CS3110 Spring 2016 Lecture 12: Developing Constructive Analysis

Reminder: Prelim in class next week. It will not cover the real numbers beyond this lecture. Lecture 13 will be a prelim review plus a bit on the reals.

Topics

- Background to Bishop's account of constructive analysis
- Bishop's preliminaries
  - *operation* versus *function* and the importance of equality
  - Bishop uses "set" where we say "type". He requires a notion of equality of elements for every set.
  - One-one function is a correspondence.
    - *Countably infinite* is 1-1 correspondence with $\mathbb{Z}^+$.
      $\mathbb{Q}$ is countably infinite. See *enumeration* of the rationals, page 17, 1.3.
    - *Finite sets* iff 1-1 correspondences with $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ (could use $\{1, 2, ..., n\}$)
    - To say that a set is *subfinite* is to say that it has *at most* n elements.

- Bishop uses *constructive logic*, related to the OCaml "logical types."

$A \Rightarrow B$	iff	there is a computable function from evidence for A to evidence for B.
$A\&B$	iff	there is (we know) evidence for A and B.
$A \vee B$	iff	there is evidence for A (tagged "left") or for B ("right")
$\sim A$	iff	$A \Rightarrow$ False False is the empty set.
$\forall x{:}T.A(x)$	iff	there is a computable function f taking any $t \in T$ to evidence for $A(t)$
$\exists x{:}T.A(x)$	iff	there is a pair $<t, a>$ where $t \in T$ and a is evidence for $A(t)$

  Note: $\forall x$ and $\exists x$ are examples of *dependent types.* (See attached pages 10-11 from Bishop.)

Constructive logic

Bishop and Bridges use *constructive logic* for their development of analysis. The development of this logic dates back to Brouwer in 1907 and then to many logicians especially in Holland, France, the US, and Russia including Poincaré, Heyting, Kleene, Kolmogorov, Markov, Martin-Löf, Curry, Howard, Girard, and many others.

Constructive logic is closely related to the program types that give a computational understanding of propositional operators.

$A\&B$	as	$\alpha * \beta$
$A \Rightarrow B$	as	$\alpha \to \beta$
$A \vee B$	as	$L\alpha \| R\beta$
False	as	Void
True	as	Unit
$\sim A$	as	$\alpha \to$ Void

When we can find data in the program types, we know that the corresponding logical expression is constructively true.

Historical background to Bishop

Greek geometry was "constructive" using straight edge and compass. But the Greeks "feared" the idea of *infinity* or unbounded constructions. They loved rational numbers and harmonics.

The idea of a *function* did not become clear until the 1800's "y varies with x according to some law."

- Cauchy – 1821 "Course in analysis."
- Weierstrauss – by 1859 (high school teacher)

	1880 split	
	↙ ↘	
Dedekind		Kronecker
Cantor		Poincaré
Weierstrauss		Weil
Hilbert		Weyl

Brouwer 1907, 1912 (Intuitionism and Formalism)
Heyting 1956, Intuitionism
Turing 1936, On computable numbers with an application to the Entscheidungs problem

Note, Turing made a mistake in defining the reals computationally, a common one. He published a correction in 1937. He originally said that a real number is computable iff we can compute its (unending) decimal by a (Turing) machine. See Bishop p.62 problem 9.

Note further, Brouwer allowed a more general notion of computability which could involve "free choice sequences." Nuprl follows Brouwer, Coq follows Bishop. There is a large library of real analysis built using Coq.

Further motivation to study constructive reals

One reason to study constructive reals is that the proof assistants are making them practical for results in *cyber-physical systems* (CPS). Another reason is that the computer science development and implementation are part of the intellectual history of constructive mathematics. Bishop's book is a landmark that computer science has "brought to life" and deepened.

The role of computer science in intellectual history is clear in *theory* (e.g. the notion of computational complexity – two Cornell Turing Awards) and in *artificial intelligence*, the understanding and extension of intelligence. *It is also there in PL as computer science enriches the type systems and capabilities of programming languages to support high level programming of cyber-physical systems, computational geometry, homotopy type theory (HTT), and other areas of mathematics.*

Differences between constructive analysis over the reals, $\mathbb{R}$, and ordinary calculus over the "classical" reals

1. In calculus books, the operations on the reals are not defined by algorithms. Indeed we imagine that we can say things in calculus that don't make sense computationally. For example, in calculus we assume that given two reals, say r_1 and r_2 we know:

    - Is $r_1 = r_2$? – In fact we can't decide this in general.
    - Is $r_1 = 0$? – We can't decide this in general.
    - Is $r_1 < r_2$? – We can't decide this in general.

    Bishop needed results such as Proposition 2.16 and Corollary 2.17, page 26, to deal with these concepts constructively.

2. We will see that all functions on the reals are continuous. It is not possible to create "step functions."

is countably infinite. A similar proof using (1.2) shows that $\mathbb{Z} \times \mathbb{Z}$ is countably infinite

A set which is in one-one correspondence with $\mathbb{Z}_n$ is said to *have n elements*, and to be *finite*. Every finite set is countable.

It is not true that every countable set is either countably infinite or subfinite. For example, let A consist of all positive integers n such that both n and $n+2$ are prime; then A is countable, but we do not know if it is either countably infinite or subfinite. This does not rule out the possibility that at some time in the future A will have become countably infinite or subfinite; it is possible that tomorrow someone will show that A is subfinite. This set A has the property that if it is subfinite, then it is finite. Not all sets have this property.

2. The Real Number System

The following definition is basic to everything that follows.

(2.1) **Definition.** A sequence (x_n) of rational numbers is *regular* if

(2.1.1) $$|x_m - x_n| \leqq m^{-1} + n^{-1} \quad (m, n \in \mathbb{Z}^+).$$

A *real number* is a regular sequence of rational numbers. Two real numbers $x \equiv (x_n)$ and $y \equiv (y_n)$ are *equal* if

(2.1.2) $$|x_n - y_n| \leqq 2n^{-1} \quad (n \in \mathbb{Z}^+).$$

The set of real numbers is denoted by $\mathbb{R}$.

(2.2) **Proposition.** *Equality of real numbers is an equivalence relation.*

Proof: Parts (i) and (ii) of (1.1) are obvious. Part (iii) is a consequence of the following lemma.

(2.3) **Lemma.** *The real numbers $x \equiv (x_n)$ and $y \equiv (y_n)$ are equal if and only if for each positive integer j there exists a positive integer N_j such that*

(2.3.1) $$|x_n - y_n| \leqq j^{-1} \quad (n \geqq N_j).$$

Proof: If $x = y$, then (2.3.1) holds with $N_j \equiv 2j$.

Assume conversely that for each j in $\mathbb{Z}^+$ there exists N_j satisfying (2.3.1). Consider a positive integer n. If m and j are any positive integers with $m \geqq \max\{j, N_j\}$, then

$$|x_n - y_n| \leqq |x_n - x_m| + |x_m - y_m| + |y_m - y_n|$$
$$\leqq (n^{-1} + m^{-1}) + j^{-1} + (n^{-1} + m^{-1}) < 2n^{-1} + 3j^{-1}.$$

Since this holds for all j in $\mathbb{Z}^+$, (2.1.2) is valid. □

Notice that the proof of Lemma (2.3) singles out a specific N_j satisfying (2.3.1). This situation is typical: every proof of a theorem which asserts the existence of an object must embody, at least implicitly, a finite routine for the construction of the object.

The rational number x_n is called the n^{th} *rational approximation* to the real number $x \equiv (x_n)$. Note that the operation from $\mathbb{R}$ to $\mathbb{Q}$ which takes the real number x into its n^{th} rational approximation is not a function.

For later use we wish to associate with each real number $x \equiv (x_n)$ an integer K_x such that

$$|x_n| < K_x \qquad (n \in \mathbb{Z}^+).$$

This is done by letting K_x be the least integer which is greater than $|x_1| + 2$. We call K_x the *canonical bound* for x.

The development of the arithmetic of the real numbers offers no surprises: we operate with real numbers by operating with their rational approximations.

(2.4) **Definition.** Let $x \equiv (x_n)$ and $y \equiv (y_n)$ be real numbers with respective canonical bounds K_x and K_y. Write

$$k \equiv \max\{K_x, K_y\}.$$

Let α be any rational number. We define

(a) $x + y \equiv (x_{2n} + y_{2n})_{n=1}^{\infty}$

(b) $xy \equiv (x_{2kn} y_{2kn})_{n=1}^{\infty}$

(c) $\max\{x, y\} \equiv (\max\{x_n, y_n\})_{n=1}^{\infty}$

(d) $-x \equiv (-x_n)_{n=1}^{\infty}$

(e) $\alpha^* \equiv (\alpha, \alpha, \alpha, \ldots)$.

(2.5) **Proposition.** *The sequences* $x + y$, xy, $\max\{x, y\}$, $-x$, *and* α^* *of Definition* (2.4) *are real numbers.*

Proof (a) Write $z_n \equiv x_{2n} + y_{2n}$ Then $x + y \equiv (z_n)$. For all positive integers m and n,

$$\begin{aligned}|z_m - z_n| &\leqq |x_{2m} - x_{2n}| + |y_{2m} - y_{2n}| \\ &\leqq (2n)^{-1} + (2m)^{-1} + (2n)^{-1} + (2m)^{-1} = n^{-1} + m^{-1}.\end{aligned}$$

Thus $x + y$ is a real number.

(b) Write $z_n \equiv x_{2kn} y_{2kn}$. Then $xy \equiv (z_n)$. For all positive integers m and n,

$$\begin{aligned}|z_m - z_n| &= |x_{2km}(y_{2km} - y_{2kn}) + y_{2kn}(x_{2km} - x_{2kn})| \\ &\leqq k|y_{2km} - y_{2kn}| + k|x_{2km} - x_{2kn}| \\ &\leqq k((2km)^{-1} + (2kn)^{-1} + (2km)^{-1} + (2kn)^{-1}) = n^{-1} + m^{-1}.\end{aligned}$$

Thus xy is a real number.

(c) Write $z_n \equiv \max\{x_n, y_n\}$ Then $\max\{x, y\} \equiv (z_n)$. Consider positive integers m and n. For simplicity assume that

$$x_m = \max\{x_m, x_n, y_m, y_n\}.$$

Then

$$\begin{aligned}|z_m - z_n| &= |x_m - \max\{x_n, y_n\}| \\ &= x_m - \max\{x_n, y_n\} \leqq x_m - x_n \leqq n^{-1} + m^{-1}.\end{aligned}$$

Thus $\max\{x, y\}$ is a real number.

(d) For all positive integers m and n,

$$|-x_m - (-x_n)| = |x_m - x_n| \leqq m^{-1} + n^{-1}.$$

Thus $-x$ is a real number

(e) This is obvious □

There is no trouble in proving that $(x, y) \mapsto x + y$, $(x, y) \mapsto xy$, and $(x, y) \mapsto \max\{x, y\}$ are functions from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, that $x \mapsto -x$ is a function from $\mathbb{R}$ to $\mathbb{R}$; and that $\alpha \mapsto \alpha^*$ is a function from $\mathbb{Q}$ to $\mathbb{R}$.

The operation

$$x \mapsto |x| \equiv \max\{x, -x\}$$

is therefore a function from $\mathbb{R}$ to $\mathbb{R}$, and the operation

$$(x, y) \mapsto \min\{x, y\} \equiv -\max\{-x, -y\}$$

is a function from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$

The next proposition states that the real numbers obey the same rules of arithmetic as the rational numbers.

(2.6) **Proposition.** *For arbitrary real numbers x, y, and z and rational numbers α and β,*

(a) $x + y = y + x$. $xy = yx$

(b) $(x+y)+z=x+(y+z)$, $x(yz)=(xy)z$

(c) $x(y+z)=xy+xz$

(d) $0^*+x=x$, $1^*x=x$

(e) $x-x=0^*$

(f) $|xy|=|x||y|$

(g) $(\alpha+\beta)^*=\alpha^*+\beta^*$, $(\alpha\beta)^*=\alpha^*\beta^*$, *and* $(-\alpha)^*=-\alpha^*$.

We omit the simple proofs of these results.

We shall use standard notations, such as $x+y+z$ and $\max\{x, y, z\}$, without further comment.

There are three basic relations defined on the set of real numbers. The first of these, the equality relation, has already been defined. The remaining relations, which pertain to order, are best introduced in terms of certain subsets $\mathbb{R}^+$ and $\mathbb{R}^{0+}$ of $\mathbb{R}$.

(2.7) **Definition.** A real number $x \equiv (x_n)$ is *positive*, or $x \in \mathbb{R}^+$, if

(2.7.1) $$x_n > n^{-1}$$

for some n in $\mathbb{Z}^+$. A real number $x \equiv (x_n)$ is *nonnegative*, or $x \in \mathbb{R}^{0+}$, if

(2.7.2) $$x_n \geqq -n^{-1} \qquad (n \in \mathbb{Z}^+).$$

The following criteria are often useful

(2.8) **Lemma.** *A real number $x \equiv (x_n)$ is positive if and only if there exists a positive integer N such that*

(2.8.1) $$x_m \geqq N^{-1} \qquad (m \geqq N).$$

A real number $x \equiv (x_n)$ is nonnegative if and only if for each n in $\mathbb{Z}^+$ there exists N_n in $\mathbb{Z}^+$ such that

(2.8.2) $$x_m \geqq -n^{-1} \qquad (m \geqq N_n).$$

Proof: Assume that $x \in \mathbb{R}^+$. Then $x_n > n^{-1}$ for some n in $\mathbb{Z}^+$. Choose N in $\mathbb{Z}^+$ with

$$2N^{-1} \leqq x_n - n^{-1}.$$

Then

$$\begin{aligned} x_m &\geqq x_n - |x_m - x_n| \geqq x_n - m^{-1} - n^{-1} \\ &\geqq x_n - n^{-1} - N^{-1} > N^{-1} \end{aligned}$$

whenever $m \geqq N$. Therefore (2.8.1) is valid.

Conversely, if (2.8.1) is valid, then (2.7 1) holds with $n = N+1$ Therefore $x \in \mathbb{R}^+$.

Assume next that $x \in \mathbb{R}^{0+}$. Then for each positive integer n,

$$x_m \geqq -m^{-1} \geqq -n^{-1} \qquad (m \geqq n).$$

Therefore (2.8.2) is valid with $N_n \equiv n$.

Assume finally that (2.8.2) holds. Then if k, m, and n are positive integers with $m \geqq N_n$, we have

$$x_k \geqq x_m - |x_m - x_k| \geqq -n^{-1} - k^{-1} - m^{-1}.$$

Since m and n are arbitrary, this gives $x_k \geqq -k^{-1}$. Therefore $x \in \mathbb{R}^{0+}$. □

As a corollary of Lemma (2.8), we see that if x and y are equal real numbers, then x is positive if and only if y is positive, and x is nonnegative if and only if y is nonnegative.

It is not strictly correct to say that a real number (x_n) *is* an element of $\mathbb{R}^+$. An element of $\mathbb{R}^+$ consists of a real number (x_n) *and* a positive integer n such that $x_n > n^{-1}$, because an element of $\mathbb{R}^+$ is not presented until both (x_n) and n are given. One and the same real number (x_n) can be associated with two distinct (but equal) elements of $\mathbb{R}^+$ Nevertheless we shall continue to refer loosely to a positive real number (x_n). On those occasions when we need to refer to an n for which $x_n > n^{-1}$, we shall take the position that it was there implicitly all along.

The proof of the following proposition is now easy, and will be left to the reader. For convenience, $\mathbb{R}^*$ represents either $\mathbb{R}^+$ or $\mathbb{R}^{0+}$.

(2.9) **Proposition.** *Let x and y be real numbers. Then*

(a) $x+y \in \mathbb{R}^*$ *and* $xy \in \mathbb{R}^*$ *whenever* $x \in \mathbb{R}^*$ *and* $y \in \mathbb{R}^*$

(b) $x+y \in \mathbb{R}^+$ *whenever* $x \in \mathbb{R}^+$ *and* $y \in \mathbb{R}^{0+}$

(c) $|x| \in \mathbb{R}^{0+}$

(d) $\max\{x, y\} \in \mathbb{R}^*$ *whenever* $x \in \mathbb{R}^*$

(e) $\min\{x, y\} \in \mathbb{R}^*$ *whenever* $x \in \mathbb{R}^*$ *and* $y \in \mathbb{R}^*$.

We now define the order relations on $\mathbb{R}$.

(2.10) **Definition.** Let x and y be real numbers. We define

$$x > y \text{ (or } y < x) \qquad \text{if } x - y \in \mathbb{R}^+$$

and

$$x \geqq y \text{ (or } y \leqq x) \qquad \text{if } x - y \in \mathbb{R}^{0+}.$$

A real number x is *negative* if $x < 0^*$ – that is, if $-x$ is positive.

Consider real numbers x, x', y, and y' such that (i) $x = x'$, $y = y'$, and $x > y$ We have

$$x' - y' = x - y \in \mathbb{R}^+$$

and therefore (ii) $x' > y'$. We express the fact that (ii) holds whenever (i) is valid by saying that $>$ is a *relation* on $\mathbb{R}$. More formally, a *relation* on a set X is a subset S of $X \times X$ such that if x, x', y, y' are elements of X with $x = x'$, $y = y'$, and $(x, y) \in S$, then $(x', y') \in S$.

We express the fact that $x > y$ if and only if $y < x$ by saying that $>$ and $<$ are *transposed relations.* Similarly, $\geqq$ and $\leqq$ are transposed relations.

If $x < y$ or $x = y$, then $x \leqq y$. The converse is not valid: as we shall see later, it is possible that we have $x \leqq y$ without being able to prove that $x < y$ or $x = y$. For this reason it was necessary to define the relations $<$ and $\leqq$ independently of each other.

The following rules for manipulating inequalities are easily proved from Proposition (2.9). We omit the proofs.

(2.11) **Proposition.** *For all real numbers x, y, z, and t,*

(a) $x < z$ *whenever either* $x < y$ *and* $y \leq z$ *or* $x \leq y$ *and* $y < z$

(b) $x \leqq z$ *whenever* $x \leqq y$ *and* $y \leqq z$

(c) $x + y \leqq z + t$ *whenever* $x \leqq z$ *and* $y \leqq t$

(d) $x + y < z + t$ *whenever* $x \leqq z$ *and* $y < t$

(e) $xy \leqq zy$ *whenever* $x \leqq z$ *and* $y \geqq 0^*$

(f) $xy < zy$ *whenever* $x < z$ *and* $y > 0^*$

(g) *if* $x < y$, *then* $-x > -y$

(h) *if* $x \leqq y$, *then* $-x \geqq -y$

(i) $\max\{x, y\} \geqq x$

(j) $\min\{x, y\} \leqq x$

(k) *if* $x \leqq y$ *and* $y \leqq x$, *then* $x = y$

(l) $|x| \geqq 0^*$

(m) $|x + y| \leqq |x| + |y|$.

An important property of the relation $<$, of which we shall make no use, is the *antisymmetry* property, which states that at most one of the relations $x < y$ and $y < x$ is valid for given real numbers x and y. This negative statement has no place in the affirmative mathematics we are trying to develop, except as motivation. Its place is taken by the affirmative statement (k) of Proposition (2.11). As a general principle, negative statements are only for counterexamples and motivation; they are not to be used in subsequent work.

(2.12) **Definition.** For real numbers x and y we write $x \neq y$ if and only if $x<y$ or $x>y$.

Inequality $\neq$ is a relation because both $<$ and $>$ are relations. As motivation we have the negative statement that at most one of the relations $x \neq y$, $x=y$ can hold for given real numbers x and y. In other words, at most one of the relations $x<y$, $x>y$, $x=y$ can hold. This is clear from the definitions.

The following proposition defines the *inverse* x^{-1} of a real number $x \neq 0^*$, and derives the basic properties of the operation $x \mapsto x^{-1}$.

(2.13) **Proposition.** *Let x be a nonzero real number (so that $|x| \in \mathbb{R}^+$). There exists a positive integer N with $|x_m| \geqq N^{-1}$ for $m \geqq N$. Define*

$$y_n \equiv (x_{N^3})^{-1} \qquad (n<N)$$

and

$$y_n \equiv (x_{nN^2})^{-1} \qquad (n \geqq N).$$

Then

$$x^{-1} \equiv (y_n)_{n=1}^{\infty}$$

is a real number which is positive if x is positive, and negative if x is negative; also $xx^{-1}=1^*$.

If t is any real number for which $xt=1^*$, then $t=x^{-1}$. The operation $x \mapsto x^{-1}$ is a function. If $x \neq 0$ and $y \neq 0$, then $(xy)^{-1}=x^{-1}y^{-1}$. If $\alpha \neq 0$ is rational, then $(\alpha^*)^{-1}=(\alpha^{-1})^*$. If $x \neq 0$, then $(x^{-1})^{-1}=x$.

Proof: Our definitions guarantee that $|y_n| \leqq N$ for all n.

Consider positive integers m and n. Write

$$j \equiv \max\{m, N\}, \qquad k \equiv \max\{n, N\}.$$

Then

$$\begin{aligned} |y_m - y_n| &= |y_m||y_n||x_{jN^2} - x_{kN^2}| \\ &\leqq N^2((jN^2)^{-1} + (kN^2)^{-1}) = j^{-1} + k^{-1} \leqq m^{-1} + n^{-1}. \end{aligned}$$

Therefore x^{-1} is a real number.

Assume now that $x>0^*$. Then by (2.8), $x_n>0$ for all sufficiently large n. Hence $y_n > K_x^{-1}$ (where K_x is the canonical bound for x) for all sufficiently large n. It follows from (2.8) that $x^{-1}>0^*$. A similar proof shows that $x^{-1}<0^*$ whenever $x<0^*$.

Let k be the maximum of the canonical bounds for x and x^{-1}. Write $xx^{-1} \equiv (z_n)$. Then

$$z_n \equiv x_{2nk} y_{2nk} \equiv x_{2nk}(x_{2nN^2k})^{-1} \qquad (n \geqq N)$$

Therefore

$$\begin{aligned} |z_n - 1^*| &= |x_{2nN^2k}|^{-1}|x_{2nk} - x_{2nN^2k}| \\ &\leqq |y_{2nk}|((2nk)^{-1} + (2nN^2k)^{-1}) \leqq n^{-1} \end{aligned}$$

for $n \geqq N$. It follows that $xx^{-1}=1^*$.

If t is any real number with $xt = 1^*$, then

$$x^{-1} = x^{-1}(xt) = (x^{-1}x)t = (xx^{-1})t = t.$$

If $x = x'$, then

$$x'x^{-1} = xx^{-1} = 1^*.$$

Therefore $x^{-1} = (x')^{-1}$. It follows that $x \mapsto x^{-1}$ is a function.

If $x \neq 0$ and $y \neq 0$, then

$$(xy)x^{-1}y^{-1} = xx^{-1}yy^{-1} = 1^*.$$

Therefore $x^{-1}y^{-1} = (xy)^{-1}$.

If $\alpha \neq 0$ is rational, then $\alpha^* \equiv (\alpha, \alpha, \ldots)$. Therefore

$$(\alpha^*)^{-1} = (\alpha^{-1}, \alpha^{-1}, \ldots) = (\alpha^{-1})^*.$$

For each x in $\mathbb{R}^+$, x^{-1} is in $\mathbb{R}^+$, and thus $(x^{-1})^{-1}$ exists. Since $x^{-1}x = xx^{-1} = 1^*$, it follows that $(x^{-1})^{-1} = x$. Similarly $(x^{-1})^{-1} = x$ if x is negative Therefore $(x^{-1})^{-1} = x$ whenever $x \neq 0$. □

Of course, we often write x/y instead of xy^{-1} when x and y are real numbers with $y \neq 0$.

As the previous propositions show, $(\alpha\beta)^* = \alpha^*\beta^*$, $(\alpha+\beta)^* = \alpha^* + \beta^*$, $(-\alpha)^* = -\alpha^*$, $(|\alpha|)^* = |\alpha^*|$, and $(\alpha^{-1})^* = (\alpha^*)^{-1}$ for all rational numbers α and β. Also $\alpha \Delta \beta$ if and only if $\alpha^* \Delta \beta^*$, where Δ stands for any of the relations $=$, $<$, $>$, and $\neq$. This situation is expressed by saying that the map $\alpha \mapsto \alpha^*$ is an *order isomorphism* from $\mathbb{Q}$ into $\mathbb{R}$. This justifies identifying $\mathbb{Q}$ with a subset of $\mathbb{R}$, as we previously identified $\mathbb{Z}$ with a subset of $\mathbb{Q}$. Henceforth we make no distinction between a rational number α and the corresponding real number α^*

The next lemma shows that the n^{th} rational approximation x_n to a real number $x \equiv (x_n)$ actually approximates x to within n^{-1}.

(2.14) **Lemma.** *For each real number $x \equiv (x_n)$, we have*

$$|x - x_n| \leqq n^{-1} \qquad (n \in \mathbb{Z}^+).$$

Proof: By (2.4) and the definition of $|\ |$, the m^{th} rational approximation to $n^{-1} - |x - x_n|$ is

$$n^{-1} - |x_{4m} - x_n| \geqq n^{-1} - ((4m)^{-1} + n^{-1}) = -(4m)^{-1} > -m^{-1}.$$

By (2.7), we have $n^{-1} - |x - x_n| \in \mathbb{R}^{0+}$. Therefore $|x - x_n| \leqq n^{-1}$. □

(2.15) **Lemma.** *If $x \equiv (x_n)$ and $y \equiv (y_n)$ are real numbers with $x < y$, then there exists a rational number α with $x < \alpha < y$.*

Proof: By (2.4), we have $y-x \equiv (y_{2n}-x_{2n})_{n=1}^{\infty}$. Since $y-x \in \mathbb{R}^+$, by (2.7) there exists n in $\mathbb{Z}^+$ with $y_{2n}-x_{2n}>n^{-1}$. Write

$$\alpha \equiv \tfrac{1}{2}(x_{2n}+y_{2n}).$$

Then

$$\alpha - x \geqq \alpha - x_{2n} - |x_{2n}-x| \geqq \tfrac{1}{2}(y_{2n}-x_{2n}) - (2n)^{-1} > 0.$$

Also,

$$y-\alpha \geqq y_{2n} - \alpha - |y_{2n}-y| \geqq \tfrac{1}{2}(y_{2n}-x_{2n}) - (2n)^{-1} > 0.$$

Therefore $x<\alpha<y$. □

As a corollary, for each x in $\mathbb{R}$ and r in $\mathbb{R}^+$ there exists α in $\mathbb{Q}$ with $|x-\alpha|<r$. Here is another corollary.

(2.16) **Proposition.** *If $x_1,\ldots,x_n$ are real numbers with $x_1+\ldots+x_n>0$, then $x_i>0$ for some i $(1 \leqq i \leqq n)$.*

Proof. By (2.15), there exists a rational number α with $0<\alpha<x_1+\ldots+x_n$. For $1 \leqq i \leqq n$ let a_i be a rational number with

$$|x_i-a_i|<(2n)^{-1}\alpha.$$

Then

$$\sum_{i=1}^{n} a_i \geqq \sum_{i=1}^{n} x_i - \sum_{i=1}^{n} |x_i-a_i| > \tfrac{1}{2}\alpha.$$

Therefore $a_i>(2n)^{-1}\alpha$ for some i. For this i it follows that

$$x_i \geqq a_i - |x_i-a_i| > 0. \quad \square$$

(2.17) **Corollary.** *If x, y, and z are real numbers with $y<z$, then either $x<z$ or $x>y$.*

Proof: Since $z-x+x-y=z-y>0$, either $z-x>0$ or $x-y>0$, by (2.16). □

The next lemma gives an extremely useful method for proving inequalities of the form $x \leqq y$.

(2.18) **Lemma.** *Let x and y be real numbers such that the assumption $x>y$ implies that $0=1$. Then $x \leqq y$.*

Proof: Without loss of generality, we take $y=0$. For each n in $\mathbb{Z}^+$, either $x_n \leqq n^{-1}$ or $x_n>n^{-1}$. The case $x_n>n^{-1}$ is ruled out, since it implies that $x>0$. Therefore $-x_n \geqq -n^{-1}$ for all n, and so $-x \geqq 0$. Thus $x \leqq 0$. □

(2.19) **Theorem.** *Let (a_n) be a sequence of real numbers, and let x_0 and y_0 be real numbers with $x_0 < y_0$ Then there exists a real number x such that $x_0 \leqq x \leqq y_0$ and $x \neq a_n$ for all n in $\mathbb{Z}^+$.*

Proof: We construct by induction sequences (x_n) and (y_n) of rational numbers such that

(i) $x_0 \leqq x_n \leqq x_m < y_m \leqq y_n \leqq y_0 \quad (m \geqq n \geqq 1)$
(ii) $x_n > a_n$ or $y_n < a_n \quad (n \geqq 1)$
(iii) $y_n - x_n < n^{-1} \quad (n \geqq 1)$.

Assume that $n \geqq 1$ and that $x_0, \ldots, x_{n-1}$, $y_0, \ldots, y_{n-1}$ have been constructed. Either $a_n > x_{n-1}$ or $a_n < y_{n-1}$. In case $a_n > x_{n-1}$, let x_n be any rational number with $x_{n-1} < x_n < \min\{a_n, y_{n-1}\}$, and let y_n be any rational number with $x_n < y_n < \min\{a_n, y_{n-1}, x_n + n^{-1}\}$. Then the relevant inequalities are satisfied In case $a_n < y_{n-1}$, let y_n be any rational number with $\max\{a_n, x_{n-1}\} < y_n < y_{n-1}$, and x_n any rational number with $\max\{a_n, x_{n-1}, y_n - n^{-1}\} < x_n < y_n$. Again, the relevant inequalities are satisfied. This completes the induction.

From (i) and (iii) it follows that

$$|x_m - x_n| = x_m - x_n < y_n - x_n < n^{-1} \qquad (m \geqq n).$$

Similarly $|y_m - y_n| < n^{-1}$ for $m \geqq n$. Therefore $x \equiv (x_n)$ and $y \equiv (y_n)$ are real numbers. By (i) and (iii), they are equal. By (i), $x_n \leqq x$ and $y_n \geqq y$ for all n. If $a_n < x_n$, then $a_n < x$ and so $a_n \neq x$. If $a_n > y_n$, then $a_n > y = x$ and so $a_n \neq x$. Thus x has the required properties. □

Theorem (2.19) is the famous theorem of Cantor, that the real numbers are uncountable. The proof is essentially Cantor's "diagonal" proof. Both Cantor's theorem and his method of proof are of great importance.

The time has come to consider some counterexamples. Let (n_k) be a sequence of integers, each of which is either 0 or 1, for which we are unable to prove either that $n_k = 1$ for some k or that $n_k = 0$ for all k. This corresponds to what Brouwer calls "a fugitive property of the natural numbers". For example, such a sequence can be defined as follows. Let n_k be 0 if $u^t + v^t \neq w^t$ for all integers u, v, w, t with $0 < u$, v, $w \leqq k$ and $3 \leqq t \leqq 2 + k$. Otherwise let n_k be 1. Then we are unable to prove $n_k = 1$ for some k, because this would disprove Fermat's last theorem. We are unable to prove $n_k = 0$ for all k, because this would prove Fermat's last theorem.

Now define $x_k \equiv 0$ if $n_j = 0$ for all $j \leqq k$, and $x_k \equiv 2^{-m}$ otherwise, where m is the least positive integer such that $n_m = 1$. Then $x \equiv (x_k)$ is a nonnegative real number, but we are unable to prove that $x>0$ or $x=0$. Since nothing is true unless and until it has been proved, it is untrue that $x>0$ or $x=0$.

Of course, if Fermat's last theorem is proved tomorrow, we shall probably still be able to define a fugitive sequence (n_k) of integers. Thus it is unlikely that there will ever exist a constructive proof that for every real number $x \geqq 0$ either $x>0$ or $x=0$. We express this fact by saying that there exists a real number $x \geqq 0$ such that it is *not* true that $x>0$ or $x=0$.

In much the same way we can construct a real number x such that it is *not* true that $x \geqq 0$ or $x \leqq 0$.

3. Sequences and Series of Real Numbers

We develop methods for defining a real number in terms of approximations by other real numbers.

(3.1) **Definition.** A sequence (x_n) of real numbers *converges* to a real number x_0 if for each k in $\mathbb{Z}^+$ there exists N_k in $\mathbb{Z}^+$ with

(3.1.1) $$|x_n - x_0| \leqq k^{-1} \quad (n \geqq N_k).$$

The real number x_0 is then called a *limit* of the sequence (x_n). To express the fact that (x_n) converges to x_0 we write

$$\lim_{n \to \infty} x_n = x_0$$

or

$$x_n \to x_0 \quad \text{as } n \to \infty$$

or simply $x_n \to x_0$.

A sequence (x_n) of real numbers is said to *converge*, or be *convergent*, if there exists a limit x_0 of (x_n).

It is easily seen that if (x_n) converges to both x_0 and x'_0, then $x_0 = x'_0$.

A convergent sequence is *bounded:* there exists r in $\mathbb{R}^+$ such that $|x_n| \leqq r$ for all n

A convergent sequence of real numbers is not determined until the limit x_0 and the sequence (N_k) are given, as well as the sequence (x_n) itself. Even when they are not mentioned explicitly, these quantities are implicitly present. Similar comments apply to many subsequent definitions, including the following.