor M' \rfloor'$, and in particular $\lfloor m + q\alpha \rfloor \in \lfloor \mathcal{M}' \rfloor'$. Putting all of this together we get

$$\begin{aligned}
\lfloor m +' q\alpha' \rfloor' -' \phi(\lfloor m + q\alpha \rfloor) &= \lfloor m +' q\alpha' \rfloor' -' \lfloor m + q\alpha \rfloor \\
&= \lfloor m' + q\alpha' \rfloor' -' \lfloor \lfloor m + q\alpha \rfloor \rfloor', \\
&= \lfloor (m + q\alpha') -' \lfloor \lfloor m + q\alpha \rfloor \rfloor' \rfloor', \\
&= \lfloor (m +' q\alpha') -' \lfloor m + q\alpha \rfloor \rfloor', \\
&= 0.
\end{aligned}$$

Therefore $\phi(\lfloor m + q\alpha \rfloor) = \lfloor m +' q\alpha' \rfloor'$. So we have $\alpha \in N \setminus M$, and an extension $\mathcal{M}' \succ \mathcal{M}$ such that $\mathcal{M}\langle\alpha\rangle_{\mathcal{N}}$ embeds into $\mathcal{M}'$ over M as required.

Case 2:

For the second case suppose $\lfloor M \rfloor \subsetneqq \lfloor N \rfloor$. Taking $\alpha \in \lfloor N \rfloor \setminus \lfloor M \rfloor$ have that

$\lfloor M \oplus \mathbb{Q}\alpha \rfloor \subseteq M \oplus \mathbb{Q}\alpha$. This is because for any $m \in M$ and $q \in \mathbb{Q}$ we can write $q = \frac{k}{n}$ where $k \in \mathbb{Z}$ and n a natural number. By lemma 4.3.3 there exists $i_n \in \{0, \ldots, n-1\}$ such that $(\alpha + i_n)/n \in \lfloor N \rfloor$, it follows that

$$\lfloor m + q\alpha \rfloor = \lfloor m - qi_n + k\frac{\alpha + i_n}{n} \rfloor = \lfloor m - qi_n \rfloor + k\frac{\alpha + i_n}{n} \in M \oplus \mathbb{Q}\alpha,$$

where the first equality is trivial, and the second is implied by $\frac{\alpha+i_n}{n} \in \lfloor N \rfloor$. So we have $|\mathcal{M}\langle\alpha\rangle_{\mathcal{N}}| = M \oplus \mathbb{Q}\alpha$ as in the first case.

Again we must produce some extension $\mathcal{M}' \succ \mathcal{M}$ such that $\mathcal{M}\langle\alpha\rangle_{\mathcal{N}}$ embeds into $\mathcal{M}'$ over M. We will use the same technique as in the first case. First a partial type is given, this is extended to a maximally consistent set of formulas, we take some realisation α' in an extension $\mathcal{M}' \succ \mathcal{M}$, then show that ϕ given by $m + q\alpha \mapsto m +' q\alpha'$ is an embedding from $\mathcal{M}\langle\alpha\rangle_{\mathcal{N}}$ into $\mathcal{M}'$ over M.

We have now fixed $\alpha \in \lfloor N \rfloor \setminus \lfloor M \rfloor$. The sets of parameters α_L and α_R are defined as in the first case, but with respect to this new α. New parameters are also introduced. For each natural $n \geq 2$ we take the unique $i_n \in \{0, \ldots, n-1\}$ given by lemma 4.3.3 such that $\frac{\alpha+i_n}{n} \in \lfloor N \rfloor$, writing $\alpha_{\mathbb{N}}$ for the collection of all such i_n. Since we can identify these natural numbers in the ground model $\mathcal{M}$, all our parameters still come from M (i_n is identified with $\lambda_{i_n}(1)$, and more generally any $q \in \mathbb{Q}$ is identified with $\lambda_q(1)$, which is an embedding by proposition 4.1.6).

We now need to show that taking the union of the order conditions, produced just as in the first case (for the new α), and the following set

$$\{(x + i_n)/n = \lfloor (x + i_n)/n \rfloor : i_n \in \alpha_{\mathbb{N}}\},$$

gives a partial type. To do this we must show that the set of formulas is finitely realisable in $\mathcal{M}$.

As in the first case, any finite collection of the order conditions gives an open interval (m_1, m_2) in M. Any finite collection of new formulas gives a finite sequence of congruences. So to finitely realise the collection we need to

realise a finite sequence of congruences in an arbitrary open interval of the ground model $\mathcal{M}$ which contains an element $\alpha \in \lfloor N \rfloor \setminus \lfloor M \rfloor$ when considered as an interval in $\mathcal{N}$. This last remark is essential to the proof, why this is the case will become clear shortly.

By the Chinese remainder theorem there exists some $k \in \mathbb{Z}$ satisfying any such finite sequence of congruences. Now it is sufficient to show that for each natural number n, there exists an element $m \in \lfloor M \rfloor \cap (m_1, m_2)$ such that $\frac{m}{n} \in \lfloor M \rfloor$. Then fixing n to be the (finite) product of denominators from the congruences, we get for any natural number j, and $i_j \in \{0, \ldots, j-1\}$ with $\frac{x+i_j}{j} = \lfloor \frac{x+i_j}{j} \rfloor$ being one of the congruences, that

$$\begin{aligned} \lfloor \frac{m+k+i_j}{j} \rfloor &= \lfloor \hat{n} \frac{m}{n} \rfloor + \lfloor \frac{k+i_j}{j} \rfloor \\ &= \hat{n} \frac{m}{n} + \frac{k+i_j}{j} \\ &= \frac{m+k+i_j}{j}, \end{aligned}$$

where $\hat{n} \coloneqq n/j$ is a clearly a natural number. So for any such $m \in M$ and $k \in \mathbb{Z}$, $m+k$ satisfies the finite sequence of congruences. By lemma 4.3.3 applied to $\lfloor m_1 \rfloor \in \lfloor M \rfloor$ and the n we have chosen as the product of the finitely many denominators from the congruences, there is $i_n \in \{0, \ldots, n-1\}$ such that $\frac{\lfloor m_1 \rfloor + i_n}{n} \in \lfloor M \rfloor$.

Now we take $m = \lfloor m_1 \rfloor + i_n + n$. Since $\alpha \notin \lfloor M \rfloor$, we have $\lfloor m_1 \rfloor + K < \alpha$ for any natural number K. Otherwise we get a contradiction as follows. If natural K exists with $\lfloor m_1 \rfloor + k \geq \alpha$ then clearly $K \neq 0$. Taking minimal K with $\lfloor m_1 \rfloor + K \geq \alpha$, we get

$$\lfloor m_1 \rfloor + K - 1 < \alpha < \lfloor m_1 \rfloor + K,$$

where the second inequality is strict as $\lfloor m_1 \rfloor + K \in \lfloor M \rfloor$. This gives

$$0 < \alpha - (\lfloor m_1 \rfloor + K - 1) < 1,$$

and therefore

$$\lfloor \alpha \rfloor - (\lfloor m_1 \rfloor + K - 1) = \lfloor \alpha - (\lfloor m_1 \rfloor + K - 1) \rfloor = 0.$$

But this implies $\alpha \in \lfloor M \rfloor$, a contradiction.

Now we take $m = \lfloor m_1 \rfloor + i_n + n$. Then as $i_n + n + k$ is a natural number, it follows that $\lfloor m_1 \rfloor + i_n + n + k \geq \lfloor m_1 \rfloor + 1 > m_1$, and therefore that $m + k \in (m_1, \alpha) \subset (m_1, m_2)$. So $m + k \in M$ realises the finite subset from the collection of formulas. Hence the collection of formulas given is finitely realisable in the ground model $\mathcal{M}$. So we have a partial type over M, and as in the first case we extend it to a maximally consistent set of formulas, then take some realisation α' in an extension $\mathcal{M}' \succ \mathcal{M}$. By the same argument as in the first case using proposition 4.3.6, we have that the order is preserved and reflected by the map ϕ since α' realises the same cut as α in M. To prove that ϕ is an embedding we just need to check that the floor function is also preserved.

We do this using the construction of α' such that it realises all the congruences given for α. For any $m \in M$ and $q \in \mathbb{Q}$ we have $q = \frac{k}{n}$ for some $k \in \mathbb{Z}$ and natural n. Then we can write $m + q\alpha = m - qi_n + k(\alpha + i_n)/n$. Since $(\alpha + i_n)/n \in \lfloor N \rfloor$ we get $\lfloor m + q\alpha \rfloor = \lfloor m - qi_n + \lfloor k(\alpha + i_n)/n \rfloor \rfloor = \lfloor m - qi_n \rfloor + k(\alpha + i_n)/n$. Now $\lfloor m - qi_n \rfloor + qi_n \in M$, so we get

$$\phi(\lfloor m + q\alpha \rfloor) = \lfloor m - qi_n \rfloor +' qi_n +' q\alpha'.$$

Since α' realises our type, we also have

$$\begin{aligned} \lfloor m + q\alpha' \rfloor' &= \lfloor m + q\alpha' + qi_n - qi_n \rfloor' \\ &= \lfloor m - qi_n \rfloor' +' qi_n +' q\alpha', \end{aligned}$$

whence $\phi(\lfloor m + q\alpha \rfloor) = \lfloor m + q\alpha' \rfloor'$ for any $m \in M$ and $q \in \mathbb{Q}$, so again $\mathcal{M}\langle\alpha\rangle_{\mathcal{N}}$ embeds into $\mathcal{M}'$ over M.

Putting both cases together, we have that $T_{\mathfrak{Q}}$ admits quantifier elimination by theorem 4.2.3.

□

Proposition 4.3.8. *$T_{\mathfrak{Q}}$ axiomatises $\mathfrak{Q}$.*

Proof. Since $T_{\mathfrak{Q}}$ admits quantifier elimination, any embedding between $T_{\mathfrak{Q}}$ models is elementary. So by proposition 4.1.6 we have that $\mathfrak{Q}$ is a prime model of $T_{\mathfrak{Q}}$, and hence is axiomatised by $T_{\mathfrak{Q}}$. □

Proposition 4.3.9. *$T_{\mathfrak{Q}}$ is a complete theory.*

Proof. This follows from the fact $\mathfrak{Q}$ is a prime-model of $T_{\mathfrak{Q}}$. □

5 Decidability of $(\mathbb{R}; <, +, \mathbb{Z})$.

We show here that the structure $\mathfrak{Q}$ is decidable using the results of section 4, and with this prove that the structure $(\mathbb{Q}; <, +, \mathbb{Z})$ is decidable by showing that $\mathfrak{Q}$ recursively defines it. After this only a few simple adaptions are needed. In particular noticing that $\mathfrak{R} = (\mathbb{R}; <, +, -, 0, 1, (\lambda_q)_{q\in\mathbb{Q}}, \lfloor\ \rfloor)$ models $T_{\mathfrak{Q}}$, and so is an elementary extension of $\mathfrak{Q}$. Then showing that $\mathfrak{R}$ recursively defines $(\mathbb{R}; <, +, \mathbb{Z})$, decidability carries over to this structure which is our original interest. The main sources used are Tressl [11] and Marker [6].

5.1 Decidability of $T_{\mathfrak{Q}}$

Definition 5.1.1. Let T be a theory in a language $\mathscr{L}$. Then we say that T is decidable if the set $\mathrm{Ded}(T)$ is recursive.

Lemma 5.1.2. *Let T be a theory in a recursive language $\mathscr{L}$. If T is recursive, complete, and satisfiable then T is decidable.*

Proof. Since T is consistent and satisfiable the sets $\{\varphi \in \mathrm{Sen}(\mathscr{L}) : T \models \varphi\}$ and $\{\varphi \in \mathrm{Sen}(\mathscr{L}) : T \models \neg\varphi\}$ partition $\mathrm{Sen}(\mathscr{L})$. By the completeness theorem these sets are equal to $\{\varphi \in \mathrm{Sen}(\mathscr{L}) : T \vdash \varphi\}$ and $\{\varphi \in \mathrm{Sen}(\mathscr{L}) : T \vdash \neg\varphi\}$ respectively. Now as T is recursive, both of these sets (once coded) are recursively enumerable, this then implies that $\{\varphi \in \mathrm{Sen}(\mathscr{L}) : T \vdash \varphi\}$ is recursive. But this says precisely that T is decidable, so we are done. □

Remark 5.1.3. The language for $\mathfrak{Q}$ is recursive. We can fix symbol numbers by sending each variable v_i to $2i$, and setting $[<] = 1$, $[+] = 3$, $[0] = 5$, $[1] = 7$, $[-] = 9$, $[\lfloor\ \rfloor] = 11$.

For the scalar multiplication we use the Cantor pairing function

$$\pi : \mathbb{N} \times \mathbb{N} \setminus \{0\}, (k_1, k_2) \mapsto \frac{1}{2}(k_1 + k_2)(k_1 + k_2 + 1) + k_1,$$

composed with $n \mapsto 2n + 11$. The composed function has cofinite, hence recursive, image. Since the images of the arity maps are finite we have a recursive language.

Proposition 5.1.4. *The axiomatisation $T_{\mathfrak{Q}}$ of $\mathfrak{Q}$ is recursive.*

Proof. There are essentially only two things we need to check here. Both (i) and (iii) contain infinitely many axioms, however these can quickly be seen to be recursive. We have, for each $n \in \mathbb{N}$, an axiom of the form $\forall x \exists y(n \cdot y = x)$, and for each pair $(j, n) \in \mathbb{Z} \times \mathbb{N}$ an axiom of the form $\forall x \lambda_n(\lambda_{j/n}(x)) = \lambda_j(x)$. Now the first are recursive as their codes are recursive, which can be seen from the fact the positions of the n summands are retrievable from the length of the string, and everything surrounding these remain fixed between all such axioms (i.e. we want all formulas $\forall x \exists y(\star = x)$, and here the candidates for $\star$ are all of the recursive form $y + ... + y$ with the number of summands being the coded length of the formula with some constant subtracted). The second set of axioms are obviously recursive because the set of codes for λ_q is recursive. □

Proposition 5.1.5. *$T_{\mathfrak{Q}}$ is decidable.*

Proof. We just saw that both the language of $\mathfrak{Q}$ and an axiomatisation are recursive. Since $\mathfrak{Q} \models T_{\mathfrak{Q}}$ we have that $T_{\mathfrak{Q}}$ is satisfiable. Now we also have that $T_{\mathfrak{Q}}$ admits quantifier elimination and has prime-model $\mathfrak{Q}$. It follows that $T_{\mathfrak{Q}}$ is complete, and hence by lemma 5.1.2 is decidable. □

5.2 Decidability of $(\mathbb{Q}; <, +, \mathbb{Z})$ and $(\mathbb{R}; <, +, \mathbb{Z})$.

Proposition 5.2.1. $\mathfrak{Q} = (\mathbb{Q}; <, +, -, 0, 1, (\lambda_q)_{q \in \mathbb{Q}}, \lfloor\ \rfloor)$ *recursively defines* $(\mathbb{Q}; <, +, \mathbb{Z})$.

Proof. The predicate $\mathbb{Z}$ is defined in $\mathfrak{Q}$ by $\varphi_{\mathbb{Z}}(x) : x = \lfloor x \rfloor$. Since the language for $\mathbb{Q}$ is finite the definition is clearly recursive. □

Theorem 5.2.2. $(\mathbb{Q}; <, +, \mathbb{Z})$ *is decidable.*

Proof. This follows from the fact that $(\mathbb{Q}; <, +, \mathbb{Z})$ is recursively definable in $\mathfrak{Q}$, which is decidable since it is recursively axiomatised by a decidable theory $T_{\mathfrak{Q}}$. □

Theorem 5.2.3. $(\mathbb{R}; <, +, \mathbb{Z})$ *is decidable.*

Proof. It is easily seen that $\mathfrak{R} = (\mathbb{R}; <, +, -, 0, 1, (\lambda_q)_{q\in\mathbb{Q}}, \lfloor\ \rfloor)$ is a model of $T_{\mathfrak{Q}}$ which admits $\mathfrak{Q}$ as a substructure. As $T_{\mathfrak{Q}}$ admits quantifier elimination we in fact have that $\mathfrak{R}$ is an elementary extension of $\mathfrak{Q}$ (by model-completeness). Since the first order theory of $\mathfrak{Q}$ is decidable, the (identical) first order theory of $\mathfrak{R}$ is hence decidable. Then as $(\mathbb{R}; <, +, \mathbb{Z})$ is (recursively) definable in $\mathfrak{R}$ (by taking for $\mathbb{Z}$ the fixed points of $\lfloor\ \rfloor$ again) we have that $(\mathbb{R}; <, +, \mathbb{Z})$ is decidable. □

6 Undecidability of $(\mathbb{R}; <, +, \times, \mathbb{Z})$.

Here we show that the first order theory of $(\mathbb{R}; <, +, \times, \mathbb{Z})$ is undecidable. This is done by recursively interpreting a well known undecidable structure $\overline{\omega} = (\omega; <, +, \times, 0, S)$ in it. Tressl[11] contains a proof of this theorem, as well as proof of the undecidability of $\overline{\omega}$, both are used without proof here.

6.1 Applying a theorem of Tarski.

Theorem 6.1.1 (Tarski)**.** *Let $\mathcal{M}$ and $\mathcal{M}'$ be structures in recursive languages $\mathscr{L}$ and $\mathscr{L}'$ respectively. Then if $\mathcal{M}'$ is undecidable and $\mathcal{M}$ recursively interprets $\mathcal{M}'$, also $\mathcal{M}$ is undecidable.*

So to prove that $(\mathbb{R}; <, +, \times, \mathbb{Z})$ is undecidable, it is sufficient to interpret (recursively) some structure which we already know to be undecidable in it. We do this with $\overline{\omega} = (\omega; <, +, \times, 0, S)$.

Theorem 6.1.2. $(\mathbb{R}; <, +, \times, \mathbb{Z})$ *is undecidable.*

Proof. We show that $(\mathbb{R}; <, +, \times, \mathbb{Z})$ interprets $\overline{\omega}$, which is known to be undecidable. In fact $\overline{\omega}$ is definable within our structure. The constants 0 and 1 are easily defined in $(\mathbb{R}; <, +, \times, \mathbb{Z})$ as the additive and multiplicative identity, so we are free to work with these. The universe of the interpretation is given by $\mathscr{U}(x) : \mathbb{Z}(x) \wedge (x > 0 \vee x = 0)$. Then all non-logical symbols are just directly inherited, with the exception of S which is interpreted in the obvious way $\varphi_S(x, y) : x + 1 = y$. Both languages are clearly finite, hence both the languages and the interpretation are recursive. So by theorem 6.1.1 $(\mathbb{R}; <, +, \times, \mathbb{Z})$ is undecidable. □

In the next section expansions of $(\mathbb{R}; <, +, \mathbb{Z})$ by scalar multiplication are discussed. Theorem 6.1.2 is used when looking at these expansions. For example, given non-quadratic $a \in \mathbb{R}$ it can be shown that expanding $(\mathbb{R}; <, +, \mathbb{Z})$ by a scalar function $\lambda_a : x \mapsto ax$ gives a structure which defines $(\mathbb{R}; <, +, \times, 0, 1, \mathbb{Z})$, and is therefore undecidable by theorem 6.1.2.

7 Further expansions of $(\mathbb{R}; <, +, \mathbb{Z})$.

Without going into great detail, this section will give a brief overview of some results established by Hieronymi in [3] and [2], and give insight into how Hieronymi is using Ostrowski representations to build on the results covered in sections 5 and 6.

We have seen that the first order theory of $(\mathbb{R}; <, +, \mathbb{Z})$ is decidable, while the first order theory of $(\mathbb{R}; <, +, \cdot, \mathbb{Z})$ is undecidable. These results give rise to a question asked by Hieronymi,

"How many traces of multiplication can be added to $(\mathbb{R}; <, +, \mathbb{Z})$ *without making the first order theory undecidable?"*[1].

Taking "traces of multiplication" to mean scalar multiplication, Hieronymi answers this question in the same paper with the following two results.

Denote $(\mathbb{R}; <, +, \mathbb{Z}, \lambda_a)$, the expansion of $(\mathbb{R}; <, +, \mathbb{Z})$ by scalar multiplication by $a \in \mathbb{R}$, as $\mathcal{S}_a$, then:

Theorem. *The theory of* $\mathcal{S}_a$ *is decidable if and only if* a *is quadratic.*

This generalises to scalar multiplication by subfields, with the result:

Theorem. *Let* K *be a subfield of* $\mathbb{R}$*, then the theory of the ordered* K*-vector space* $\mathbb{R}$ *expanded by a predicate for* $\mathbb{Z}$ *is decidable if and only if* K *is a quadratic field.*

If a is not quadratic then it can be shown that $\mathcal{S}_a$ defines full multiplication on $\mathbb{R}$. It follows that $\mathcal{S}_a$ is undecidable by the undecidability of $(\mathbb{R}; <, +, \cdot, \mathbb{Z})$ (see section 6).

The more involved task is to show that if a is quadratic the theory of $\mathcal{S}_a$ is decidable. To show this, Hieronymi shows that for quadratic a the structure $\mathcal{R}_a = (\mathbb{R}; <, +, \mathbb{Z}, \mathbb{Z}a)$ defines $\mathcal{S}_a$. Combining this with the result that the

[1] Hieronymi [3] page 1

theory of $\mathcal{R}_a$ is decidable for quadratic a we are done, but this result is of course not trivial.

In order to prove that $\mathcal{R}_a$ is decidable for quadratic a, Hieronymi uses properties of Ostrowski representations of both natural and real numbers to show that for quadratic a the structure $\mathcal{R}_a$ is definable in $\mathcal{B}$. Here $\mathcal{B}$ is the structure $(\mathbb{N}, \mathcal{P}(\mathbb{N}), s_{\mathbb{N}}, \in)$, the monadic second order structure of the natural numbers. Using automaton theory Büchi showed that $\mathcal{B}$ is decidable, and so the decidability of $\mathcal{R}_a$ is within grasp at this point.

To give a small indication of how Ostrowski representations come into play, defining $\mathcal{R}_a$ in $\mathcal{B}$ involves using results such as the following.

Fixing $d \in \mathbb{Q}$, with $d \neq c^2$ for any $c \in \mathbb{Q}$, we get that the continued fraction for $\sqrt{d}$ is periodic, say with minimal period length m. Taking the sequences ζ_k and β_k from the continued fraction of $\sqrt{d}$ (see definition 2.2.4 and definition 2.4.1 respectively), we get the following result:

Fact ((2.2), Hieronymi [3])**.**

$$\zeta_1 \cdots \zeta_{m+1} \cdot \beta_{k+m} = (-1)^m \cdot \beta_k.$$

Which gives us (with some work!) that multiplying any real number in the interval $[-1/\zeta_1, 1 - 1/\zeta_1)$ by $\zeta_1 \cdots \zeta_{m+1}$ corresponds to an m-shift in the Ostrowski representation of that number based on the continued fraction of $\sqrt{d}$.

The first step towards defining $\mathcal{R}_a$ in $\mathcal{B}$ is to define sets in $\mathcal{B}$ corresponding to Ostroswki representations based on the continued fraction of a. Then, as an example, the fact above can be used in defining scalar multiplication by appropriate numbers as shifts in the Ostrowski representations, which are definable within $\mathcal{B}$.

References

[1] Jean-Paul Allouche and Jeffrey Shallit. *Automatic Sequences: Theory, Applications, Generalizations*. Cambridge University Press, 2003.

[2] Philipp Hieronymi. Expansions of the ordered additive group of real numbers by two discrete subgroups, 2014, arXiv:1407.7002v2.

[3] Philipp Hieronymi. When is scalar multiplication decidable?, 2015, arXiv:1505.08055v1.

[4] Philipp Hieronymi and Alonza Terry Jr. Ostrowski numeration systems, addition and finite automata, 2014, arXiv:1407.7000v2.

[5] Wilfred Hodges. *Model Theory*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1993.

[6] David Marker. *Model Theory: An Introduction*. Springer, 2011.

[7] Chris Miller. Expansions of dense linear orders with the intermediate value property. *Journal of Symbolic Logic*, 66(4):1783–1790, 2001.

[8] Andrew M Rockett and Peter Szusz. *Continued Fractions*. World Scientific Publishing Company, 1992.

[9] William Stein. *Elementary Number Theory: Primes, Congruences, and Secrets: A Computational Approach (Undergraduate Texts in Mathematics)*. Springer, 2008.

[10] Marcus Tressl. Lecture notes on Model Theory, 2010-2011.

[11] Marcus Tressl. Lecture notes on Gödel's Incompleteness Theorems, 2016-2017.