Signed-Bit Representations of Real Numbers

Robert S. Lubarsky
Fred Richman
Florida Atlantic University
Dept. of Mathematical Sciences
777 Glades Rd., Boca Raton, FL 33431, USA
Robert.Lubarsky@alum.mit.edu
richman@fau.edu

21 July 2009

Abstract

The signed-bit representation of real numbers is like the binary representation, but in addition to 0 and 1 you can also use -1. It lends itself especially well to the constructive (intuitionistic) theory of the real numbers. The first part of the paper develops and studies the signed-bit equivalents of three common notions of a real number: Dedekind cuts, Cauchy sequences, and regular sequences. This theory is then applied to homomorphisms of Riesz spaces into $\mathbb{R}$.

1 Introduction

In [4], Coquand and Spitters studied the Stone-Yosida representation theorem for lattice ordered vector spaces (Riesz spaces). They gave a constructive proof of this theorem for separable, seminormed Riesz spaces which used Dependent Choice (DC). They then asked whether DC is necessary and suggested a construction which would show that it was. This question was answered in [10] and [8] along the lines they suggested.

In thinking about this question, we were led to representing real numbers in a tree-like structure. This representation is a lot like the classical signed-bit representation, a modification of the binary representation where -1 is allowed as well as 0 and 1. The signed-bit representation is especially suitable to constructivism and computability because you can show constructively (with DC) that every real number has a signed-bit representation, but not that every real number has a binary representation.

The thrust of this paper (Section 2) is this signed-bit representation. In Sections 3 and 4, the representation is applied to various questions about real numbers and about homomorphisms of Riesz spaces into $\mathbb{R}$. The benefits of these applications include a reformulation of the choice principles involved, a generalization from countable and separable Riesz space to ones of arbitrary size, and a recasting of the issues in a form more familiar to classical set theorists.

2 Signed-bit representations of real numbers

2.1 Three kinds of real numbers

We are interested in studying real numbers from a constructive point of view without using countable choice principles. We consider three kinds of real numbers: Dedekind, regular, and Cauchy (see also [5] and [9]). The latter two kinds are given by sequences of rational numbers (see below). A *real number*, simpliciter, is a Dedekind real number, that is, a real number is determined by a located Dedekind cut [3, Problem 2.6], [13, p. 170]. A *located Dedekind cut* can be defined as a nonempty proper open subset L of the rational numbers $\mathbb{Q}$ such that for all pairs of rational numbers $u < v$, either $u \in L$ or $v \notin L$. If r is the real number defined by L, then $L = \{u \in \mathbb{Q} : u < r\}$. The Dedekind real numbers are exactly the things that can be approximated coherently by rational numbers.

If r is any real number, then for each positive integer n there is a rational number u such that $|u - r| \leq 1/n$. Using countable choice, we could construct a sequence q of rational numbers so that $|q_n - r| \leq 1/n$. Such a sequence q is a *regular sequence* in the sense that

$$|q_m - q_n| \leq \frac{1}{m} + \frac{1}{n}$$

for all m and n. Note that a regular sequence is a Cauchy sequence, and we leave it as an exercise to show that every Cauchy sequence converges to some real number. Conversely, if a regular sequence q converges to the real number r, then $|q_n - r| \leq 1/n$ for all n. Bishop [3] *defines* a real number to be a regular sequence of rational numbers.

Theorem 2.1 *Let q be a sequence of rational numbers and μ a sequence of positive integers. Then the following two conditions are equivalent*

1. *For all i, j, if $m \geq \mu_i$ and $n \geq \mu_j$, then*

$$|q_m - q_n| \leq \frac{1}{i} + \frac{1}{j}.$$

2. *There is a real number r so that for all i, if $m \geq \mu_i$, then*

$$|q_m - r| \leq 1/i.$$

Proof: If 1 holds, then q is a Cauchy sequence, hence converges to a real number r. If $m \geq \mu_i$, then

$$|q_m - q_n| \leq \frac{1}{i} + \frac{1}{j}$$

whenever $n \geq \mu_j$. In particular, this inequality holds for arbitrarily large values of n and j, so $|q_m - r| \leq 1/i$. Conversely, suppose 2 holds. Then

$$|q_m - q_n| \leq |q_m - r| + |r - q_n| \leq \frac{1}{i} + \frac{1}{j}$$

for all $m \geq \mu_i$ and $n \geq \mu_j$. ▮

We say that μ is a *modulus of convergence* for q if either of the equivalent conditions in Theorem 2.1 hold.

If q is a regular sequence, then it has the modulus of convergence $\mu_m = m$. Conversely, if μ is a modulus of convergence for q, then the sequence q_{μ_m} is a regular sequence converging to the limit r of q. So a real number r is the limit of a regular sequence of rational numbers if and only if it is the limit of a sequence of rational numbers that has a modulus of convergence. We call such a real number a *regular real number*. Troelstra and van Dalen [13] define a Cauchy real number to be what we are calling here a regular real number.

Theorem 2.2 *If r is a regular real number, then every sequence of rational numbers converging to r has a modulus of convergence.*

Proof: Let q be a regular sequence of rational numbers converging to r. Let p be a sequence of rational numbers converging to r. We need to find a modulus of convergence μ for the sequence p.

Given m we define μ_m as follows. Choose k so that $|p_n - r| \leq 1/6m$ for all $n \geq k$. So, if $n \geq k$, we have

$$|p_n - q_{3m}| \leq |p_n - r| + |r - q_{3m}| \leq \frac{1}{6m} + \frac{1}{3m} \leq \frac{1}{2m}$$

Let $\mu_m \leq k$ be the smallest integer such that

$$|p_n - q_{3m}| \leq \frac{1}{2m}$$

for $n = \mu_m, \ldots, k$. Then μ_m is the smallest integer for which the above inequality holds for all $n \geq \mu_m$, so μ_m does not depend on the choice of k.

It remains to show that $|p_n - r| \leq 1/m$ for all $n \geq \mu_m$. But, if $n \geq \mu_m$, then

$$|p_n - r| \leq |p_n - q_{3m}| + |q_{3m} - r| \leq \frac{1}{2m} + \frac{1}{3m} \leq \frac{1}{m}$$

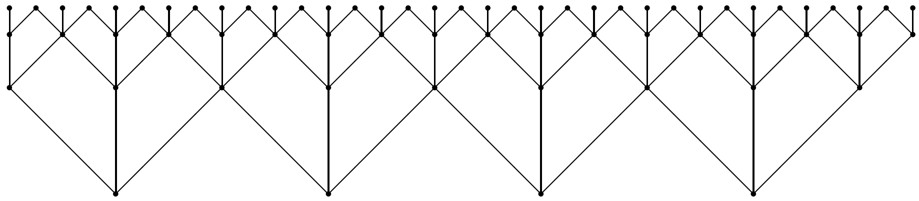
∎

In particular, every sequence of rational numbers that converges to a rational number has a modulus of convergence. Irrational numbers are also regular real numbers—in fact, they have decimal expansions. By an *irrational number* we mean a real number r such that $|r - q| > 0$ for each rational number q. It follows that algebraic real numbers, because they are either rational or irrational, are regular real numbers.

In the absence of countable choice, not every real number can be written as the limit of a sequence of rational numbers, regular or otherwise. A real number r that can be so written is called a *Cauchy real number* because it is the limit of a Cauchy sequence of rational numbers. Not every Cauchy real number is a regular real number (see [9]).

2.2 The pseudotree

We want to consider the following infinite tree-like structure T, the *ternary pseudotree*:



The structure continues infinitely far in all directions (left, right, up, and down). The nodes are dyadic intervals $(k/2^n, (k+2)/2^n)$ where k and n are integers. The descendants of a node are its subintervals. For example, the bottom four nodes in the figure could be the intervals $(-1, 0)$, $(-1/2, 1/2)$, $(0, 1)$, and $(1/2, 3/2)$. The children (immediate descendants) of the node $(0, 1)$ are $(0, 1/2)$, $(1/4, 3/4)$, and $(1/2, 1)$.

The level of a node corresponds inversely to its radius. For instance, $(0, 1)$ is on level 1 because it has a radius of 2^{-1}. In general, the nodes on level l are those with radius 2^{-l}, and (hence) length 2^{1-l}.

A path through T corresponds exactly to a signed-bit representation of a real number.[1] Just as a number written in binary is a sequence of 0s and 1s, indexed by $\mathbb{Z}$, in which all entries below some index n are 0, a signed-bit number, also known as a signed-binary or signed-digit number, is such a $\mathbb{Z}$-indexed sequence of 0s, 1s, and -1s. The sequence a represents the number $\sum_i a_i 2^{-i}$. No number has a unique representation. The corresponding path in T starts at the node of length 2^{n+2} with midpoint 0. At stage i the path goes left, middle, or right, depending on whether a_i is -1, 0, or 1 respectively. Actually, the only paths generated in this way are those that start at some node with midpoint 0. Those with no such start, or no start at all, would not correspond to a signed-bit representation in the sense described here.

If I is a node, we denote the three children of I by λI, μI, and ρI (left, middle, and right). An *extreme descendant* of I is a node of the form $\lambda^i I$ or $\rho^i I$ for some i.

2.3 Ideals in T and their real numbers

Given a real number r, let O_r be $\{I \in T \mid r \in I\}$, the set of nodes in T that contain r. Note that O_r is closed downwards (under superset) and closed under join (intersection). An *o-ideal* is a nonempty set O of nodes closed downwards and under join, such that every node in O has a nonextreme descendant in O.

Theorem 2.3 *The function $r \mapsto O_r$ is a bijection from the real numbers to the o-ideals.*

[1] Apparently the first use of the ternary pseudotree for the signed-bit representation is in [1]. There T is called the *Stern-Brocot* or *Farey tree*, even though we find enough difference between each of those trees and T to warrant the use of a different name. For more on signed-bit representations themselves, see [14].

Proof: To prove that O_r is an o-ideal, we must show that each node of O_r has a nonextreme descendant in O_r. Suppose $((k-1)/2^n, (k+1)/2^n) \in O_r$, that is

$$\frac{k-1}{2^n} < r < \frac{k+1}{2^n}$$

Then there exists k' and n' such that

$$\frac{k-1}{2^n} < \frac{k'-1}{2^{n'}} < r < \frac{k'+1}{2^{n'}} < \frac{k+1}{2^n}$$

But this makes $((k'-1)/2^{n'}, (k'+1)/2^{n'})$ a nonextreme descendant of $((k-1)/2^n, (k+1)/2^n)$ in O_r. Indeed, for $k'/2^{n'}$ to be the midpoint of an extreme descendant, it must be of the form

$$\left(2^i(k-1)+1\right)/2^{n+i} \text{ or } \left(2^i(k+1)-1\right)/2^{n+i}$$

so $k' = 2^{n'-n}(k \mp 1) \pm 1$. But

$$2^{n'-n}(k+1) - 1 > k' > 2^{n'-n}(k-1) + 1$$

To see that the function is a bijection, let O be an o-ideal. Then O defines a set of nonempty open intervals closed under finite intersection and containing arbitrarily small intervals. So there is a unique real number r that is contained in all the closures of intervals in O. But because each open interval J in O has a nonextreme descendant, the number r is contained in J itself. To see that $O = O_r$, suppose some dyadic open interval J contains r. Then every sufficiently small dyadic interval that contains r is contained in J. As O is a downset, J must be in O. ▮

We can also consider the closed interval correlates. For a real number r, let C_r be $\{I \in T \mid r \in \overline{I}\}$, where $\overline{I}$ is the (topological) closure of I. The subset C_r is not closed under join, but it does satisfy the following closure conditions:

1. Each node in C_r has a child in C_r.
2. The nodes at each level in C_r are adjacent, and there are at most three of them.
3. $\neg I \notin C_r \Rightarrow I \in C_r$.
4. If I is a node in C_r, then $\lambda I \notin C_r \Rightarrow \rho I \in C_r$, and $\rho I \notin C_r \Rightarrow \lambda I \in C_r$. (By property 3, these are equivalent.)
5. If $\rho^i I \in C_r$ for all i, then I is the leftmost member of three adjacent nodes in the downset, and conversely. Same with ρ replaced by λ and "leftmost" by "rightmost".
6. If two nodes of C_r have a join in T, then that join is in C_r.

A *c-ideal* is a nonempty set of nodes satisfying the six conditions above.

Theorem 2.4 *The function $r \mapsto C_r$ is a bijection from the real numbers to the c-ideals.*

Proof: We first show that C_r is a c-downset. Clearly 1, 2, and 6 hold. Property 3 holds because if J is a closed interval, then $r \in J$ if and only if $\neg d\,(r, J) > 0$. To see 4, note that if $r \in J$, but $r \notin \lambda J$, then $r \in \rho J$, and vice versa. For 5, note that if $r \in \rho^i J$ for all i, then r is the right endpoint of J.

Now suppose that C is a c-downset. We first show that the intersection of the intervals $J \in C$ is equal to $\{r\}$ for some real number r. Since from 1 there are arbitrarily small intervals in C, it suffices to check the finite intersection property. So let F be a finite set of nodes of C. If there is a node J in C above all these nodes, then J is contained in I for all $I \in F$, so the intersection is nonempty. Otherwise, by 6, there are two nodes in F with no join in T. By 2 this can only happen if there are three adjacent nodes in C, in which case there is a dyadic rational in all the intervals corresponding to nodes of I.

We want to show that $C = C_r$. As $r \in J$ for every $J \in C$, we have $C \subset C_r$. We must show that if $r \in J$, then $J \in C$. By 3 it suffices to assume $J \notin C$ and derive a contradiction. There is some node I at the level of J that is in C. So $I \neq J$, by the assumption, and also $r \in I$. If the node I is not next to J, then r is the dyadic rational which is the common endpoint of I and J . This contradicts 5: all the children of I in C must lean toward J because they all contain r, so by 5 there are three adjacent nodes in C. So I and J are next to each other. Similarly, if I's other neighbor K were in C, then all of K's children must lean toward J, contradicting 5. By the adjacency of the nodes in C (property 2) I is the only node in C at that level. But that also can't happen: If $\lambda I \in C$ then I's left neighbor is in C by downward closure, so $\lambda I \notin C$. Symmetrically, $\rho I \notin C$. By 4, both ρI and λI are in C, the final contradiction.

Since every c-downset is of the form C_r, the function is onto. It's one-to-one, because if $r \neq r'$ then $C_r \neq C_{r'}$. ∎

If r is a real number, then the infinite paths in C_r correspond exactly to the *signed-bit representations* of r. Of course we may not be able to find any such path in the absence of choice. With choice, property 1 guarantees that every node of C_r is contained in some infinite path. The midpoints of the nodes of an infinite path in C_r form a sequence which is exactly what Heyting [7] calls a *canonical number-generator*, so we see that the latter is essentially a signed-digit representation.

Theorem 2.5 *For each real number r, the following are equivalent:*

1. *O_r is countable*
2. *O_r contains an infinite path*
3. *C_r contains an infinite path*
4. *r is a regular real number.*

Proof: 1) implies 2): Starting from any node in O_r, taking the first child and first parent in the counting of O_r produces an infinite path.

2) implies 3): $O_r \subset C_r$.

3) implies 4): The midpoints of the intervals of any infinite path in C_r form a regular sequence converging to r.

4) implies 1): Let J be some node in O_r. Let J_n be a counting of J's siblings and their descendants such that each node occurs infinitely often. Let c_m be a sequence of rational numbers so that $|c_m - r| \leq 1/m$. At stage i, let $s_i = J_i$ if the closed interval $[c_i - 1/i,\ c_i + 1/i]$ is contained in J_i, undefined otherwise. This gives a function s from a detachable subset of $\mathbb{N}$ onto that part of O_r at J's level and beyond, so the latter is countable by definition. It is easy to alter that counting to include their ancestors too. ∎

Note that the conditions in Theorem 2.5 are not equivalent to C_r's being countable:

Theorem 2.6 *If C_r is countable for all regular real numbers r, then for each binary sequence α, there exists a binary sequence β such that $\alpha_m = 0$ for all m if and only if $\beta_m = 1$ for some m.*

Proof: Let α be a binary sequence and set $r = \sum \alpha_m/2^m$. Let $C_r = \{c_1, c_2, c_3, \ldots\}$. Define $\beta_m = 1$ if $c_m = (-1, 0)$, and $\beta_m = 0$ otherwise. Note $a_m = 0$ for all m if and only if $r = 0$. If $r = 0$, then $(-1, 0) \in C_r$ so $\beta_m = 1$ for some m. Conversely, if $(-1, 0) \in C_r$, then $r \leq 0$, hence $r = 0$. ∎

The conclusion of Theorem 2.6 is a form of the weak Kripke schema [13, p. 241]. This conclusion, together with MP (Markov's Principle), implies LPO (the limited principle of omniscience): any binary sequence α either contains a one or is all zeros. Indeed, because the sequence $\alpha + \beta$ cannot be all zeros, by MP it must contain a nonzero element $\alpha_m + \beta_m$; if $\alpha_m = 1$ than α contains a 1, and if $\beta_m = 1$ then α is all 0s. Since MP holds in the recursive interpretation of constructive mathematics, the conclusion of Theorem 2.6 would imply the solvability of the halting problem. Hence in the recursive interpretation the conditions of Theorem 2.5 are not equivalent to C_r's being countable. It would be nice to have a clean characterization of those real numbers r for which C_r is countable.

For arbitrary Cauchy real numbers the situation is a bit more complicated. We say that a subset S of T is a *Cauchy subset* if it is closed downwards, contains nodes from arbitrarily high levels, and for all p there is a level l such that $|j/2^s - k/2^t| < 2^{-p}$ for all nodes $(j/2^s, (j+2)/2^s)$ and $(k/2^t, (k+2)/2^t)$ beyond l in S. The first clause in that definition says that S is a downset, the second that S is unbounded. The last says that S converges: given p and l as in the last clause, and $(j/2^s, (j+2)/2^s)$ with $s > l$, then $(j+1)/2^s$ is within $2^{-p} + 2^{-l}$ of the limit of S. So a Cauchy subset is an unbounded, convergent downset.

Examples of Cauchy subsets S of T are O_r and C_r. More generally, S might also contain bounded branches or subsets that peter out at a certain point.

It is not hard to see that $O_r \subseteq S$, for the real number r to which S converges. Hence O_r is the intersection of all the Cauchy subsets converging to r. As for C_r, say that a subset S of T is *unblocked* if every node in S has a child in S. Both O_r and C_r are unblocked. We can characterize C_r as the biggest unblocked Cauchy subset that converges to r.

Theorem 2.7 *Any unblocked Cauchy subset of T that converges to r is contained in C_r. So C_r is the union of all unblocked Cauchy subsets that converge to r.*

Proof: Let S be an unblocked subset that converges to r, let $I \in S$. We must show that $r \in \overline{I}$. As S is unblocked, I has descendants – subsets – at every level beyond I's and these get arbitrarily close to r. Thus there are elements in I that are arbitrarily close to r. As $\overline{I}$ is closed, this means that $r \in \overline{I}$. ▮

As for the Cauchy real numbers themselves:

Theorem 2.8 *A real number r is a Cauchy real number if and only if O_r is contained in a countable Cauchy subset of T.*

Proof: Suppose r is a Cauchy real number, say the limit of the sequence of rational numbers c_n. Let $J_n = (k/2^n, (k+2)/2^n)$ where k is the greatest integer such that $k/2^n \leq c_n$. Then J_n is a node at level n in T, and the sequence J_n converges to r. Let S be the downset generated by the terms in the sequence J_n. Conversely, suppose O_r is contained in a countable Cauchy subset S. Then S converges to r and if we let c_n be the midpoint of the first element of S at level n, then c_n converges to r. ▮

3 Choice principles

We have looked at three kinds of real numbers: Dedekind real numbers, Cauchy real numbers, and regular real numbers. It is easy to see that with Countable Choice we can show that these are the same: we can build a Cauchy sequence from a Dedekind cut by countably many choices of rationals, and we can build a modulus of convergence for a Cauchy sequence, by making an appropriate countable sequence of choices of integers. In fact, since the choices made are either of a rational number or an integer, we need only make countably many choices from a countable set, an axiom variously called AC-NN, AC_{00}, and $\mathrm{AC}_{\omega\omega}$. In fact, we can get by on even less:

Theorem 3.1 *The following choice principles are equivalent:*

1. *$\mathrm{AC}_{\omega 2}$: Given a sequence S_n of nonempty subsets of $\{0, 1\}$, there exists a binary sequence a_n such that $a_n \in S_n$.*

2. *$AC_{\omega b}$ for all b: For any positive integer b and sequence S_n of nonempty subsets of $\{0, \ldots, b-1\}$, there exists a sequence $a_n \in \{0, \ldots, b-1\}$ such that $a_n \in S_n$.*

3. *Given a sequence S_n of nonempty subsets of $\mathbb{Z}$ of uniformly bounded lengths (diameters), there exists a sequence $a_n \in \mathbb{Z}$ such that $a_n \in S_n$.*

Proof: To go from 1 to 2, we induct on b. Certainly 2 holds for $b = 1$. If $b > 1$, let $\varphi : \{0, \ldots, b\} \to \{0, \ldots, b-1\}$ be the retraction that takes b to $b-1$. Let $T_n = \varphi(S_n)$. Then we apply induction to get a sequence $t_n \in T_n$, and apply 1 to get a sequence $a_n \in \varphi^{-1}(t_n)$.

The length of a subset S of $\mathbb{Z}$ is bounded by b if the difference of any two elements of S is at most b. To go from 2 to 3, let b be a bound on the lengths of the S_n, and look at the images of S_n modulo $b+1$ considered as subsets of $\{0, \ldots, b\}$. So we get a sequence $a_n \in \{0, \ldots, b\}$ so that each S_n contains an element congruent to a_n modulo $b+1$. But that element of S_n is unique.

Of course 3 implies 1. ▮

Clearly $AC_{\omega\omega}$ implies the properties above. To refine the matter even more, let $AC_{\omega,<\omega}$ be the statement that there is a choice function for the sequence S_n, where each S_n is a bounded set of natural numbers, while perhaps not uniformly so. Then $AC_{\omega\omega}$ implies $AC_{\omega,<\omega}$, which in turn implies $AC_{\omega 2}$. The reason we are looking at this is:

Corollary 3.2 *$AC_{\omega 2}$ implies that every real number is regular.*

Proof: Let r be a real number. We will construct a sequence a_n of rational numbers such that $|r - a_n| \leq 1/n$. To this end, let $S_n = \{m \in \mathbb{Z} : |r - m/n| \leq 1/n\}$. Then S_n is nonempty: since r is real, there is a rational q within $1/2n$ of r, meaning that r is in the open interval $(q - 1/2n, q + 1/2n)$; the closed interval $[q - 1/2n, q + 1/2n]$ contains either one or two fractions of the form m/n; and the numerator of any such fraction will be in S_n. Also, S_n is of length at most 2: suppose $|r - j/n|, |r - k/n| \leq 1/n$, with $j < k$. From the first inequality, $r \in [(j-1)/n, (j+1)/n]$, and from the second $r \in [(k-1)/n, (k+1)/n]$. Hence those intervals must overlap, and so $k - 1 \leq j + 1$, or $k - j \leq 2$.

Applying (the third version of) $AC_{\omega 2}$, we get a sequence m_n; $a_n = m_n/n$ is as desired. ▮

Presumably we could get by with something less than $AC_{\omega 2}$, since it seems unlikely that $AC_{\omega 2}$ would follow from every Dedekind real number's being a Cauchy real number, every Cauchy real number's being a regular real number, or anything similar. On the other hand, some kind of choice is necessary, as those equivalences are not theorems in IZF (see [9]). So exactly what choice principles are those statements about the real numbers equivalent to? Well, they themselves could be taken as choice principles.

Moreover, it might well be that among all equivalent formulations, those are the simplest, and so are the best formulations of some weak choice principles. Still, it might be useful to have different formulations, and the versions in terms of the pseudotree T follow immediately from the work of the previous section.

Corollary 3.3 *Every real number is a Cauchy real number if and only if every o-ideal of T is contained in a countable Cauchy subset of T.*

Corollary 3.4 *Every Cauchy real number is regular if and only if every countable Cauchy subset of T contains an infinite path.*

4 Riesz spaces

By a *Riesz space* we mean a lattice-ordered vector space V over the rational numbers. We assume that V has a *unit*: a distinguished element 1 such that if $x \in V$, then $x \leq n1$ for some natural number n. If V is nontrivial, then $q \mapsto q1$ gives an embedding of the rational numbers into V. We will identify a rational number q with its image $q1$ in V and write $x < q$ to mean that $x \leq q'$ for some rational number $q' < q$.

For $x \in V$, let $x^+ = x \vee 0$ and $x^- = -x \vee 0$. It follows that $x = x^+ - x^-$. Also, let $|x| = x^+ + x^- \geq 0$. We say that an element $x \in V$ is an *infinitesimal* if $|x| \leq q1$ for every positive rational number q, and that V is *archimedean* if its only infinitesimal element is zero. Note that $\mathbb{R}$ is an archimedean Riesz space.

Although the field of scalars for a Riesz space is usually taken to be $\mathbb{R}$ rather than $\mathbb{Q}$, the latter choice results in a more general structure for the purpose of constructing homomorphisms into $\mathbb{R}$, our ultimate interest. That's because any Riesz $\mathbb{Q}$-homomorphism from a Riesz space over $\mathbb{R}$ into $\mathbb{R}$ is also an $\mathbb{R}$-homomorphism.

Theorem 4.1 *Let V and W be Riesz spaces over $\mathbb{R}$. If W is archimedean, then any Riesz homomorphism from V to W over $\mathbb{Q}$ is a homomorphism over $\mathbb{R}$.*

Proof: Let $f : V \to W$ be a Riesz homomorphism over $\mathbb{Q}$. For $x \in V$ and $r \in \mathbb{R}$ we must show that $f(rx) = rf(x)$. As x is the difference of two positive elements of V, we may assume that $x \geq 0$, so $f(x) \geq 0$. Let p and q be arbitrary rational numbers such that $p \leq r \leq q$. Then $px \leq rx \leq qx$ so $pf(x) \leq f(rx) \leq qf(x)$ and $pf(x) \leq rf(x) \leq qf(x)$. It follows that

$$(p-q)f(x) \leq f(rx) - rf(x) \leq (q-p)f(x)$$

Because $|q - p|$ can be arbitrarily small, and W is archimedean, this implies that $f(rx) = rf(x)$. ∎

We cannot eliminate the condition that W be archimedean from this theorem because of the following classical counterexample. Let $V = \mathbb{R} \times \mathbb{R}$ with the lexicographic order. Note that we cannot find a constructive proof of the existence of the join of two elements in V. Let $g : \mathbb{R} \to \mathbb{R}$ be a linear transformation over $\mathbb{Q}$ and define $f : V \to V$

by $f(x, y) = (x, g(x) + y)$. It is easy to see that f is a Riesz homomorphism over $\mathbb{Q}$, and that f is a homomorphism over $\mathbb{R}$ if and only if g is a linear transformation over $\mathbb{R}$.

The canonical example of an archimedean Riesz space is a space E of bounded real-valued functions on a set X that contains the constant function 1. Evaluation at a point of X is a Riesz homomorphism from E into $\mathbb{R}$. The set of homomorphisms from a Riesz space to $\mathbb{R}$ has a natural topology and is often called the *spectrum* of the Riesz space [4, 6].

Conversely, any archimedean Riesz space V can be embedded as a subspace of the space of real-valued continuous functions on its spectrum (the Stone-Yosida representation theorem). The embedding of V takes $a \in V$ to the function $\hat{a}(\sigma) = \sigma(a)$. This is why we are interested in homomorphisms of V into $\mathbb{R}$. The standard proofs of the Stone-Yosida theorem are not constructive as they rely heavily on both the law of excluded middle and the axiom of choice.

Following [4], let $U(a) = \{q \in \mathbb{Q} \mid a < q\}$. The set $U(a)$ is an upper cut in the rational numbers, but need not be located, so might not correspond to a real number. Still, $U(a)$ has many of the characteristics of a real number (and so is sometimes called an *upper real number*, for instance in [4]). For instance, for p rational, we will have need of the predicates $p \leq U(a)$, which means $p \leq q$ for all $q \in U(a)$, and $p < U(a)$, which means that $p < q \leq U(a)$ for some rational number q.

If $U(a)$ is located, then it is the upper cut of a (Dedekind) real number $\sup(a)$. If $U(a)$ is located for every $a \in V$, then $\sup(|\cdot|)$ is a seminorm on V. This will be a norm exactly when V is archimedean.

If I is the interval (p, q), then we let the string of symbols "$a \in I$" denote the Riesz space element $(a - p) \wedge (q - a)$. We will be working with the predicate Pos(a) = "$0 < U(a)$", even if $U(a)$ is not located. Note that if V is a function space, with 1 the constant function with value 1, then classically Pos($a \in I$) exactly when a takes on a value in I.

We denote the set of functions from A to B by ${}^{A}B$. If B is a partially ordered set, and $f_i \in {}^{A_i}B$, then we set $f_1 \leq f_2$ if $A_1 \subseteq A_2$ and $f_1(a) \leq f_2(a)$ for all $a \in A_1$.

Definition 4.2 *Let X be a set and χ a set of functions from finite subsets of X to T.*

a) We say that χ is **well-formed***, and that X is the domain of χ, if*

- $X = \bigcup_{\mathbf{I} \in \chi} dom(\mathbf{I})$*, and*
- *χ is closed downwards.*

b) A well-formed χ is **extendible** *if, for all $\mathbf{I} \in \chi$, $u \in X$, and $n \in \mathbb{N}$, there is a $\mathbf{J} \in \chi$ extending $\mathbf{I}$ with $u \in$ dom($\mathbf{J}$) and level(J_u) $\geq n$.*

c) Let X be a subset of a Riesz space V. The **signed-bit representation** *of X, with notation X_T, is the subset of $\bigcup_Y {}^{Y}T$, as Y ranges over all finite subsets of X, such that $\mathbf{I}$ = $(I_y)_{y \in Y} \in X_T$ iff Pos($\bigwedge_{y \in Y} y \in I_y$).*

It is immediate that the signed-bit representation X_T is well-formed, with domain X. The essence of the Coquand-Spitters construction is that, if $U(a)$ is located for all

$a \in V$, then V_T is also extendible. The way they use this is to build Riesz homomorphisms of a separable Riesz space V into $\mathbb{R}$ (there called *representations*), as follows. They take X to be a countable dense subset of V and let $\mathbf{I}$ be any starting point in X_T. Using DC, they then extend $\mathbf{I}$ to all levels and to include all of X, yielding a homomorphism of X, which, by density, can be extended uniquely to all of V.

Definition 4.3 *An o-ideal through χ is an assignment of an o-ideal r_x through T to each x in the domain X of χ such that, for all $\mathbf{I} = (I_y)_{y \in Y} \in \Pi_y r_y$, $\mathbf{I} \in \chi$.*

Theorem 4.4 *There is a canonical bijection between Riesz homomorphisms of V into $\mathbb{R}$ and o-ideals through V_T.*

Proof: By results of the section 2, an o-ideal can be considered to be a real number. So both homomorphisms of V into $\mathbb{R}$ and o-ideals through V_T are assignments of real numbers to the members of V. The coherence conditions on a Riesz homomorphism correspond to the positivity predicate in the definition of the extendible set V_T.

The main technical lemma needed is that, if f is such a homomorphism, and $f(a) > 0$, then Pos(a). So let q be such that $f(a) \geq q > 0$. Suppose $r \in U(a)$. Then $r > a$, and $r = f(r) \geq f(a) \geq q > 0$, as desired.

In some detail, let $f : V \to \mathbb{R}$ be a Riesz homomorphism. The induced o-ideal is given by $x \mapsto O_{f(x)}$. (Recall that O_r is the o-ideal corresponding to r.) We must show that this is through V_T, which means that if $I_y \in O_{f(y)}$ for each y in a finite set Y then $(I_y)_{y \in Y} \in V_T$. And that means Pos($\bigwedge_{y \in Y} y \in I_y$). By the lemma, it suffices to show that $f(\bigwedge_{y \in Y} y \in I_y) > 0$. Because f is a homomorphism, the left-hand side equals $\bigwedge_{y \in Y} f(y \in I_y)$. The infinimum of a finite set of real numbers is positive if and only if each of those reals is positive. So we need to show that $I \in O_{f(y)}$ implies $f(y \in I) > 0$. Recall that $I \in O_r$ iff $r \in I$ iff $\inf I < r < \sup I$. Also recall that $y \in I$ is an abbreviation for $y - \inf I \wedge \sup I - y$. So what we need to show is that $\inf I < f(y) < \sup I$ implies $f(y - \inf I \wedge \sup I - y) > 0$. Again using that f is a homomorphism, the latter assertion reduces to $f(y) - \inf I > 0$ and $\sup I - f(y) > 0$, which is exactly the hypothesis.

In the other direction, suppose that $x \mapsto O_{r_x}$ is an o-ideal through V_T. Let $f(x) = r_x$. We must show that f is a Riesz homomorphism: $f(x+y) = f(x)+f(y)$, $f(rx) = rf(x)$, $f(1) = 1$, and $f(x \wedge y) = f(x) \wedge f(y)$. We will prove the first statement, and leave the others, all similar, to the reader.

Given $\epsilon > 0$, let $1/2^n < \epsilon/4$ and $I_x \in O_{r_x}, I_y \in O_{r_y}$ have length $1/2^n$. Then the interval $I_x + I_y$ has length less than $\epsilon/2$. We claim that any $I \in O_{r_{x+y}}$ has to have a non-empty intersection with $I_x + I_y$. To this end, let $I \in O_{r_{x+y}}$. Because we're dealing with intervals with rational endpoints, we can assume that the intersection is empty and come up with a contradiction. For the intersection to be empty, either $\inf I \geq \sup(I_x) + \sup(I_y)$ or $\sup I \leq \inf(I_x) + \inf(I_y)$; we will consider the former case only. Because the system O_{r_x} is an o-ideal through V_T, we have that the triple (I_x, I_y, I) is in V_T, i.e. Pos($x \in I_x \wedge y \in I_y \wedge x + y \in I$). Unpacking that Riesz space element, we get Pos($x - \inf(I_x) \wedge \sup(I_x) - x \wedge y - \inf(I_y) \wedge \sup(I_y) - y \wedge (x + y) - \inf I \wedge \sup I - (x + y)$). That latter Riesz space element is less than or equal to $\sup(I_x) - x \wedge \sup(I_y) - y \wedge (x + y) - \inf I$, which, by the case hypothesis, is less than or equal to $\sup(I_x) - x \wedge \sup(I_y) - y \wedge (x+y) - (\sup(I_x) + \sup(I_y))$. This last element is of the form $e \wedge f \wedge (-e-f)$, which can be shown by elementary Riesz space considerations to be ≤ 0, in other words not $\text{Pos}(e \wedge f \wedge (-e-f))$, which is the desired contradiction.

Now pick an interval I in $O_{r_{x+y}}$ of length less than $\epsilon/2$. This I, which contains $f(x+y)$, overlaps $I_x + I_y$, which contains $f(x) + f(y)$, so $f(x+y)$ is within ϵ of $f(x) + f(y)$. ∎

So by converting a real number to a substructure of the tree-like partial order T, homomorphisms of V are converted to substructures of products of T. Similar theorems hold for other natural substructures of T.

Definition 4.5 *An o-ideal through χ is countable if each r_x is countable.*

Theorem 4.6 *There is a canonical bijection between Riesz homomorphisms of V into the regular real numbers and countable o-ideals through V_T.*

Definition 4.7 *An o-ideal through χ is countably extendible if each r_x is a subset of a countable Cauchy subtree of T.*

Theorem 4.8 *There is a canonical bijection between Riesz homomorphisms of R into the Cauchy real numbers and countably extendible o-ideals through V_T.*

The proofs here are the same as in theorem 4.4, with the additional observation that, when transforming Riesz homomorphisms into o-ideals and vice versa, Cauchy reals are taken to Cauchy reals and regular reals to regular reals.

Similar considerations apply to extending Riesz homomorphisms from dense subsets. That is, suppose X is a dense subset of a Riesz space V. Then it makes no sense in general to talk about a Riesz homomorphism of X, since X might not even be a Riesz space. However, X_T contains the nearness information about V, so that an o-ideal through X_T induces a homomorphism of V. In fact, these observations could be combined with those above, so that X need be taken only as a Riesz generating subset of a dense set, for instance as the members of a dense set between 0 and 1. Then an o-ideal through X_T is canonically extendible to the generated Riesz space, which by density could be extended to one through the whole Riesz space.

When extending homomorphisms this way, you no longer have a choice of what kind of real numbers to use. That is, when dealing with only Riesz-space structure (addition, scalar multiplication, and sup), the corresponding operations on real numbers never take you outside of any given class of real numbers: the sum of two countable o-ideals is again countable, as is any multiple or sup of such, and so on. However, the same no longer applies to limits when dealing with density. A limit or accumulation point may not have any countable sequence approaching it, so it should be clear that attaching a Cauchy sequence, even if regular, to dense many points in a neighborhood will not necessarily yield a Cauchy sequence at the given point. Worse yet, even if we had that every point in V were the limit of a countable sequence from X, there would still be problems going from Cauchy sequences on X to ones on all of V: choosing a limiting sequence, choosing a Cauchy sequence for each point in the sequence, etc. (For similar issues in the simpler context of the real numbers alone, see [9].) So the best we really can say is that any kind of o-ideal on X_T induces simply an o-ideal on V_T, i.e. a Riesz homomorphism of V into the Dedekind real numbers.

These considerations lead to the following

Theorem 4.9 *If every extendible χ with X of cardinality κ has an o-ideal, then every seminormed Riesz space with a dense subset of cardinality κ has a Riesz homomorphism into $\mathbb{R}$.*

By cardinality here, we mean simply the Cantorian theory of equinumerosity. So κ is simply a set, and a set X has cardinality κ if it can be put into one-to-one correspondence with κ. The latter principle has the flavor of a restricted form of Martin's Axiom, hence the following definition.

Definition 4.10 *Martin's Axiom for o-ideals of cardinality κ, written $MA_{o\text{-}id(\kappa)}$, is the assertion that every extendible χ with X of cardinality κ has an o-ideal.*

One possible benefit of the reformulation of the existence of such homomorphisms as $\mathrm{MA}_{\text{o-id}(\kappa)}$ is that it can help show that such homomorphisms do not exist. In [4], Coquand and Spitters show, under DC, that every separable, seminormed V has a Riesz homomorphism into $\mathbb{R}$, essentially by showing $\mathrm{MA}_{\text{o-id}(\omega)}$. Of course, they don't refer to signed-bit representations, and their definition of *countable* is broader than "equinumerous with ω", as is standard in constructive analysis (see [3]). They then ask whether DC is necessary. One way to approach that problem is to find a model in which $\mathrm{MA}_{\text{o-id}(\omega)}$ fails in such a way that an equivalent Riesz space can be constructed from this failure. In fact, this project was carried out. It was later simplified [8] to refer not to T and its paths but more simply to $\mathbb{R}$, which is better understood.

A limitation of the last theorem is that it is not a biconditional. Indeed, we could not find any equivalence between well-formed sets, possibly with extra conditions, on the one hand, and any kind of Riesz spaces on the other. In the current formulation, for instance, having Riesz homomorphisms into $\mathbb{R}$ for every Riesz space might not be enough to get o-ideals through all extendible χs, because χ might not correspond to a Riesz space. Furthermore, there seems to be no elegant formulation of a well-formed χ coming from a Riesz space. One could consider instead all extendible χs, with domain X, and extend X to a Riesz space V so that the signed-bit representation of X is exactly χ. The problem there is guaranteeing that V is seminormed, with again apparently no nice way of identifying those χs for which the induced V is seminormed. One could try to be more general, and eliminate the restriction of V being seminormed. There are examples of function spaces that are not seminormed for which the signed-bit representation is not extendible. You might then think to eliminate the requirement of extendibility. But then there are problems representing faithfully partial information about a Riesz space in a well-formed set. In the end, it remains unclear what an exact correspondence here would be. It would be interesting to see such a theorem.

References

[1] ARCHIBALD, MARGARET, VASCO BRATTKA, AND CLEMENS HEUBERGER, Randomness with respect to the signed-digit representation, *Fundamenta Informaticae*, **83** (2008), p. 1–19

[2] BARONI, M. A., *Constructive Aspects of Riesz Spaces with Applications in Economics*, Ph.D. thesis, 2004

[3] BISHOP, ERRETT, *Foundations of Constructive Analysis*, McGraw-Hill, 1967

[4] COQUAND, THIERRY AND BAS SPITTERS, Formal topology and constructive mathematics: the Gelfand and Stone-Yosida representation theorems, *Journal of Universal Computer Science*, **11** (2005), p. 1932–1944

[5] FOURMAN, M. P. AND J.M.E. HYLAND, Sheaf models for analysis, in Fourman, M. P., C.J. Mulvey and D.S. Scott (eds.), *Applications of Sheaves, Lecture Notes in Mathematics Vol. 753* Springer 1979, 280-301

[6] D.H. FREMLIN, *Measure Theory, Vol. 3*, Torres Fremlin, Colchester, 2002

[7] HEYTING, AREND, *Intuitionism, an Introduction*, North Holland 1956

[8] LUBARSKY, ROBERT S., Geometric spaces with no points, preprint available at http://math.fau.edu/lubarsky/pubs.html

[9] LUBARSKY, ROBERT S., On the Cauchy completeness of the constructive Cauchy reals, *Mathematical Logic Quarterly*, **53** (2007), p. 396–414

[10] LUBARSKY, ROBERT S., AND FRED RICHMAN, Zero sets of univariate polynomials, *Trans. Amer. Math. Soc.*, to appear

[11] RICHMAN, FRED, The fundamental theorem of algebra: a constructive development without choice, *Pacific J. Math.*, **196** (2000), p. 213–230

[12] RUITENBURG, WIM, Constructing roots of polynomials over the complex numbers, *Computational Aspects of Lie Group Representations and Related Topics* (Amsterdam 1996) p. 107–128, CWI Tract, **84**, Math. Centrum, Centrum Wisk. Inform., Amsterdam 1991

[13] TROELSTRA, ANNE S. AND DIRK VAN DALEN, *Constructivism in Mathematics, Vol. 1* (North Holland, Amsterdam New York Oxford Tokyo, 1988)

[14] WEIHRAUCH, K., *Computable Analysis*, (Springer, Berlin, 2000)