Constructive Analysis with Witnesses

Helmut SCHWICHTENBERG

Mathematisches Institut der Ludwig-Maximilians-Universität München

Theresienstraße 39, D-80333 München

We are interested in *exact real numbers*, as opposed to floating point numbers. The final goal is to develop the basics of real analysis in such a way that from a proof of an existence formula one can extract a program. For instance, from a proof of the intermediate value theorem we want to extract a program that, given an arbitrary error bound 2^{-k}, computes a rational x where the given function is zero up to the error bound.

Why should we be interested in logic in a study of constructive analysis? There are at least two reasons.

(1) Obviously we need to be aware of the difference of the classical and the constructive existential quantifier, and try to prove the stronger statements involving the latter whenever possible. Then one is forced to give "constructive" proofs, whose algorithmic content can be "seen" and then used as a basis to formulate a program for computing the solution. This was the point of view in BISHOP's classic textbook [3], and more explicitely carried through in ANDERSSON's recent Master's thesis [2] (based on PALMGREN's [15]), with MATHEMATICA as the target programming language.

(2) However, one can go one step further and automatize the step from the (formalized) constructive proof to the corresponding program. This can be done by means of the so-called realizability interpretation, whose existence was clear from the beginnings of constructive logic. The desire to have "mathematics as a numerical language" in this sense was clearly expressed by BISHOP in his article [4] (with just that title). There are now many implementations of these ideas, for instance NUPRL, COQ, MINLOG and recently also ISABELLE, to mention only a few.

What are the requirements on a constructive logic that should guide us in our design?

- It should be as close as possible to the mathematical arguments we want to use. Variables should carry (functional) types, with free algebras (e.g., natural numbers) as base types. Over these, inductive definitions and the corresponding introduction and elimination axioms should be allowed.
- The constants of the language should denote computable functionals in the SCOTT-ERSOV sense, and hence the higher-order quantifiers should range over their (mathematically correct) domain, the partial continuous functionals.
- The language of the logic should be strong (in the sense of being expressive), but the existence axioms used should be weak.
- Type parameters (ML style) should be allowed, but quantification over types should be disallowed in order to keep the theory predicative. Similarly, predicate variables should be allowed as place-holders for properties, but quantification over them should be disallowed, again to ensure predicativity.

Compared with the literature, the novel aspect of the present work is the development of elementary constructive analysis in such a way that witnesses have as low a type level as possible. This clearly is important for the complexity of the extracted programs. Here are some examples.

(1) A continuous function on the reals is determined by its values on the rationals, and hence can be represented by a type-one (rather that type-two) object.
(2) In the proof that the range of a continuous function on a compact intervall has a supremum (see Corollary 3.11), BROUWER's notion of a *totally bounded* set of reals (which has type-level two) is replaced by the notion of being *bounded above* (which has type-level one).
(3) The CAUCHY-EULER construction of approximate solutions to ordinary differential equations can be seen as a type-level one process.

Acknowledgements. Some of the material on calculus from a constructive point of view is taken form [16]. The section on ordinary differential equations is based on Chapter 1 of HUREWICZ's textbook [12], adapted to our constructive setting. I have also made use of a recent note of BRIDGES [7].

1. Real Numbers

We shall view a real as a CAUCHY sequence of rationals with a separately given modulus.

Definition 1.1. A real number x is a pair $((a_n)_{n\in\mathbb{N}}, M)$ with $a_n \in \mathbb{Q}$ and $M\colon \mathbb{N} \to \mathbb{N}$ such that $(a_n)_n$ is a CAUCHY sequence with modulus M, that is

$$\forall k, m, n.\ M(k) \le m, n \to a_m \le a_n + 2^{-k},$$

and M is weakly increasing. M is called CAUCHY modulus of x.

We shall loosely speak of a real $(a_n)_n$ if the CAUCHY modulus M is clear from the context or inessential. Every rational a is tacitly understood as the real represented by the constant sequence $a_n = a$ with the constant modulus $M(k) = 0$.

Definition 1.2. Two reals $x := ((a_n)_n, M)$, $y := ((b_n)_n, N)$ are called *equivalent* (or *equal* and written $x = y$, if the context makes clear what is meant), if

$$\forall k(|a_{M(k+1)} - b_{N(k+1)}| \le 2^{-k}).$$

We need to show that this is an equivalence relation. Reflexivity and symmetry are clear, and for transitivity we need the following easy lemma:

Lemma 1.3. *For reals $x := ((a_n)_n, M)$, $y := ((b_n)_n, N)$ the following are equivalent:*

(a) $x = y$;
(b) $\forall k \exists^{\mathrm{cl}} q \forall n.\ q \le n \to |a_n - b_n| \le 2^{-k}$;
(c) $\forall k \exists q \forall n.\ q \le n \to |a_n - b_n| \le 2^{-k}$.

For every function on the reals we certainly want compatibility with equality. This however is not always the case; here is an important example.

Lemma 1.4. *For every real $x := ((a_n)_n, M)$ we can find an upper bound 2^{k_x} on the elements of the* CAUCHY *sequence: $a_n \le 2^{k_x}$ for all n.*

Proof. Let k_x be such that $\max\{ a_n \mid n \le M(0) \} + 1 \le 2^{k_x}$, hence $a_n \le 2^{k_x}$ for all n. ∎

Clearly this assignment of k_x to x is not compatible with equality.

Definition 1.5. A real $x := ((a_n)_n, M)$ is called *nonnegative* (written $x \in \mathbb{R}^{0+}$) if

$$\forall k(-2^{-k} \leq a_{M(k)}).$$

It is *k-positive* (written $x \in_k \mathbb{R}^+$, or $x \in \mathbb{R}$ if k is not needed) if

$$2^{-k} \leq a_{M(k+1)}.$$

One can see easily that both $x \in \mathbb{R}^{0+}$ and $x \in \mathbb{R}^+$ are compatible with equality.

Given real numbers $x := ((a_n)_n, M)$ and $y := ((b_n)_n, N)$, we define each z from the list $x + y$, $-x$, $|x|$, $x \cdot y$, and $\frac{1}{x}$ (the latter only provided that $|x| \in_l \mathbb{R}^+$) as represented by the respective sequence (c_n) of rationals with modulus L:

z	c_n	$L(k)$
$x+y$	$a_n + b_n$	$\max\bigl(M(k+1), N(k+1)\bigr)$
$-x$	$-a_n$	$M(k)$
$\lvert x\rvert$	$\lvert a_n\rvert$	$M(k)$
$x \cdot y$	$a_n \cdot b_n$	$\max\bigl(M(k+1+k_{\lvert y\rvert}), N(k+1+k_{\lvert x\rvert})\bigr)$
$\frac{1}{x}$ for $\lvert x\rvert \in_l \mathbb{R}^+$	$\begin{cases} \frac{1}{a_n} & \text{if } a_n \neq 0 \\ 0 & \text{if } a_n = 0 \end{cases}$	$M(2(l+1)+k)$,

where 2^{k_x} is the upper bound provided by Lemma 1.4.

One can show easily that for reals x, y also $x + y$, $-x$, $|x|$, $x \cdot y$ and (provided that $|x| \in_l \mathbb{R}^+$) also $1/x$ are reals, and moreover that he functions $x + y$, $-x$, $|x|$, $x \cdot y$ and (provided that $|x| \in_l \mathbb{R}^+$) also $1/x$ are compatible with equality.

Lemma 1.6. *For reals x, y, z*

$$x + (y + z) = (x + y) + z \qquad x \cdot (y \cdot z) = (x \cdot y) \cdot z$$
$$x + 0 = x \qquad x \cdot 1 = x$$
$$x + (-x) = 0 \qquad 0 < |x| \to x \cdot \frac{1}{x} = 1$$
$$x + y = y + x \qquad x \cdot y = y \cdot x$$
$$x \cdot (y + z) = x \cdot y + x \cdot z$$

Proof. Routine. □

Lemma 1.7. *For reals x, y from $x \cdot y = 1$ we can infer $0 < |x|$.*

Proof. Pick k such that $|b_n| \leq 2^k$ for all n. Pick q such that $q \leq n$ implies $1/2 \leq a_n \cdot b_n$. Then for $q \leq n$, $1/2 \leq |a_n| \cdot 2^k$, and hence $2^{-k-1} \leq |a_n|$. □

Lemma 1.8. *For reals x, y,*

(a) $x, y \in \mathbb{R}^{0+} \to x + y, x \cdot y \in \mathbb{R}^{0+}$,
(b) $x, y \in \mathbb{R}^+ \to x + y, x \cdot y \in \mathbb{R}^+$,
(c) $x \in \mathbb{R}^{0+} \to -x \in \mathbb{R}^{0+} \to x = 0$.

Proof. (a), (b). Routine. (c). Let k be given. Pick p such that $-2^{-k} \leq a_n$ and $-2^{-k} \leq -a_n$ for $n \geq p$. Then $|a_n| \leq 2^{-k}$. □

We write $x \leq y$ for $y - x \in \mathbb{R}^{0+}$ and $x < y$ for $y - x \in \mathbb{R}^+$. Unwinding the definitions yields that $x \leq y$ is to say that for every k there exists p_k such that $a_n \leq b_n + 2^{-k}$ for all $n \geq p_k$. Furthermore, $x < y$ is a shorthand for the presence of k, q with $a_n + 2^{-k} \leq b_n$ for all $n \geq q$; we then write $x <_{k,q} y$ (or simply $x <_k y$ if q is not needed) whenever we want to call these witnesses.

Lemma 1.9. *$0 \leq x$ and $0 <_k y$ implies $0 <_{k+1} x + y$.*

Proof. From $0 \le x$ we have $\forall l \exists p \forall n.\ p \le n \to -2^{-l} \le a_n$. From $0 <_k y$ we have some q such that $\forall n.\ q \le n \to 2^{-k} \le b_n$. Pick p for $k+1$. Then $p, q \le n$ implies $0 \le a_n + 2^{-k-1}$ and $2^{-k-1} \le b_n - 2^{-k-1}$, hence $2^{-k-1} \le a_n + b_n$. □

Lemma 1.10. *For reals x, y, z,*

$$\begin{array}{ll} x \le x & x \not< x \\ x \le y \to y \le x \to x = y & x < y \to y < z \to x < z \\ x \le y \to y \le z \to x \le z & x < y \to x + z < y + z \\ x \le y \to x + z \le y + z & x < y \to 0 < z \to x \cdot z < y \cdot z \\ x \le y \to 0 \le z \to x \cdot z \le y \cdot z & \end{array}$$

Proof. Lemma 1.8. □

Lemma 1.11. $x \le y \to y <_k z \to x <_{k+1} z$.

Proof. Lemma 1.9. □

As is to be expected in view of the existential and universal character of the predicates $<$ and $\le$ on the reals, we have:

Lemma 1.12. $x \le y \leftrightarrow y \not< x$.

Proof. $\to$. Assume $x \le y$ and $y < x$. By Lemma 1.11 we obtain $x < x$. contradicting Lemma 1.10.

$\leftarrow$. It clearly suffices to show $0 \not< z \to z \le 0$, for a real z given by $(c_n)_n$. Assume $0 \not< z$. We must show $\forall k \exists p \forall n.\ p \le n \to c_n \le 2^{-k}$. Let k be given. By assumption $0 \not< z$, hence $\neg \exists l (2^{-l} \le c_{M(l+1)})$, hence $\forall l (c_{M(l+1)} < 2^{-l})$. For $l := k+1$ this implies $c_{M(k+2)} < 2^{-k-1}$, hence $c_n \le c_{M(k+2)} + 2^{-k-2} < 2^{-k}$ for $M(k+2) \le n$. □

Constructively, we cannot compare two reals, but we can compare every real with a nontrivial interval.

Lemma 1.13 (Approximate Splitting Principle)**.** *Let x, y, z be given and assume $x < y$. Then we can find k, q such that either $z <_{k,q} y$ or $x <_{k,q} z$.*

Proof. Let $x := ((a_n)_n, M)$, $y := ((b_n)_n, N)$, $z := ((c_n)_n, L)$. Assume p, k are given such that with $\varepsilon := 2^{-k}$

$$\forall n.\ p \le n \to a_n + 3\varepsilon \le b_n - 3\varepsilon.$$

Let $q := \max\bigl(M(k), N(k), L(k), p\bigr)$.

Case $c_q \le b_q - 3\varepsilon$. Then for $q \le n$

$$c_n + \varepsilon \le c_q + 2\varepsilon \le b_q - \varepsilon \le b_n,$$

hence $z <_{k,q} y$.

Case $b_q - 3\varepsilon < c_q$, hence by assumption $a_q + 3\varepsilon < c_q$. Then for $q \le n$

$$a_n + \varepsilon \le a_q + 2\varepsilon < c_q - \varepsilon \le c_n,$$

hence $x <_{k,q} z$. □

Notice that the boolean object determining whether $z < y$ or $x < z$ depends on the representation of x and y. In particular this assignment is not compatible with our equality relation.

One might think that the non-available comparison of two reals could be circumvented by using a maximum function. Indeed, such a function can easily be defined (component wise), and it has the expected properties $x, y \le \max(x, y)$ and $x, y \le z \to \max(x, y) \le z$. However, what is missing is the knowledge that $\max(x, y)$ equals one of its arguments, i.e., we do not have $\max(x, y) = x \vee \max(x, y) = y$.

However, in many cases it is sufficient to pick the up to ε largest real out of finitely many given ones. This is indeed possible. We give the proof for two reals; it can be easily generalized.

Lemma 1.14 (Maximum of Two Reals). *Let $x := ((a_n)_n, M)$ and $y := ((b_n)_n, N)$ be reals, and $k \in \mathbb{N}$. Then for $\varepsilon := 2^{-k}$ either $x \le y + \varepsilon$ or else $y \le x + \varepsilon$.*

Proof. Let $p := \max\bigl(M(k+1), N(k+1)\bigr)$.

Case $a_p \le b_p$. Then for $p \le n$

$$a_n \le a_p + \frac{\varepsilon}{2} \le b_p + \frac{\varepsilon}{2} \le b_n + \varepsilon.$$

This holds for all n, therefore $x \le y + \varepsilon$.

Case $b_p < a_p$. Then for $p \le n$

$$b_n \le b_p + \frac{\varepsilon}{2} < a_p + \frac{\varepsilon}{2} \le a_n + \varepsilon.$$

This holds for all n, therefore $y \le x + \varepsilon$. □

Recall that every rational a is tacitly understood as the real represented by the constant sequence $a_n = a$ with the constant modulus $M(k) = 0$.

Lemma 1.15 ($\mathbb{Q}$ is dense in $\mathbb{R}$). *For any two reals $x < y$ there is a rational a such that $x < a < y$.*

Proof. Let $z := (x+y)/2$ be given by $(c_n)_n$. Then for some k we have $x <_k z <_k y$. Let $a := c_{M(k+1)}$. □

Notice that a depends on the representations of x and y.

Theorem 1.16 (Cantor). *Let a sequence (x_n) of reals be given. Then we can find a real y with $0 \le y \le 1$ that is apart from every x_n, in the sense that $x_n < y \vee y < x_n$.*

Proof. We construct two sequences $(a_n)_n$, $(b_n)_n$ of rationals such that for all n

$$0 = a_0 \le a_1 \le \cdots \le a_n < b_n \le \cdots \le b_1 \le b_0 = 1, \tag{1}$$

$$x_n < a_{n+1} \vee b_{n+1} < x_n, \tag{2}$$

$$b_n - a_n \le 2^{-n}. \tag{3}$$

Let $a_0, \dots, a_n$ and $b_0, \dots, b_n$ be already constructed such that (1)-(3) hold (as far as they are defined). Now compare the real x_n with $a_n < b_n$.

Case 1. $x_n < b_n$. Let $b_{n+1} := b_n$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, we can find a rational a_{n+1} such that

$$\max\bigl(x_n, a_n, b_n - 2^{-n-1}\bigr) < a_{n+1} < b_{n+1} = b_n.$$

Case 2. $a_n < x_n$. Let $a_{n+1} := a_n$, and find a rational b_{n+1} such that

$$a_n = a_{n+1} < b_{n+1} < \min\bigl(x_n, b_n, a_n + 2^{-n-1}\bigr).$$

Clearly (1)-(3) continue to hold for $n+1$ (as far as defined). $y := (a_n)_n$ is a Cauchy sequence, since for $m \ge n$ we have $|a_m - a_n| = a_m - a_n \le b_n - a_n \le 2^{-n}$. Similarly $z := (b_n)_n$ is a Cauchy sequence. $y = z$ follows from (3), and from (2) together with (1) we obtain $x_n < y \vee z < x_n$. □

After some computations involving real numbers it is to be expected that the rational numbers occurring in the Cauchy sequences may become rather complex. Hence under computational aspects it is necessary to be able to *clean up* a real, as follows.

Lemma 1.17. *For every real $x = ((a_n)_n, M)$ we can construct an equivalent real $y = ((b_n)_n, N)$ where the rationals b_n are of the form $c_n/2^n$ with integers c_n, and with modulus $N(k) = k + 2$.*

Proof. Let $c_n := \lfloor a_{M(n)} \cdot 2^n \rfloor$ and $b_n := c_n \cdot 2^{-n}$, hence

$$\frac{c_n}{2^n} \le a_{M(n)} < \frac{c_n}{2^n} + \frac{1}{2^n} \quad \text{with } c_n \in \mathbb{Z}.$$

Then for $m \le n$

$$\begin{aligned} |b_m - b_n| &= |c_m \cdot 2^{-m} - c_n \cdot 2^{-n}| \\ &\le |c_m \cdot 2^{-m} - a_{M(m)}| + |a_{M(m)} - a_{M(n)}| + |a_{M(n)} - c_n \cdot 2^{-n}| \\ &\le 2^{-m} + 2^{-m} + 2^{-n} \\ &< 2^{-m+2}, \end{aligned}$$

hence $|b_m - b_n| \le 2^{-k}$ for $n \ge m \ge k+2 =: N(k)$, so $(b_n)_n$ is a Cauchy sequence with modulus N.

To prove that x is equivalent to $y := ((b_n)_n, N)$, observe

$$\begin{aligned} |a_n - b_n| &\le |a_n - a_{M(n)}| + |a_{M(n)} - c_n \cdot 2^{-n}| \\ &\le 2^{-k-1} + 2^{-n} \quad \text{for } n, M(n) \ge M(k+1) \\ &\le 2^{-k} \quad \text{if in addition } n \ge k+1. \end{aligned}$$

Hence $|a_n - b_n| \le 2^{-k}$ for $n \ge \max(k+1, M(k+1))$, and therefore $x = y$. □

2. Sequences and Series of Real Numbers

Definition 2.1. A sequence $(x_n)_{n\in\mathbb{N}}$ of reals is a Cauchy *sequence* with modulus $M\colon \mathbb{N} \to \mathbb{N}$ whenever $|x_m - x_n| \le 2^{-k}$ for $m, n \ge M(k)$, and *converges* with modulus $M\colon \mathbb{N} \to \mathbb{N}$ to a real y, its *limit*, whenever $|x_n - y| \le 2^{-k}$ for $n \ge M(k)$.

Clearly the limit of a convergent sequence of reals is uniqely determined.

Lemma 2.2. *Every modulated* Cauchy *sequence of rationals converges with the same modulus to the real number it represents.*

Proof. Let $x := ((a_n)_n, M)$ be a real. We must show $|a_n - x| \le 2^{-k}$ for $n \ge M(k)$. Fix $n \ge M(k)$. It suffices to show $|a_m - a_n| \le 2^{-k}$ for $n \ge M(k)$. But this holds by assumption. □

By the triangle inequality, every convergent sequence of reals with modulus M is a Cauchy sequence with modulus $k \mapsto M(k+1)$. We now prove the reverse implication.

Theorem 2.3 (Sequential Completeness). *For every* Cauchy *sequence of reals we can find a real to which it converges.*

Proof. Let $(x_n)_{n\in\mathbb{N}}$ be a Cauchy sequence of reals with modulus M; assume x_n is $((a_{nk})_k, N_n)$. Note first that, for each $n \in \mathbb{N}$ and every p, by Lemma 2.2 we have $|x_n - a_{nl}| \le 2^{-p}$ for all $l \ge N_n(p)$. Next, set

$$b_n = a_{nN_n(n)}$$

for every $n \in \mathbb{N}$, so that $|x_n - b_n| \le 2^{-n}$ for all $n \in \mathbb{N}$ by the particular case $l = N_n(n)$ of the foregoing consideration. Then

$$|b_m - b_n| \le |b_m - x_m| + |x_m - x_n| + |x_n - b_n| \le 2^{-m} + 2^{-q-1} + 2^{-n} \le 2^{-q}$$

for all $m, n \ge \max(M(q+1), q+2)$, which is to say that $y := (b_n)_n$ is a Cauchy sequence with modulus $L(q) := \max(M(q+1), q+2)$. Moreover, again by Lemma 2.2

$$|x_n - y| \le |x_n - b_n| + |b_n - y| \le 2^{-n} + 2^{-q-1} \le 2^{-q}$$

for all $n \ge L(q+1)$; in other words: (x_n) converges to y with modulus $q \mapsto L(q+1)$. □

It will be useful to characterize convergence of a sequence of reals in terms of their approximations.

Lemma 2.4. *For reals x_i, y represented by $(a_{i,n})_n, (b_n)_n$ the following are equivalent:*
(a) $(x_i)_i$ *converges to* y, *i.e.*, $\forall k \exists q \forall i{\ge}q\, (|x_i - y| \le 2^{-k})$;
(b) $\forall k \exists p \forall i, n{\ge}p\, (|a_{in} - b_n| \le 2^{-k})$.

Proof. (a) $\Rightarrow$ (b). Given k, pick q by (a) such that $|x_i - y| \le 2^{-k-1}$ for $i > q$. Then by definition $|a_{in} - b_n| \le 2^{-k-1} + 2^{-k-1}$ for $n \ge r$ with r depending on k only.

(b) $\Rightarrow$ (a). Given k, we have to find q such that $|x_i - y| \le 2^{-k}$ for $i > q$. It suffices to have $|a_{in} - b_n| \le 2^{-k} + 2^{-l}$ for $n \ge r$ with r depending on l. But by (b) we even have $|a_{in} - b_n| \le 2^{-k}$ for $n \ge p$. $\square$

3. Continuous Functions

An inhabited, closed finite interval is called a *compact interval*. By default we shall assume that a compact interval $I = [a, b]$ has rational end-points.

Definition 3.1. Let S be a set of reals. A real y is an *upper bound* of S if $x \le y$ for all $x \in S$. A real y is a *supremum* of S if y is an upper bound of S, and in addition for every rational $a < y$ there is real $x \in S$ such that $a \le x$. A set S of reals is *order located above* if for every $a < b$, either $x \le b$ for all $x \in S$ or else $a \le x$ for some $x \in S$.

Every set S can have at most one supremum. To see this, assume that y, z are suprema of S. It is enough to show $y \le z$, and for this it suffices to show $z \not< y$. So assume $z < y$. Then $z < a < y$ for some rational a, hence $a \le x$ for some $x \in S$, contradicting the assumption that z is an upper bound of S. If the supremum of S exists, it is denoted by $\sup S$.

Theorem 3.2 (Least-Upper-Bound Principle)**.** *Assume that S is an inhabited set of reals that is bounded above. Then S has a supremum iff it is order located above.*

Proof. If $\sup S$ exists and $a < b$, then either $\sup S < b$ or else $a < \sup S$. In the former case $x \le b$ for all $x \in S$, and in the latter case clearly $a \le x$ for some $x \in S$. Hence S is order located above.

For the converse it is useful to consider

$$\Pi_S(a, b): \qquad \text{both } y \le b \text{ for all } y \in S \text{ and } a < x \text{ for some } x \in S$$

as a property of any pair a, b of rational numbers with $a < b$. By assumption we have $a, b \in \mathbb{Q}$ with $a < b$ such that $\Pi_S(a, b)$. We construct two sequences $(c_n)_n$ and $(d_n)_n$ of rationals such that for all n

$$a = c_0 \le c_1 \le \dots \le c_n < d_n \le \dots \le d_1 \le d_0 = b, \tag{4}$$

$$\Pi_S(c_n, d_n), \tag{5}$$

$$d_n - c_n \le \left(\frac{2}{3}\right)^n (b - a). \tag{6}$$

Let $c_0, \dots, c_n$ and $d_0, \dots, d_n$ be already constructed such that (4)-(6) hold. Let $c = c_n + \frac{1}{3}(d_n - c_n)$ and $d = c_n + \frac{2}{3}(d_n - c_n)$. Since S is order located above, either $s \le d$ for all $s \in S$ or else $c < r$ for some $r \in S$. In the first case let $c_{n+1} := c_n$ and $d_{n+1} := d$, and in the second case let $c_{n+1} := c$ and $d_{n+1} := d_n$. Then clearly $\Pi_S(c_{n+1}, d_{n+1})$, (4) and (6) continue to hold for $n + 1$, and the real number $x = y$ given by the modulated Cauchy sequences of rationals $(c_n)_n$ and $(d_n)_n$ is the least upper bound of S. $\square$

Definition 3.3. A *continuous function* $f: I \to \mathbb{R}$ on a compact interval I with rational end points is given by

(a) an approximating map $h_f: (I \cap \mathbb{Q}) \times \mathbb{N} \to \mathbb{Q}$ and a map $\alpha_f: \mathbb{N} \to \mathbb{N}$ such that $(h_f(a, n))_n$ is a Cauchy sequence with (uniform) modulus α_f;

(b) a modulus $\omega_f\colon \mathbb{N} \to \mathbb{N}$ of (uniform) continuity, which satisfies

$$|a-b| \le 2^{-\omega_f(k)+1} \to |h_f(a,n) - h_f(b,n)| \le 2^{-k}$$

for $n \ge \alpha_f(k)$. α_f and ω_f are required to be weakly increasing.

Notice that a continuous function is given by the objects h_f, α_f, ω_f of type level 1 only. This is due to the fact that it suffices to define its values on rational numbers.

An example is the squaring function $\mathsf{sq}\colon [0,1] \to \mathbb{R}$ given by

(a) the approximating map $h_{\mathsf{sq}}(a,n) := a^2$ and modulus $\alpha_{\mathsf{sq}}(k) := 0$, and

(b) the modulus $\omega_{\mathsf{sq}}(k) := k+2$ of uniform continuity, for $-\omega_{\mathsf{sq}}(k)+1 = -k-1$ and

$$|a-b| \le 2^{-k-1} \to |a^2 - b^2| = |(a-b)(a+b)| \le 2^{-k},$$

because $a+b \le 2$.

Similarly all polynomials with rational coefficients on finite intervals can be viewed as continuous functions in our sense.

Another example is the inverse function $\mathsf{inv}\colon [2^{-l}, c] \to \mathbb{R}$ given by

(a) the approximating map $h_{\mathsf{inv}}(a,n) := \frac{1}{a}$ and modulus $\alpha_{\mathsf{inv}}(k) := 0$, and

(b) the modulus $\omega_{\mathsf{inv}}(k) := k+2l+1$ of uniform continuity, for $-\omega_{\mathsf{inv}}(k)+1 = -k-2l$ and

$$|a-b| \le 2^{-k-2l} \to \left|\frac{1}{a} - \frac{1}{b}\right| = \left|\frac{b-a}{ab}\right| \le 2^{-k},$$

because $ab \ge 2^{-2l}$.

Since the approximating map operates on rationals only, we need to define separately what it means to apply a continuous function in our sense to a real.

Definition 3.4. *Application* of a continuous function $f\colon I \to \mathbb{R}$ (given by h_f, α_f, ω_f) to a real $x := ((a_n)_n, M)$ in I is defined to be

$$(h_f(a_n, n))_n$$

with modulus $\max(\alpha_f(k+2), M(\omega_f(k+1)-1))$. This is a modulus, for

$$\begin{aligned}
&|h_f(a_m,m) - h_f(a_n,n)| \\
&\le |h_f(a_m,m) - h_f(a_m,p)| + |h_f(a_m,p) - h_f(a_n,p)| + |h_f(a_n,p) - h_f(a_n,n)| \\
&\le 2^{-k-2} + 2^{-k-1} + 2^{-k-2}
\end{aligned}$$

if $m,n \ge M(\omega_f(k+1)-1)$ and $p \ge \alpha_f(k+1)$ (for the middle term), and moreover $m,n,p \ge \alpha_f(k+2)$ (for the first and last term). We denote this real by $f(x)$. The set of all such reals is called the *range* of f.

We want to show that application is compatible with equality.

Lemma 3.5. *Let f be a continuous function. Then*

$$x = y \to f(x) = f(y).$$

Proof. Let $x := ((a_n)_n, M)$ and $y := ((b_n)_n, N)$, and assume $x = y$. We must show that $(h_f(a_n,n))_n = (h_f(b_n,n))_n$. This follows from

$$\begin{aligned}
&|h_f(a_n,n) - h_f(b_n,n)| \\
&\le |h_f(a_n,n) - h_f(a_n,p)| + |h_f(a_n,p) - h_f(b_n,p)| + |h_f(b_n,p) - h_f(b_n,n)| \\
&\le 2^{-k-2} + 2^{-k-1} + 2^{-k-2}
\end{aligned}$$

if $n,p \ge \alpha_f(k+2)$ (the first and the last term), and for the middle term in addition $n \ge p$ with p provided by Lemma 1.3(c) (for $\omega_f(k+1)-1$). ∎

Next we show that indeed a continuous function f has ω_f as a modulus of uniform continuity.

Lemma 3.6. *Let f be continuous and x, y be reals in its domain. Then*

$$|x - y| \le 2^{-\omega_f(k)} \to |f(x) - f(y)| \le 2^{-k}.$$

Proof. Let $x := ((a_n)_n, M)$ and $y := ((b_n)_n, N)$. Assume $|a_n - b_n| \le 2^{-\omega_f(k)} + 2^{-l_0}$ for $n \ge p_{l_0}$, with $l_0 := \omega_f(k)$. It suffices to show that for an arbitrary l we can find q_l such that $|h_f(a_n, n) - h_f(b_n, n)| \le 2^{-k} + 2^{-l}$ for $n \ge q_l$. This follows from

$$\begin{aligned} &|h_f(a_n, n) - h_f(b_n, n)| \\ &\le |h_f(a_n, n) - h_f(a_n, p)| + |h_f(a_n, p) - h_f(b_n, p)| + |h_f(b_n, p) - h_f(b_n, n)| \\ &\le 2^{-l-1} + 2^{-k} + 2^{-l-1} \end{aligned}$$

if $n, p \ge \alpha_f(l + 1)$ (the first and the last term), and for the middle term in addition $p \ge \alpha_f(k)$, because then the assumption $|a_n - b_n| \le 2^{-\omega_f(k)+1}$ implies $|h_f(a_n, p) - h_f(b_n, p)| \le 2^{-k}$. ∎

We define the composition of two continuous functions.

Definition 3.7. Assume that $f : I \to \mathbb{R}$ and $g : J \to \mathbb{R}$ are continuous, and that $h_f[(I \cap \mathbb{Q}) \times \mathbb{N}] \subseteq J$. Then the function $g \circ f : I \to \mathbb{R}$ is defined by

(a) the approximating map $h : (I \cap \mathbb{Q}) \times \mathbb{N} \to \mathbb{Q}$, $h(a, n) := h_g(h_f(a, n), n)$ with modulus $\alpha_{g \circ f}(k) := \max\big(\alpha_g(k + 2), \alpha_f(\omega_g(k + 1) - 1)\big)$;

(b) the modulus $\omega_{g \circ f}(k) := \omega_f(\omega_g(k) - 1) + 1$ of (uniform) continuity for $g \circ f$.

We need to show that this indeed defines a continuous function.

Lemma 3.8. *Under the assumptions of the definition above we have*

(a) $\alpha_{g \circ f}$ *is a* CAUCHY *modulus;*

(b) $\omega_{g \circ f}$ *is a modulus of uniform continuity for* $g \circ f$.

Proof. (a).

$$\begin{aligned} |h_g(h_f(a, m), m) - h_g(h_f(a, n), n)| &\le |h_g(h_f(a, m), m) - h_g(h_f(a, m), p)| + \\ &\quad\; |h_g(h_f(a, m), p) - h_g(h_f(a, n), p)| + \\ &\quad\; |h_g(h_f(a, n), p) - h_g(h_f(a, n), n)| \\ &\le 2^{-k-2} + 2^{-k-1} + 2^{-k-2} \end{aligned}$$

if $m, n \ge \alpha_f(\omega_g(k + 1) - 1)$ and $p \ge \alpha_g(k + 1)$ (for the middle term), and moreover $m, n, p \ge \alpha_g(k + 2)$ (for the first and last term).

(b). Assume $|a - b| \le 2^{-\omega_f(\omega_g(k)-1)+1}$. Then $|h_f(a, n) - h_f(b, n)| \le 2^{-\omega_g(k)+1}$ provided $n \ge \alpha_f(\omega_g(k) - 1)$, and therefore $|h_g(h_f(a, n), n) - h_g(h_f(b, n), n)| \le 2^{-k}$ provided also $n \ge \alpha_g(k)$. Both conditions on n hold for $n \ge \alpha_{g \circ f}(k)$, since α_g, α_f and ω_g are weakly increasing. ∎

For example, assume that $f : I \to \mathbb{R}$ is continuous and that for some l, $2^{-l} \le h_f(c, n) \in \mathbb{Q}$ for all n and all rationals $c \in I$. Then we can form the inverse $1/f$ as a continuous map $I \to \mathbb{R}$, by composing $\mathsf{inv} \circ f$.

Since every continuous function on a compact interval comes with a modulus of uniform continuity, we can explicitely construct a bound for its values, even for the values of its approximating map.

Lemma 3.9. *Let $f : [a, b] \to \mathbb{R}$ be continuous, given by h_f, α_f and ω_f. Then for all $n \ge n_0 := \alpha_f(0)$ and rationals $c \in I$*

$$|h_f(c, n)| \le M := |h_f(a, n_0)| + N + 1,$$

where $(c - a)2^{\omega_f(0)-1} \le N \in \mathbb{N}$. Hence the range of f is bounded above by M.

Proof. Recall that for $c, d \in [a, b]$

$$|c - d| \le 2^{-\omega_f(0)+1} \to |h_f(c, n_0) - h_f(d, n_0)| \le 1.$$

Let $\varepsilon := (c - a)/N$ and $a_i := a + i\varepsilon$ for $i = 0, \dots, N$. Then $a_N = a + N\varepsilon = c$ and

$$\bigl|h_f(c, n_0) - h_f(a, n_0)\bigr| \le \sum_{i=0}^{N-1} \bigl|h_f(a_{i+1}, n_0) - h_f(a_i, n_0)\bigr| \le N,$$

hence $|h_f(c, n_0)| \le |h_f(a, n_0)| + N$ and therefore $|h_f(c, n)| \le |h_f(a, n_0)| + N + 1$ for $n \ge n_0 := \alpha_f(0)$. □

The supremum of the range of a continuous function on a compact interval can be shown to exist constructively.[1] We prove that the range is order located above, which entails (by Theorem 3.2) that it has a supremum.

Lemma 3.10. *Let $f\colon I \to \mathbb{R}$ be continuous, I compact with rational end points. Then the range of f is order located above.*

Proof. Let h_f, α_f and ω_f be the data for f. Given a, b with $a < b$, fix k such that $2^{-k} \le \frac{1}{3}(b - a)$. Take a partition $a_0, \dots, a_l$ of I of mesh $\le 2^{-\omega_f(k)+2}$. Then for every $c \in I$ there is an i such that $|c - a_i| \le 2^{-\omega_f(k)+1}$. Let $n_k := \alpha_f(k)$ and consider all finitely many

$$h(a_i, n_k) \quad \text{for } i = 0, \dots, l.$$

Let $h(a_j, n_k)$ be the maximum of all those.

Case $h(a_j, n_k) \le a + \frac{1}{3}(b - a)$. We show that $f(x) \le b$ for all x. Let $x = ((b_n)_n, M)$. Then for $n \ge n_k$

$$\begin{aligned} h_f(b_n, n) &\le h_f(b_n, n_k) + 2^{-k} \\ &\le h_f(a_i, n_k) + 2^{-k+1} \quad \text{for } i \text{ such that } |b_n - a_i| \le 2^{-\omega_f(k)+1} \\ &\le h_f(a_j, n_k) + 2^{-k+1} \\ &\le b. \end{aligned}$$

Case $a + \frac{1}{3}(b - a) < h(a_j, n_k)$. We show $a \le f(x)$ for $x := a_j$. Then $f(x)$ is given by the Cauchy sequence $(h_f(a_j, n))_n$. We have for $n \ge n_k$

$$h_f(a_j, n) \ge h_f(a_j, n_k) - 2^{-k} \ge a + \frac{1}{3}(b - a) - 2^{-k} \ge a.$$

Hence $a \le f(x)$. □

Corollary 3.11. *Let $f\colon I \to \mathbb{R}$ be continuous, I compact with rational end points. Then the range of f has a supremum, denoted $\|f\|_I$.*

Proof. By Lemma 3.9 we know that the range of f is bounded above, and by Lemma 3.10 it is order located above. Hence by Theorem 3.2 it has a supremum. □

We next supply the standard constructive versions of the *intermediate value theorem.*

Theorem 3.12 (Approximate Intermediate Value Theorem)**.** *Let $a < b$ be rational numbers. For every continuous function $f\colon [a, b] \to \mathbb{R}$ with $f(a) \le 0 \le f(b)$, and every k, we can find $c \in [a, b]$ such that $|f(c)| \le 2^{-k}$.*

[1] This is proved in [5], using the notion of a "totally bounded" set. However, the latter is a type-level 2 concept, which we wish to avoid.

Proof. In the sequel we repeatedly invoke Lemma 1.13. Given k, let $\varepsilon := 2^{-k}$. We 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 l so that, for all $x, y \in [a, b]$, if $|x - y| \leq 2^{-l}$, then $|f(x) - f(y)| \leq \varepsilon$, and divide $[a, b]$ into $a = a_0 < a_1 < \cdots < a_m = b$ such that $|a_{i-1} - a_i| \leq 2^{-l}$. 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 $|a_{j+1} - a_j| \leq 2^{-l}$. ∎

Alternative Proof. We give a different proof, which more directly makes use of the fact that our continuous functions come with witnessing data.

We may assume $f(a) < -2^{-k-1}$ and $2^{-k-1} < f(b)$ (see above). Divide $[a, b]$ into $a = a_0 < a_1 < \cdots < a_m = b$ such that $|a_{i-1} - a_i| \leq 2^{-\omega_f(k+1)}$. Consider all finitely many

$$h(a_i, n_0) \quad \text{for } i = 1, \ldots, m,$$

with $n_0 := \alpha_f(k + 1)$. Pick j such that $h(a_{j-1}, n_0) \leq 0 \leq h(a_j, n_0)$; this can be done because $f(a) < -2^{-k-1}$ and $2^{-k-1} < f(b)$. We show $|f(a_j)| \leq 2^{-k}$; for this it clearly suffices to show $|h(a_j, n)| \leq 2^{-k}$ for $n \geq n_0$. Now

$$|h(a_j, n)| \leq \big|h(a_j, n) - h(a_j, n_0)\big| + \big|h(a_j, n_0)\big| \leq 2^{-k-1} + 2^{-k-1},$$

where the first estimate holds by the choice of n_0, and the second one follows from the choice of a_j and $|h(a_{i-1}, n) - h(a_i, n)| \leq 2^{-k-1}$. ∎

A function $f\colon [a, b] \to \mathbb{R}$ is *locally nonconstant* whenever if $a \leq a' < b' \leq b$ and z is an arbitrary real, then $f(x) \neq z$ for some real $x \in [a', b']$. Note that if f is continuous, then there also is a rational with that property. Strictly monotonous functions are clearly locally nonconstant, and so are nonconstant real polynomials.

Proposition 3.13 (Intermediate Value Theorem)**.** *Let $a < b$ be rational numbers. If $f\colon [a, b] \to \mathbb{R}$ is continuous with $f(a) < 0 < f(b)$, and locally nonconstant, then we can find $x \in [a, b]$ with $f(x) = 0$.*

Proof. We construct two sequences $(c_n)_n$ and $(d_n)_n$ of rationals such that for all m

$$a = c_0 \leq c_1 \leq \cdots \leq c_m < d_m \leq \cdots \leq d_1 \leq d_0 = b, \tag{7}$$

$$f(c_m) < 0 < f(d_m), \tag{8}$$

$$d_m - c_m \leq \left(\frac{2}{3}\right)^m (b - a). \tag{9}$$

Let $c_0, \ldots, c_m$ and $d_0, \ldots, d_m$ be already constructed such that (7)-(9) hold. Let $c = c_m + \frac{1}{3}(d_m - c_m)$ and $d = c_m + \frac{2}{3}(d_m - c_m)$. By assumption we have a rational $a_m \in [c_m, d_m]$ with $f(a_m) \neq 0$. In case $0 < f(a_m)$ let $c_{m+1} = c_m$ and $d_{m+1} = a_m$, and in case $f(a_m) < 0$ let $c_{m+1} = a_m$ and $y_{m+1} = y_m$. Let x, y be given by the modulus Cauchy sequences $(c_n)_n$ and $(d_n)_n$ of rationals. As f is continuous, $f(x) = 0 = f(y)$ for the real number $x = y$. ∎

4. Differentiation

Definition 4.1. Let $f, g\colon I \to \mathbb{R}$ be continuous. g is called *derivative* of f with modulus $\delta_f\colon \mathbb{N} \to \mathbb{N}$ of differentiability if for $a, b \in I$ with $a < b$,

$$b \leq a + 2^{-\delta_f(k)} \to \left|f(b) - f(a) - g(a)(b-a)\right| \leq 2^{-k}(b-a).$$

f is said to be *differentiable* on I and g is called a *derivative* of f on I.

To say that g is a derivative of f we write

$$g = f', \quad g = Df, \quad \text{or} \quad g(x) = \frac{df(x)}{dx}.$$

If f has two derivatives, then clearly they are equal functions.

For example, a constant function has derivative 0, and the identity function has the constant 1 function as derivative.

We show that a bound on the derivative of f serves as a Lipschitz constant of f:

Lemma 4.2. *Let $f\colon I \to \mathbb{R}$ be continuous with derivative f'. Assume that f' is bounded on I by M. Then for $a, b \in I$ with $a < b$,*

$$\left|f(b) - f(a)\right| \leq M(b-a).$$

Proof. Given $k \in \mathbb{N}$, it suffices to prove

$$\left|f(b) - f(a)\right| \leq M(b-a) + 2^{-k}$$

Choose l such that $2^{-l}(b-a) \leq 2^{-k}$, and let $a = a_0 < a_1 < \cdots < a_n = b$ such that $a_{i+1} \leq a_i + 2^{-\delta_f(l)}$, where δ_f is the modulus of differentiability of f. Then

$$\begin{aligned}
&\left|f(b) - f(a)\right| \\
&= \left|\sum_{i=0}^{n-1} f(a_{i+1}) - f(a_i)\right| \\
&= \left|\sum_{i=0}^{n-1} f'(a_i)(a_{i+1} - a_i) + \sum_{i=0}^{n-1} f(a_{i+1}) - f(a_i) - f'(a_i)(a_{i+1} - a_i)\right| \\
&\leq M(b-a) + 2^{-l}(b-a).
\end{aligned}$$

This proves the claim. ∎

Lemma 4.3. *Let $f, g\colon I \to \mathbb{R}$ be continuous with derivatives f', g' of moduli δ_f, δ_g. Then*

$$(f+g)' := f' + g'$$

is a derivative of $f + g$ with modulus

$$\delta_{f+g}(k) := \max\bigl(\delta_f(k+1), \delta_g(k+1)\bigr).$$

Proof. Let $a < b \leq a + 2^{-m}$. Then

$$\begin{aligned}
&\left|f(b) + g(b) - f(a) - g(a) - (f'(a) - g'(a))(b-a)\right| \\
&\leq \left|f(b) - f(a) - f'(a)(b-a)\right| + \left|g(b) - g(a) - g'(a)(b-a)\right| \\
&\leq 2^{-k-1}(b-a) + 2^{-k-1}(b-a).
\end{aligned}$$

for $m \geq \delta_f(k+1), \delta_g(k+1)$. ∎

Lemma 4.4. *Let $f, g\colon I \to \mathbb{R}$ be continuous with derivatives f', g' of moduli δ_f, δ_g. Then*

$$(fg)' := f'g + fg'$$

is a derivative of fg with modulus

$$\delta_{fg}(k) := \max\bigl(\omega_g(r+k+1), \delta_f(k+q+2), \delta_g(k+p+2)\bigr),$$

where $2^r, 2^p, 2^q$ are upper bounds for f', f, g in I, respectively.

Proof. Let $a < b \le a + 2^{-m}$. Then, using Lemma 4.2

$$\begin{aligned}
&\bigl|f(b)g(b) - f(a)g(a) - f'(a)g(a)(b-a) - f(a)g'(a)(b-a)\bigr| \\
&= \bigl|\bigl(f(b) - f(a)\bigr)g(b) + f(a)\bigl(g(b) - g(a)\bigr) - \\
&\qquad f'(a)g(a)(b-a) - f(a)g'(a)(b-a)\bigr| \\
&= \bigl|\bigl(f(b) - f(a)\bigr)\bigl(g(b) - g(a)\bigr) + \bigl(f(b) - f(a) - f'(a)(b-a)\bigr)g(a) + \\
&\qquad f(a)\bigl(g(b) - g(a) - g'(a)(b-a)\bigr)\bigr| \\
&\le 2^r(b-a)2^{-r-k-1} + 2^{-k-q-2}(b-a)\bigl|g(a)\bigr| + \bigl|f(a)\bigr|(b-a)2^{-k-p-2} \\
&\le 2^{-k}(b-a)
\end{aligned}$$

for $m \ge \omega_g(r+k+1), \delta_f(k+q+2), \delta_g(k+p+2)$. ∎

Lemma 4.5. *Let $g\colon I \to \mathbb{R}$ be continuous with derivative g' of modulus δ_g, and $|g'(a)| \le 2^q$ for all $a \in I$. Moreover assume that $2^{-p} \le |g(a)|$ for all $a \in I$. Then*

$$\Bigl(\frac{1}{g}\Bigr)' := -\frac{g'(a)}{g(a)^2}$$

is a derivative of $\frac{1}{g}$ with modulus

$$\delta_{\frac{1}{g}}(k) := \max\bigl(\delta_g(k+2p+1), \omega_{\frac{1}{g}}(p+q+k+1)\bigr).$$

Proof. Let $a < b \le a + 2^{-m}$. Then

$$\begin{aligned}
&\Bigl|\frac{1}{g(b)} - \frac{1}{g(a)} - \frac{g'(a)}{g(a)^2}(b-a)\Bigr| \\
&= \Bigl|\frac{1}{g(b)g(a)}\bigl(g(b) - g(a) - g'(a)(b-a)\bigr) + \frac{g'(a)}{g(a)}(b-a)\Bigl(\frac{1}{g(b)} - \frac{1}{g(a)}\Bigr)\Bigr| \\
&\le 2^p \cdot 2^p \cdot 2^{-k-2p-1} \cdot (b-a) + 2^p \cdot 2^q \cdot (b-a) \cdot 2^{-p-q-k-1} \\
&\le 2^{-k}(b-a)
\end{aligned}$$

for $m \ge \delta_g(k+2p+1), \omega_{\frac{1}{g}}(p+q+k+1)$. ∎

Theorem 4.6 (Chain Rule)**.** *Let $f\colon I \to J$ and $g\colon J \to \mathbb{R}$ be continuous with derivatives f', g' of moduli δ_f, δ_g. Then*

$$(g \circ f)' = (g' \circ f) \cdot f'$$

is a derivative of $g \circ f$ with modulus

$$\delta_{g\circ f}(k) = \max\bigl(\delta_g(k+1+r), \delta_f(k+1+q)\bigr),$$

where $2^r, 2^q$ are upper bounds for f', g' in I, J, respectively.

Proof. Let $a < b \le a + 2^{-m}$. Then, using Lemma 4.2

$$\begin{aligned}
&\bigl|g(f(b)) - g(f(a)) - g'(f(a))f'(a)(b-a)\bigr| \\
&\le \bigl|g(f(b)) - g(f(a)) - g'(f(a))\bigl(f(b) - f(a)\bigr)\bigr| + \\
&\qquad \bigl|g'(f(a))\bigr| \cdot \bigl|f(b) - f(a) - f'(a)(b-a)\bigr| \\
&\le 2^{-k-1-r}\bigl|f(b) - f(a)\bigr| + 2^q\bigl|f(b) - f(a) - f'(a)(b-a)\bigr| \\
&\le 2^{-k-1}(b-a) + 2^q\bigl|f(b) - f(a) - f'(a)(b-a)\bigr| \\
&\le 2^{-k-1}(b-a) + 2^q 2^{-k-1-q}(b-a) \\
&= 2^{-k}(b-a)
\end{aligned}$$

for $m \ge \delta_g(k+1+r), \delta_f(k+1+q)$. □

Lemma 4.7 (Rolle). *Let $f\colon [a,b] \to \mathbb{R}$ be continuous with derivative f', and assume $f(a) = f(b)$. Then for every $k \in \mathbb{N}$ we can find $c \in [a,b]$ such that $|f'(c)| \le 2^{-k}$.*

Proof. Let δ_f be the modulus of differentiability of f, and let $a = a_0 < a_1 < \cdots < a_n = b$ such that $a_{i+1} \le a_i + 2^{-\delta_f(k+2)}$. Compare all $|f'(a_i)|$ with $2^{-k-1} < 2^{-k}$. If some is $< 2^{-k}$, we are done. Otherwise we argue as in Lemma 4.2:

$$\begin{aligned}
&f(b) - f(a) \\
&= \sum_{i=0}^{n-1}\bigl(f(a_{i+1}) - f(a_i)\bigr) \\
&= \sum_{i=0}^{n-1}\bigl(f'(a_i)(a_{i+1} - a_i)\bigr) + \sum_{i=0}^{n-1}\bigl(f(a_{i+1}) - f(a_i) - f'(a_i)(a_{i+1} - a_i)\bigr) \\
&\ge 2^{-k-1}(b-a) - 2^{-k-2}(b-a) > 0.
\end{aligned}$$

This contradiction proves the claim. □

Theorem 4.8 (Mean Value Theorem)**.** *Let $f\colon [a,b] \to \mathbb{R}$ be continuous with derivative f'. Then for every $k \in \mathbb{N}$ we can find $c \in [a,b]$ such that*

$$\bigl|f(b) - f(a) - f'(c)(b-a)\bigr| \le 2^{-k}(b-a).$$

Proof. Let $2^{-l} \le 2^{-k}(b-a)$ and define a continuous $h\colon [a,b] \to \mathbb{R}$ by

$$h(x) := (x-a)\bigl(f(b) - f(a)\bigr) - f(x)(b-a).$$

Then $h(a) = h(b) = -f(a)(b-a)$. Hence by Lemma 4.7 we can find c in $[a,b]$ such that

$$\bigl|h'(c)\bigr| = \bigl|f(b) - f(a) - f'(c)(b-a)\bigr| \le 2^{-l}.$$

This proves the claim. □

5. Integration

For simplicity we define $\int_a^b f(a)\,dx$ for rational end points a, b only. For reals a, b one can easily define $\int_a^b f(x)\,dx$ by rational approximation.

Definition 5.1. Let a, b be rationals with $a < b$. A list $P = a_0, \dots, a_n$ of rationals is a *partition* of the interval $[a,b]$, if $a = a_0 \le a_1 \le \cdots \le a_n = b$. $\max\{\, a_{i+1} - a_i \mid i < n \,\}$ is the *mesh* of P. A partition $Q = a'_0, \dots, a'_m$ of $[a,b]$ is a *refinement* of P, if $\forall i \le n \exists j \le m(a'_j = a_i)$. If $f\colon [a,b] \to \mathbb{R}$ is a continuous function given by h_f, α_f and ω_f, and $P = a_0, a_1, \dots, a_n$ a partition of $[a,b]$, then an arbitrary sum of the form

$\sum_{i=0}^{n-1} h_f(e_i, n) \cdot (a_{i+1} - a_i)$ with $e_i \in [a_i, a_{i+1}]$ is denoted by $S(f, P)$. In particular for $a_i = a + \frac{i}{n}(b - a)$

$$S(f, a, b, n) := \frac{b-a}{n} \sum_{i=0}^{n-1} h_f(a_i, n)$$

is one of the numbers $S(f, P)$.

Theorem 5.2. *Assume that $f\colon [a, b] \to \mathbb{R}$ is continuous with modulus ω_f of (uniform) continuity. Then $(S(f, a, b, n))_{n\in\mathbb{N}}$ is a* CAUCHY *sequence of rationals with modulus $\alpha(p) = 2^{\omega_f(p+q+1)}(b - a)$, where q is such that $b - a \leq 2^q$; we denote this real by*

$$\int_a^b f(x)\, dx.$$

Moreover, if P is a partition of mesh $\leq 2^{-\omega_f(l)}$, then

$$\left|S(f, P) - \int_a^b f(x)\, dx\right| \leq 2^{-l}(b - a).$$

Proof. Let k, l be given and $P = a_0, \dots, a_n$, $Q = b_0, \dots, b_m$ partitions of $[a, b]$ with mesh $\leq 2^{-\omega_f(k)}$ or $\leq 2^{-\omega_f(l)}$, respectively. Let $R = c_0, \dots, c_r$ be the common refinement of P and Q, obtained by arranging $a_0, \dots, a_n, b_0, \dots, b_m$ into a monotone sequence (here we make use of the fact that a_i, b_j are assumed to be rational). Let $d_k \in [c_k, c_{k+1}]$ for $k < r$. For every $i < n$ denote by $\sum_i$ the summation over all indices k such that $a_i \leq c_k < a_{i+1}$. Then

$$\begin{aligned}
&|S(f, P) - S(f, R)| \\
&= \left|\sum_{i=0}^{n-1} h_f(e_i, n) \cdot (a_{i+1} - a_i) - \sum_{k=0}^{r-1} h_f(d_k, r) \cdot (c_{k+1} - c_k)\right| \\
&= \left|\sum_{i=0}^{n-1} h_f(e_i, n) \sum_i (c_{k+1} - c_k) - \sum_{i=0}^{n-1} \sum_i h_f(d_k, r) \cdot (c_{k+1} - c_k)\right| \\
&\leq \sum_{i=0}^{n-1} \sum_i |h_f(e_i, n) - h_f(d_k, r)|(c_{k+1} - c_k) \\
&\leq \sum_{i=0}^{n-1} \sum_i \big(|h_f(e_i, n) - h_f(e_i, r)| + |h_f(e_i, r) - h_f(d_k, r)|\big)(c_{k+1} - c_k) \\
&\leq \sum_{i=0}^{n-1} \sum_i 2^{-k}(c_{k+1} - c_k) \quad \text{for } n \geq \alpha_f(k + 1) \\
&= 2^{-k}(b - a)
\end{aligned}$$

Similarly we have, again for $n \geq \alpha_f(k + 1)$

$$|S(f, Q) - S(f, R)| \leq 2^{-l}(b - a),$$

hence

$$|S(f, P) - S(f, Q)| \leq (2^{-k} + 2^{-l})(b - a).$$

In particular

$$|S(f, a, b, m) - S(f, a, b, n)| \leq 2^{-k+1}(b - a)$$

for $m, n \geq 2^{\omega_f(k)}(b - a), \alpha_f(k + 1)$. Hence $|S(f, a, b, m) - S(f, a, b, n)| \leq 2^{-p}$ for $m, n \geq 2^{\omega_f(p+q+1)}(b - a), \alpha_f(p + q + 2)$, where q is such that $b - a \leq 2^q$; therefore $\big(S(f, a, b, n)\big)_n$ is a CAUCHY sequence.

Moreover we have for $n \geq 2^{\omega_f(l)}(b-a), \alpha_f(l+1)$

$$|S(f,P) - S(f,a,b,n)| \leq (2^{-k} + 2^{-l})(b-a).$$

Now let $n \to \infty$ and $k \to \infty$. Then we obtain

$$|S(f,P) - \int_a^b f(x)\,dx| \leq 2^{-l}(b-a),$$

as was to be shown. ∎

Up to now we have always considered the integral with respect to a fixed integration interval. Now we view the upper bound of this interval as variable and study the function obtained in this way. It is called the "undetermined integral".

Given a continuous $f\colon [a_0, b_0] \to \mathbb{R}$, we first need to establish $F(x) := \int_{a_0}^x f(t)\,dt$ as a continuous function. This means that we have to come up with h_F, α_F and ω_F. For simplicity assume $[a_0, b_0] = [0, 1]$. Let

$$h_F(a,n) := S(f, 0, a, n).$$

By Theorem 5.2 we already know that $(h_F(a,n))_n$ is a CAUCHY sequence with modulus $k \mapsto 2^{\omega_f(k+1)}$. It remains to provide a modulus ω_F of (uniform) continuity. To this end, we divide the intervals $[0,a]$ and $[0,b]$ in n pieces each, and let $a_i := \frac{i}{n}a$ and $b_i := \frac{i}{n}b$. Then

$$\begin{aligned}
\big|h_F(a,n) - h_F(b,n)\big| &= \big|S(f,0,a,n) - S(f,0,b,n)\big| \\
&= \frac{1}{n}\Big|a\sum_{i=0}^{n-1} h_f(a_i,n) - b\sum_{i=0}^{n-1} h_f(b_i,n)\Big| \\
&\leq \frac{1}{n}\sum_{i=0}^{n-1}\big(a\big|h_f(a_i,n) - h_f(b_i,n)\big| + |a-b|\cdot|h_f(b_i,n)|\big) \\
&\leq \frac{1}{n}\sum_{i=0}^{n-1}\big(a\cdot 2^{-k-1} + |a-b|\cdot 2^p\big) \leq 2^{-k}
\end{aligned}$$

provided $|a_i - b_i| \leq 2^{-\omega_f(k+1)+1}$ and $|a-b| \leq 2^{-p-k-1}$, where p is chosen according to Lemma 3.9 such that $h_f(b_i,n) \leq 2^p$, for $n \geq \alpha_f(0)$. So let

$$\alpha_F(k) := \max\big(\alpha_f(0), 2^{\omega_f(k+1)}\big), \quad \omega_F(k) := \max\big(p+k, \omega_f(k+1)\big).$$

Theorem 5.3. *Let $f\colon [a,b] \to \mathbb{R}$ be continuous with modulus ω_f of (uniform) continuity. For $x \in [a,b]$ let*

$$F(x) := \int_a^x f(t)\,dt.$$

be the continuous function just described. Then this function $F\colon [a,b] \to \mathbb{R}$ has f as derivative, with modulus ω_f. Morover, if G is any differentiable function on $[a,b]$ with $G' = f$, then the difference $F - G$ is a constant function.

Proof. Let $m \geq \omega_f(k)$ and $h := \pm 2^{-m}$. Then

$$\begin{aligned}
\Big|\frac{F(y)-F(x)}{h} - f(x)\Big| &= \Big|\frac{1}{h}\Big(\int_a^y f(t)\,dt - \int_a^x f(t)\,dt\Big) - f(x)\Big| \\
&= \Big|\frac{1}{h}\int_x^y f(t)\,dt - \frac{1}{h}\int_x^y f(x)\,dt\Big| \\
&\leq \frac{1}{h}\int_x^y |f(t)-f(x)|\,dt \\
&\leq \frac{1}{h}\int_x^y 2^{-k}\,dt = 2^{-k}.
\end{aligned}$$

This was to be shown. Now let G be any differentiable function on $[a,b]$ with $G' = f$. Then $(F-G)' = F' - G' = f - f = 0$. Hence by the Mean Value Theorem 4.8 $(F-G)(c) = (F-G)(d)$ for any c, d in $[a,b]$. ∎

Theorem 5.4 (Fundamental Theorem of Calculus)**.** *Let $f\colon I \to \mathbb{R}$ be continuous and $F\colon I \to \mathbb{R}$ such that $F' = f$. Then for all $a, b \in I$*

$$\int_a^b f(x)\,dx = F(b) - F(a).$$

Proof. For $x \in I$ define

$$F_0(x) := \int_a^x f(t)\,dt.$$

By Theorem 5.3 we have $F_0' = f$. Clearly

$$F_0(a) = 0 \qquad \text{and} \qquad F_0(b) = \int_a^b f(t)\,dt.$$

Hence for any $F\colon I \to \mathbb{R}$ such that $F' = f$, again by Theorem 5.3 there is a constant $c \in \mathbb{R}$ such that $F - F_0 = c$. Therefore

$$F(b) - F(a) = F_0(b) - F_0(a) = F_0(b) = \int_a^b f(t)\,dt,$$

which was to be shown. ∎

It is common to use the notation

$$F(x)\Big|_a^b \quad \text{or} \quad \Big[F(x)\Big]_a^b \quad \text{for} \quad F(b) - F(a).$$

The formula from Theorem 5.4 can then we written as

$$\int_a^b f(x)\,dx = F(x)\Big|_a^b \quad \text{or} \quad \int_a^b f(x)\,dx = \Big[F(x)\Big]_a^b$$

which is often abbreviated to

$$\int f(x)\,dx = F(x).$$

However, this notation is somewhat problematic, since F is determined up to a constant only.

6. Sequences of Functions

We define the notion of uniform convergence of a sequence of continuous functions $f_i \colon I \to \mathbb{R}$ to a continuous function $f \colon I \to \mathbb{R}$.

Definition 6.1. Let $f_i, f \colon I \to \mathbb{R}$ be continuous, with approximating maps h_i, h and Cauchy moduli α_i, α. The sequence $(f_i)_{i\in\mathbb{N}}$ is *uniformly convergent* to f if

$$\forall k \exists p \forall i{\ge}p \forall a \, \big|h_i(a, \alpha_i(k+2)) - h(a, \alpha(k+2))\big| \le 2^{-k}.$$

Lemma 6.2. *Let $f_i, f \colon I \to \mathbb{R}$ be continuous, with approximating maps h_i, h. Then the following are equivalent.*

(a) *The sequence $(f_i)_{i\in\mathbb{N}}$ is uniformly convergent to f.*
(b) $\forall k \exists p \forall i, n{\ge}p \forall a \, |h_i(a,n) - h(a,n)| \le 2^{-k}$.

Proof. (a) $\Rightarrow$ (b).

$$\begin{aligned} \big|h_i(a,n) - h(a,n)\big| &\le \big|h_i(a,n) - h_i(a,\alpha_i(k+3))\big| + \\ &\qquad \big|h_i(a,\alpha_i(k+3)) - h(a,\alpha(k+3))\big| + \\ &\qquad \big|h(a,\alpha(k+3)) - h(a,n)\big| \\ &\le 2^{-k-3} + 2^{-k-1} + 2^{-k-3} \end{aligned}$$

if $n \ge \alpha_i(k+3), \alpha(k+3)$ (for the first and last term) and $i \ge p$ with p provided for $k+1$ by (a).

(b) $\Rightarrow$ (a).

$$\begin{aligned} \big|h_i(a,\alpha_i(k+2)) - h(a,\alpha(k+2))\big| &\le \big|h_i(a,\alpha_i(k+2)) - h_i(a,n)\big| + \\ &\qquad \big|h_i(a,n) - h(a,n)\big| + \\ &\qquad \big|h(a,n) - h(a,\alpha(k+2))\big| \\ &\le 2^{-k-2} + 2^{-k-1} + 2^{-k-2} \end{aligned}$$

if $n \ge \alpha_i(k+2), \alpha(k+2)$ (for the first and last term) and in addition $i, n \ge p$ with p provided for $k+1$ by (b). □

The notion of uniform convergence has been defined in terms of witnesses for the given continuous functions f_i, in order to ensure that from a proof of uniform convergence we can extract the right data. The next Lemma shows that a uniformly convergent sequence indeed is uniformly convergent in the usual sense.

Lemma 6.3. *Let $f_i, f \colon I \to \mathbb{R}$ be continuous. Assume that the sequence $(f_i)_{i\in\mathbb{N}}$ is uniformly convergent to f. Then*

$$\forall k \exists p \forall i{\ge}p \forall x \, \big|f_i(x) - f(x)\big| \le 2^{-k}.$$

Proof. Let $x = ((a_n)_n, M)$, and let h_i, h be approximating maps for f_i, f, respectively. By Lemma 6.2(b)

$$\forall k \exists p \forall n{\ge}p \, |h_n(a_n, n) - h(a_n, n)| \le 2^{-k},$$

whence the claim. □

The next Lemma gives a useful criterion as to when and how we can construct the limit function. It will be used in the proof of Theorem 7.7.

Lemma 6.4. *Let $f_i \colon I \to \mathbb{R}$ be continuous functions, given by approximating functions h_i and moduli α of Cauchyness and ω of (uniform) continuity, where the latter two are* independent *of i. Assume we have a modulus $\delta \colon \mathbb{N} \to \mathbb{N}$ of* uniform convergence *satisfying*

$$\big|h_i(a,n) - h_j(a,n)\big| \le 2^{-k}$$

for $i, j \geq \delta(k)$ and $n \geq \alpha(k)$, and all $a \in I$. Then $(f_i)_{i\in\mathbb{N}}$ uniformly converges to the continuous function $f\colon I \to \mathbb{R}$ given by

$$h_f(a,n) := h_n(a,n), \quad \alpha_f(k) := \max\bigl(\delta(k+1), \alpha(k+1)\bigr), \quad \omega_f := \omega.$$

Proof. It is easy to see that this function $f\colon I \to \mathbb{R}$ given by h_f, α_f and ω_f is indeed continuous: α_f is a Cauchy modulus, because

$$\begin{aligned}|h_n(a,n) - h_m(a,m)| &\leq |h_n(a,n) - h_m(a,n)| + |h_m(a,n) - h_m(a,m)| \\ &\leq 2^{-k-1} + 2^{-k-1}\end{aligned}$$

for $m, n \geq \alpha_f(k)$, and ω is a modulus of (uniform) continuity, because

$$|a-b| \leq 2^{-\omega(k)+1} \to |h_n(a,n) - h_n(b,n)| \leq 2^{-k}$$

for $n \geq \alpha_f(k)$. Moreover, for a given k we may pick $p := \max(\delta(k), \alpha(k))$. Then for $i, n \geq p$ and all a, $|h_i(a,n) - h_n(a,n)| \leq 2^{-k}$. By Lemma 6.2(b) this means that $(f_i)_{i\in\mathbb{N}}$ uniformly converges to f. □

We now show that for a uniformly convergent sequence of continuous functions, integration and limits can be exchanged.

Theorem 6.5. *Let $f_i, f\colon [a,b] \to \mathbb{R}$ be continuous. Assume that the sequence $(f_i)_{i\in\mathbb{N}}$ is uniformly convergent to f. Then*

$$\lim_{i\to\infty} \int_a^b f_i(t)\,dt = \int_a^b f(t)\,dt.$$

Proof. Let

$$\int_a^b f_i(t)\,dt = (S(f_i,a,b,n))_n =: x_i \quad \text{and} \quad \int_a^b f(t)\,dt = (S(f,a,b,n))_n =: x.$$

We show that $(x_i)_i$ converges to x, using Lemma 2.4(b).

$$\begin{aligned}\bigl|S(f_i,a,b,n) - S(f,a,b,n)\bigr| &\leq \frac{b-a}{n}\sum_{j=0}^{n-1}\bigl|h_i(a_j,n) - h(a_j,n)\bigr| \\ &\leq \frac{b-a}{n} n 2^{-l} \leq 2^{-k},\end{aligned}$$

for $n, i \geq p_l$, where $a_j := a + \frac{j}{n}(b-a)$. p_l is defined in Lemma 6.2(b), and l is such that $(b-a)2^{-l} \leq 2^{-k}$. □

7. Ordinary Differential Equations

Consider a differential equation

$$y' = f(x,y), \tag{10}$$

where $f\colon D \to \mathbb{R}$ is a continuous function on some subset D of $\mathbb{R}^2$. A solution of (10) on an interval I is a function $\varphi\colon I \to \mathbb{R}$ with a continuous derivative φ' such that for all $x \in I$

$$(x,\varphi(x)) \in D \text{ (hence } f(x,\varphi(x)) \text{ is defined) and } \varphi'(x) = f(x,\varphi(x)).$$

We want to construct approximate solutions to (10), by means of the the Cauchy-Euler approximation method.

Definition 7.1. Let $f\colon D \to \mathbb{R}$ be continuous, and consider an interval I. A function $\varphi\colon I \to \mathbb{R}$ is a *solution up to* 2^{-k} of (10) if

(a) φ is *admissible*, i.e., $(x,\varphi(x)) \in D$ for $x \in I$.
(b) φ is continuous.
(c) φ has a piecewise continuous derivative on I.

(d) $|\varphi'(x) - f(x, \varphi(x))| \leq 2^{-k}$ for all $x \in I$ where $\varphi'(x)$ is defined.

Theorem 7.2. *Let $f\colon D \to \mathbb{R}$ be continuous, and $(a_0, b_0) \in D$ such that the rectangle R given by $|x - a_0| \leq a$, $|y - b_0| \leq b$ is in D. Assume $|f(x, y)| \leq M$ for $(x, y) \in R$, and let $h := \min(a, b/M)$. Then for every $k \in \mathbb{N}$ we can construct an approximate solution $\varphi\colon [a_0 - h, a_0 + h] \to \mathbb{R}$ of (10) up to 2^{-k} such that $\varphi(a_0) = b_0$.*

Proof. By definition of h, the rectangle

$$S \text{ given by } |x - a_0| \leq h,\ |y - b_0| \leq Mh$$

is in D. f is continuous, hence comes with a modulus of (uniform) continuity; so for our given k we have an l such that

$$|f(\tilde{x}, \tilde{y}) - f(x, y)| \leq 2^{-k-1} \tag{11}$$

for $(\tilde{x}, \tilde{y}), (x, y)$ in D and $|\tilde{x} - x|, |\tilde{y} - y| \leq 2^{-l}$.

We now divide the interval $[a_0, a_0 + h]$ such that

(a) $a_0 < a_1 < \cdots < a_{n-1} < a_n = a_0 + h$
(b) $a_i - a_{i-1} \leq \min(2^{-l}, 2^{-l}/M)$ for $i = 1, \ldots, n$

and construct an approximate solution on $[a_0, a_0 + h]$; similarly this can be done on $[a_0 - h, a_0]$.

The idea is to start at (a_0, b_0) and draw a line with slope $f(a_0, b_0)$ until it intersects $x = a_1$, say at (a_1, b_1), then starting from (a_1, b_1) draw a line with slope $f(a_1, b_1)$ until it intersects $x = a_2$, say at (a_2, b_2), etc. Since we want an approximate solution which maps rationals to rationals, we approximate the slopes $f(a_{i-1}, b_{i-1})$ by rationals s_{i-1}.

More precisely, we recursively define for $i = 1, \ldots, n$

$$\begin{aligned}
&\varphi(x) = b_{i-1} + (x - a_{i-1}) s_{i-1} \quad \text{for } a_{i-1} \leq x \leq a_i, \\
&b_i := \varphi(a_i), \\
&-M \leq s_{i-1} \leq M \quad \text{such that } |s_{i-1} - f(a_{i-1}, b_{i-1})| \leq 2^{-k-1}.
\end{aligned}$$

Clearly φ is continuous, admissible and has piecewise derivatives

$$\varphi'(x) = s_{i-1} \quad \text{for } a_{i-1} < x < a_i.$$

Now for $a_{i-1} < x < a_i$ we have $|x - a_{i-1}| \leq 2^{-l}$ and

$$|\varphi(x) - b_{i-1}| \leq |x - a_{i-1}| \cdot |s_{i-1}| \leq \frac{2^{-l}}{M} \cdot M = 2^{-l},$$

hence by (11)

$$\begin{aligned}
|\varphi'(x) - f(x, \varphi(x))| &= |s_{i-1} - f(x, \varphi(x))| \\
&\leq |s_{i-1} - f(a_{i-1}, b_{i-1})| + |f(a_{i-1}, b_{i-1}) - f(x, \varphi(x))| \\
&\leq 2^{-k-1} + 2^{-k-1} = 2^{k}.
\end{aligned}$$

Hence φ is an approximate solution up to 2^{-k}. ∎

The approximate solutions we have constructed are *rational polygons*, i.e., piecewise differentiable continuous functions with rational corners and rational slopes.

Lemma 7.3. *Given a rational polygon φ on $[a, b]$ and $c \in [a, b]$. Then one of the following alternatives will hold.*

(a) *$0 \leq \varphi(x)$ for $a \leq x \leq b$, or*
(b) *$\varphi(x) \leq 0$ for $a \leq x \leq b$, or*
(c) *there is a $d < c$ such that $\varphi(d) = 0$ and either $0 \leq \varphi(x)$ for $d \leq x \leq c$, or else $\varphi(x) \leq 0$ for $d \leq x \leq c$.*

Proof. Let $a = a_0 < a_1 < \cdots < a_n = b$ be the exception points for φ. We can locate c in $a = a_0 < a_1 < \cdots < a_n = b$. Pick i maximal such that $a_{i-1} \le c$. Compare $\varphi(a_0)$, $\varphi(a_1)$, $\varphi(a_{i-1})$ and $\varphi(c)$. If all have the same sign, we are done. Otherwise pick j maximal such that $\varphi(a_j)$ and $\varphi(a_{j+1})$ (or $\varphi(c)$, respectively) change sign. Then we are done as well. ◻

We need an additional restriction in order to estimate the difference of approximate solutions.

Definition 7.4. A function $f\colon D \to \mathbb{R}$, $D \subseteq \mathbb{R}^2$ is said to satisfy a *Lipschitz condition* w.r.t. its second argument for the constant $L > 0$, if for every $(x, y_1), (x, y_2) \in D$

$$|f(x, y_1) - f(x, y_2)| \le L|y_1 - y_2|.$$

Theorem 7.5 (Fundamental Inequality). *Let $f\colon D \to \mathbb{R}$ be continuous, and satisfy a* Lipschitz *condition w.r.t. its second argument for the constant $L > 0$. Let*

$$\varphi, \psi\colon [a, b] \to \mathbb{R}$$

be solutions up to $2^{-k}, 2^{-l}$ of (10). Assume $\varphi \le \psi$ on I, or else that φ and ψ are rational polygons. Then

$$\bigl|\psi(x) - \varphi(x)\bigr| \le e^{L(x-a)}\bigl|\psi(a) - \varphi(a)\bigr| + \frac{2^{-k} + 2^{-l}}{L}\bigl(e^{L(x-a)} - 1\bigr)$$

for all $x \in [a, b]$.

Proof. Part 1. $\varphi \le \psi$ in I. Let $\sigma := \psi - \varphi$. By Definition 7.1 we have for all points except finitely many

$$\bigl|\varphi'(x) - f(x, \varphi(x))\bigr| \le 2^{-k} \quad \text{and} \quad \bigl|\psi'(x) - f(x, \psi(x))\bigr| \le 2^{-l},$$

hence with $\varepsilon := 2^{-k} + 2^{-l}$

$$\psi'(x) - \varphi'(x) \le \bigl|f(x, \psi(x)) - f(x, \varphi(x))\bigr| + \varepsilon \le L\bigl(\psi(x) - \varphi(x)\bigr) + \varepsilon$$

by the Lipschitz condition, hence

$$\sigma'(x) \le L\sigma(x) + \varepsilon.$$

Therefore

$$\int_a^x e^{-Lt}\bigl(\sigma'(t) - L\sigma(t)\bigr)\, dt \le \varepsilon \int_a^x e^{-Lt}\, dt.$$

The integrand on the left-hand side has finitely many discontinuities but a continuous indefinite integral, so

$$\begin{aligned}
&\bigl[e^{-Lt}\sigma(t)\bigr]_a^x \le \varepsilon\bigl[-\frac{1}{L}e^{-Lt}\bigr]_a^x \\
&e^{-Lx}\sigma(x) - e^{-La}\sigma(a) \le \frac{\varepsilon}{L}\Bigl(e^{-La} - e^{-Lx}\Bigr) \\
&\sigma(x) \le e^{L(x-a)}\sigma(a) + \frac{\varepsilon}{L}\bigl(e^{L(x-a)} - 1\bigr),
\end{aligned}$$

which is the required inequality.

Part 2. φ and ψ are rational polygons. It suffices to prove the claim for a rational c. By Lemma 7.3 we can assume $\varphi(d) = \psi(d)$ for some $d < c$, and $\varphi(x) \le \psi(x)$ for $d \le x \le c$. Then by the first part

$$\psi(c) - \varphi(c) \le \frac{2^{-k} + 2^{-l}}{L}\bigl(e^{L(c-d)} - 1\bigr),$$

which is an even stronger inequality. ◻

To prove uniqueness of solutions as well as the existence of exact solutions, we again need the Lipschitz condition.

Theorem 7.6 (Uniqueness). *Let $f\colon D \to \mathbb{R}$ be continuous, and satisfy a* Lipschitz *condition w.r.t. its second argument. Let*

$$\varphi, \psi\colon I \to \mathbb{R}$$

be two (exact) solutions of (10). *If $\varphi(a) = \psi(a)$ for some $a \in I$, then $\varphi(x) = \psi(x)$ for all $x \in I$.*

Proof. We show that $\varphi(x) = \psi(x)$ for $a \le x \le a + L/2$, $x \in I$. Similarly this can be shown for $a - L/2 \le x \le a$; hence the claim follows.

Integrating the two equations

$$\varphi'(x) = f(x, \varphi(x)) \quad \text{and} \quad \psi'(x) = f(x, \psi(x))$$

we obtain from $\varphi(a) = \psi(a)$

$$\varphi(x) - \psi(x) = \int_a^x \big(f(t, \varphi(t)) - f(t, \psi(t))\big)\, dt$$

and hence

$$|\varphi(x) - \psi(x)| \le \int_a^x \big|f(t, \varphi(t)) - f(t, \psi(t))\big|\, dt \le L \int_a^x \big|\varphi(t) - \psi(t)\big|\, dt.$$

Let M be the supremum of the range of $|\varphi - \psi|$ on $[a, a+L/2]$. Then for $a \le x \le a+L/2$

$$|\varphi(x) - \psi(x)| \le L(x-a)M \le \frac{1}{2}M,$$

hence $M = 0$ and therefore $\varphi = \psi$ on $[a, a + L/2]$. ∎

The example

$$y' = y^{1/3}, \quad y(0) = y_0. \tag{12}$$

shows that the Lipschitz condition is indeed necessary for uniqueness: for $y_0 = 0$ we have two solutions $\varphi(x) = 0$ und $\varphi(x) = (\frac{2}{3}x)^{3/2}$.

Theorem 7.7 (Exact Solution). *Let $f\colon D \to \mathbb{R}$ be continuous, and satisfy a* Lipschitz *condition w.r.t. its second argument. Let $(a_0, b_0) \in D$ such that the rectangle R given by $|x - a_0| \le a$, $|y - b_0| \le b$ is in D. Assume $|f(x,y)| \le M$ for $(x,y) \in R$, and let $h := \min(a, b/M)$. Then we can construct an exact solution $\varphi\colon [a_0 - h, a_0 + h] \to \mathbb{R}$ of* (10) *such that $\varphi(a_0) = b_0$.*

Proof. By Theorem 7.2 we have an approximate solution φ_n up to 2^{-n}, which is a rational polygon, over $I := [a_0 - h, a_0 + h]$.

By Lemma 6.4 the sequence $(\varphi_n)_{n\in\mathbb{N}}$ uniformly converges over I to a continuous function φ. Hence the sequence $(f(x, \varphi_n(x)))_n$ of continuous functions uniformly converges over I to the continuous function $f(x, \varphi(x))$.[2] Therefore, by Theorem 6.5,

$$\lim_{n\to\infty} \int_a^b f(t, \varphi_n(t))\, dt = \int_a^b f(t, \varphi(t))\, dt.$$

We now prove that φ is an exact solution. By the choice of φ_n

$$\big|\varphi_n'(x) - f(x, \varphi_n(x))\big| \le 2^{-n}$$

for all $x \in I$ where $\varphi_n'(x)$ is defined. Integrating this inequality from a_0 to x gives

$$\left|\int_{a_0}^x \left[\varphi_n'(t) - f(t, \varphi_n(t))\right] dt\right| \le 2^{-n}(x - a_0) \le 2^{-n}h.$$

[2] This is best proved by a slightly more general setup, where metric spaces (e.g., $\mathbb{R}^2$) are considered. One shows that if φ_n, ψ_n are uniformly convergent to φ, ψ, respectively, then (φ_n, ψ_n) is uniformly convergent to (φ, ψ), and if φ_n is uniformly convergent to φ, then $f(\varphi_n(x))$ is uniformly convergent to $f(\varphi(x))$.

Since φ_n is continuous, by the Fundamental Theorem 5.4 of Calculus

$$\left|\varphi_n(x) - \varphi_n(a_0) - \int_{a_0}^{x} f(t, \varphi_n(t))\, dt\right| \leq 2^{-n}h.$$

Approaching this limit gives

$$\varphi(x) - \varphi(a_0) - \int_{a_0}^{x} f(t, \varphi(t))\, dt = 0.$$

Differentiation yields $\varphi'(x) = f(x, \varphi(x))$, and $\varphi_n(a_0) = b_0$ entails $\varphi(a_0) = b_0$. □

For the construction above of an exact solution we have made use of the LIPSCHITZ condition. However, it is well known that classically one has PEANO's existence theorem, which does not require a LIPSCHITZ condition.

Following [1, 7] we now want to argue that PEANO's existence theorem entails that for every real x we can decide whether $x \geq 0$ or $x \leq 0$, hence we cannot expect to be able to prove it constructively.

Consider again the initial value problem (12). First note that the continuous function $f(x, y) := y^{1/3}$ satisfies a LIPSCHITZ condition w.r.t. its second argument, for $0 < a < y < b$ (and similarly for $b < y < a < 0$). To see this, use Lemma 4.2. So it suffices to find a bound on the derivative of $y^{1/3}$. But this is easy, since $\frac{d}{dy} y^{1/3} = \frac{1}{3} y^{-2/3} < \frac{1}{3} a^{-2/3}$ for $0 < a < y < b$.

Therefore in case $y_0 > 0$ the solution $\varphi_+(x) := (\frac{2}{3}x + y_0^{2/3})^{3/2}$ is unique, and similarly in case $y_0 < 0$ the solution $\varphi_-(x) := -(\frac{2}{3}x + |y_0|^{2/3})^{3/2}$ is unique. Pick $|y_0|$ small enough such that $(\frac{2}{3} - |y_0|^{2/3})^{3/2} > \frac{1}{2}$.

Now suppose that (12) has a solution φ, for a given real y_0. Compare $\varphi(1)$ with $[-1/2, 1/2]$. If $\varphi(1) < 1/2$, then $y_0 \not> 0$, hence $y_0 \leq 0$. If $-1/2 < \varphi(1)$, then $y_0 \not< 0$, hence $y_0 \geq 0$.

8. Related Work on Exact Real Numbers

There are many approaches to exact real number computation in the literature. One of those - using MÖBIUS (or linear fractional) transformations - has been put forward by EDALAT; a good survey can be found in [8] (see also [9]). Exact real numbers based on the so-called redundant b-adic notation have been treated by WIEDMER [18] and by BÖHM and CARTWRIGHT [6], and based on continued fractions by GOSPER (1972), VUILLEMIN [17], NIELSEN and KORNERUP [14] and recently by GEUVERS and NIQUI [11].

Generally, one can see these approaches as either using CAUCHY sequences with (fixed or separately given) modulus, or else DEDEKIND cuts. We prefer CAUCHY sequences over DEDEKIND cuts, since the latter are given by sets, and hence we would need additional enumerating devices in order to compute approximations of a real number presented as a DEDEKIND cut. There is not much of a difference between fixed or separate moduli for CAUCHY sequences: one can always transform one form into the other. However, in order to keep the standard series representations of particular reals (like e) we prefer to work with separate moduli.

A recent treatment (including an implementation in MATHEMATICA) has been given by ANDERSSON in his Master's thesis [2] (based on PALMGREN's [15]). He treats trigonometric functions, and includes PICARD's and EULER's methods to constructively prove the existence of solutions for differential equations.

Some authors (in particular the so-called Russian school) restrict attention to computable real numbers. We do not want to make this restriction, since it makes sense, also constructively, to speak about arbitrary sequences. This view of higher type computability is the basis of Scott/Ershov domain theory, and we would like to adopt it here.

However, the domain theoretic setting for dealing with exact real numbers (cf. Escardó, Edalat and the recent [10]) is usually done in such a way that continuous functions are viewed as objects of the function domain, and hence are objects of type level 2. This clearly is one type level higher than necessary, since a continuous function is determined by its values on the rational numbers already. In particular from the point of view of program extraction it seems crucial to place objects as basic as continuous functions at the lowest possible type level. Therefore we propose a special concept of continuous functions, as type 1 objects.

References

1. Oliver Aberth, *Computable analysis and differential equations*, In A. Kino and Vesley [13], pp. 47–52.
2. Patrik Andersson, *Exact real arithmetic with automatic error estimates in a computer algebra system*, Master's thesis, Mathematics department, Uppsala University, 2001.
3. Errett Bishop, *Foundations of constructive analysis*, McGraw-Hill, New York, 1967.
4. ______, *Mathematics as a numerical language*, In A. Kino and Vesley [13], pp. 53–71.
5. Errett Bishop and Douglas Bridges, *Constructive analysis*, Grundlehren der mathematischen Wissenschaften, vol. 279, Springer, Berlin, 1985.
6. Hans Boehm and Robert Cartwright, *Exact real arithmetic. formulating real numbers as functions*, Research Topics in Functional Programming, Addison Wesley, 1990, pp. 43–64.
7. Douglas Bridges, *A Note on the Existence of Solutions for ODEs*, Unpublished note, June 2003.
8. Abbas Edalat, *Exact real number computation using linear fractional transformations*, Tech. report, Imperial College, Dept. of Computing, 2003.
9. Abbas Edalat and Reinhold Heckmann, *Computing with real numbers: (i) LFT approach to real computations, (ii) domain-theoretic model of computational geometry*, Proc APPSEM Summer School in Portugal (G. Barthe et al., ed.), LNCS, Springer Verlag, Berlin, Heidelberg, New York, 2001.
10. Abbas Edalat and Dirk Pattinson, *Initial value problems in domain theory*, To appear: Computation in Analysis.
11. Herman Geuvers and Milad Niqui, *Constructive reals in coq: Axioms and categoricity*, Proc. Types 2000 (P. Callaghan, Z. Luo, J. McKinna, and R. Pollack, eds.), LNCS, vol. 2277, Springer Verlag, Berlin, Heidelberg, New York, 2000, pp. 79–95.
12. Witold Hurewicz, *Lectures on ordinary differential equations*, MIT Press, Cambridge, Mass., 1958.
13. A. Kino, J. Myhill, and R.E. Vesley (eds.), *Intuitioninism and proof theory*, Studies in logic and the foundations of mathematics, North–Holland, Amsterdam, 1970.
14. Asger Munk Nielsen and Peter Kornerup, *MSB-first digit serial arithmetic*, Journal of Univ. Comp. Science **1** (1995), no. 7, 523–543.
15. Erik Palmgren, *Constructive nonstandard analysis*, Méthods et analyse non standard (A. Petry, ed.), vol. 9, Cahiers du Centre de Logique, 1996, pp. 69–97.
16. Peter Schuster and Helmut Schwichtenberg, *Constructive solutions of continuous equations*, One Hundred Years of Russell's Paradox. International Conference in Logic and Philosophy. Munich, Germany, June 2–5, 2001 (G. Link, ed.), de Gruyter, 2003, To appear, pp. ??–??
17. Jean Vuillemin, *Exact real computer arithmetic with continued fractions*, IEEE Transactions on Computers **39** (1990), no. 8, 1087–1105.
18. E. Wiedmer, *Computing with infinite objects*, Theoretical Computer Science **10** (1980), 133–155.