Notes from the logbook of a proof-checcher's project*

Domenico Cantone[1], Eugenio G. Omodeo[2], Jacob T. Schwartz[3], Pietro Ursino[1]

[1] University of Catania, Dipartimento di Matematica e Informatica
{cantone,ursino}@dmi.unict.it
[2] University of L'Aquila, Dipartimento di Informatica omodeo@di.univaq.it
[3] University of New York, Department of Computer Science, Courant Institute of Mathematical Sciences schwartz@cs.nyu.edu

Introduction

We are developing a software system which ingests proofs formalized within Zermelo-Fraenkel set theory and checks their compliance with mathematical rigor. It will accept trivial steps as obvious, without necessarily being clever at discovering how to fill large gaps in a proposed mathematical argument. It will be able to process large proof scripts (say dozens of thousands of proofware lines written on persistent files), without necessarily acting as a highly interactive proof assistant. Over the years, the documentation of our project (entrusted, to a large extent, to electronic correspondence) has come to form a thick logbook, of which we will transcribe three extracts in this paper.

The design of a proof checker must face a variety of design issues, partly because proof technology as a whole has not reached, as of today, a plateau on which applications, for example in the areas of program correctness and security protocol verification, can firmly rely. On the other hand, such a wealth of ideas is encompassed in the software of state-of-the-art proof systems as to give us an embarrassingly wide choice: which techniques and methods should we include among our basic inference ingredients, from which reasoning paradigms can we gain deep insights and intellectual stimuli for further research?

In any project, a yardstick is needed to judge on virtues and drawbacks of technical solutions and to keep under constant focus the most critical design issues on which ultimate success depends: in our case the yardstick is a huge proof script, our privileged "scenario" file, which evolves in parallel with our prototype proof-checker, supports its functional testing, and brings to light the need for new functions and linguistic features. It was decided from the outset that our scenario should lead from "first principles", namely the rudiments of set theory, to a most important achievement of classical mathematical analysis, the Cauchy Integral Theorem. The "backbone" of the scenario, consisting only of definitions and theorem statements, became available very early in the project;

* Work partially supported by MURST/MIUR 40% project *Aggregate- and number-reasoning for computing: from decision algorithms to constraint programming with multisets, sets, and maps*

then it was progressively fleshed out with proof details. We can roughly assess that 50% of the scenario development has been carried out and that, once completed, the scenario will consist of 20 to 25 thousand lines of proofware. Only occasionally we have digressed into the specification of peripheral proof scripts: this happened, for instance, when we exercised with a "rib" to be grafted at some early point in the backbone of analysis, namely the treatment of inductive sets which we will outline in Sec.1; it happened again when we wanted to assess how easily amenable to our computerized proof environment would be a program correctness verification.

The issue of proof modularization acquires great importance as the size of proof scripts increases. The obvious goal of modularization is to avoid repeating similar steps when the proofs of two theorems are closely analogous. Modularization must also conceal the details of a proof once they have been fed into the proof-checker and successfully certified. We discussed this issue at length in [8], of which this paper is a continuation, and therefore will limit ourselves here to producing new examples (cf. Sec.1). We will delay again a deep discussion on the nature of the basic inference steps a proof-verifier rooted in set theory should (and reasonably can) handle; however, since decision algorithms for fragments of first-order theories play a crucial role in this connection, we will take into consideration a sample case, related to ordered Abelian groups, and dissect it in Sec.2.

The third newsletter in this paper (Sec.3) concerns a turning point in our main scenario: how to define the set of real numbers and prove their basic properties. Historically this been done in several ways,which offer competing advantages when computer-based verification is intended. In Dedekind's approach, which is the most directly set-theoretic of all, a real number is defined simply as a non-null set of rational numbers, bounded above, which contains no largest element and which contains each rational number smaller than any of its elements. Sums are easily defined for real numbers defined in this way, but it is only easy to define products for positive reals directly. This forces separate treatment of real products involving negative reals, causing the proof of statements like the associativity of multiplication to break up into an irritating number of separate cases. For this reason, we choose a different approach, originally developed by Cantor in 1872, in a simplified contemporary variant which we draw from [2].

[····· TO BE ELABORATED ·····]

1 Inductive sets

Inductive sets occur often in mathematics and in computer science. The most classical of them is the set $\mathbb{N}$ of *natural numbers*, generated from the singleton $\{0\}$ by the unitary increment operation. Another classical example is the set of all *finite lists* with components drawn from a fixed, though generic, base set A. A third example is the set of all *terms over a signature*. Inductive sets can be conceived of dynamically: namely, in each specific instance we can identify a set of *seeds* and a *generating map* which—we may think—repeatedly puts new

elements into a set whose initial value is the set of seeds and whose ending value, the inductive set, is reached when a certain 'plateau' (that is, the fulfillment of a certain closure property) has been achieved, perhaps by a transfinite number of iterations. Below, in specifying the notion of inductive set formally, we will insist that seeds should not be reachable again as the construction proceeds. More generally, the construction of an inductive set should be carried out under some guarantee that no element of the inductive set can admit more than one construction. This will make reasoning about the elements of an inductive set particularly plain and effective.

Notice that the generating map is not necessarily single-valued: while in the paradigmatic case of natural numbers it is such, to best treat the other two cases mentioned above we will figure out two suitable multi-valued generating maps. (For uniformity, as regards $\mathbb{N}$, we will proceed from the definitions

$$0 =_{\text{Def}} \emptyset \quad \text{and} \quad \mathsf{hasNext}(X, Y) \leftrightarrow_{\text{Def}} Y = X \text{ with } X,$$

even though the definition $\mathsf{next}(X) =_{\text{Def}} X \text{ with } X$ might seem better tailored to the case than the one of $\mathsf{hasNext}$.) Another crucial design choice is whether the generating map should be a 'small' relation (representable as a set of pairs) or a global relation (representable by a formula $\varphi \equiv \varphi(X, Y)$). We opt here for a *global map*.

A more than adequate technical surrogate for the above-hinted (and intuitively more appealing) dynamic construction of an inductive set will consist of two steps:

1. Identify a superset of the desired inductive set. This must contain the seeds and must be closed w.r.t. the generating map.
2. Extract the inductive set from the superset determined at Step 1.

Since inductive sets are normally infinite, the *infinity axiom*

$$\mathbf{s}_\infty \neq \emptyset \,\&\, [\forall\, x \in \mathbf{s}_\infty \mid \{x\} \in \mathbf{s}_\infty]$$

of Zermelo-Fraenkel set theory will be needed to effect Step 1. To make Step 2 a plain routine matter, we will design a THEORY offering adequate support to it.

This revolution of replacing potential infinity by actual infinity in mathematical reasoning was made by Cantor and Dedekind in the late nineteenth century (cf. [1]). Thanks to the availability of the recursive definition scheme, a single actual infinite set, even one which is as indistinct as $\mathbf{s}_\infty$ is, suffices to get started.

1.1 How to frame an inductive set

To convey an intuitive grasp of the notion of inductive set, we state beforehand that the set $\mathbf{s}_\infty$ may fail to be inductive *relative* to the singleton set $\{\mathbf{arb}\,(\mathbf{s}_\infty)\}$ of seeds and to the generating map $\mathsf{Sngl}(X, Y) \leftrightarrow_{\text{Def}} Y = \{X\}$. As a matter of fact, momentarily assuming for definiteness that $\mathbf{arb}\,(\mathbf{s}_\infty) = \emptyset$, we should not regard $\mathbf{s}_\infty$ as being inductive relative to $\{\emptyset\}, \mathsf{Sngl}$ if it had such 'superfluous' elements as $\{\emptyset, \{\emptyset\}\}$ or $\{\emptyset, \{\emptyset, \{\{\emptyset\}\}\}\}$ instead of consisting of *only* the 'mandatory' elements in the following infinite list:

$$\emptyset,\ \{\emptyset\},\ \{\{\emptyset\}\},\ \{\{\{\emptyset\}\}\}, \ldots\ .$$

We will develop in Sec.1.2 the machinery needed to form the subset of $\mathbf{s}_\infty$ consisting *precisely* of the sets $\mathbf{arb}\,(\mathbf{s}_\infty)$, $\{\mathbf{arb}\,(\mathbf{s}_\infty)\}$, and $\{\cdots\{\mathbf{arb}\,(\mathbf{s}_\infty)\}\cdots\}$. The best we can say now is that $\mathbf{s}_\infty$ FRAMES the desired inductive set. Below we will exploit $\mathbf{s}_\infty$ to construct sets which frame other important inductive sets such as the set $\mathbb{N}$ of all natural numbers, the family $\mathbb{H}$ of all hereditarily finite sets, and the set $\mathsf{tuples}(A)$ of all finite lists over A.

Before continuing, we must provide the formal definition of INDUCTIVELY CLOSED SET, which presupposes a couple of notions regarding a global map R (in a sense *into-ness* and *injectivity*):

$$\begin{aligned}
\mathsf{Maps}(R,S,T) &\leftrightarrow_{\text{Def}} [\forall x \in S\, \forall y \,|\, R(x,y) \longrightarrow y \in T],\\
\mathsf{Disj}(R,S) &\leftrightarrow_{\text{Def}} [\forall u \in S, v \in S\, \forall y \,|\, R(u,y)\ \&\ R(v,y) \longrightarrow u = v],\\
\mathsf{IndClosed}(N,R,A) &\leftrightarrow_{\text{Def}} A \subseteq N\ \&\ \mathsf{Maps}(R,N,N \setminus A)\ \&\ \mathsf{Disj}(R,N)\\
&\qquad\ \&\ [\forall t \,|\, A \subseteq t\ \&\ \mathsf{Maps}(R,t,t) \longrightarrow N \subseteq t].
\end{aligned}$$

A set S which candidates to frame a set N such that $\mathsf{IndClosed}(N,R,A)$ will be required to meet a *less stringent* condition than being inductively closed, namely the following:

$$\mathsf{Frames}(S,R,A) \leftrightarrow_{\text{Def}} A \subseteq S\ \&\ \mathsf{Maps}(R,S,S \setminus A)\ \&\ \mathsf{Disj}(R,S).$$

How to frame the inductive set $\mathbb{N}$ of natural numbers After recalling that

$$0 =_{\text{Def}} \emptyset, \quad \mathsf{next}(X) =_{\text{Def}} X \text{ with } X, \quad \text{and} \quad \mathsf{hasNext}(X,Y) \leftrightarrow_{\text{Def}} Y = \mathsf{next}(X),$$

let us recursively define for all X:

$$f(X) =_{\text{Def}} \{0\} \cup \{\, \mathsf{next}(v) : u \in X,\ v \in f(u) \,\}.$$

It is obvious that $\mathsf{SngVal}(\mathsf{hasNext})$ holds, where *single-valuedness* is defined as follows:

$$\mathsf{SngVal}(R) \leftrightarrow_{\text{Def}} [\forall x,u,v \,|\, R(x,u)\ \&\ R(x,v) \longrightarrow u = v].$$

Moreover, we have the following:

Lemma 1 $\mathsf{Frames}(f(\mathbf{s}_\infty), \mathsf{hasNext}, \{0\})$.

Proof. Obviously $0 \in f(\mathbf{s}_\infty)$ and $\mathbf{arb}\,(\mathbf{s}_\infty) \in \mathbf{s}_\infty\ \&\ 0 \in f(\mathbf{arb}\,(\mathbf{s}_\infty))$ hold, and therefore $\mathsf{next}(0) \in f(\mathbf{s}_\infty)$. It can also be proved that $Y \in f(\mathbf{s}_\infty) \longrightarrow \mathsf{next}(Y) \in f(\mathbf{s}_\infty)$: If $Y = 0$ this has just been seen; When $0 \neq Y \in f(\mathbf{s}_\infty)$, pick u, v such that $u \in \mathbf{s}_\infty\ \&\ v \in f(u)\ \&\ Y = \mathsf{next}(v)$, hence $Y \in f(\{u\})$, where $\{u\} \in \mathbf{s}_\infty$, so that $\mathsf{next}(Y) \in f(\mathbf{s}_\infty)$. We readily get $\mathsf{Maps}(\mathsf{hasNext}, f(\mathbf{s}_\infty), f(\mathbf{s}_\infty) \setminus \{0\})$ from the above argument. Then we get $\mathsf{next}(X) = \mathsf{next}(Y) \longrightarrow X = Y$ since, if by absurd hypothesis $X \neq Y$ held along with $X \cup \{X\} = Y \cup \{Y\}$, then $X \in Y\ \&\ Y \in X$ would hold, and hence the set $\{X,Y\}$ would violate the regularity axiom. Hence $\mathsf{Disj}(\mathsf{hasNext}, f(\mathbf{s}_\infty))$ holds, and the thesis follows. ∎

How to frame the family of hereditarily finite sets The construction of a set H satisfying both $\emptyset \in H$ and the implication

$$X \in H \longrightarrow \mathcal{P}(X) \subseteq H$$

for all X, parallels very closely the construction just seen, the main change being that we define

$$f(X) =_{\text{Def}} \{\emptyset\} \cup \{\, v \cup \mathcal{P}(v) : u \in X,\ v \in f(u) \,\},$$

and replace hasNext by the single-valued map $\mathsf{hasPow}(X, Y) \leftrightarrow_{\text{Def}} Y = X \cup \mathcal{P}(X)$.

The only detail where the proof of $\mathsf{Frames}(f(\mathsf{s}_\infty), \mathsf{hasPow}, \{\emptyset\})$ differs from the proof of Lemma 1 is the way we get $X \cup \mathcal{P}(X) = Y \cup \mathcal{P}(Y) \longrightarrow X = Y$: If by absurd hypothesis $X \cup \mathcal{P}(X) = Y \cup \mathcal{P}(Y)$ and $X \neq Y$ held together, then we would have $(X \subseteq Y \ \vee \ X \in Y) \,\&\, (Y \subseteq X \,\&\, Y \in X)$; but we must discard $X \subseteq Y \subseteq X$ (which would contradict $X \neq Y$), as well as $X \in Y \in X$ (which would conflict with the regularity axiom), as well as $X \subseteq Y \in X$ (which would imply $Y \in Y$, conflicting with regularity again), as well as $Y \subseteq X \in Y$.

How to frame the inductive sets of based tuples Constructing a set which frames the inductive set which we will elect as the domain of all flat tuples over a base set A will be easier if we begin with a THEORY, devoid of assumptions, on ordered pairs:[1]

THEORY orderedPair()
$\Longrightarrow$ (cons, car, cdr, nl, len)
$\mathsf{car}\big(\mathsf{cons}(X, Y)\big) = X$
$\mathsf{cdr}\big(\mathsf{cons}(X, Y)\big) = Y$
$\mathsf{cons}(X, Y) = \mathsf{cons}(U, V) \longrightarrow X = U \,\&\, Y = V$
$\mathsf{nl} \neq \mathsf{cons}(X, Y)$ -- *plausibly, nl is an alias of* $\emptyset$
$\mathsf{len}(\mathsf{nl}) = 0$
$\mathsf{len}(\mathsf{cons}(X, Y)) = \mathsf{next}(\mathsf{len}(Y))$
END orderedPair.

We make the invocation

APPLY $([-, -], \mathsf{hd}, \mathsf{tl}, [\,], \mathsf{lth})$ orderedPair()

in sight of exploiting the operations thus introduced to build the desired theory

THEORY tuples()
$\Longrightarrow$ (tups, len)
$[\,] \in \mathsf{tups}(A)$

[1] Inside the THEORY orderedPair, if we adopt the pair construction proposed in [8], then we can recursively define len as follows:

$$\mathsf{len}(T) =_{\text{Def}} \mathbf{arb}\left(\left\{\mathsf{next}(\mathsf{len}(r)) : x \in T,\ y \in x,\ r \in y \,|\, [\exists \ell \,|\, T = \langle \ell, r \rangle]\right\}\right) .$$

$V \in \mathsf{tups}(A) \longrightarrow A \times \{V\} \subseteq \mathsf{tups}(A) \setminus \{[\,]\}$
$[\,] \in T \;\&\; [\forall\, v \in T \mid A \times \{v\} \subseteq T] \longrightarrow \mathsf{tups}(A) \subseteq T$
$\mathsf{len}([\,]) = 0$
$\mathsf{len}([\,-\,,\, T\,]) = \mathsf{next}(\mathsf{len}(T))$
END tuples.

During the construction of this theory, before we can indicate how to build the inductive set $\mathsf{tups}(A)$ for each fixed A, we will need a set that frames $\mathsf{tups}(A)$. We concentrate on this problem for the time being, postponing to the end of Sec.1.2 the discussion on how to use the framing set to achieve what is desired.

We recursively define an auxiliary function tups in two parameters:

$$\mathsf{tups}(A, V) \;=_{\text{Def}}\; \{\,[\,]\,\} \cup \bigcup\{A \times \mathsf{tups}(A, w) : w \in V\}\,.$$

E.g., it should be intuitively clear that when V is a finite ordinal (intended *à la* von Neumann), $\mathsf{tups}(A, V)$ will consist of those tuples over the base set A whose length does not exceed V.

For any fixed A, we then put

$$\begin{aligned} \mathsf{Pads}(V, W) &\;\leftrightarrow_{\text{Def}}\; W \in A \times \{V\}, \\ \mathsf{tupp} &\;\leftrightarrow_{\text{Def}}\; \mathsf{tups}(A, \mathbf{s}_\infty), \end{aligned}$$

after which we can easily prove that

$$\begin{aligned} &[\,] \in \mathsf{tupp}, \\ &V \in \mathsf{tupp} \;\&\; \mathsf{Pads}(V, W) \longrightarrow W \in \mathsf{tupp}, \\ &\mathsf{Maps}(\mathsf{Pads}, \mathsf{tupp}, \mathsf{tupp} \setminus \{[\,]\}), \\ &U \neq V \;\&\; \mathsf{Pads}(U, W) \longrightarrow \neg\, \mathsf{Pads}(V, W), \end{aligned}$$

to wit,

$$\mathsf{Frames}(\mathsf{tupp},\ \mathsf{Pads},\ \{[\,]\})\,.$$

How to frame the inductive sets of terms Once we will own the theory tuples specified above, in order to frame the desired inductive set terms of all terms over a signature S, we can proceed as follows.

We will begin with an auxiliary function terms in two parameters:

$$\begin{aligned} \mathsf{terms}(S, X) =_{\text{Def}} \bigcup\{\langle \mathsf{car}(p), \mathit{args}\rangle :\ & p \in S, y \in X, \mathit{args} \in \mathsf{tups}(\mathsf{terms}(S, y)) \\ & \mid\ \mathsf{len}(\mathit{args}) = \mathsf{cdr}(p)\}\,, \end{aligned}$$

where tups and len result from an invocation

$$\textbf{APPLY}\ (\mathsf{tups}, \mathsf{len})\ \ \mathsf{tuples}()\,,$$

and where each p in S is interpreted as a "symbol" whose two components are the "lexeme" and the degree (often called "arity"), respectively.

For any fixed signature σ, after (locally) putting

$$\begin{aligned} \mathsf{termm} &=_{\text{Def}} \mathsf{terms}(\sigma, \mathbf{s}_\infty)\,, \\ \mathsf{Pads}(V, W) &=_{\text{Def}} [\exists p \in \sigma,\ a \in \mathsf{tups}(\mathsf{termm}) \setminus \{[\,]\} \mid W = \langle \mathsf{car}(p), a\rangle \;\&\; \mathsf{len}(a) = \mathsf{cdr}(p) \\ &\qquad\qquad \&\; \mathsf{car}(a) = V], \\ \mathsf{consts} &\;\leftrightarrow_{\text{Def}}\; \{\,\langle \mathsf{car}(p), [\,]\rangle : p \in \sigma \mid \mathsf{cdr}(p) = 0\,\}, \end{aligned}$$

one can prove that

$$\mathsf{Frames}(\mathsf{termm},\ \mathsf{Pads},\ \mathsf{consts})\ .$$

1.2 Theories related to inductive closure

[····· TO BE ELABORATED ·····]

Weak induction What confers an inductive set n its appeal is the following THEORY,

THEORY $\mathsf{weakInduction}(\mathsf{n}, \mathsf{r}, \mathsf{a}, \mathsf{p})$
$\mathsf{IndClosed}(\mathsf{n}, \mathsf{r}, \mathsf{a})$
$X \in \mathsf{a} \longrightarrow \mathsf{p}(X)$
$X \in \mathsf{n}\ \&\ \mathsf{p}(X)\ \&\ \mathsf{r}(X, Y) \longrightarrow \mathsf{p}(Y)$
$\Longrightarrow$
$\mathsf{a} = \emptyset \longrightarrow \mathsf{n} = \emptyset$
$\mathsf{Exhs}(\mathsf{r}, \mathsf{n} \setminus \mathsf{a}, \mathsf{n})$
-- *Hint: if any* $w \in \{v \in \mathsf{n} \setminus \mathsf{a} \mid [\forall x \in \mathsf{n} \mid \neg \mathsf{r}(x, v)]\}$ *existed, removing*
-- *it from* n *would lead to a set contradicting the minimality of* n
$X \in \mathsf{n} \longrightarrow \mathsf{p}(X)$
-- *Hint:* $\mathsf{a} \subseteq \{x \in \mathsf{n} \mid \mathsf{p}(x)\}\ \&\ \mathsf{Maps}(\mathsf{r}, \{x \in \mathsf{n} \mid \mathsf{p}(x)\}, \{x \in \mathsf{n} \mid \mathsf{p}(x)\})$
END weakInduction,

where the *surjectivity* notion

$$\mathsf{Exhs}(R, T, S) \ \leftrightarrow_{\mathrm{Def}}\ [\forall y \in T\ \exists x \in S \mid R(x, y)]$$

is involved.

Weak induction constitutes a familiar reasoning template which every reader knows from experience (if only with arithmetic induction) to be extremely versatile; moreover, this scheme can be generalized into *strong* induction, as we will see soon.

Getting an inductive set from a framing set The following THEORY circumscribes a given set a of seeds with an inductive set n, while also associating an inductive subtree with each element of n:

THEORY $\mathsf{indClosure}(\mathsf{s}, \mathsf{r}, \mathsf{a})$
$\mathsf{Frames}(\mathsf{s}, \mathsf{r}, \mathsf{a})$
$\Longrightarrow$ $(\mathsf{n}, \mathsf{indCl})$
-- *Hint:* $\mathsf{indCl}(B) =_{\mathrm{Def}} \bigcap\{t \subseteq \mathsf{s} \mid (B \subseteq s \longrightarrow B \subseteq t)\ \&\ \mathsf{Maps}(\mathsf{r}, t, t)\}$, *i.e.,*
-- $\mathsf{indCl}(B) =_{\mathrm{Def}} \{x \in \mathsf{s} \mid [\forall t \subseteq \mathsf{s} \mid (B \subseteq \mathsf{s} \longrightarrow B \subseteq t)\ \&\ \mathsf{Maps}(\mathsf{r}, t, t) \longrightarrow x \in t]\}$
$\mathsf{n} = \mathsf{indCl}(\mathsf{a})$
$\mathsf{a} \subseteq \mathsf{n}\ \&\ \mathsf{n} \subseteq \mathsf{s}$
$B \subseteq \mathsf{n}\ \&\ [\forall x \in \mathsf{indCl}(B)\ \forall y \mid \mathsf{r}(x, y) \longrightarrow y \notin B] \longrightarrow \mathsf{IndClosed}(\mathsf{indCl}(B), \mathsf{r}, B)$
$B \subseteq \mathsf{a} \longrightarrow \mathsf{IndClosed}(\mathsf{indCl}(B), \mathsf{r}, B)$
$\mathsf{IndClosed}(\mathsf{n}, \mathsf{r}, \mathsf{a})$

$\mathsf{Exhs}(\mathsf{r}, \mathsf{indCl}(B) \setminus B, \mathsf{indCl}(B))$
$B \subseteq \mathsf{n} \longrightarrow B \subseteq \mathsf{indCl}(B)$ & $\mathsf{indCl}(B) \subseteq \mathsf{n}$
$Y \in \mathsf{n}$ & $X \neq Y$ & $X \in \mathsf{indCl}(\{Y\}) \longrightarrow Y \notin \mathsf{indCl}(\{X\})$
$X \in \mathsf{n} \longrightarrow \mathsf{IndClosed}(\mathsf{indCl}(\{X\}), \mathsf{r}, \{X\})$
END indClosure.

A well-founded relation is naturally associated with any inductive set n endowed with subtrees:

THEORY subTree(n, r, a, tree)
IndClosed(n, r, a)
$X \in \mathsf{n} \longrightarrow \mathsf{IndClosed}(\mathsf{tree}(X), \mathsf{r}, \{X\})$
$\Longrightarrow$
$X \in \mathsf{n} \longrightarrow \mathsf{tree}(X) \subseteq \mathsf{n}$
--*Hint:* **APPLY** (t, indCl) indClosure(n, r, a) *provides* $\mathsf{indCl}(\{X\})$
-- *s.t.* $\mathsf{Maps}(\mathsf{r}, \mathsf{indCl}(\{X\}), \mathsf{indCl}(\{X\}))$ & $\mathsf{indCl}(\{X\}) \subseteq \mathsf{t} \subseteq \mathsf{n}$
$X \in \mathsf{n} \longrightarrow \neg\, \mathsf{r}(X, X)$
-- *Hint: if* $X \in \mathsf{n}$ & $\mathsf{r}(X, X)$, *then removal of* X *from* n *would lead*
-- *to a set contradicting the minimality of* n
$T \neq \emptyset$ & $T \subseteq \mathsf{n} \longrightarrow [\exists m \in T\ \forall u \in T \mid m \notin \mathsf{tree}(u) \setminus \{u\}]$
-- *N.B.: this paves the way to recursive constructions over* n
$X \in \mathsf{n}$ & $\mathsf{r}(X, Y) \longrightarrow \mathsf{tree}(Y) \subsetneq \mathsf{tree}(X)$
$X \in \mathsf{n}$ & $Y \in \mathsf{tree}(X)$ & $X \in \mathsf{tree}(Y) \longrightarrow X = Y$
$\mathsf{a} \neq \emptyset$ & $[\forall x \in \mathsf{n}\ \exists y \mid R(x, y)]) \longrightarrow \mathsf{Infinite}(n)$
-- *here the following notion of* Infinite *is being referred to:*
-- $\mathsf{Infinite}(I) =_{Def} \big[\exists c \mid [\exists k \in c \mid k \subseteq I]$ & $[\forall k \in c\ \exists h \in c \mid h \subsetneq k]\big]$,
-- *and a clue on how to get a witness* c *of the infiniteness of* n *is:*
-- *pick* $c =_{Def} \{\mathsf{tree}(X) : X \in n\}$
END subTree.

[····· TO BE ELABORATED ·····]

Strong induction

THEORY strongInduction(n, r, a, tree, p)
IndClosed(n, r, a)
$X \in n \longrightarrow \mathsf{IndClosed}(\mathsf{tree}(X), \mathsf{r}, \{X\})$
$Y \in n$ & $[\forall x \in n \mid Y \in \mathsf{tree}(x) \setminus \{x\} \longrightarrow \mathsf{p}(x)] \longrightarrow \mathsf{p}(Y)$
$\Longrightarrow$
$X \in n \longrightarrow p(X)$
-- *Hint: Assuming the contrary, we could fix (exploiting* subTree*)*
-- *an* m *in* n *s.t.* $\neg\, \mathsf{p}(m)$ & $[\forall u \in n \mid m \in \mathsf{tree}(u) \setminus \{u\} \longrightarrow \mathsf{p}(u)]$
END strongInduction.

Uniqueness of natural numbers Let us now momentarily restrict our study to the special case when the seeds (whose set is passed as third parameter to the

THEORYes weakInduction, indClosure, and subTree seen above) form a singleton set $\mathsf{a} = \{\mathsf{e}\}$, and moreover the generating map (which is passed as second parameter to the said THEORYes) is single-valued.

To ease the subsequent discussion, we introduce notions which combine single-valuedness with the notions Maps, Exhs, and Disj (*into-ness*, *surjectivity*, and *injectivity*) introduced earlier. Along with them, we introduce the new notion of *bijectivity*, which like the others refers to a global function G instead of to a more generic global dyadic relation. Moreover, we supply a restricted notion of inductively closed set:

$$\begin{aligned}
\mathsf{Sends}(G,S,T) &\leftrightarrow_{\mathrm{Def}} [\forall x \in S \mid G(x) \in T],\\
\mathsf{Surj}(G,T,S) &\leftrightarrow_{\mathrm{Def}} [\forall y \in T \mid \exists x \in S)\big(G(x) = y\big],\\
\mathsf{Inj}(G,S,T) &\leftrightarrow_{\mathrm{Def}} [\forall u \in S, v \in S, y \in T \mid G(u) = y \,\&\, G(v) = y \rightarrow u = v],\\
\mathsf{Bij}(G,S,T) &\leftrightarrow_{\mathrm{Def}} \mathsf{Surj}(G,T,S) \,\&\, \mathsf{Inj}(G,S,T),\\
\mathsf{SuccClosed}(N,G,A) &\leftrightarrow_{\mathrm{Def}} A \subseteq N \,\&\, \mathsf{Sends}(G,N,N \setminus A) \,\&\, \mathsf{Inj}(G,N,N)\\
&\qquad\qquad \&\, [\forall t \mid A \subseteq t \,\&\, \mathsf{Sends}(G,t,t) \rightarrow N \subseteq t]\,.
\end{aligned}$$

As one should expect, the following THEORY, where segments take the place of trees, easily ensues from subTree:

THEORY subSegm(n, succ, e, segm)
  $\mathsf{n} = \mathsf{segm}(\mathsf{e})$
  SngVal(succ)
  $\mathsf{e} \in \mathsf{n}$
  $X \in \mathsf{n} \rightarrow \mathsf{IndClosed}(\mathsf{segm}(X), \mathsf{succ}, \{X\})$
$\Longrightarrow$
  $X \in \mathsf{n} \,\&\, \mathsf{succ}(X,Y) \rightarrow \mathsf{segm}(Y) = \mathsf{segm}(X) \setminus \{X\}$
  -- *i.e.*, $U \in \mathsf{n} \,\&\, \mathsf{succ}(U,V) \,\&\, W \in \mathsf{segm}(U) \setminus \{U\} \rightarrow W \in \mathsf{segm}(V)$
  $T \neq \emptyset \,\&\, T \subseteq \mathsf{n} \rightarrow [\exists m \in T\, \forall u \in T \mid u \in \mathsf{segm}(m)]$
  $X, Y \in \mathsf{n} \rightarrow X \in \mathsf{segm}(Y) \;\vee\; Y \in \mathsf{segm}(X)$
  $U, V, W \in \mathsf{n} \,\&\, V \in \mathsf{segm}(U) \,\&\, W \in \mathsf{segm}(V) \rightarrow W \in \mathsf{segm}(U)$
  $[\forall\, x \in \mathsf{n}\, \exists\, y \mid R(x,y)]) \rightarrow \mathsf{Infinite}(\mathsf{n})$
END subSegm.

It should be clear that such n, e, and g are meant to represent the natural numbers, their first element, and their successor function, respectively. The fact that this representation is essentially unique should emerge from a theory with the following traits:

THEORY uniqNat(n, g, e, nn, gg, ee)
  SuccClosed(n, g, { e })
  SuccClosed(nn, gg, { ee })
$\Longrightarrow$ (p, q)
  $\mathsf{p}(\mathsf{e}) = \mathsf{ee}$
  $\mathsf{q}(\mathsf{ee}) = \mathsf{e}$
  $X \in \mathsf{n} \rightarrow \mathsf{p}\big(\mathsf{f}(X)\big) = \mathsf{ff}\big(\mathsf{p}(X)\big)$
  $Y \in \mathsf{nn} \rightarrow \mathsf{q}\big(\mathsf{ff}(Y)\big) = \mathsf{f}\big(\mathsf{q}(Y)\big)$

$\mathsf{Bij}(\mathsf{p}, \mathsf{n}, \mathsf{nn})$
$\mathsf{Bij}(\mathsf{q}, \mathsf{nn}, \mathsf{n})$
$X \in \mathsf{n} \longrightarrow q\big(\mathsf{p}(X)\big) = X$
$Y \in \mathsf{nn} \longrightarrow p\big(\mathsf{q}(Y)\big) = Y$
END uniqNat.

[····· TO BE ELABORATED ·····]

Free closure relative to given constructors Inductive sets can also be generated by a set ff of constructors:

THEORY freeClosure(s, ff, a)
$\mathsf{a} \subseteq \mathsf{s}$
$F \in \mathsf{ff} \longrightarrow \mathsf{Maps}(F, \mathsf{s}, \mathsf{s} \setminus \mathsf{a})$
$F \in \mathsf{ff} \longrightarrow \mathsf{Disj}(F, \mathsf{s})$
$F, G \in \mathsf{ff}\ \&\ F \neq G\ \&\ F(U, Y) \longrightarrow \neg\, G(V, Y)$
-- *Accordingly,* $\mathsf{Maps}(\bigcup \mathsf{ff}, \mathsf{s}, \mathsf{s} \setminus \mathsf{a})\ \&\ \mathsf{Disj}(\bigcup \mathsf{ff}, \mathsf{s})$
$\Longrightarrow$ (n, tree)
$\mathsf{IndClosed}(\mathsf{n}, \bigcup \mathsf{ff}, \mathsf{a})$
$X \in \mathsf{n} \longrightarrow \mathsf{IndClosed}(\mathsf{tree}(X), \bigcup \mathsf{ff}, \{X\})$
END freeClosure.

However, the constructors have, in many applications, a degree (or *"arity"*) which should be taken into account. We do not discuss here how to deal with this complication.

[····· TO BE ELABORATED ·····]

2 A decision procedure for ordered Abelian groups

Ordered Abelian groups G are characterized by the presence of an associative-commutative addition operator '+', with identity '0' and inverse '−', and also a comparison operator $x > y$ satisfying

$$[\forall x \in G, y \in G \,|\, \neg x > x\ \&\ (x > y \vee x = y \vee x < y)]\,,$$
$$[\forall x \in G, y \in G, z \in G \,|\, (x > y\ \&\ y > z) \longrightarrow x > z]\,,$$
$$[\forall x \in G, y \in G, z \in G \,|\, x > y \longrightarrow z - y > z - x]\,.$$

The last axiom plainly implies that

$$[\forall x \in G, y \in G, z \in G \,|\, x > y \longrightarrow x + z > y + z]\,.$$

A standard theorem prover, e.g. Otter [7], can be successfully exploited to prove many theorems about such groups (cf. Figure 1, where a variant axiomatic system is adopted); moreover, the decision problem for the fully quantified theory of Abelian ordered groups (OAG, for short) was solved by Yu. Gurevich in [3]. Normally the user of our proof-checking environment is in charge of providing proofs within THEORYes; however, in a favorable case such as the one at hand,

```
formula_list(usable)      -- axioms and definitional extensions
    -- Abelian group axioms
    [∀x, ∀y, ∀z | (x⊕y)⊕z=x⊕(y⊕z)]          -- associativity
    [∀x | x⊕e=x]                             -- right unit
    [∀x | x⊕⊖x=e]                            -- right inverse
    [∀x, ∀y | x⊕y=y⊕x]                       -- commutativity
    -- ordering axioms (axioms concerning non-negativeness)
    [∀x, ∀y | nneg(x) & nneg(y) → nneg(x⊕y)]
    [∀x | nneg(x) ∨ nneg(⊖x)]
    [∀x | nneg(x) & nneg(⊖x) → x=e]
    -- definitional extensions (below we will also use A⊖B as a short for A⊕⊖B)
    [∀x | nneg(x) → |x|=x]                   -- definition of the absolute value ...
    [∀x | ¬nneg(x) → |x|=⊖x]                 -- ... def'n of the absolute value
    [∀x, ∀y | x≼y ↔ nneg(y⊖x)]               -- definition of comparison
end_of_list
formula_list(usable)      -- provable laws
    [∀x, ∀y, ∀z | x⊕y=x⊕z → y=z]             -- A1: cancellation law
    [∀x, ∀y | ⊖(x⊖y)=y⊖x]                    -- B (from A1, Ba, Bb alone)
    [∀x, ∀y | x≼y ∨ y≼x]                     -- C: totality
    [∀x | x≼x]                               -- D: reflexivity
    [∀x, ∀y, ∀z | x≼y & y≼z → x≼z]           -- E: transitivity
    [∀x, ∀y, ∀z | x≼y & x≠y & y≼z → x≠z]     -- E1: transitivity
    [∀x, ∀y, ∀z | x≼y & y≼z & y≠z → x≠z]     -- E2: transitivity
    [∀x, ∀y, ∀z | x≼y → x⊕z≼y⊕z]            -- F: additivity
    [∀x, ∀y, ∀z | x⊕z=y⊕z → x=y]            -- A2: cancellation law
    [∀x, ∀y, ∀z | x≼y & x≠y → x⊕z≠y⊕z]      -- F1, strict additivity
    [∀x | |x⊖x|=e]                           -- 1
    [∀x | x≼|x|]                             -- 2
    [∀x | |(|x|)|=|x|]                       -- 3
    [∀x | |x|=e ↔ x=e]                       -- 4
    [∀x | |⊖x|=|x|]                          -- 5
    [∀x, ∀y | x⊕y≼|x|⊕|y|]                   -- 6
    [∀x, ∀y | |x⊕y|≼|x|⊕|y|]                 -- 7
    [∀x, ∀y, ∀z | |x⊖z|≼|x⊖y|⊕|y⊖z|]         -- 8
    [∀x, ∀y | ¬nneg(x) → x≼|y| & x≠|y|]      -- 9
    [∀x, ∀y | nneg(y) → x⊖y≼x⊕y]             -- 10
    [∀x, ∀y | ||x|⊖|y||≼|x⊖y|]               -- 11
    [∀x, ∀y | |x|⊖||y|⊖|x||≼|y|]             -- 12
end_of_list
```

Fig. 1. Basic lemmas on ordered Abelian groups proved with Otter's assistance

if we supply the decision method for OAG, then the user can view it as a THEORY which is able to find autonomously the proof of any asserted theorem, and to reject a wrong statement. Incidentally, note that this theory has plenty of applications: the standard additive groups based on $\mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ (see Sec.3), to mention a few, satisfy the axioms of OAG.

Here we provide a simple decision procedure for finite collections of *unquantified* statements in the theory OAG, whose correctness is based on very basic facts of Abelian group theory and the theory of reals.

For standard notation and classical results in group theory we shall refer to [5].

Our decision procedure will be based upon the following considerations. Let C be a conjunction of unquantified statements of OAG.

Fact 1 *If such a conjunction C is satisfiable, i.e. has a model which is an ordered Abelian group G', it can plainly be modeled by the subgroup G of G' generated by the elements of G' which correspond to the symbols which appear in the statements of C. Hence it has a model which is an ordered Abelian group with* finitely many *generators. Conversely, if there exists such a model, then C is satisfiable.*

Therefore we can base our analysis on an understanding of the structure of finitely generated ordered Abelian groups G.

The additive group of reals contains many such ordered subgroups with finitely many generators, as does the additive group of real vectors of dimension d for any d, if we order these vectors lexicographically. We will see in what follows that these examples are generic, in the sense that any finitely generated ordered Abelian group with m generators can be embedded into the additive group of real vectors of dimension (at most) m by an order-preserving isomorphism (we will call such isomorphisms 'order-isomorphisms').

Fact 2 *For any given Abelian group G, the following two conditions are equivalent:*

- *G is finitely generated;*
- *G is a direct sum of a finite number of cyclic groups.*

Fact 3 *Infinite cyclic groups are isomorphic to the group $\mathbb{Z}$ of integers.*

Facts 2 and 3 state well-known results, which can be found in any book on group theory (for instance, see [5]).

Since the order axiom plainly rules out any finite cyclic summands, we can conclude that

Fact 4 *Our conjunction C is satisfiable if and only if it is satisfied in an ordered Abelian group which can be decomposed as direct sum of finitely many copies of $\mathbb{Z}$.*

Groups which can be decomposed as direct sums of infinite cyclic groups are called *free groups*.

Fact 5 *Up to an isomorphism, a finitely generated free group G is uniquely determined by the number m of its direct summands, which is called the* rank of G.

To show, as anticipated, that any finitely generated ordered free group of rank m can be embedded into the additive group of real vectors of dimension m ordered lexicographically, it is convenient to study the possible orderings that such groups can have.

Definition 1 *Let G be an Abelian ordered group. An element $x \in G$ is said to be* infinitesimal *if there exists a $y \in G$ such that $mx \leq y$ holds for all signed integers m.*

An ordered Abelian group with no infinitesimals is said to be Archimedean.

We will establish by elementary means the following two facts, which taken together will give the decision result of our interest.

Fact 6 *Every Archimedean ordered Abelian group is order-isomorphic to a subgroup of $\mathbb{R}$.*

Fact 7 *Every (non-Archimedean) finitely generated ordered Abelian group $(G, <)$ of rank m is order-isomorphic to a lexicographically ordered direct sum of the type*

$$((G_0, <_0) \oplus (G_1, <_1), \oplus \cdots \oplus (G_k, <_k), <_{lex}),$$

where $k \leqslant m$ and where $(G_i, <_i)$ is an Archimedean Abelian ordered group, for $1 \leqslant i \leqslant k$.

Remark 1 Notice that proofs of the above two facts can be found in [4]. For the reader's convenience, we will give below self-contained elementary proofs.

The above considerations lead us immediately to the following result.

Lemma 2 *Let C be a conjunction of unquantified statements of the theory* OAG*, involving n distinct variables. Then C is satisfiable in the theory* OAG *if and only if C is satisfiable in the additive group of real vectors of dimension n, endowed with the lexicographic order.*

Proof. Plainly, if C is satisfiable in the additive group of real vectors of dimension n endowed with the lexicographic order, then C is satisfiable in the theory OAG.

Conversely, assume that C is satisfiable in the theory OAG and let G be an ordered Abelian group in which C is satisfiable. From Fact 1, we can assume that G is also finitely generated. Therefore, from Facts 6 and 7, it follows that G can be embedded in the additive group of real vectors of dimension n, ordered lexicographically, thus concluding the proof of the theorem. ■

It is easy to reduce the satisfiability problem for the lexicographically ordered additive group of real vectors of dimension n to the satisfiability problem for the additive group of reals. Indeed, a real vector of dimension n is just a collection

of n real numbers $x_1, ..., x_n$, addition of two such vectors is just addition of their individual components, and the condition $x < y$ for two vectors x and y can be written as the disjunction

$$(x_1 < y_1) \vee (x_1 = y_1 \ \& \ x_2 < y_2) \vee \ldots \vee (x_1 = y_1 \ \& \ \ldots \ \& \ x_{n-1} = y_{n-1} \ \& \ x_n < y_n).$$

This observation shows that the satisfiability problem for any collection of unquantified statements in the theory of ordered Abelian groups reduces without difficulty to the problem of satisfying a corresponding collection of real linear equations and inequalities. This is the standard problem of linear programming, which can be tested for solvability using any convenient linear programming algorithm (cf. [6]).

Therefore we have:

Corollary 1 *The collection of unquantified statements of the theory* OAG *has a decidable satisfiability problem.* ■

2.1 Proof of Fact 6

Let G be an Archimedean ordered Abelian group. We show that G is order-isomorphic to a subgroup of $\mathbb{R}$.

If there is just one generator, then G is plainly isomorphic to the ordered group of integers.

Let us fix $y > 0$. Then for each x we consider the following set

$$S(x) =_{def} \{m/n : m, n \in \mathbb{N} \mid n > 0 \ \& \ nx > my\}.$$

Notice that the set $S(x)$ is defined independently of the way that m/n is represented by a fraction, since the order axioms imply that if $nx > my$ then $knx > kmy$ for each positive k, and conversely if $knx > kmy$ then $nx \leqslant my$ is impossible.

We show next that $S(x)$ is a Dedekind cut in the set of rationals, for each $x \in G$. Let $x \in G$, then there is a positive integer n such that $n \notin S(x)$ and $-n \in S(x)$, so $S(x)$ is neither empty or all the rationals. In addition $S(x)$ is bounded above, because if $m/n \notin S(x)$ (i.e., $my \geqslant nx$) and $m'/n' > m/n$ (i.e., $nm' > mn'$), then $m'/n' \notin S(x)$ (i.e., $m'y \geqslant n'x$). Moreover, if $m/n \in S(x)$ then there are m', n' such that $m'/n' \in S(x)$ and $m'/n' > m/n$. Summing up, $S(x)$ is a cut in the set of rationals, so that the following definition is well-given

$$r(x) =_{def} \sup S(x)\,.$$

We claim that the mapping r maps G to the reals in an order-preserving manner. First we show that r is an isomorphism from G into the reals. Let $m/n < r(x)$ and $m'/n' < r(x')$, both denominators n and n' being positive. Then $nx > my$ and $n'x > m'y$, so $nn'x > mn'y$ and $nn'x > m'ny$, and therefore

$$nn'(x + x') > (mn' + m'n)y$$

from which it follows that $m/n + m'/n'$ belongs to $S(x + x')$. This proves that $r(x+x') \geqslant r(x)+r(x')$. Now suppose that $r(x+x') > r(x)+r(x')$, and let m/n and m'/n' respectively be rationals which approximate $r(x)$ (resp. $r(x')$) well enough from above so that we have $m/n+m'/n' \in S(x+x')$, while $m/n > r(x)$ and $m'/n' > r(x')$. This implies that $nx \leq my$, $n'x \leq m'y$, and $nn'(x + x') > (mn' + m'n)y$. This is impossible since our first two inequalities imply that $nn'(x+x') \leq (mn'+m'n)y$. It follows that $r(x+x') > r(x)+r(x')$ is impossible, so $r(x+x') = r(x)+r(x')$, i.e. r is a homomorphism of G into the ordered group of reals. Finally, suppose that $r(x) = 0$. Then we cannot have $x > 0$, since if we did then $nx > y$ would be true for some positive n, so $1/n$ would be a member of $S(x)$, implying that $r(x) \geqslant 1/n$, which is impossible. Similarly if $x < 0$ it would follow that $r(-x) \geq 1/n$ for some positive n, also impossible. Since r has been seen to be additive $r(-x) = -r(x)$, and it follows that x must be 0, proving that r is an isomorphism of G into the reals.

Next we show that the mapping r is also order-preserving. Indeed, if $x' > x$, and the rational number m/n (with positive denominator) belongs to $S(x)$, then $nx > my$, and so $nx' > my$ also, proving that m/n belongs to $S(x')$. That is, $x' > x$ implies that $S(x') \supseteq S(x)$, and thus plainly implies that $r(x') \geqslant r(x)$. On the other hand, if $r(x') = r(x)$, we would have $r(x' - x) = 0$, which implies $x' - x = 0$, i.e., $x' = x$, a contradiction. Thus, we must have $r(x') > r(x)$, completing our treatment of the case in which G is Archimedean.

2.2 Proof of Fact 7

Given an ordered Abelian group $(G, <)$, for any subset A of G we use the following notation:

$$A^+ =_{def} \{x \in A \mid x > 0\}.$$

Definition 2 *Let H be a subgroup of an ordered Abelian group G. We say that H is* isolated in *G if for every $x \in H$ and $y \in (G \setminus H)^+$ we have $x < y$.*

Definition 3 When $\{(G_i, <_i)\}_{i \in I}$ is a finite collection of ordered Abelian groups, we denote by $(\oplus_{i \in I}(G_i, <_i), <_{lex})$ the direct sum of the above groups equipped with lexicographic order inherited from the defined orders $\{(<_i)\}_{i \in I}$.

It is straightforward to verificate that the described object is an ordered Abelian group.

Definition 4 Given two ordered Abelian groups $(G_1, <_1)$ and $(G_2, <_2)$, we write $(G_1, <_1) \cong_G (G_2, <_2)$ to mean that $(G_1, <_1)$ and $(G_2, <_2)$ have isomorphic group structure. Likewise, we write $(G_1, <_1) \cong_{\leq} (G_2, <_2)$ to mean that $(G_1, <_1)$ and $(G_2, <_2)$ have isomorphic orderings. Finally, we write $(G_1, <_1) \cong (G_2, <_2)$ to mean that that there exists a group isomorphism from $(G_1, <_1)$ onto $(G_2, <_2)$ which is also an ordering isomorphism. In this case we say briefly that $(G_1, <_1)$ and $(G_2, <_2)$ are *order-isomorphic*.

From now on, all the groups are intended to be ordered free Abelian groups.

Proposition 1 *Let $(G,<)$ be a finitely generated ordered Abelian group and let I_G be the collection of all infinitesimals of $(G,<)$. Then*

(i) $(I_G,<)$ is an ordered Abelian subgroup of G;
(ii) if in addition $(G,<)$ is a non-trivial finitely generated group, then $G \neq I_G$.

Proof. (i) It is sufficient to show that I_G is closed under the group operation $+$. Let $x_1, x_2 \in I_G$ and let $y_1, y_2 \in G$ be such that $nx_i < y_i$, for every signed integer n. Then, for every signed integer n we have:

$$n(x_1 + x_2) = nx_1 + nx_2 < y_1 + y_2 \leqslant 2\max(y_1, y_2)\,,$$

so that $x_1 + x_2 \in I_G$.

(ii) Let $g_1, \ldots, g_k$ be a system of generators for G. We show that at least one among the generators must be non-infinitesimal. If by contradiction each g_i is infinitesimal, then for each $i = 1, \ldots, k$ there exist an element y_i such that $ng_i < y_i$, for every signed integer n. Consider the element $y_1 + \ldots + y_k$. This can be written as $\overline{n}_1 g_1 + \ldots + \overline{n}_k g_k$, for suitable signed integers $\overline{n}_1, \ldots, \overline{n}_k$. But since, $\overline{n} g_i < y_i$, for $i = 1, \ldots, k$, we also have $\overline{n}_1 g_1 + \ldots + \overline{n}_k g_k < y_1 + \ldots + y_k$, which is a contradiction. ■

Proposition 2 *Let $(B,<)$ be an ordered subgroup of $(G,<)$. Define the following relation $<_{G/B}$ over $G/B \times G/B$:*

$$\alpha <_{G/B} \beta \qquad \textit{iff} \qquad x < y, \textit{ for some } x \in \alpha \ \ \& \ \ y \in \beta\,,$$

for $\alpha, \beta \in G/B$, with $\alpha \neq \beta$.

If $(B,<)$ is isolated in $(G,<)$, then $(G/B, <_{G/B})$ is an ordered Abelian group.

Proof. We only check that the relation $<_{G/B}$ is well-defined. So, let $\alpha, \beta \in G/B$, with $\alpha \neq \beta$ and assume by contradiction that there exist $x_1, x_2 \in \alpha$ and $y \in \beta$, such that

$$x_2 < x_1\,, \qquad y < x_1\,, \qquad \text{and} \ \ x_2 < y.$$

Then $x_1 - x_2 \in B^+$. Moreover, by the ordering axioms we get $x_1 - x_2 > x_1 - y > 0$. This contradicts the isolation hypothesis on B, since $x_1 - y \notin B$. ■

Remark 2 *It can easily be checked that*

(i) the subgroup I_G of the infinitesimals of an ordered Abelian group G is isolated in G;
(ii) the group $(G/I_G, <_{G/I_G})$ has no infinitesimals.

Proposition 3 *Let $(B,<)$ be a ordered subgroup of a finitely generated ordered Abelian group $(G,<)$. If $(B,<)$ is isolated in $(G,<)$, then*

$$(G,<) \cong ((G/B, <_{G/B}) \oplus (B,<), <_{lex}).$$

Proof. Let $\alpha_1 \dots \alpha_s$ be a system of generators for G/B. Let us pick $a_i \in \alpha_i$, for $i = 1, \dots, s$. Also, let $a_{s+1} \dots a_t$ be a system of generators for B. Let x be an element of G and let $[x]$ be the class of G/B which contains x. Then $[x] = \sum_{i=1}^{s} k_i \alpha_i$, for suitable $k_i \in \mathbb{N}$, with $i = 1, \dots, s$, so that $x - \sum_{i=1}^{s} k_i a_i = \sum_{i=s+1}^{t} k_i a_i$, for suitable $k_i \in \mathbb{N}$, with $i = s+1, \dots, t$. Hence $a_1, \dots, a_t$ is a system of generators for G.

It can easily be shown that the map from G to $G/B \oplus B$ induced by the following correspondence of generators

$$\begin{aligned} a_1 &\to \alpha_1 \\ &\dots \\ a_s &\to \alpha_s \\ a_{s+1} &\to a_{s+1} \\ &\dots \\ a_t &\to a_t \end{aligned}$$

is a group-isomorphism from G onto $G/B \oplus B$.

Hence, we only need to show that such a map also preserves ordering. Let $x, y \in G$ be such that $x < y$. Let $x = \sum_{i=1}^{t} k_i a_i$ and $y = \sum_{i=1}^{t} m_i a_i$. Then

$$\left(\sum_{i=1}^{s} k_i \alpha_i, \sum_{i=s+1}^{t} k_i a_i \right) <_{lex} \left(\sum_{i=1}^{s} m_i \alpha_i, \sum_{i=s+1}^{t} m_i a_i \right). \tag{1}$$

Indeed, by Proposition 2 we cannot have $[x] >_{G/B} [y]$. If $[x] <_{G/B} [y]$, we have (1) immediately. On the other hand, if $[x] = [y]$, then $k_i = m_i$ for all $i \in \{1 \dots s\}$ and since $x < y$ implies that $\sum_{i=s+1}^{t} (m_i - k_i) a_i > 0$, we have again (1). ∎

Theorem 1 *Let $(G, <)$ be a finitely generated ordered Abelian group. Then*

$$(G, <) \cong ((G_0, <_0) \oplus (G_1, <_1) \oplus \dots \oplus (G_k, <_k), <_{lex}),$$

where each $(G_i, <_i)$ is a finitely generated Archimedean ordered Abelian group, for $i = 0, 1, \dots, k$.

Proof. We proceed by induction on the rank of G. Let I_G be the subgroup of the infinitesimals of G (cf. Proposition 1 (i)). If I_G is the null subgroup, then we are done, since G itself is Archimedean. On the other hand, if I_G is non-trivial, then by Proposition 3 we have

$$(G, <) \cong ((G/I_G, <_{G/I_G}) \oplus (I_G, <), <_{lex}),$$

since, as observed in Remark 2, I_G is isolated in G. Notice also that $(G/I_G, <_{G/I_G})$ is a finitely generated Archimedean ordered Abelian group. Let φ_1 be an order-isomorphism from $(G, <)$ onto $((G/I_G, <_{G/I_G}) \oplus (I_G, <), <_{lex})$.

From Proposition 1 (ii), $I_G \subset G$, so that the quotient group $(G/I_G, <_{G/I_G})$ is non-trivial. Therefore the rank of I_G is strictly less than the rank of G. By induction we have

$$(I_G, <) \cong ((G_1, <_1) \oplus \dots \oplus (G_k, <_k)),$$

where $(G_i, <_i)$ is a finitely generated Archimedean ordered Abelian group, for $i = 1, \ldots, k$. Let φ_2 be an order-isomorphism from $(I_G, <)$ onto $((G_1, <_1) \oplus \ldots \oplus (G_k, <_k)$.

Let us put

$$(G_0, <_0) =_{def} (G/I_G, <_{G/I_G}) .$$

Then we claim that

$$(G, <) \cong ((G_0, <_0) \oplus (G_1, <_1) \oplus \cdots \oplus (G_k, <_k), <_{lex}) ,$$

Let us define the map

$$\varphi : G \to G_0 \oplus G_1 \oplus \cdots \oplus G_k$$

by putting

- $\varphi(a) = (a_0, a_1, \ldots, a_k)$, where $\varphi_1(a) = (a_0, a^*)$, for some $a^* \in I_G$, and
- $\varphi_2(a^*) = (a_1, \ldots, a_k)$.

Plainly, φ is a group-isomorphism from G onto $G_0 \oplus G_1 \oplus \cdots \oplus G_k$. Hence, we only need to prove that φ is preserves also ordering.

To this end, let $a, b \in G$ be two distinct elements such that $a < b$. Let

$$\begin{aligned} (a_0, a^*) &=_{def} \varphi_1(a) \\ (b_0, b^*) &=_{def} \varphi_1(b) \\ (a_1, \ldots, a_k) &=_{def} \varphi_2(a^*) \\ (b_1, \ldots, b_k) &=_{def} \varphi_2(b^*) . \end{aligned}$$

Plainly $a_0 \leqslant_{G/I_G} b_0$. If $a_0 <_{G/I_G} b_0$, we are done. On the other hand, if $a_0 = b_0$, then we must have $a^* < b^*$. Therefore, we have $(a_1, \ldots, a_k) <_{lex} (b_1, \ldots, b_k)$, which it plainly implies $(a_0, a_1, \ldots, a_k) <_{lex} (b_0, b_1, \ldots, b_k)$, namely $\varphi(a) <_{lex} \varphi(b)$, since we are under the assumption that $a_0 = b_0$. ■

3 Defining real numbers using Bishop's 'regular' Cauchy sequences

With Cantor's approach, real numbers are defined as follows. Call an infinite sequence x_n of rational numbers a *Cauchy sequence* if, for every positive rational r, there exists an integer N such that the absolute value $|x_n - x_m|_{\mathbb{Q}}$ is less than r whenever m and n are both larger than N. Sequences of this kind can be added, subtracted, and multiplied componentwise and their sums, differences, and products are still Cauchy sequences. We can now introduce an equivalence relationship Same_real between pairs x, y of such sequences: Same_real(x, y) is true if and only if, for every positive rational r, there exists an integer N such that the absolute value $|x_n - y_n|_{\mathbb{Q}}$ is less than r whenever n is larger than N. The set of equivalence classes of Cauchy sequences, formed using the equivalence relationship Same_real, is then the set of real numbers. If two pairs of Cauchy

sequences x, y and w, z are equivalent, then the (componentwise) sum of x and w is equivalent to the sum of y and z, and similarly for the products and differences. Hence these operations define corresponding operations on the real numbers, which are easily seen to have the same properties of associativity, commutativity, and distributivity, and the same relationship to comparison operators defined similarly.

Given any rational number r we can form a sequence repeating r infinitely often, and then map r to the equivalence class (under Same_real) of this sequence. This construction is readily seen to embed the rationals into the reals, in a manner that preserves addition, multiplication, and subtraction. The zero rational maps in this way into an additive identity for real addition, and the unit rational into the multiplicative identity for reals. If a Cauchy sequence y_n is not equivalent to the zero of reals, then it is easily seen that for all sufficiently large n the absolute values $|y_n|_{\mathbb{Q}}$ are non-zero and have a common lower bound. Hence for any other Cauchy sequence x_n we can form the rational quotients $x_n \,/_{\mathbb{Q}}\, y_n$ for all sufficiently large n, and it is easy to see that this gives a Cauchy sequence whose equivalence class depends only on that of x and y. It follows that this construction defines a quotient operator $x \,/_{\mathbb{R}}\, y$ for real numbers, and it is not hard to prove that this quotient operator relates to real multiplication in the appropriate inverse way.

[····· TO BE ELABORATED ·····]

In preparation for definition of the real numbers and real arithmetic we introduce the usual fractional notation and absolute value operation for rational numbers:

$$N \,/\, M =_{\text{Def}} \mathsf{Fr\_to\_rats}(\langle N, \emptyset\rangle, \langle M, \emptyset\rangle)\,,$$
$$|Q|_{\mathbb{Q}} =_{\text{Def}} \textbf{if } \mathsf{is\_nonneg}_{\mathbb{Q}}(Q) \textbf{ then } Q \textbf{ else } \mathsf{Rev}_{\mathbb{Q}}(Q) \textbf{ fi}\,,$$

where $N, M \in \mathbb{N}$ and $Q \in \mathbb{Q}$.

The following list of statements gives some basic facts about these operations. In particular, they imply that the operation which associates the value $|a -_{\mathbb{Q}} b|_{\mathbb{Q}}$

with every pair a, b of rational numbers can be viewed as a 'distance' function:

$$
\begin{array}{l}
P \in \mathbb{Q} \rightarrow [\exists \ell \in \mathbb{N}, \mathsf{m} \in \mathbb{N} \mid \mathsf{m} \neq \emptyset \,\&\, \ell \,/\, \mathsf{m} = P]\,, \\
\{J, K, M, N\} \subseteq \mathbb{N} \setminus \{\emptyset\} \,\&\, L \in \mathbb{N} \,\&\, N \subseteq M \,\&\, K \neq L \,\&\, K \neq M \\
\quad \rightarrow L \,/\, M \in \mathbb{Q} \,\&\, J \,/\, M \leqslant_{\mathbb{Q}} J \,/\, N \,\&\, N \,/\, K \leqslant_{\mathbb{Q}} M \,/\, K \,\&\, K \,/\, N \neq L \,/\, N \\
\qquad \&\, J \,/\, K \neq J \,/\, M \,\&\, \mathbf{0}_{\mathbb{Q}} \leqslant_{\mathbb{Q}} L \,/\, M \,\&\, (\mathbf{0}_{\mathbb{Q}} = L \,/\, M \leftrightarrow L = \emptyset) \\
\qquad \&\, 1 \,/\, K +_{\mathbb{Q}} 1 \,/\, K = 2 \,/\, K \,\&\, 1 \,/\, (2 * K) +_{\mathbb{Q}} 1 \,/\, (2 * K) = 1 \,/\, K\,, \\
P \in \mathbb{Q} \,\&\, Q \in \mathbb{Q} \,\&\, R \in \mathbb{Q} \rightarrow P \leqslant_{\mathbb{Q}} |P|_{\mathbb{Q}} \,\&\, \Big||P|_{\mathbb{Q}}\Big|_{\mathbb{Q}} = |P|_{\mathbb{Q}} \\
\quad \&\, (|P|_{\mathbb{Q}} = \mathbf{0}_{\mathbb{Q}} \leftrightarrow P = \mathbf{0}_{\mathbb{Q}}) \,\&\, |\mathsf{Rev}_{\mathbb{Q}}(P)|_{\mathbb{Q}} = |P|_{\mathbb{Q}} \,\&\, |P +_{\mathbb{Q}} Q|_{\mathbb{Q}} \leqslant_{\mathbb{Q}} |P|_{\mathbb{Q}} +_{\mathbb{Q}} |Q|_{\mathbb{Q}} \\
\quad \&\, \Big||P|_{\mathbb{Q}} -_{\mathbb{Q}} |Q|_{\mathbb{Q}}\Big|_{\mathbb{Q}} \leqslant_{\mathbb{Q}} |P -_{\mathbb{Q}} Q|_{\mathbb{Q}} \,\&\, |Q -_{\mathbb{Q}} Q|_{\mathbb{Q}} = \mathbf{0}_{\mathbb{Q}} \\
\quad \&\, |P -_{\mathbb{Q}} Q|_{\mathbb{Q}} = |Q -_{\mathbb{Q}} P|_{\mathbb{Q}} \,\&\, |P -_{\mathbb{Q}} Q|_{\mathbb{Q}} \leqslant_{\mathbb{Q}} |P -_{\mathbb{Q}} R|_{\mathbb{Q}} +_{\mathbb{Q}} |R -_{\mathbb{Q}} Q|_{\mathbb{Q}} \\
\quad \&\, |Q|_{\mathbb{Q}} -_{\mathbb{Q}} \Big||P|_{\mathbb{Q}} -_{\mathbb{Q}} |Q|_{\mathbb{Q}}\Big|_{\mathbb{Q}} \leqslant_{\mathbb{Q}} |P|_{\mathbb{Q}}\,, \\
|P *_{\mathbb{Q}} Q|_{\mathbb{Q}} = |P|_{\mathbb{Q}} *_{\mathbb{Q}} |Q|_{\mathbb{Q}}\,, \\
Q \in \mathbb{Q} \rightarrow [\exists \mathsf{m} \in \mathbb{N} \mid Q <_{\mathbb{Q}} \mathsf{m} \,/\, 1]\,, \\
P \in \mathbb{Q} \,\&\, J \in \mathbb{N} \,\&\, J \neq \emptyset \,\&\, [\forall \mathsf{k} \in \mathbb{N} \mid \mathsf{k} \neq \emptyset \rightarrow |P|_{\mathbb{Q}} <_{\mathbb{Q}} J \,/\, \mathsf{k}] \rightarrow P = \mathbf{0}_{\mathbb{Q}}\,.
\end{array}
$$

An infinite sequence $s_1, s_2, \ldots, s_N, \ldots$ of rational numbers is said to be *regular* if its N-th component and its M-th component differ (in absolute value) by at most $1 \,/\, N +_{\mathbb{Q}} 1 \,/\, M$ for all pairs N, M of positive integers. The formal definition given below looks slightly more complicated than this because we number sequence components starting with 0 instead of with 1. On the other hand, we find it unnecessary to impose single valuedness; this is why our first definition introduces 'regular_maps' instead of 'regular_seqs'. An example of a regular sequence is one whose components are all equal. Note also that the sequence $\{\langle n, 2 \,/\, \mathsf{next}(n)\rangle : n \in \mathbb{N}\}$ is not regular, because e.g. $|2 \,/\, 1 -_{\mathbb{Q}} 2 \,/\, 4|_{\mathbb{Q}} = 6 \,/\, 4 >_{\mathbb{Q}} 5 \,/\, 4 = 1 \,/\, 1 +_{\mathbb{Q}} 1 \,/\, 4$.

$$
\begin{array}{l}
\mathsf{regular\_maps} =_{\mathrm{Def}} \{\mathsf{s} : \mathsf{s} \subseteq \mathbb{N} \times \mathbb{Q} \mid \mathbb{N} = \mathbf{dom}\, \mathsf{s} \,\&\, [\forall \mathsf{p} \in \mathsf{s}, \mathsf{q} \in \mathsf{s} \mid \\
\qquad\qquad |\mathsf{cdr}(\mathsf{p}) -_{\mathbb{Q}} \mathsf{cdr}(\mathsf{q})|_{\mathbb{Q}} \leqslant_{\mathbb{Q}} 1 \,/\, \mathsf{next}(\mathsf{car}(\mathsf{p})) +_{\mathbb{Q}} 1 \,/\, \mathsf{next}(\mathsf{car}(\mathsf{q}))]\}\,, \\
Q \in \mathbb{Q} \rightarrow \{\langle \mathsf{n}, Q\rangle : \mathsf{n} \in \mathbb{N}\} \in \mathsf{regular\_maps}\,.
\end{array}
$$

In using regular sequences to represent real numbers, we regard two regular sequences s, t as being 'the same' (in the sense of representing the same real number) if, for all N, their corresponding components s_N, t_N differ by $2 \,/\, N$ at most. Taking our 'numbering from 0' unit into account once more, we define:

$$
\begin{array}{l}
\mathsf{Same\_regmap}(S, T) \leftrightarrow_{\mathrm{Def}} [\forall \mathsf{p} \in S, \mathsf{q} \in T \mid \mathsf{car}(\mathsf{p}) = \mathsf{car}(\mathsf{q}) \\
\qquad\qquad\qquad\qquad \rightarrow |\mathsf{cdr}(\mathsf{p}) -_{\mathbb{Q}} \mathsf{cdr}(\mathsf{q})|_{\mathbb{Q}} \leqslant_{\mathbb{Q}} 2 \,/\, \mathsf{next}(\mathsf{car}(\mathsf{p}))]\,.
\end{array}
$$

The following theorem is used to derive the fact that the Same_regmap relationship is transitive and hence is an equivalence relation. It states that if s and t are equivalent regular sequences, then for each positive integer k there is an m such that for all N greater than or equal to m, the corresponding components

s_N and t_N of s and t differ at most by $1 \,/\, k$.

$S \in \mathsf{regular\_maps} \,\&\, T \in \mathsf{regular\_maps} \longrightarrow (\mathsf{Same\_regmap}(S,T) \leftrightarrow [\forall \mathsf{k} \in \mathbb{N} \mid$
$\mathsf{k} \neq \emptyset \longrightarrow [\exists \mathsf{m} \in \mathbb{N}, \forall \mathsf{p} \in S, \mathsf{q} \in T \mid \mathsf{m} \subseteq \mathsf{car(p)} \,\&\, \mathsf{car(p)} = \mathsf{car(q)}$
$\longrightarrow |\mathsf{cdr(p)} -_{\mathbb{Q}} \mathsf{cdr(q)}|_{\mathbb{Q}} \leqslant_{\mathbb{Q}} 1 \,/\, \mathsf{k}]])\,,$
$S \in \mathsf{regular\_maps} \,\&\, T \in \mathsf{regular\_maps} \,\&\, R \in \mathsf{regular\_maps} \longrightarrow \mathsf{Same\_regmap}(S,S)$
$\&\, (\mathsf{Same\_regmap}(T,R) \,\&\, \mathsf{Same\_regmap}(R,S) \longrightarrow \mathsf{Same\_regmap}(S,T))\,.$

The following auxiliary theories ease derivation of the reflexivity of Same_regmap, and give us a convenient way of obtaining a regular sequence from a regular map.

THEORY shifted_regmap(s, f, m)
  s ∈ regular_maps
  [∀n ∈ ℕ | f(n) ∈ ℕ & n⊆f(n)]
⟹ (t)
  t={[k, cdr(p)] : k ∈ ℕ, p ∈ s | car(p)=f(k)}
  Same_regmap(t, s)
  Svm(s) ⟶ Svm(t)
END shifted_regmap ,

THEORY regmap_to_seq(t)
  t ∈ regular_maps
⟹ (s)
  -- s={[n, **arb** ({cdr(p) : p ∈ t | car(p)=n})] : n ∈ ℕ}
  s ∈ regular_maps
  Svm(s)
  Same_regmap(t, s)
END regmap_to_seq .

We are now ready to define real numbers via application of the THEORY equivalence_classes, which also gives a natural embedding of the rational numbers into the reals.

APPLY equivalence_classes(P(x, y) ↦ Same_regmap(x, y), s ↦ regular_maps)
⟹ (ℝ, Seq_to_Re)
  [∀x ∈ regular_maps | Seq_to_Re(x) ∈ ℝ]
  [∀x ∈ ℝ | **arb** (x) ∈ regular_maps & Seq_to_Re(**arb** (x))=x]
  [∀x ∈ regular_maps, y ∈ regular_maps | Same_regmap(x, y)
    ↔ Seq_to_Re(x)=Seq_to_Re(y)]
  [∀x ∈ regular_maps | Same_regmap(x, **arb** (Seq_to_Re) (x))] ,

-- Rational-to-Real conversion:
Ra_to_Re(X) $=_{\mathrm{Def}}$ Seq_to_Re({⟨n, X⟩ : n ∈ ℕ}) ,
-- Real 0:
$\mathbf{0}_{\mathbb{R}} =_{\mathrm{Def}}$ Ra_to_Re($\mathbf{0}_{\mathbb{Q}}$) ,
-- Real 1:
$\mathbf{1}_{\mathbb{R}} =_{\mathrm{Def}}$ Ra_to_Re($\mathbf{1}_{\mathbb{Q}}$) .

To introduce the algebraic operations on the set $\mathbb{R}$ of reals we need an auxiliary bound for the terms of a regular sequence s of rational numbers. We define the 'canonical' bound of such an s to be the least integer m which is at least 2 greater than the absolute value of the first component of s. It follows easily that m is greater than the absolute value of s_N for all N:

$$\begin{aligned}&\mathsf{canon\_bound}(X) =_{\mathrm{Def}}\\ &\qquad \mathbf{arb}\left(\{\mathsf{m} : \mathsf{m}\in\mathbb{N} \mid [\exists \mathsf{p}\in X \mid \mathsf{car}(\mathsf{p})=\emptyset \;\&\; |\mathsf{cdr}(\mathsf{p})|_{\mathbb{Q}} +_{\mathbb{Q}} 2\,/\,1 <_{\mathbb{Q}} \mathsf{m}\,/\,1]\}\right),\\ &S\in \mathsf{regular\_maps} \;\&\; P\in S \longrightarrow |\mathsf{cdr}|_{\mathbb{Q}}(P) <_{\mathbb{Q}} \mathsf{canon\_bound}(S)\,/\,1\,.\end{aligned}$$

The arithmetic operations on real numbers x, y are now defined in terms of their rational approximations x_N, y_N (more precisely, $\mathbf{arb}\,(x)_N$ and $\mathbf{arb}\,(y)_N$.

$$\begin{aligned}&\text{-- Real Sum:}\\ X +_{\mathbb{R}} Y =_{\mathrm{Def}}\ &\mathsf{Seq\_to\_Re}\big(\{\langle \mathsf{n}, \mathsf{cdr}(\mathsf{p}) +_{\mathbb{Q}} \mathsf{cdr}(\mathsf{q})\rangle : \mathsf{n}\in\mathbb{N}, \mathsf{p}\in\mathbf{arb}\,(X), \mathsf{q}\in\mathbf{arb}\,(Y)\\ &\qquad\qquad \mid \mathsf{next}(\mathsf{n}+\mathsf{n})=\mathsf{car}(\mathsf{p}) \;\&\; \mathsf{car}(\mathsf{p})=\mathsf{car}(\mathsf{q})\}\big)\,,\\ &\text{-- Real Negative:}\\ \mathsf{Rev}_{\mathbb{R}}(X) =_{\mathrm{Def}}\ &\mathsf{Seq\_to\_Re}\big(\{\langle \mathsf{car}(\mathsf{p}), \mathsf{Rev}_{\mathbb{Q}}(\mathsf{cdr}(\mathsf{p}))\rangle : \mathsf{p}\in\mathbf{arb}\,(X)\}\big)\,,\\ &\text{-- Real Subtraction:}\\ X -_{\mathbb{R}} Y =_{\mathrm{Def}}\ &X +_{\mathbb{Q}} \mathsf{Rev}_{\mathbb{R}}(Y)\,,\\ &\text{-- Real Multiplication:}\\ X *_{\mathbb{R}} Y =_{\mathrm{Def}}\ &\mathsf{Seq\_to\_Re}\big(\{\langle \mathsf{n}, \mathsf{cdr}(\mathsf{p}) *_{\mathbb{Q}} \mathsf{cdr}(\mathsf{q})\rangle : \mathsf{n}\in\mathbb{N}, \mathsf{p}\in\mathbf{arb}\,(X), \mathsf{q}\in\mathbf{arb}\,(Y)\\ &\qquad \mid 2 * ((\mathsf{canon\_bound}(X)\cup\mathsf{canon\_bound}(Y)) * \mathsf{next}(\mathsf{n}))=\mathsf{next}(\mathsf{car}(\mathsf{p}))\\ &\qquad\qquad \;\&\; \mathsf{car}(\mathsf{p})=\mathsf{car}(\mathsf{q})\}\big)\,,\\ &\text{-- Absolute value , i.e. the larger of } X \text{ and } \mathsf{Rev}_{\mathbb{R}}(X):\\ |X|_{\mathbb{R}} =_{\mathrm{Def}}\ &\mathsf{Seq\_to\_Re}(\{\langle \mathsf{car}(\mathsf{p}), |\mathsf{cdr}(\mathsf{p})|_{\mathbb{Q}}\rangle : \mathsf{p}\in\mathbf{arb}\,(X)\})\,,\end{aligned}$$

$$\begin{aligned}\mathsf{is\_nonneg}_{\mathbb{R}}(X) \leftrightarrow_{\mathrm{Def}}\ &|X|_{\mathbb{R}}=X\,,\\ \mathsf{Z\_aux}(X) =_{\mathrm{Def}}\ &\mathbf{arb}\Big(\{\mathsf{m} : \mathsf{m}\in\mathbb{N} \mid \mathsf{m}\neq\emptyset \;\&\\ &\qquad [\forall \mathsf{p}\in X \mid \mathsf{m}\leqslant_{\mathbb{Q}} \mathsf{next}(\mathsf{car}(\mathsf{p})) \longrightarrow 1\,/\,\mathsf{m}\leqslant_{\mathbb{Q}} |\mathsf{cdr}(\mathsf{p})|_{\mathbb{Q}}]\}\Big)\,,\\ &\text{-- Real Reciprocal:}\\ \mathsf{Recip}_{\mathbb{R}}(X) =_{\mathrm{Def}}\ &\mathsf{Seq\_to\_Re}(\{\langle \mathsf{n}, \mathsf{Recip}_{\mathbb{Q}}(\mathsf{cdr}(\mathsf{p}))\rangle : \mathsf{n}\in\mathbb{N}, \mathsf{p}\in\mathbf{arb}\,(X),\\ &\mathsf{m}\in\mathbb{N} \mid \mathsf{m}=\mathsf{Z\_aux}(\mathbf{arb}\,(X)) \;\&\; \mathsf{next}(\mathsf{car}(\mathsf{p}))=(\mathsf{n}\cup\mathsf{m}) * (\mathsf{m} * \mathsf{m}))\}\,,\\ &\text{-- Real Quotient:}\\ X\,/_{\mathbb{R}}\,Y =_{\mathrm{Def}}\ &X *_{\mathbb{R}} \mathsf{Recip}_{\mathbb{R}}(Y)\,.\end{aligned}$$

Here, for example, the definition of $\mathsf{Recip}_{\mathbb{R}}$ states that in order to get the reciprocal of a real number X, one must consider a regular sequence $s_1, s_2, \ldots, s_N, \ldots$ in X, determine the least positive integer m satisfying $(1\,/\,m) \leqslant_{\mathbb{Q}} |s_i|_{\mathbb{Q}}$ for all i greater than or equal to m, and then construct the regular sequence t whose first m components $t_1, t_2, \ldots, t_m$ all equal $\mathsf{Recip}_{\mathbb{Q}}(s_{m*m*m})$ and whose subsequent components t_N with m in N are defined as $t_N = \mathsf{Recip}_{\mathbb{Q}}(s_{N*m*m})$: the desired reciprocal Y of X will be the real number to which t belongs.

It is important to show that the above operations produce real numbers when their operands are reals, and that the results of the arithmetic operations do not

depend on the way in which one chooses a representative sequence from each of the equivalence classes representing reals. For example, for real addition, we need to know that

$$
\begin{array}{l}
S \in \mathsf{regular\_maps} \,\&\, T \in \mathsf{regular\_maps} \\
\quad \longrightarrow \big\{\langle \mathsf{n}, \mathsf{cdr(p)} +_{\mathbb{Q}} \mathsf{cdr(q)}\rangle : \mathsf{n} \in \mathbb{N}, \mathsf{p} \in S, \mathsf{q} \in T \\
\qquad\qquad | \; \mathsf{next(n+n)}{=}\mathsf{car(p)} \,\&\, \mathsf{car(p)}{=}\mathsf{car(q)}\big\} \in \mathsf{regular\_maps}\,, \\
X \in \mathbb{R} \,\&\, Y \in \mathbb{R} \longrightarrow X +_{\mathbb{R}} Y \in \mathbb{R}\,, \\
S_1 \in \mathsf{regular\_maps} \,\&\, S_2 \in \mathsf{regular\_maps} \,\&\, T_1 \in \mathsf{regular\_maps} \\
\quad \& \, T_2 \in \mathsf{regular\_maps} \,\&\, \mathsf{Same\_regmap}(S_1, S_2) \,\&\, \mathsf{Same\_regmap}(T_1, T_2) \\
\qquad \longrightarrow \mathsf{Same\_regmap}(\big\{\langle \mathsf{n}, |\mathsf{cdr}|_{\mathbb{Q}}(\mathsf{p}) +_{\mathbb{Q}} |\mathsf{cdr}|_{\mathbb{Q}}(\mathsf{q})\rangle : \mathsf{n} \in \mathbb{N}, \mathsf{p} \in S_1, \mathsf{q} \in T_1 \\
\qquad\quad | \; \mathsf{next(n+n)}{=}\mathsf{car(p)} \,\&\, \mathsf{car(p)}{=}\mathsf{car(q)}\big\}, \\
\qquad\qquad\qquad \big\{\langle \mathsf{n}, |\mathsf{cdr}|_{\mathbb{Q}}(\mathsf{p}) +_{\mathbb{Q}} |\mathsf{cdr}|_{\mathbb{Q}}(\mathsf{q})\rangle : \mathsf{n} \in \mathbb{N}, \mathsf{p} \in S2, \mathsf{q} \in T_2 \\
\qquad\quad | \; \mathsf{next(n+n)}{=}\mathsf{car(p)} \,\&\, \mathsf{car(p)}{=}\mathsf{car(q)}\big\}\big)\,.
\end{array}
$$

Analogously, for the real reciprocal operation, we need to know that

$$
\begin{array}{l}
S \in \mathsf{regular\_maps} \,\&\, \neg\mathsf{Same\_regmap}(S, \{\langle \mathsf{n}, \mathbf{0}_{\mathbb{Q}}\rangle : \mathsf{n} \in \mathbb{N}\}) \\
\quad \longrightarrow [\exists \mathsf{m} \in \mathbb{N} \,|\, \mathsf{m}{\neq}\emptyset \,\&\, [\forall \mathsf{p} \in S \,|\, \mathsf{m} \leqslant_{\mathbb{Q}} \mathsf{next(car(p))} \longrightarrow 1 \,/\, \mathsf{m} \leqslant_{\mathbb{Q}} |\mathsf{cdr(p)}|_{\mathbb{Q}}]]\,, \\
S \in \mathsf{regular\_maps} \,\&\, M \in \mathbb{N} \,\&\, M{\neq}\emptyset \,\&\, [\forall \mathsf{p} \in S \,|\, M \leqslant_{\mathbb{Q}} \mathsf{next(car(p))} \longrightarrow 1 \,/\, M \leqslant_{\mathbb{Q}} |\mathsf{cdr(p)}|_{\mathbb{Q}}] \\
\quad \longrightarrow \{\langle \mathsf{n}, \mathsf{Recip}_{\mathbb{Q}}(\mathsf{cdr(p)})\rangle : \mathsf{n} \in \mathbb{N}, \mathsf{p} \in S \,|\, \mathsf{next(car(p))}{=}(\mathsf{n}{\cup}M) * (M * M)\} \in \mathsf{regular\_maps}\,, \\
X \in \mathbb{R} \,\&\, X{\neq}\mathbf{0}_{\mathbb{R}} \longrightarrow \mathsf{Recip}_{\mathbb{R}}(X) \in \mathbb{R}\,, \\
S \in \mathsf{regular\_maps} \,\&\, M_1 \in \mathbb{N} \,\&\, M_2 \in \mathbb{N} \,\&\, M_1{\neq}\emptyset \,\&\, M_2{\neq}\emptyset \\
\quad \& \, [\forall \mathsf{p} \in S \,|\, M_1 \leqslant_{\mathbb{Q}} \mathsf{next(car(p))} \longrightarrow 1 \,/\, M_1 \leqslant_{\mathbb{Q}} |\mathsf{cdr(p)}|_{\mathbb{Q}}] \\
\quad \& \, [\forall \mathsf{p} \in S \,|\, M_2 \leqslant_{\mathbb{Q}} \mathsf{next(car(p))} \longrightarrow 1 \,/\, M_2 \leqslant_{\mathbb{Q}} |\mathsf{cdr(p)}|_{\mathbb{Q}}] \longrightarrow \mathsf{Same\_regmap}\big(\\
\qquad \{\langle \mathsf{n}, \mathsf{Recip}_{\mathbb{Q}}(\mathsf{cdr(p)})\rangle : \mathsf{n} \in \mathbb{N}, \mathsf{p} \in S \,|\, \mathsf{next(car(p))}{=}(\mathsf{n}{\cup}M_1) * (M_1 * M_1)\}, \\
\qquad \{\langle \mathsf{n}, \mathsf{Recip}_{\mathbb{Q}}(\mathsf{cdr(p)})\rangle : \mathsf{n} \in \mathbb{N}, \mathsf{p} \in S \,|\, \mathsf{next(car(p))}{=}(\mathsf{n}{\cup}M_2) * (M_2 * M_2)\}\big)\,.
\end{array}
$$

We also need to derive the algebraic properties of the basic operations on reals from the definitions given above, e.g.

$$
\begin{array}{l}
X \in \mathbb{R} \,\&\, Y \in \mathbb{R} \,\&\, W \in \mathbb{R} \\
\quad \longrightarrow X +_{\mathbb{R}} Y{=}Y +_{\mathbb{R}} X \,\&\, W +_{\mathbb{R}} (X +_{\mathbb{R}} Y){=}(W +_{\mathbb{R}} X) +_{\mathbb{R}} Y \,\&\, X +_{\mathbb{R}} \mathbf{0}_{\mathbb{R}}{=}X \\
\qquad \& \, X +_{\mathbb{R}} \mathsf{Rev}_{\mathbb{R}}(X){=}\mathbf{0}_{\mathbb{R}} \,\&\, X *_{\mathbb{R}} Y{=}Y *_{\mathbb{R}} X \,\&\, \mathbf{1}_{\mathbb{R}} *_{\mathbb{R}} X{=}X \\
\qquad \& \, X *_{\mathbb{R}} \mathbf{1}_{\mathbb{R}}{=}X \,\&\, (X{\neq}\mathbf{0}_{\mathbb{R}} \longrightarrow (X *_{\mathbb{R}} Y{=}\mathbf{1}_{\mathbb{R}} \leftrightarrow Y{=}\mathsf{Recip}_{\mathbb{Q}}(X)))\,.
\end{array}
$$

There are important connections between rational and real numbers, such as the fact that $\mathbb{Q}$ is 'order dense' in $\mathbb{R}$. The following definitions and theorems define the ordering of reals and state this fact.

$$
\begin{array}{rcl}
 & & \text{-- Real Maximum:} \\
X \;\mathbf{max}_{\mathbb{R}}\; Y & =_{\mathrm{Def}} & \mathsf{Seq\_to\_Re}\big(\big\{\langle \mathsf{car(p)}, \mathbf{if}\ \mathsf{cdr(p)} \leqslant_{\mathbb{Q}} \mathsf{cdr(q)}\ \mathbf{then}\ \mathsf{cdr(q)}\ \mathbf{else}\ \mathsf{cdr(p)}\ \mathbf{fi}\rangle \\
 & & \qquad\qquad : \mathsf{p} \in \mathbf{arb}\,(X)\,, \mathsf{q} \in \mathbf{arb}\,(Y) \;|\; \mathsf{car(p)}{=}\mathsf{car(q)}\big\}\big)\,, \\
 & & \text{-- Real Ordering:} \\
X \leqslant_{\mathbb{R}} Y & \leftrightarrow_{\mathrm{Def}} & X \;\mathbf{max}_{\mathbb{R}}\; Y{=}Y\,, \\
X <_{\mathbb{R}} Y & \leftrightarrow_{\mathrm{Def}} & X \;\mathbf{max}_{\mathbb{R}}\; Y{\neq}X\,,
\end{array}
$$

$$
\begin{array}{l}
X \in \mathbb{R} \,\&\, \langle N, Y\rangle \in \mathbf{arb}\,(X) \longrightarrow |X -_{\mathbb{R}} \mathsf{Ra\_to\_Re}(Y)|_{\mathbb{R}} \leqslant_{\mathbb{R}} \mathsf{Ra\_to\_Re}(1 \,/\, N)\,, \\
X \in \mathbb{R} \,\&\, Y \in \mathbb{R} \longrightarrow [\exists \mathsf{r} \in \mathbb{Q} \,|\, X <_{\mathbb{R}} \mathsf{Ra\_to\_Re(r)} \,\&\, \mathsf{Ra\_to\_Re(r)} <_{\mathbb{R}} Y]\,.
\end{array}
$$

Another important connection between real and rational numbers lies in Dedekind cuts, which are the nonnull sets d of rational numbers, bounded above,

such that every rational not in d is larger than any rational in d. (If we added the requirement that to any x in d there must correspond a larger rational y in d, then we could establish a one-to-one correspondence between Dedekind cuts and real numbers; but this is of no concern to us here.) Below we specify this notion formally, and define a function translating Dedekind cuts into real numbers, and then define the operation which determines the least upper bound of any nonnull set of real numbers bounded above:

$$\mathsf{dedekind\_cuts} =_{\mathrm{Def}} \{\mathsf{d} : \mathsf{d} \subseteq \mathbb{Q} \mid \emptyset \neq \mathsf{d} \;\&\; \mathsf{d} \neq \mathbb{Q} \;\&\; [\forall \mathsf{x} \in \mathsf{d}, \mathsf{y} \in \mathbb{Q} \mid \mathsf{y} <_{\mathbb{Q}} \mathsf{x} \longrightarrow \mathsf{y} \in \mathsf{d}]\}\,,$$

-- Cut-to-Real conversion:

$$\mathsf{Dedek\_to\_Re}(D) =_{\mathrm{Def}} \mathsf{Seq\_to\_Re}\big(\{\langle \mathsf{n}, \mathbf{arb}\,(D) +_{\mathbb{Q}} \mathbf{arb}\,(\{\mathsf{h} \,/\, \mathsf{next}(\mathsf{n}) : \mathsf{h} \in \mathbb{N} \mid \mathbf{arb}\,(D) +_{\mathbb{Q}} \mathsf{next}(\mathsf{h}) \,/\, \mathsf{next}(\mathsf{n}) \notin D\})\rangle : \mathsf{n} \in \mathbb{N}\}\big)\,,$$

$$D \in \mathsf{dedekind\_cuts} \longrightarrow \mathsf{Dedek\_to\_Re}(D) \in \mathbb{R}\,,$$

-- Least Upper Bound:

$$\mathsf{Re\_LUB}(X) =_{\mathrm{Def}} \mathsf{Dedek\_to\_Re}(\bigcup\{\mathsf{q} : \mathsf{q} \in \mathbb{Q} \mid [\exists \mathsf{x} \in X \mid \mathsf{Ra\_to\_Re}(\mathsf{q}) <_{\mathbb{R}} \mathsf{x}]\})\,,$$

$$I \in \mathbb{R} \;\&\; I \neq \emptyset \;\&\; [\exists \mathsf{y} \in \mathbb{R}, \forall \mathsf{x} \in I \mid \mathsf{x} \leqslant_{\mathbb{R}} \mathsf{y}] \longrightarrow \mathsf{Re\_LUB}(I) \in \mathbb{R} \;\&\; [\forall \mathsf{y} \in \mathbb{R} \mid \mathsf{Re\_LUB}(I) <_{\mathbb{R}} \mathsf{y} \leftrightarrow [\forall \mathsf{x} \in I \mid \mathsf{x} \leqslant_{\mathbb{R}} \mathsf{y}]]\,.$$

[····· TO BE ELABORATED ·····]

References

1. E. W. Beth. *The foundations of mathematics*. Horth-Holland, 1959.
2. D. S. Bridges. *Foundations of real and abstract analysis*. Springer-Verlag, Graduate Texts in Mathematics vol.174, 1997.
3. J. Gurevič. Elementary properties of ordered Abelian groups. *Translations of AMS*, 46, pp. 165-192, 1965.
4. A.I. Kokorin, V.M. Kopytov. *Fully ordered groups*. Wiley and Sons, 1974.
5. L. Fuchs. *Abelian groups*. Academic Press, 1970.
6. J. P. Ignizio and T. M. Cavalier. *Linear Programming*. International Series in Industrial and Systems Engineering. Prentice Hall, New Jersey, 1994.
7. W. W. McCune. *Otter 2.0 User Guide*. ANL-90/9, Argonne National Laboratory, Argonne, Illinois, 1990.
8. E.G. Omodeo and J. T. Schwartz. A 'theory' mechanism for a proof-verifier based on first-order set theory. In A. Kakas and F. Sadri, editors, *Computational Logic: Logic Programming and Beyond – Essays in honour of Bob Kowalski,* Part II, volume 2408 of *Lecture Notes in Artificial Intelligence*, pages 214–230. Springer-Verlag, Berlin, 2002.