Constructive Solutions of Continuous Equations

Peter Schuster and Helmut Schwichtenberg
Mathematisches Institut, Universität München
Theresienstraße 39, D-80333 München
{pschust,schwicht}@mathematik.uni-muenchen.de

April 2, 2003

Abstract

We modify some seminal notions from constructive analysis, by providing witnesses for (strictly) positive quantifiers occurring in their definitions. For instance, we understand a real number as nothing but a modulated CAUCHY sequence of rationals. This approach allows us to avoid many of the putatively necessary invocations of countable choice. From this point of view some basic machinery of constructive analysis is recalled and explicated; this includes choice-free proofs of sequential and order completeness of the real numbers, and of the approximate intermediate value theorem. Moreover, we unwind the KNESER proof of the fundamental theorem of algebra, by giving a (rather detailed) choice-free proof.

1 Introduction

Since its conception in BISHOP's seminal monograph [3], constructive analysis has attracted the attention of many researchers. It particular, it was and is a challenge to design logical systems which allow for a smooth formalization. There are obvious reasons why one wants to get clear about the possibility of such formalizations, among them the prospect to use formal proofs of existential theorems as a means to develop correct programs, in this case involving exact real numbers.

For such purposes it is of importance that the system does not include (countable or dependent) choice axioms. The aim of the present paper is to sketch the development of elementary constructive analysis on this basis, up to and including the fundamental theorem of algebra. The key for such a choice-free treatment is to provide witnesses of (strictly) positive existential quantifiers in all definitions.

2 Elementary Constructive Analysis

We understand real numbers as modulated CAUCHY sequences of rationals.[1] So a *real number,* or simply *real*, is nothing but a sequence $(a_m)_{m\in\mathbb{N}}$ of rational

[1] Inasmuch as we do not focus on fixed moduli, we deviate from [2, 3, 21]. An approach similar to the present one was chosen in [22, 16].

numbers together with a modulus $M\colon \mathbb{Q}^+ \to \mathbb{N}$ such that $|a_m - a_n| \le \varepsilon$ for $m,n \ge M(\varepsilon)$. Let us stress that throughout we strictly identify the notions "real number" and "modulated CAUCHY sequence of rationals" with each other, even though we sometimes say that an instance of the latter represents, gives, or defines the corresponding instance of the former. As usual, we denote the set[2] of real numbers by $\mathbb{R}$.

Every rational q is tacitly understood as the real represented by the constant sequence $a_m = q$ with the constant modulus $M(\varepsilon) = 1$. For any rational q with $|q| < 1$, a less trivial representation of a real (in fact, of the rational $\frac{1}{1-q}$) is that given by the partial sums $a_n = \sum_{i=0}^n q^i$ of the geometric series: as $|a_m - a_n| \le \frac{2}{|1-q|}|q|^{n+1}$ whenever $m \ge n$, an appropriate modulus is $M(\varepsilon) = \min\{\, n \in \mathbb{N} \mid |q|^{n+1} \le \frac{|1-q|}{2}\varepsilon \,\}$.

A real a is *nonnegative* (written $a \in \mathbb{R}^{0+}$) if $-\varepsilon \le a_{M(\varepsilon)}$ for all rationals $\varepsilon > 0$, and *positive* (written $a \in \mathbb{R}^+$) if $\varepsilon \le a_{M(\frac{\varepsilon}{2})}$ for some rational $\varepsilon > 0$. For every rational $\varepsilon > 0$ that ensures $a \in \mathbb{R}^+$ as in the definition thereof, we write $a \in_\varepsilon \mathbb{R}^+$. So if $a \in_\varepsilon \mathbb{R}^+$, then $a_m \ge \frac{\varepsilon}{2}$ for all $m \ge M(\frac{\varepsilon}{2})$.

Given real numbers a, b represented by sequences of rationals $(a_m)_{m\in\mathbb{N}}$, $(b_m)_{m\in\mathbb{N}}$ with moduli M, N, we define each c from the list $a+b$, $-a$, $|a|$, $a \cdot b$, and $\frac{1}{a}$ (the latter only provided that $|a| \in_\eta \mathbb{R}^+$) as represented by the respective sequence (c_m) of rationals with modulus L:

c	c_m	$L(\varepsilon)$
$a+b$	$a_m + b_m$	$\max\{M(\frac{\varepsilon}{2}), N(\frac{\varepsilon}{2})\}$
$-a$	$-a_m$	$M(\frac{\varepsilon}{2})$
$\|a\|$	$\|a_m\|$	$M(\varepsilon)$
$a \cdot b$	$a_m \cdot b_m$	$\max\left\{M\left(\frac{\varepsilon}{2K_{\|b\|}}\right), N\left(\frac{\varepsilon}{2K_{\|a\|}}\right)\right\}$
$\frac{1}{a}$ for $\|a\| \in_\eta \mathbb{R}^+$	$\begin{cases} \frac{1}{a_m} & \text{if } a_m \neq 0 \\ 0 & \text{if } a_m = 0 \end{cases}$	$\max\left\{M(\frac{\eta}{2}), N(\frac{\varepsilon\eta^2}{4})\right\}$

where the rational number $K_a = \max\{\, a_n \mid n \le M(1) \,\} + 1$ is so that $a_m \le K_a$ for all $m \in \mathbb{N}$. Needless to say, $a - b$ and $\frac{a}{b}$ (for $b \in \mathbb{R}^+$) stand for $a + (-b)$ and $a \cdot \frac{1}{b}$, respectively.

We write $a \le b$ for $b - a \in \mathbb{R}^{0+}$ and $a < b$ for $b - a \in \mathbb{R}^+$. Unwinding the definitions yields that $a \le b$ is to say that for every rational $\eta > 0$ there exists $P_\eta \in \mathbb{N}$ such that $a_m \le b_m + \eta$ for all $m \ge P_\eta$. Furthermore, $a < b$ is a shorthand for the presence of a rational $\eta > 0$ and a positive integer Q with $a_m + \eta \le b_m$ for all $m \ge Q$; we then write $a <_{\eta,Q} b$ (or simply $a <_\eta b$ if Q is not needed) whenever we want to call these witnesses.

Constructively, equality $a = b$ and inequality $a \neq b$ between real numbers are to be defined as $a \ge b \wedge a \le b$ and $a < b \vee a > b$, respectively. Some routine proofs show that the arithmetic of real numbers respects equality. Moreover, $a \le b$ could equivalently be defined as $\neg(a > b)$, and $a = b$ as $\neg(a \neq b)$, whereas $a < b$ and $a \neq b$ are constructively stronger than $\neg(a \ge b)$ and $\neg(a = b)$, respectively.[3] Intervals are then defined in the familiar way, so $[a, b]$ as the set $\{\, c \in \mathbb{R} \mid a \le c \le b \,\}$.

[2] As we hesitate to devote ourselves to a set theory whatsoever, we wish to understand each set identified with the defining property of its elements.

[3] This is clear in view of the existential and universal character of the predicates $\in \mathbb{R}^+$ and $\in \mathbb{R}^{0+}$, respectively.

Except for the completeness properties which we shall discuss subsequently, it is routine to verify that the reals as defined above possess all the features of the reals that are commonly considered to be constructive [4]. Constructively, in particular, we cannot compare two reals, but can compare each real with every nontrivial interval, as in the following *approximate splitting principle*.

Lemma 1. *For all real numbers a, b, c, if $a < b$, then either $a < c$ or $c < b$.*

Proof. Let M, N, L denote the moduli of a, b, c, respectively, and assume that $a <_{7\eta,P} b$, i.e.

$$a_m + 3\eta < a_m + 4\eta \leq b_m - 3\eta$$

for every $m \geq P$. For $Q = \max\{M(\eta), N(\eta), L(\eta), P\}$, we either have $c_Q < a_Q + 4\eta$ or else $a_Q + 4\eta \leq c_Q$, but not both. In the former case, $c_Q < b_Q - 3\eta$ and thus

$$c_m + \eta \leq c_Q + 2\eta < b_Q - \eta \leq b_m$$

for every $m \geq Q$, which is to say that $c <_{\eta,Q} b$. In the latter case, $a_Q + 3\eta < c_Q$ and thus

$$a_m + \eta \leq a_Q + 2\eta < c_Q - \eta \leq c_m$$

for every $m \geq Q$, which is to say that $a <_{\eta,Q} c$. □

It is noteworthy that although $a < c$ and $c < b$ may well happen simultaneously, the proof of Lemma 1 contains a routine that in every such case automatically pins down one of the alternatives. This virtue, which of course stands and falls with the presence of the moduli for a, b, c and the witness for $a < b$, is of particular relevance whenever the approximate splitting principle is applied infinitely often, e.g. in the proof of Theorem 12 below. By employing that routine, namely, we can avoid the usual invocation of dependent choice to successively construct a sequence of real numbers.

An immediate consequence of Lemma 1 is that $b \leq c$ is to say that $a < b$ implies $a < c$ for all reals c.

For $1 \leq j \leq n$ let a_j be a real number given by the sequence of rationals $(a_{jm})_{m\in\mathbb{N}}$ with modulus M_j. Then the *maximum* $\max\{\, a_j \mid j \leq n \,\}$ is the real number represented by the sequence of rationals $\big(\max\{\, a_{jm} \mid j \leq n \,\}\big)_{m\in\mathbb{N}}$ with modulus $\max\{\, M_j \mid j \leq n \,\}$. Constructively, one cannot pick an index i for which $a_i = \max\{\, a_j \mid j \leq n \,\}$, but for each $\varepsilon > 0$ we can find – as follows – an index i such that a_i is maximal *up to* ε among all the a_j.

Lemma 2. *For all real numbers $a_1, \ldots, a_n$ and each rational $\varepsilon > 0$ we can find an $i \leq n$ so that $a_j \leq a_i + \varepsilon$ for every $j \leq n$.*

Proof. For each $j \leq n$ let a_j be represented by the sequence of rationals $(a_{jm})_{m\in\mathbb{N}}$ with modulus M_j. Given a rational $\varepsilon > 0$, set

$$M = \max\{\, M_j\big(\tfrac{\varepsilon}{2}\big) \mid j \leq n \,\}, \quad b = \max\{\, a_{jM} \mid j \leq n \,\},$$

and

$$i = \min\{\, k \leq n \mid a_{kM} = b \,\}.$$

For each $j \leq n$ we then have

$$a_{jm} \leq a_{jM} + \frac{\varepsilon}{2} \leq a_{iM} + \frac{\varepsilon}{2} \leq a_{im} + \varepsilon$$

for every $m \geq M$, so that $a_j \leq a_i + \varepsilon$ as required. □

As for Lemma 1 above, we wish to stress that by virtue of the presence of moduli the algorithm given through the proof of Lemma 2 always picks a definite index i even when there are several ones fulfilling its specification. This feature again allows to do proofs without countable choice.

Let us now have a look at the completeness properties characteristic for the real numbers. We first consider sequential completeness. A sequence $(a_m)_{m\in\mathbb{N}}$ of reals is a CAUCHY *sequence* with modulus $M\colon \mathbb{Q}^+ \to \mathbb{N}$ whenever $|a_m - a_n| \leq \varepsilon$ for $m, n \geq M(\varepsilon)$, and *converges* with modulus $M\colon \mathbb{Q}^+ \to \mathbb{N}$ to a real b, its *limit*, whenever $|a_m - b| \leq \varepsilon$ for $m \geq M(\varepsilon)$.

Lemma 3. *Every modulated* CAUCHY *sequence of rationals converges with the same modulus to the real number it represents.*

Proof. Let $(a_m)_{m\in\mathbb{N}}$ be a CAUCHY sequence of rationals with modulus M, and let b be the real number it represents. For each rational $\varepsilon > 0$ and every $m \geq M(\varepsilon)$, we have to prove $|a_m - b| \leq \varepsilon$, i.e. $c_m \geq 0$ for $c_m = \varepsilon - |a_m - b|$. Now the real c_m is represented by the sequence $\big(\varepsilon - |a_m - a_k|\big)_{k\in\mathbb{N}}$ of rationals, which again has modulus M: for every rational $\eta > 0$ and all $k, l \geq M(\eta)$, we have

$$|c_k - c_l| = \big||a_m - a_k| - |a_m - a_l|\big| \leq \big|(a_m - a_k) - (a_m - a_l)\big| = |a_k - a_l| \leq \eta.$$

Therefore $c_m \geq 0$ is equivalent to $-\eta \leq \varepsilon - |a_m - a_{M(\eta)}|$ for all rationals $\eta > 0$. This follows from

$$|a_m - a_{M(\eta)}| \leq |a_m - a_{\max\{M(\varepsilon),M(\eta)\}}| + |a_{\max\{M(\varepsilon),M(\eta)\}} - a_{M(\eta)}| \leq \varepsilon + \eta\,,$$

which holds by virtue of $m \geq M(\varepsilon)$. ☐

By the triangle inequality, every convergent sequence of reals with modulus M is a CAUCHY sequence with modulus $\varepsilon \mapsto M(\frac{\varepsilon}{2})$. Writing $\lceil\varepsilon\rceil$ for the least integer $\geq \varepsilon$ whenever $\varepsilon > 0$ is rational, we now prove the reverse implication.[4]

Theorem 4 (Sequential Completeness). *For every modulated* CAUCHY *sequence of reals we can find a real number to which it converges with modulus.*

Proof. Let $(a_m)_{m\in\mathbb{N}}$ be the CAUCHY sequence of reals with modulus M; for every $m \in \mathbb{N}$, let a_m be represented by a CAUCHY sequence $(a_{mk})_{k\in\mathbb{N}}$ of rationals with modulus M_m. Note first that, for each $m \in \mathbb{N}$ and every rational $\eta > 0$, by Lemma 3 we have $|a_m - a_{ml}| \leq \frac{1}{m}$ for all $l \geq M_m(\frac{1}{m})$. Next, set

$$b_m = a_{mM_m\left(\frac{1}{m}\right)}$$

for every $m \in \mathbb{N}$, so that $|a_m - b_m| \leq \frac{1}{m}$ for all $m \in \mathbb{N}$ by the particular case $l = M_m\big(\frac{1}{m}\big)$ of the foregoing consideration. Then

$$|b_m - b_n| \leq |b_m - a_m| + |a_m - a_n| + |a_n - b_n| \leq \frac{1}{m} + \frac{\varepsilon}{2} + \frac{1}{n} \leq \varepsilon$$

for all $m, n \geq N(\varepsilon) = \max\big\{M(\frac{\varepsilon}{2}), \lceil\frac{4}{\varepsilon}\rceil\big\}$, which is to say that (b_m) is a Cauchy sequence with modulus N, and therefore represents a real number b. Moreover,

$$|a_m - b| \leq |a_m - b_m| + |b_m - b| \leq \frac{1}{m} + \frac{\varepsilon}{2} \leq \varepsilon$$

[4] This stems from lecture notes of the second author.

for all $m \geq N(\frac{\varepsilon}{2}) = \max\left\{M(\frac{\varepsilon}{4}), \lceil\frac{8}{\varepsilon}\rceil\right\}$; in other words: (a_m) converges to b with modulus $\varepsilon \mapsto N(\frac{\varepsilon}{2})$. $\square$

This proof happens not to need countable choice but requires a certain conceptual choice made in advance: that each real number is meant to be nothing but a modulated CAUCHY sequences of rationals. Given this presupposition, it seems to cause no reservations from the choice-free perspective that a single sequence of reals is understood as a double sequence of rationals.[5]

On the other hand, countable choice would become indispensable for the proof of sequential completeness as soon as the concept of reals was relaxed either to CAUCHY sequences of rationals without moduli or to equivalence classes, modulo $=$, of modulated CAUCHY sequences of rationals. To start our proof of Theorem 4 in the former case, one had to choose, for every m, the integer l with $|a_m - a_{ml}| \leq \frac{1}{m}$, which in the presence of the modulus M_m of a_m we can simply define by setting $l = M_m(\frac{1}{m})$. In the latter case, one had to choose first, again for every m, a representative $(a_{mk})_{k\in\mathbb{N}}$ of the real a_m, which we already understand as to consist in nothing but such a sequence of rationals.

Following [2, 3, 5] in the style of [18], let us now consider order completeness. To this end, let S be a set of real numbers. A real b is an *upper bound* of S, or S is *bounded from above* by b, whenever $s \leq b$ for all $s \in S$, and a *least upper bound* or *supremum* $\sup S$ of S if, in addition, for every real a with $a < b$ there is an $r \in S$ with $r > a$.[6]

If b is a least upper bound and a an upper bound of S, then $a < b$ is impossible, so that $b \leq a$; whence up to equality there is at most one supremum of S. If S has a supremum, then S is inhabited and bounded from above, but even when S has the two latter properties, the former is not granted constructively. A simple exception is the maximum of finitely many reals (see above), which of course is the supremum thereof.

A more relevant sufficient condition for the constructive existence of the supremum of a general set S of real numbers (being inhabited and bounded from above) it that S be *order located from above*[7], which is to say that

$$\Sigma_S(a,b): \qquad \text{either } s \leq b \text{ for all } s \in S \text{ or } a < r \text{ for some } r \in S$$

holds for all pairs a, b of real numbers with $a < b$. To aim at the sufficiency of these three conditions, it is useful to consider

$$\Pi_S(a,b): \qquad \text{both } s \leq b \text{ for all } s \in S \text{ and } a < r \text{ for some } r \in S$$

as a property of any pair a, b of real numbers with $a < b$. Note that $\Sigma_S(a,b)$ and $\Pi_S(a,b)$ are the disjunction and conjunction, respectively, of the same pair of propositions.

[5] When one wants to read this proof as a completeness proof for the sequential completion of an arbitrary metric space, one again has to view sequences in this completion – the space of (modulated) CAUCHY sequences in the original space – as double sequences in the latter. Any such interpretation may only look somewhat strange in cases which are more complex than that of the completion of the rationals to the reals.

For this observation, and for many others on the role of countable choice in constructive mathematics, the first author is indebted to Fred RICHMAN, for whose position we refer to [15].

[6] This is a positive way to say that every real a with $a < b$, however close it may be to b, is no upper bound of S.

[7] This name was coined in [8]. The same property has been called "located above" by Peter ACZEL and Michael RATHJEN [1], and "lower located" by Erik PALMGREN [11].

Theorem 5 (Order Completeness). *Let $S \subset \mathbb{R}$ be inhabited, bounded from above, and order located from above. Then S has a least upper bound.*

Proof. We may assume that we have $a, b \in \mathbb{Q}$ with $a < b$ such that $\Pi_S(a, b)$. We construct $c, d\colon \mathbb{N} \to \mathbb{Q}$ such that for all m

$$a = c_0 \leq c_1 \leq \cdots \leq c_m < d_m \leq \cdots \leq d_1 \leq d_0 = b, \tag{1}$$

$$\Pi_S(c_m, d_m), \tag{2}$$

$$d_m - c_m \leq \left(\frac{2}{3}\right)^m (b - a). \tag{3}$$

Let $c_0, \ldots, c_m$ and $d_0, \ldots, d_m$ be already constructed such that (3) holds. Let $x = c_m + \frac{1}{3}(d_m - c_m)$ and $y = c_m + \frac{2}{3}(d_m - c_m)$. Since S is order located from above, either $s \leq y$ for all $s \in S$ or else $x < r$ for some $r \in S$. In the first case let $c_{m+1} := c_m$ and $d_{m+1} := y$, and in the second case let $c_{m+1} := x$ and $d_{m+1} := d_m$. Then clearly $\Pi_S(c_{m+1}, d_{m+1})$, and also (1) and (3) continue to hold for $m + 1$. We claim that the real numbers $c = d$ given by the modulated CAUCHY sequence of rationals (c_m) and (d_m) is the least upper bound of S. Indeed, it is an upper bound because for $\varepsilon > 0$ we have $d \leq d_m < d + \varepsilon$ for some m and d_m is an upper bound of S, and similarly $c - \varepsilon < c_m \leq c$ for some m and $c_m < r$ for some $r \in S$. □

One might think that dependent choice has been used this proof: in the case distiction "either $s \leq y$ for all $s \in S$ or else $x < r$ for some $r \in S$" the cases may well overlap. However, reference to the algorithm provided by the assumption that S is order located from above make this choice superfluous.

Another important condition sufficient for the existence of a supremum is that S is a *totally bounded* set of reals. Let us consider this concept next.

To start with, let us call an arbitrary set *finite* if there is a mapping from $\{1, \ldots, n\}$ onto that set with $n \geq 1$; in particular, finite sets are inhabited.[8] A set S of real numbers is *totally bounded* whenever for every (rational) $\varepsilon > 0$ there is an *ε-approximation* to S: that is, a finite subset T of S such that each element of S is within ε of an element of T. Totally bounded sets of real numbers are obviously inhabited and bounded.

Note that the definition of total boundedness involves two witnessing objects: the sequence $(T_m)_{m \geq 1}$ of finite subsets of S so that each T_m is an $\frac{1}{m}$-approximation to S, and also a function assigning to each element of S an ε-close element of T. Notice also that the latter function, having a finite range, is necessarily non-continuous.

Clearly every totally bounded set of reals is order located from above; therefore we immediately obtain from Theorem 5:

Corollary 6. *Every totally bounded set of real numbers has a supremum.*

As a digression, let us recall the standard application of Corollary 6.

Proposition 7. *Let $D \subset \mathbb{R}$ and $f\colon D \to \mathbb{R}$ a uniformly continuous function. If the domain D of f is totally bounded, then so is the range $f(D)$ of f.*

[8] In this respect we follow [2, 3] rather than [5, 10], where finite sets are allowed to be empty. For the sake of simplicity, we also use "finite" instead of the constructively more correct term "finitely enumerable" (due to Ray MINES) or "subfinite" (coined by Errett BISHOP). Usually "finite" is reserved for the sets that are in a bijective correspondence to sets of the form $\{1, \ldots, n\}$, and which necessarily are discrete.

Proof. For $\varepsilon > 0$, pick $\delta > 0$ so that, for all $x, y \in D$, if $|x - y| \leq \delta$, then $|f(x) - f(y)| \leq \varepsilon$. Now if T is a finite δ-approximation to D, then $f(T)$ is a finite ε-approximation to $f(D)$. □

Corollary 8. *If $f\colon D \to \mathbb{R}$ is a uniformly continuous function on a totally bounded subset D of $\mathbb{R}$, then the supremum of $f(D)$ exists.*

In particular, although one cannot expect a constructive method to locate a point in D at which f attains its supremum, for every $\varepsilon > 0$ there is an $x \in D$ so that $\sup f(D) - \varepsilon < f(x)$. Compare this with Lemma 2, and note that the existence of the maximum of finitely many reals is a special case of Corollary 8.

Note that sequential completeness can be deduced from order completeness in a choice-free way [18][9]. However, when one literally transfers that deduction to the present context, it fails to automatically supply the required moduli. As a digression, let us thus provide a better suited argument, which still does not make any use of countable choice.

Reduction of sequential to order completeness. Let $(a_m)_{m\in\mathbb{N}}$ be a Cauchy sequence of real numbers, and define L as the set of all the $p \in \mathbb{Q}$ for which there is an $N \in \mathbb{N}$ so that $p < a_m$ for all $m \geq N$. This L clearly is inhabited and bounded above; we first show that L is order located from above. To this end, let $r < s$ be rational numbers. For $\varepsilon = \frac{s-r}{3}$, we have

$$a_{M(\varepsilon)} - \varepsilon \leq a_m \leq a_{M(\varepsilon)} + \varepsilon \quad \text{for all } m \geq M(\varepsilon),$$

and still $r + \varepsilon < s - \varepsilon$, so that either $r + \varepsilon < a_{M(\varepsilon)}$ or $a_{M(\varepsilon)} < s - \varepsilon$. In the former case, $r < q < a_{M(\varepsilon)} - \varepsilon$ for some $q \in \mathbb{Q}$, for which $q \in L$. In the latter case, $p < s$ for every $p \in L$.

By order completeness, L has a supremum b. To conclude the proof, we now verify that (a_m) converges to b with modulus $\varepsilon \mapsto M\left(\frac{\varepsilon}{2}\right)$. Given a rational $\varepsilon > 0$, pick $p \in L$ with $b - \frac{\varepsilon}{2} < p$, and $N \in \mathbb{N}$ with $p < a_m$ for all $m \geq N$. For $K = \max\left\{N, M\left(\frac{\varepsilon}{2}\right)\right\}$, observe first that $b - \frac{\varepsilon}{2} < a_k$ and thus $b - \varepsilon < a_m$ for all $m \geq M\left(\frac{\varepsilon}{2}\right)$. Assume next that $a_k > b + \frac{\varepsilon}{2}$. Then $a_k - \frac{\varepsilon}{2} > b$, so that $b < p < a_k - \frac{\varepsilon}{2}$ for some rational p, for which, in particular, $p < a_m$ for all $m \geq M\left(\frac{\varepsilon}{2}\right)$ and thus $p \in L$, a contradiction to $p > b$. Hence $a_k \leq b + \frac{\varepsilon}{2}$ and thus also $a_m \leq b + \varepsilon$ for all $m \geq M\left(\frac{\varepsilon}{2}\right)$. □

Needless to say, the approach to greatest lower bounds alias infima is completely analogous to that of least upper bounds alias suprema.

We next supply the standard constructive versions of the *intermediate value theorem.* A function $f\colon [a, b] \to \mathbb{R}$ is *locally nonconstant* whenever if $a \leq a' < b' \leq b$ and d is an arbitrary real, then $f(c) \neq d$ for some real $c \in [a', b']$. Note that if f is continuous, then there also is a rational c with that property. Strictly monotonous functions are clearly locally nonconstant, and so are nonconstant real polynomials.

Proposition 9 (Intermediate Value Theorem for Locally Nonconstant Functions). *Let $a < b$ be real numbers. If $f\colon [a, b] \to \mathbb{R}$ is continuous with $f(a) < 0 < f(b)$, and locally nonconstant, then we can find $c \in [a, b]$ with $f(c) = 0$.*

[9] Also the deduction given in [4] can easily be reformulated without choice.

Proof. We may assume that $a, b \in \mathbb{Q}$. We construct $c, d \colon \mathbb{N} \to \mathbb{Q}$ such that for all m

$$a = c_0 \leq c_1 \leq \cdots \leq c_m < d_m \leq \cdots \leq d_1 \leq d_0 = b, \tag{4}$$
$$f(c_m) < 0 < f(d_m), \tag{5}$$
$$d_m - c_m \leq \left(\frac{2}{3}\right)^m (b - a). \tag{6}$$

Let $c_0, \ldots, c_m$ and $d_0, \ldots, d_m$ be already constructed such that (6) holds. Let $x = c_m + \frac{1}{3}(d_m - c_m)$ and $y = c_m + \frac{2}{3}(d_m - c_m)$. By assumption we have a rational $z \in [c_m, d_m]$ with $f(z) \neq 0$. In case $0 < f(z)$ let $c_{m+1} = c_m$ and $d_{m+1} = z$, and in case $f(z) < 0$ let $c_{m+1} = z$ and $d_{m+1} = d_m$. As f is continuous, $f(c) = 0 = f(d)$ for the real numbers $c = d$ given by the modulated CAUCHY sequence of rationals (c_m) and (d_m). □

One might think that dependent choice has been used in this proof: whether $f(z) > 0$ or $f(z) < 0$ may well depend on the choice of z. However, this is not so, inasmuch we can refer to the algorithm contained in the assumption that f is locally nonconstant.

In Section 3, however, we can do the proof of the fundamental theorem of algebra only with the following basic tool at hand. Notice that clearly every real polynomial is uniformly continuous on $[a, b]$.

Theorem 10 (Approximate Intermediate Value Theorem). *Let $a < b$ be real numbers. For every uniformly continuous function $f \colon [a, b] \to \mathbb{R}$ with $f(a) \leq 0 \leq f(b)$, and every $\varepsilon > 0$, we can find $c \in [a, b]$ such that $|f(c)| \leq \varepsilon$.*

Proof. In the sequel we repeatedly invoke Lemma 1. Let $\varepsilon > 0$, and compare $f(a)$ and $f(b)$ with $-\varepsilon < -\frac{\varepsilon}{2}$ and $\frac{\varepsilon}{2} < \varepsilon$, respectively. If $-\varepsilon < f(a)$ or $f(b) < \varepsilon$, then $|f(c)| < \varepsilon$ for $c = a$ or $c = b$; whence we may assume that

$$f(a) < -\frac{\varepsilon}{2} \quad \text{and} \quad \frac{\varepsilon}{2} < f(b).$$

Now pick $\delta > 0$ so that, for all $x, y \in [a, b]$, if $|x - y| \leq \delta$, then $|f(x) - f(y)| \leq \varepsilon$, and divide $[a, b]$ into $a = a_0 < a_1 < \cdots < a_m = b$ such that $|a_{i-1} - a_i| \leq \delta$. Compare every $f(a_i)$ with $-\frac{\varepsilon}{2} < \frac{\varepsilon}{2}$. By assumption $f(a_0) < -\frac{\varepsilon}{2}$ and $\frac{\varepsilon}{2} < f(a_m)$; whence we can find j minimal such that

$$f(a_j) < \frac{\varepsilon}{2} \quad \text{and} \quad -\frac{\varepsilon}{2} < f(a_{j+1}).$$

Finally, compare $f(a_j)$ with $-\varepsilon < -\frac{\varepsilon}{2}$ and $f(a_{j+1})$ with $\frac{\varepsilon}{2} < \varepsilon$. If $-\varepsilon < f(a_j)$, we have $|f(a_j)| < \varepsilon$. If $f(a_{j+1}) < \varepsilon$, we have $|f(a_{j+1})| < \varepsilon$. If both $f(a_j) < -\frac{\varepsilon}{2}$ and $\frac{\varepsilon}{2} < f(a_{j+1})$, then we would have $|f(a_{j+1}) - f(a_j)| > \varepsilon$, contradicting $|a_{j+1} - a_j| \leq \delta$. □

Unlike the proofs of this result we know from the literature, the foregoing proof is entirely choice-free.[10] It seems to be characteristic of constructions of (uniquely determined or) approximate solutions that they do not even require countable choice [18].

[10] Again, this proof originates in lecture notes of the second author.

3 The Fundamental Theorem of Algebra

In the framework of constructive analysis sketched above we now give a detailed proof of the fundamental theorem of algebra, essentially following Martin KNESER [9].[11] The point is that we present the proof in a choice-free form; this of course includes all auxiliary lemmata. Our exposition is rather detailed, because – as mentioned in the introduction – we want to make the algorithmic content of this proof as clear as possible, keeping in mind that it later may serve as a basis for extracting a program.

A somewhat different presentation of KNESER's proof has been given in [22]. However, it is stressed in [22, p.437] that this proof "essentially rests on the axiom of choice".[12]

As usual, real numbers give rise to complex numbers, which in the present context are represented by pairs of modulated CAUCHY sequences of rationals, and thus are also sequentially complete (Theorem 4).

Fix the degree $n \geq 1$ of the polynomials to be considered. The bulk of the technical work is in the proof of the following Lemma.

Lemma 11. *We can find a $q \in \mathbb{Q}$ with $0 < q < 1$ (depending only on our fixed $n \in \mathbb{N}$) such that for every monic polynomial $f(\xi) = \xi^n + a_{n-1}\xi^{n-1} + \cdots + a_1\xi + a_0 \in \mathbb{C}[\xi]$ of degree n and with $|a_0| > 0$ we can find a $z \in \mathbb{C}$ satisfying*

$$|z| \leq \left(\frac{|a_0|}{q}\right)^{\frac{1}{n}} \quad \textit{and} \quad |f(z)| \leq q|a_0|.$$

From the proof it will be clear that the approximate root $z \in \mathbb{C}$ we construct depends on the *representation* of the coefficients in $\mathbb{C}$, i.e. on the choice of the pairs of modulated CAUCHY sequences of rationals which represent them. This is to be expected, for e.g. there is no continuous function $f : \mathbb{C} \to \mathbb{C}$ such that $f(z)^2 = z$: to resolve the non-uniqueness of the roots one needs RIEMANN surfaces.

Theorem 12 (Fundamental Theorem of Algebra). *For every monic polynomial $g(\xi) = \xi^n + b_{n-1}\xi^{n-1} + \cdots + b_1\xi + b_0 \in \mathbb{C}[\xi]$ of degree $n \geq 1$ we can find a $w \in \mathbb{C}$ such that $g(w) = 0$.*

Proof. Choose $c > 0$ with $|b_0| \leq c$. Let q (depending on n) be supplied by Lemma 11 (for g in place of f). It clearly suffices to inductively construct a sequence $(w_m)_{m \in \mathbb{N}}$ of complex numbers such that

$$|w_{m+1} - w_m| \leq (q^{m-1}c)^{\frac{1}{n}} \tag{7}$$

and

$$|g(w_m)| \leq q^m c\,. \tag{8}$$

Any such sequence, namely, is a modulated CAUCHY sequence in $\mathbb{C}$ whose limit is a root of g.

[11] Once more, our version of this proof stems from lecture notes of the second author. It has even been a basis of an implementation of the fundamental theorem of algebra in the interactive prover COQ [12], done by BARENDREGT, GEUVERS, POLLACK, WIEDIJK and ZWANENBURG [7].

[12] We also use the occasion to mention in print a small oversight in the proof in [22]: the specification of α on page 434 contains a circularity. This has been first noted by BARENDREGT and GEUVERS, and a correction can be found on TROELSTRA's home page.

To start with, set $w_0 = 0$. For the induction step, assume that w_m has already been found; then $f_m(\xi) = g(w_m + \xi) \in \mathbb{C}[\xi]$ is a monic polynomial of degree n with constant coefficient $g(w_m)$. By comparing $|g(w_m)|$ with $0 < q^{m+1}c$, we either have $|g(w_m)| < q^{m+1}c$ or $|g(w_m)| > 0$ (Lemma 1). In the former case, we may take $w_{m+1} = w_m$. In the latter case, applying Lemma 11 to f_m yields $z \in \mathbb{C}$ such that

$$|z| \leq \left(\frac{|g(w_m)|}{q}\right)^{\frac{1}{n}} \leq_{(8)} (q^{m-1}c)^{\frac{1}{n}} \quad \text{and} \quad |f_m(z)| \leq q|g(w_m)| \leq_{(8)} q^{m+1}c.$$

So in this case we may set $w_{m+1} = w_m + z$, for which $g(w_{m+1}) = f_m(z)$. □

In this proof of Theorem 12, the tacit invocation of sequential completeness is fairly inessential, since – just as the z supplied by Lemma 11 – each w_m can easily be constructed so that $w_m = a_m + ib_m$ with *rational*real and imaginary part a_m and b_m. (This is possible in virtue of the approximate character of either result.) As then (a_m) and (b_m) both are a modulated Cauchy sequences of rationals, they respectively represent real numbers a and b, so that $w = a + ib$ is the requested complex number with $g(w) = 0$.

In the induction step the cases of the crucial distinction may overlap, and thus a choice – which even may depend on the foregoing one – seems to be necessary whenever both cases happen simultaneously. However, Lemma 1 automatically makes this choice in every given situation. In other words, countable choice is not involved in the present proof of the fundamental theorem of algebra, let alone dependent choice. Also the proof of the fundamental theorem of algebra given by Ruitenburg in [16] is without any choice, and designed for complex numbers as represented by pairs of modulated Cauchy sequences of rationals. It is done by first proving the discrete fundamental theorem of algebra (i.e. that for algebraic rather than complex numbers) by field-theoretic means (splitting fields, minimal polynomials, ...), and then approximating complex numbers by algebraic ones.

Similar in strategy, Richman's choice-free approach [14] to an approximate version of the fundamental theorem of algebra appears to be independent of any specific presentation of the reals. Part of the price one has to pay for this generality is that one gets a bit less: a multiset of algebraic numbers as close as one pleases to the imagined multiset of complex roots. To extend this result to an exact version, by picking elements from those multisets, does only require a fairly weak and classically valid fragment of countable choice [6].[13]

Unlike these two proofs, the following one is truly elementary, which might be of importance for the form of an extracted program.

Proof of Lemma 11. Before going into the details, let us briefly sketch the approach that will prove successful in the following. First, we pick an appropriate one of the monomials $a_1\xi, \ldots, a_n\xi^n = \xi^n$, say $a_k\xi^k$, and next determine z such that a_0 and $a_k z^k$ differ by a negative factor. For $|z| = r$ we assume only that this monomial is sufficiently small, i.e. $|a_k|r^k \leq |a_0| + \varepsilon$. Then we obtain (see

[13] Roughly speaking, this is countable choice with the additional presupposition that all choices but at most one – of which of course one does not know when it occurs – are choices (!) from a singleton set. It is further noteworthy that many invocations of countable choice can be reduced to that weaker principle.We may refer to [15] for more details.

(15))

$$|f(z)| \le |a_0 + a_k z^k| + \sum_{i\neq 0,k} |a_i z^i| \le |a_0| - |a_k| r^k + 2\varepsilon + \sum_{i\neq 0,k} |a_i| r^i.$$

So the point is to choose k and r in such a way that the monomials $|a_i|r^i$ $(i \neq 0, k)$ are small compared to $|a_k|r^k$, but on the other hand are not too small compared to $|a_0|$ (see (14)).

Step 0. To start with the construction, set

$$q = 1 - \frac{1}{4\cdot 3^{2n^2-1}} \quad \text{and} \quad \varepsilon = \min\left\{ \frac{|a_0|}{2(n+1)} \cdot \frac{1}{4\cdot 3^{2n^2-1}}, (q^{-1}-1)|a_0| \right\}.$$

(These choices will be explained in steps 6, 10 und 11 below.)

Step 1. Let $m(s) := \max\{\, |a_i|s^i \mid i = 1,\ldots,n\,\}$ for every real s. Pick $t \in \mathbb{Q}$, $t > 0$, such that

$$|m(t) - |a_0|| \le \varepsilon. \tag{9}$$

This is possible by the approximate intermediate value theorem (Theorem 10), for $m(0) = 0 < |a_0|$ and, because of $s^n \le m(s)$, there is an $s_0 > 0$ such that $|a_0| < m(s_0)$; note in this context that m is uniformly continuous on the compact interval $[0, s_0]$.

Step 2. For $i = 1,\ldots,n$ choose $y_i \in \mathbb{Q}$, $y_i > 0$, such that $|y_i - |a_i|t^i| \le \varepsilon$. With $y_{ij} := \frac{y_i}{3^{ij}}$ (for $j \in \mathbb{Z}$) we obtain

$$\left| y_{ij} - |a_i| \left(\frac{t}{3^j}\right)^i \right| = \left| \frac{y_i}{3^{ij}} - \frac{|a_i|t^i}{3^{ij}} \right| \le \frac{\varepsilon}{3^{ij}}. \tag{10}$$

Step 3. For every $j \in \mathbb{Z}$, pick $k_j \in \{1,\ldots,n\}$ minimal such that $y_{ij} \le y_{k_j j}$ for $i = 1,\ldots,n$. So

$$|a_i| \left(\frac{t}{3^j}\right)^i \le y_{ij} + \frac{\varepsilon}{3^{ij}} \le y_{k_j j} + \frac{\varepsilon}{3^{ij}} \le |a_{k_j}| \left(\frac{t}{3^j}\right)^{k_j} + \frac{\varepsilon}{3^{k_j j}} + \frac{\varepsilon}{3^{ij}}. \tag{11}$$

Step 4. We have

$$k_j \ge k_{j+1}. \tag{12}$$

Indeed, for $i \ge k_j$,

$$y_{k_j(j+1)} = \frac{1}{3^{k_j(j+1)}} y_{k_j} = \frac{1}{3^{k_j}} y_{k_j j} \ge_{(*)} \frac{1}{3^i} y_{ij} = \frac{1}{3^{i(j+1)}} y_i = y_{i(j+1)}\,;$$

whence $k_{j+1} \le k_j$ according to the choice of k_{j+1} ("least possible").

Step 5. Choose $j > 0$ minimal such that $k_{j-1} = k_j = k_{j+1} =: k$. Because of (12) we have

$$n \ge k_{-1} \ge k_0 \ge k_1 \ge \cdots \ge k_{j-1} = k_j = k_{j+1},$$

where out of each pair of two consecutive $\ge$ (exept for the first one) at least one must be $>$. Hence for $2i - 1 \le j$ we have $k_{2i-1} \le n - i$.

Case 1. j is of the form $2i - 1$. Then

$$k_j \le n - i = n - \frac{j+1}{2} \to$$

$$\begin{aligned}&2k_j \leq 2n - j - 1 \to \\ &j \leq 2(n - k_j) - 1\,.\end{aligned}$$

Case 2. j is of the form $2i$. Then

$$\begin{aligned}&k_j = k_{j-1} \leq n - i = n - \frac{j}{2} \to \\ &2k_j \leq 2n - j \to \\ &j \leq 2(n - k_j)\,.\end{aligned}$$

Hence generally we have

$$j \leq 2(n-k). \tag{13}$$

Step 6. Let $r := \frac{t}{3^j} \in \mathbb{Q}$. We estimate $|a_k|r^k$ against $|a_0|$. For $i = 1, \ldots, n$, by (11) and $k = k_j$ we have $|a_k|r^k = |a_k|(\frac{t}{3^j})^k \geq |a_i|(\frac{t}{3^j})^i - 2\varepsilon \geq \frac{1}{3^{nj}}|a_i|t^i - 2\varepsilon$, hence

$$\begin{aligned}|a_k|r^k &\geq \frac{1}{3^{nj}} m(t) - 2\varepsilon \quad \text{for } m(t) = \max\{\, |a_i|t^i \mid i = 1, \ldots, n \,\} \text{ as before} \\ &\geq \frac{1}{3^{nj}}|a_0| - 3\varepsilon \qquad \text{by the choice of } t \text{ in (9).}\end{aligned}$$

By (13) we have $nj \leq 2n(n-k) \leq 2n^2 - k$ and therefore

$$|a_k|r^k \geq \frac{1}{3^{2n^2-k}}|a_0| - 3\varepsilon. \tag{14}$$

In particular $|a_k| > 0$ because of $\varepsilon < \frac{|a_0|}{3} \cdot \frac{1}{3^{2n^2-1}}$.

Step 7. We first determine $z \in \mathbb{C}$ with $|z| = r$ such that a_0 and $a_k z^k$ differ by a negative factor. Write $a_0 = |a_0|e^{ix_0}$ and $a_k = |a_k|e^{ix_k}$, and let $z = |r|e^{iy}$ with y such that $x_0 + \pi = x_k + ky$.

We show $|a_0 + a_k z^k| \leq |a_0| - |a_k z^k| + 2\varepsilon$. Now $a_k z^k = -ca_0$ with $c \in \mathbb{R}$, $c > 0$, and by the choice of t in (9) also $|a_k z^k| \leq |a_0| + \varepsilon$. Therefore

$$c|a_0| = |a_k z^k| \leq |a_0| + \varepsilon \quad \text{and} \quad 0 < c \leq 1 + \frac{\varepsilon}{|a_0|},$$

hence

$$\begin{aligned}|a_0 + a_k z^k| &= |a_0| \cdot |1 - c| \\ &= |a_0| \max(1 - c, c - 1) \\ &= |a_0| \max(1 - c, 1 - c + 2(c - 1)) \\ &\leq |a_0| \max\Big(1 - c, 1 - c + 2\frac{\varepsilon}{|a_0|}\Big) \\ &= |a_0|(1 - c) + 2\varepsilon \\ &= |a_0| - |a_k z^k| + 2\varepsilon.\end{aligned}$$

We now obtain

$$\begin{aligned}|f(z)| &\leq |a_0 + a_k z^k| + \sum_{i \neq 0,k} |a_i z^i| \\ &\leq |a_0| - |a_k z^k| + 2\varepsilon + \sum_{i \neq 0,k} |a_i z^i| \\ &= |a_0| - |a_k|r^k + 2\varepsilon + \sum_{i \neq 0,k} |a_i|r^i.\end{aligned} \tag{15}$$

Step 8. Estimate of $\sum_{1\le i<k}|a_i|r^i$. Let $1\le i<k$. Then

$$\begin{aligned}
|a_i|r^i &= 3^i|a_i|\Big(\frac{r}{3}\Big)^i\\
&= 3^i|a_i|\Big(\frac{t}{3^{j+1}}\Big)^i\\
&\le 3^i\Big(|a_k|\big(\frac{t}{3^{j+1}}\big)^k + \frac{\varepsilon}{3^{i(j+1)}} + \frac{\varepsilon}{3^{k(j+1)}}\Big) \quad \text{by (11), for } k=k_{j+1}\\
&\le 3^i\Big(|a_k|\big(\frac{t}{3^j}\big)^k\frac{1}{3^k} + 2\frac{\varepsilon}{3^i}\Big)\\
&= \frac{1}{3^{k-i}}|a_k|r^k + 2\varepsilon,
\end{aligned}$$

hence (using $\frac{1}{3^{k-1}}+\dots+\frac{1}{3}=\frac{1}{2}\big(1-\frac{1}{3^{k-1}}\big)$)

$$\sum_{1\le i<k}|a_i|r^i \le |a_k|r^k\frac{1}{2}\Big(1-\frac{1}{3^{k-1}}\Big)+2(k-1)\varepsilon. \tag{16}$$

Step 9. Estimate of $\sum_{k<i\le n}|a_i|r^i$. Let $k<i\le n$. Then

$$\begin{aligned}
|a_i|r^i &= \frac{1}{3^i}|a_i|(3r)^i\\
&= \frac{1}{3^i}|a_i|\Big(\frac{t}{3^{j-1}}\Big)^i\\
&\le \frac{1}{3^i}\Big(|a_k|\big(\frac{t}{3^{j-1}}\big)^k + \frac{\varepsilon}{3^{i(j-1)}} + \frac{\varepsilon}{3^{k(j-1)}}\Big) \quad \text{by (11), for } k=k_{j-1}\\
&\le \frac{1}{3^i}\Big(|a_k|\big(\frac{t}{3^j}\big)^k\cdot 3^k + 2\cdot 3^k\varepsilon\Big)\\
&\le \frac{1}{3^{i-k}}|a_k|r^k + 2\varepsilon,
\end{aligned}$$

hence (using $\frac{1}{3}+\dots+\frac{1}{3^{n-k}}=\frac{1}{2}\big(1-\frac{1}{3^{n-k}}\big)$)

$$\sum_{k<i\le n}|a_i|r^i \le |a_k|r^k\frac{1}{2}\Big(1-\frac{1}{3^{n-k}}\Big)+2(n-k)\varepsilon. \tag{17}$$

Step 10. From (15), (16) and (17) one obtains

$$\begin{aligned}
|f(z)| &\le |a_0| - |a_k|r^k + 2\varepsilon + \sum_{i\ne 0,k}|a_i|r^i\\
&\le 2n\varepsilon + |a_0| - |a_k|r^k + |a_k|r^k\frac{1}{2}\Big(1-\frac{1}{3^{k-1}}\Big) + |a_k|r^k\frac{1}{2}\Big(1-\frac{1}{3^{n-k}}\Big)\\
&\le 2n\varepsilon + |a_0| - \frac{1}{2}\cdot\frac{1}{3^{k-1}}|a_k|r^k\\
&\le 2n\varepsilon + |a_0| - \frac{1}{2\cdot 3^{k-1}}\Big(\frac{1}{3^{2n^2-k}}|a_0| - 3\varepsilon\Big) \quad \text{by (14)}\\
&\le 2(n+1)\varepsilon + \Big(1-\frac{1}{2\cdot 3^{2n^2-1}}\Big)|a_0|\\
&\le \underbrace{\Big(1-\frac{1}{4\cdot 3^{2n^2-1}}\Big)}_{=q}|a_0| \quad \text{for } \varepsilon\le\frac{|a_0|}{2(n+1)}\cdot\frac{1}{4\cdot 3^{2n^2-1}}
\end{aligned}$$

Step 11. Observe $|z| = r$, hence

$$|z|^n = r^n \leq t^n \leq m(t) \leq |a_0| + \varepsilon \leq q^{-1}|a_0|$$

because of $\varepsilon \leq (q^{-1} - 1)|a_0|$. Therefore we have $|z| \leq (q^{-1}|a_0|)^{\frac{1}{n}}$, as required. □

4 Dedekind Reals and Order Completeness

By a DEDEKIND *real* we understand a located DEDEKIND cut in the rationals: that is, a disjoint pair (L, U) of inhabited open subsets of $\mathbb{Q}$ that is *cut located* inasmuch as either $p \in L$ or $q \in U$ for all $p, q \in \mathbb{Q}$ with $p < q$. In particular, $p < q$ whenever $p \in L$ and $q \in U$. The *lower cut* L and the *upper cut* U uniquely determine each other, as one is the open interior of the complement of the other.[14] Needless to say, every rational r is identified with the DEDEKIND real $(\{ p \in \mathbb{Q} \mid p < r \}, \{ q \in \mathbb{Q} \mid r < q \})$.

Every lower cut L (respectively, upper cut U) is bounded from above (respectively, from below) and *downwards monotone* (respectively, *upwards monotone)*: that is, for all $p, q \in \mathbb{Q}$ with $p < q$, if $q \in L$, then $p \in L$ (respectively, if $p \in U$, then $q \in U$). Moreover, every DEDEKIND real is *approximable*: that is, for every rational $\varepsilon > 0$ there are $p \in L$ and $q \in U$ with $q - p < \varepsilon$. For the latter observation, and for the second part of the following, we may refer to [22, Chapter 5, Section 5]; the first part is routine to verify.

Lemma 13.

(a) *If L is an open subset of $\mathbb{Q}$ and U denotes the open interior of $\mathbb{Q} \setminus L$, then (L, U) is cut located if and only if L is downwards monotone and order located from above.*

(b) *The following items are equivalent for a pair (L, U) of subsets of $\mathbb{Q}$:*

   (i) *L is inhabited, U is inhabited, and (L, U) is cut located.*

   (ii) *L is downwards monotone, U is upwards monotone, and (L, U) is approximable.*

The strict partial order of DEDEKIND reals is given by $(L, U) < (L', U')$ if and only if $L' \cap U$ is inhabited. By way of this, $\leq$, $\neq$, and $=$ could be introduced – for DEDEKIND reals just as for any other type of reals – as the negation of $<$, the disjunction of $<$ and $>$, and the conjunction of $\geq$ and $\leq$, respectively. For DEDEKIND reals, however, all these relations admit of a simpler definition: namely, $(L, U) \leq (L', U')$ as $L \subset L'$ or, equivalently, as $U \supset U'$; $(L, U) = (L', U')$ as $L = L'$ or, equivalently, as $U = U'$; $(L, U) \neq (L', U')$ as $L' \cap U$ or $L \cap U'$ being inhabited. Referring to [22, Chapter 5, Section 5] for further details, so for arithmetic, we write $\mathbb{D}$ for the set of DEDEKIND reals.

Let $\mathfrak{R}$ be an archimedean ordered and valued Heyting field: that is, a model of all the axioms – for the moment, except for order completeness – that were

[14] Although it may thus seem redundant, we have chosen to define a DEDEKIND real as a pair rather than just as either a lower or an upper cut. Among our reasons for so doing is that pairs are more suited when it comes to considering *generalised* real numbers, i.e. not necessarily located DEDEKIND cuts, as e.g. in [13, 20].

listed by BRIDGES in [4].[15] (In compliance with Theorem 5 above, we say that any such $\mathfrak{R}$ is *order complete* whenever the statement of that theorem is valid for this $\mathfrak{R}$ in place of $\mathbb{R}$.) These axioms – of course, together with order completeness – embody all the properties of real numbers, such as the approximate splitting principle (cf. Lemma 1), that are commonly accepted in constructive mathematics. In particular, any such $\mathfrak{R}$ contains $\mathbb{Q}$ as an ordered subfield that is *dense* in the sense that for all $x, y \in \mathfrak{R}$ with $x < y$ there is $q \in \mathbb{Q}$ such that $x < q < y$.

Both the DEDEKIND reals and the real numbers as defined earlier on in this paper, by way of modulated CAUCHY sequences of rationals, form a perfect model of those axioms. As we have seen above and shall remember below, this includes order completeness.

If $S \subset \mathfrak{R}$ is inhabited, bounded from above, and order located from above, then $\xi_S = (L_S, U_S)$ is a DEDEKIND real with L_S and U_S as the open interiors of

$$\{\, p \in \mathbb{Q} \mid p < r \text{ for some } r \in S \,\} \quad \text{and} \quad \{\, q \in \mathbb{Q} \mid s \leq q \text{ for all } s \in S \,\}\,,$$

respectively. In particular, we can assign a DEDEKIND real $\pi(x)$ to each $x \in \mathfrak{R}$ by setting

$$\pi(x) = (\{\, p \in \mathbb{Q} \mid p < x \,\}, \{\, q \in \mathbb{Q} \mid x < q \,\}) \;.$$

Then $\pi(q) = q$ for all rationals q, and $\pi(x) < \pi(x')$ precisely when $x < x'$; whence we actually have defined an injective mapping $\pi\colon \mathfrak{R} \to \mathbb{D}$.

In other words, $\mathfrak{R}$ is canonically embedded into $\mathbb{D}$, which rephrases the saying that there are *at least* as many DEDEKIND reals as there are real numbers of an arbitrary kind like $\mathfrak{R}$. The question we address now is under which circumstances there are *exactly* as many, or rather – in view of the canonical character of π – when π is a one-to-one correspondence.

In [18], it is proved,[16] without invoking any choice principle, that $\mathfrak{R}$ is order complete if and only if a mapping $\sigma\colon \mathbb{D} \to \mathfrak{R}$ exists that preserves $<$ and operates as the identity on $\mathbb{Q}$. In fact, if $\xi = (L, U) \in \mathbb{D}$, then $L \subset \mathbb{Q}$ – considered as a subset of $\mathfrak{R}$ – is inhabited, bounded from above, and order located from above; whence the supremum of L exists provided that $\mathfrak{R}$ is order complete. Now it is routine to verify that

$$\sigma\colon \mathbb{D} \to \mathfrak{R},\ \xi = (L, U) \mapsto \sup L$$

is a mapping with $\sigma(\xi) < \sigma(\xi')$ precisely when $\xi < \xi'$, and with $\sigma(q) = q$ for all $q \in \mathbb{Q}$. Conversely, if we are given such a mapping $\sigma\colon \mathbb{D} \to \mathfrak{R}$, and if $S \subset \mathfrak{R}$ is inhabited, bounded from above, and order located from above, then $\sigma(\xi_S)$ – with ξ_S as defined before – is a supremum of S.

As a consequence, the DEDEKIND reals are order complete: the identity mapping on $\mathbb{D}$ clearly meets the specifications of such a σ. Moreover, if $\mathfrak{R}$ is order complete and thus $\sigma\colon \mathbb{D} \to \mathfrak{R}$ can be defined as above, it automatically is the two-sided inverse of π, so that if (and, of course, only if) $\mathfrak{R}$ is order complete, then $\mathfrak{R}$ is order isomorphic to the DEDEKIND reals with $\mathbb{Q}$ being invariant under

[15] There and in other places order completeness is called the "(constructive) least-upper-bound principle". See also [17] for a case study of real numbers as black boxes that, among other things, serves to justify the choice of these axioms.

[16] This goes back to an idea of Fred RICHMAN (personal communication to the first author).

the isomorphism. So $\mathbb{D}$ can legitimately be characterised as the order completion of $\mathbb{Q}$ inasmuch as the statement of Theorem 5 is the right way to phrase order completeness – which from the constructive perspective it definitely is.

TROELSTRA and VAN DALEN stated in [22, Chapter 5, 5.12.iii] that, roughly speaking, $\mathbb{D}$ is – up to order isomorphism – the one and only ordered extension of $\mathbb{Q}$ in which every lower cut in the rationals possesses a least upper bound. This characterisation of $\mathbb{D}$ turns out equivalent to the one we gave above, by way of order completeness. In fact, the former follows from the latter, because every lower cut satisfies the hypotheses of order completeness: according to the first part of Lemma 13, it is inhabited, bounded from above, and order located from above. For the reverse implication, it suffices to notice that if L_S is assigned to $S \subset \mathfrak{R}$ as before, and if $\sup L_S \in \mathfrak{R}$ exists, then it also is the supremum of S.

In retrospect, we have achieved the subsequent characterisation.

Theorem 14. *The following items all are equivalent:*

(a) $\mathfrak{R}$ *is order complete.*

(b) *Every lower cut in* $\mathbb{Q}$ *has a supremum in* $\mathfrak{R}$.

(c) *There is a mapping* $\sigma : \mathbb{D} \to \mathfrak{R}$ *that preserves* $<$ *and each rational.*

(d) *The canonical mapping* $\pi : \mathfrak{R} \to \mathbb{D}$ *is bijective.*

(e) $\mathfrak{R}$ *is order isomorphic to* $\mathbb{D}$.

In view of Theorem 5, we have the following

Corollary 15. $\mathbb{R}$ *is order isomorphic to* $\mathbb{D}$.

Note that this does not require countable choice; we have stressed the presence of witnesses all the time.

References

[1] Peter Aczel and Michael Rathjen. Notes on constructive set theory. Draft of an extended and revised version of the preprint available at the Mittag-Leffler Institute, 2002.

[2] Errett Bishop. *Foundations of Constructive Analysis.* McGraw-Hill, New York, 1997.

[3] Errett Bishop and Douglas Bridges. *Constructive Analysis*, volume 279 of *Grundlehren der mathematischen Wissenschaften.* Springer, Berlin, 1985.

[4] Douglas Bridges. Constructive mathematics: a foundation for computable analysis. *Theoret. Comput. Sci.*, 219:95–109, 1999.

[5] Douglas Bridges and Fred Richman. *Varieties of Constructive Mathematics.* Cambridge University Press, Cambridge, 1987.

[6] Douglas Bridges, Fred Richman, and Peter Schuster. A weak countable choice principle. *Proc. Amer. Math. Soc.*, 128:2749–2752, 2000.

[7] Herman Geuvers, Randy Pollack, Freek Wiedijk, and Jan Zwanenburg. Theory development leading to the fundamental theorem of algebra. Manuscript (automatically generated), June 2000.

[8] Hajime Ishihara and Peter Schuster. A constructive uniform continuity theorem. *Quart. J. Math*, 53:185–193, 2002.

[9] Martin Kneser. Ergänzung zu einer Arbeit von Hellmuth Kneser über den Fundamentalsatz der Algebra. *Math. Z.*, 177:285–287, 1981.

[10] Ray Mines, Fred Richman, and Wim Ruitenburg. *A Course in Constructive Algebra.* Springer Verlag, Berlin, Heidelberg, New York, 1987.

[11] Erik Palmgren. Constructive completions of ordered sets, groups and fields. Preprint, Uppsala University, 2003.

[12] Christine Paulin-Mohring and Benjamin Werner. Synthesis of ML programs in the system Coq. *J. Symbolic Computation*, 11:1–34, 1993.

[13] Fred Richman. Generalised real numbers in constructive mathematics. *Indag. Mathem. (N.S.)*, 9:595–606, 1998.

[14] Fred Richman. The fundamental theorem of algebra: a constructive development without choice. *Pacific J. Math.*, 196:213–230, 2000.

[15] Fred Richman. Constructive mathematics without choice. In Schuster et al. [19], pages 199–205.

[16] Willem Bastiaan Gijsbertus Ruitenburg. Constructing roots of polynomials over the complex numbers. In A. M. Cohen, editor, *Computational Aspects of Lie Group Representations and Related Topics. Proc. 1990 Computer Algebra Seminar*, number 84 in CWI Tract, pages 107–128, Amsterdam, 1991. Centrum voor Wiskunde en Informatica.

[17] Peter Schuster. Real numbers as black boxes. *New Zealand J. Math.*, 31:189–202, 2002.

[18] Peter Schuster. Unique existence, approximate solutions, and countable choice. *Theoret. Comput. Sci.*, to appear.

[19] Peter Schuster, Ulrich Berger, and Horst Osswald, editors. *Reuniting the Antipodes – Constructive and Nonstandard Views of the Continuum*, volume 306 of *Synthese Library*, Dordrecht, 2001. Kluwer Academic Publisher.

[20] Peter M. Schuster. A constructive look at generalised Cauchy reals. *Math. Logic Quart.*, 46:125–134, 2000.

[21] Rudolf Taschner. *Lehrgang der konstruktiven Mathematik. Drei Bände.* Manz and Hölder-Pichler-Tempsky, 2nd ed. of vols. 1,2, ibid., 1995 edition, 1991, 1992, 1993.

[22] Anne S. Troelstra and Dirk van Dalen. *Constructivism in Mathematics. An Introduction*, volume 121, 123 of *Studies in Logic and the Foundations of Mathematics.* North–Holland, Amsterdam, 1988.