数理解析研究所講究録
1169 巻 2000 年 76-83

Feasibly constructive analysis

Hajime Ishihara
School of Information Science
Japan Advanced Institute of Science and Technology
Tatsunokuchi, Ishikawa 923-1292, Japan.

1 Introduction

In the constructive theory of real numbers developed, for example in [4, Chapter 5], we assume that a universe $\mathcal{U}$ of functions on natural numbers satisfies certain closure conditions; a very weak axiom of choice QF-AC_{00}:

$$\forall\vec{m}\exists nA(\vec{m},n) \implies \exists\alpha\in\mathcal{U}\forall\vec{m}A(\vec{m},\alpha(\vec{m})) \quad (A \text{ quantifier-free})$$

expressing the fact that $\mathcal{U}$ is closed under *recursive in* is assumed in [4, Chapter 5].

On the other hand, various classes of functions on natural numbers have been defined as function algebras [1]; a *function algebra* is the smallest class of functions containing certain initial functions and closed under certain operations (especially composition and recursion scheme). For example, A. Cobham [2] characterized the polynomial time computable functions as the smallest class closed under *bounded recursion on notation*; see [3] for other characterizations of the polytime functions.

We give some elementary results and problems on the constructive theory of real numbers and analysis with a universe $\mathcal{U}$ which contains zero-function $0(m)=0$, projection $P_k^n(m_1,\ldots,m_n)=m_k$, the binary successor functions $s_0(m)=2\cdot m, s_1(m)=2\cdot m+1$, the length in binary function $|m|=\lceil\log_2(m+1)\rceil$, addition $+$, cut-off subtraction $\dot{-}$ ($m\dot{-}n=m-n$ if $m\geq n$ 0 otherwise) and $pad(m,n)=2^{|n|}\cdot m$, and closed under composition: if $g_1,\ldots,g_k,h\in\mathcal{U}$, then there is an $f\in\mathcal{U}$ such that

$$f(\vec{m})=h(g_1(\vec{m}),\ldots,g_k(\vec{m})).$$

Furthermore we assume that a universe $\mathcal{U}$ contains a pairing function $\langle\cdot,\cdot\rangle$ and its inverses π_1, π_2 such that

$$\pi_1(\langle m,n\rangle) = m, \quad \pi_2(\langle m,n\rangle) = n;$$

for then $\langle m,n\rangle$ code the integer $m-n$, $\langle m,n\rangle =_{\mathbb{Z}} \langle m',n'\rangle$ if $m+n' = m'+n$,

$$\begin{aligned}
\langle m,n\rangle +_{\mathbb{Z}} \langle m',n'\rangle &:= \langle m+m', n+n'\rangle, \\
-\langle m,n\rangle &:= \langle n,m\rangle, \\
|\langle m,n\rangle| &:= (m \dot{-} n) + (n \dot{-} m), \\
pad_{\mathbb{Z}}(\langle m,n\rangle, l) &:= \langle (pad(m,l), pad(n,l))
\end{aligned}$$

etcetc; and then $\langle i,m\rangle$ code the dyadic rationals $i/2^{|m|}$ where i is an integer, $\langle i,m\rangle =_{\mathbb{Q}} \langle j,n\rangle$ if $pad_{\mathbb{Z}}(i,n) =_{\mathbb{Z}} pad_{\mathbb{Z}}(j,m)$,

$$\begin{aligned}
\langle i,m\rangle +_{\mathbb{Q}} \langle j,n\rangle &:= \langle pad_{\mathbb{Z}}(i,n) + pad_{\mathbb{Z}}(j,m), pad(m,n)\rangle, \\
-\langle i,m\rangle &:= \langle -i, m\rangle, \\
|\langle i,m\rangle| &:= \langle |i|, m\rangle
\end{aligned}$$

etcetc.

2 Real numbers

Definition 1. A *real number* is a sequence $\{p_n\}_n$ of dyadic rationals such that

$$\forall mn \left(|p_m - p_n| < 2^{-|m|} + 2^{-|n|}\right).$$

We shall use a notation $\{p_n\}_n \in \mathbb{R}$ to mean $\{p_n\}_n$ is a real number.

Definition 2. Let $x := \{p_n\}_n, y := \{q_n\}_n \in \mathbb{R}$, and put

$$x < y := \exists n \left(q_n - p_n > 2^{-|n|+2}\right).$$

Lemma 3. *Let* $x, y, z \in \mathbb{R}$. *Then*

1. $\neg(x < y \wedge y < x)$,

2. $x < y \implies x < z \vee z < y$.

Proof. (1). Let $x = \{p_n\}_n$ and $y = \{q_n\}_n$, and suppose that $x < y \wedge y < x$. Then there exist n, n' such that

$$q_n - p_n > 2^{-|n|+2} \quad \text{and} \quad p_{n'} - q_{n'} > 2^{-|n'|+2},$$

and hence

$$\begin{aligned} 0 &= (q_n - p_n) + (p_{n'} - q_{n'}) - (p_{n'} - p_n) - (q_n - q_{n'}) \\ &> 2^{-|n|+2} + 2^{-|n'|+2} - \left(2^{-|n'|} + 2^{-|n|}\right) - \left(2^{-|n|} + 2^{-|n'|}\right) \\ &= 2^{-|n|+1} + 2^{-|n'|+1} \\ &> 0, \end{aligned}$$

a contradiction.

(2). Let $x = \{p_n\}_n$, $y = \{q_n\}_n$ and $z = \{r_n\}_n$, and suppose that $x < y$. Then there exists n such that

$$q_n - p_n > 2^{-|n|+2}.$$

Letting $N := 8n + 7$, either $(p_n + q_n)/2 < r_N$ or $r_N \leq (p_n + q_n)/2$. In the former case, we have

$$\begin{aligned} r_N - p_N &> \frac{p_n + q_n}{2} - p_N \\ &= \frac{p_n + q_n}{2} - p_n - (p_N - p_n) \\ &= \frac{q_n - p_n}{2} - (p_N - p_n) \\ &> 2^{-|n|+1} - (2^{-|n|-3} + 2^{-|n|}) \\ &= 7 \cdot 2^{-|n|-3} > 2^{-|N|+2}, \end{aligned}$$

and hence, $x < z$. In the latter case, we have

$$\begin{aligned} q_N - r_N &\geq q_N - \frac{p_n + q_n}{2} \\ &= (q_N - q_n) + q_n - \frac{p_n + q_n}{2} \\ &= (q_N - q_n) + \frac{q_n - p_n}{2} \\ &> -(2^{-|n|-3} + 2^{-|n|}) + 2^{-|n|+1} \\ &> 2^{-|N|+2}, \end{aligned}$$

and hence $z < y$. □

Definition 4. For $x, y \in \mathbb{R}$, define

1. $x\#y := (x < y \vee y < x)$,
2. $x = y := \neg(x\#y)$,
3. $x \leq y := \neg(y < x)$.

Lemma 5. *Let $x, y, z \in \mathbb{R}$. Then*

1. $x\#y \iff y\#x$,
2. $x\#y \implies x\#z \vee z\#y$.

Proof. Straightforward. □

Proposition 6. *Let $x, y, z \in \mathbb{R}$. Then*

1. $x = x$,
2. $x = y \implies y = x$,
3. $x = y \wedge y = z \implies x = z$.

Proof. (1), (2). Trivial

(3). If $x = y \wedge y = z$, then $\neg(x\#y) \wedge \neg(y\#z)$, and hence $\neg(x\#y \vee y\#z)$. Therefore $\neg(x\#z)$ by Lemma 5 (2), and so $x = z$. □

Proposition 7. *Let $x, x', y, y' \in \mathbb{R}$. Then*

1. $x = x' \wedge y = y' \wedge x < y \implies x' < y'$,
2. $\neg\neg(x < y \vee x = y \vee y < x)$,
3. $x < y \wedge y < z \implies x < z$.

Proof. (1). Suppose that $x = x' \wedge y = y' \wedge x < y$. Then either $x < x'$ or $x' < y$ by Lemma 3 (2). In the former case, we have $x\#x'$, and hence $\neg(x = x')$, a contradiction. In the latter case, we have $x' < y' \vee y' < y$; if $y' < y$, then $\neg(y' = y)$, a contradiction, and hence $x' < y'$.

(2). Trivial.

(3). Suppose that $x < y \wedge y < z$ Then either $x < z$ or $z < y$. In the latter case, we have a contradiction by Lemma 3 (1). Thus the former must be the case. □

Corollary 8. *Let $x, x', y, y', z \in \mathbb{R}$. Then*

1. $x = x' \wedge y = y' \wedge x \# y \implies x' \# y'$,
2. $x = x' \wedge y = y' \wedge x \leq y \implies x' \leq y'$,
3. $x \leq y \iff \neg\neg(x < y \vee x = y)$,
4. $\neg\neg(x \leq y \vee y \leq x)$,
5. $x \leq y \wedge y \leq x \implies x = y$,
6. $x < y \wedge y \leq z \implies x < z$,
7. $x \leq y \wedge y < z \implies x < z$,
8. $x \leq y \wedge y \leq z \implies x \leq z$.

Proof. (1), (2), (3), and (4) are straightforward.

(5). Suppose that $x \leq y \wedge y \leq x$ Then $\neg(y < x \vee x < y)$, and hence $\neg(x \# y)$. Thus $x = y$.

(6). Suppose that $x < y \wedge y \leq z$ Then either $x < z$ or $z < y$. In the latter case, we have a contradiction. Thus the former must be the case.

(7). Similar to (6).

(8). Suppose that $x \leq y \wedge y \leq z$ and $z < x$. Then either $z < y$ or $y < x$. In the former case, we have $y < y$ by (7), a contradiction. In the latter case, we have $x < x$, a contradiction. Thus $x \leq z$. □

Lemma 9. *For each $x := \{p_n\}_n \in \mathbb{R}$, we have*

$$\forall n \left(|p_n - x| \leq 2^{-|n|} \right).$$

Proof. Suppose that $|p_n - x| > 2^{-|n|}$. Then there exists m such that

$$2^{-|m|+2} < |p_n - p_{2m+1}| - 2^{-|n|} < 2^{-|m|-1},$$

a contradiction. □

3 Completeness

Definition 10. A *sequence of real numbers* $\{x_m\}_m$ is a double sequence $\{\{p_n^m\}_n\}_m$ of dyadic rationals such that $\{p_n^m\}_n \in \mathbb{R}$ for each m.

Definition 11. A sequence $\{x_n\}_n$ of reals is said to *converge* to x with *modulus* $\beta \in \mathbb{N} \to \mathbb{N}$ if

$$\forall kn(|x - x_{\beta k+n}| < 2^{-|k|}).$$

Then x is said to be the *limit* of $\{x_n\}_n$.

Definition 12. A sequence $\{x_n\}_n$ of reals is said to be a *Cauchy sequence* with *modulus* $\alpha \in \mathbb{N} \to \mathbb{N}$ if

$$\forall kmn(|x_{\alpha k+m} - x_{\alpha k+n}| < 2^{-|k|}).$$

Theorem 13. *Each Cauchy sequence of reals converges to a limit.*

Proof. Let $\{x_m\}_m := \{\{p_n^m\}_n\}_m$ be a Cauchy sequence of reals with modulus α, i.e.

$$\forall kmn(|x_{\alpha k+m} - x_{\alpha k+n}| < 2^{-|k|}),$$

and define a sequence $\{q_n\}_n$ of dyadic rationals by

$$q_n := p_{2n+1}^{\alpha(2n+1)}.$$

Then since $|q_n - x_{\alpha(2n+1)}| \leq 2^{-|n|-1})$ for all n, we have

$$\begin{aligned} |q_m - q_n| &\leq |q_m - x_{\alpha(2m+1)}| + |x_{\alpha(2m+1)} - x_{\alpha(2n+1)}| + |x_{\alpha(2n+1)} - q_n| \\ &\leq 2^{-|m|-1} + 2^{-|m|-1} + 2^{-|n|-1} + 2^{-|m|-1} = 2^{-|m|} + 2^{-|n|}. \end{aligned}$$

Therefore $x := \{q_n\}_n$ is a real number. Furthermore we have

$$\begin{aligned} |x - x_{\alpha(4k+3)+m}| &\leq |x - q_{2k+1}| + |q_{2k+1} - x_{\alpha(4k+3)}| + |x_{\alpha(4k+3)} - x_{\alpha(4k+3)+m}| \\ &< 2^{-|k|-1} + 2^{-|k|-2} + 2^{-|k|-2} = 2^{-|k|}, \end{aligned}$$

and hence $\{x_n\}_n$ converges to x with a modulus $\beta n := \alpha(4n+3)$. □

4 Intermediate-value

In this section, we assume that our universe $\mathcal{U}$ is closed under *full concatenation recursion on notation* (FCRN) which is used in [3] to characterize the polytime functions: if $g, h_0, h_1 \in \mathcal{U}$ with $h_0(m, \vec{n}, l), h_1(m, \vec{n}, l) \leq 1$, then there is an $f \in \mathcal{U}$ such that

$$\begin{aligned} f(0, \vec{n}) &= g(\vec{n}), \\ f(s_i(m), \vec{n}) &= s_{h_i(m,\vec{n},f(m,\vec{n}))}(f(m, \vec{n})) \quad (\text{if } i \neq 0 \text{ or } m \neq 0) \end{aligned}$$

Theorem 14. *Let $f \in [0,1] \to \mathbb{R}$ be continuous with $f(0) \leq 0 \leq f(1)$. Then*

$$\forall k \exists x \in [0,1](|f(x)| < 2^{-|k|}.$$

Proof. Let $\lambda(n, k, m)$ be the characteristic function of the predicate

$$\left(f\left(\frac{2m+1}{2^{|n|+1}}\right)\right)_{2k+1} < 0,$$

define a function ϕ by FCRN

$$\begin{aligned} \phi(0, k) &= 0 \\ \phi(s_i(n), k) &= s_{\lambda(n,k,\phi(n,k))}(\phi(n, k)), \quad (\text{if } i \neq 0 \vee n \neq 0) \end{aligned}$$

and let

$$p_{n,k} := \frac{\phi(n,k)}{2^{|n|}} \quad \text{and} \quad q_{n,k} := \frac{\phi(n,k)+1}{2^{|n|}}.$$

Then we can show, by induction, that for each n

$$(f(p_{n,k}))_{2k+1} \leq 0 \quad \text{and} \quad (f(q_{n,k}))_{2k+1} \geq 0.$$

They are trivial when $n = 0$. Suppose that $n = s_i(n')$ and $i \neq 0 \vee n' \neq 0$. Then either $\lambda(n', k, \phi(n', k)) = 0$ or $\lambda(n', k, \phi(n', k)) = 1$. In the former case, since

$$p_{n,k} = \frac{s_0(\phi(n',k))}{2^{|s_0(n')|}} = \frac{2\phi(n',k)}{2^{|n'|+1}} = p_{n',k},$$

we have

$$(f(p_{n,k}))_{2k+1} = (f(p_{n',k}))_{2k+1} \leq 0$$

by the induction hypothesis, and since $\lambda(n', k, \phi(n', k)) = 0$, we have

$$(f(q_{n,k}))_{2k+1} = \left(f\left(\frac{2\phi(n',k)+1}{2^{|n'|+1}}\right)\right)_{2k+1} \geq 0.$$

Similarly, in the latter case, we have the inequalities. Therefore we have

$$f(p_{n,k}) \leq (f(p_{n,k}))_{2k+1} + 2^{-|k|-1} \leq 2^{-|k|-1}$$

and

$$f(q_{n,k}) \geq (f(q_{n,k}))_{2k+1} - 2^{-|k|-1} \geq -2^{-|k|-1}.$$

Letting $x := \{p_{n,k}\}_n$ and $y := \{q_{n,k}\}_n$, we have $x, y \in \mathbb{R}$ and $x = y$. Since $\{p_{n,k}\}_n$ and $\{q_{n,k}\}_n$ converge to x and f is continuous, we have $|f(x)| \leq 2^{-|k|-1} < 2^{-|k|}$. □

References

[1] P. Clote, *Computational models and functional algebras*, in E.R. Griffor ed., Handbook of Computability Theory, North-Holland, forthcomming.

[2] A. Cobham, *The intrinsic computational difficulty of functions*, in Y. Bar-Hillel ed., Logic, Methodology and Philosophy of Science II, North-Holland, 1965, 24-30.

[3] H. Ishihara, *Function algebraic characterizations of the polytime functions*, Computational Complexity, to appear.

[4] A. S. Troelstra and D. van Dalen, *Constructivism in Mathematics*, Vol. 1, North-Holland, 1988.