A Brief Tour of Constructive Mathematics

A.R. Sheive

May 19, 2006

Any proof by contradiction relies on the principle of the excluded middle, that $P \vee \neg P$ is true for any proposition, P. The average mathematician would just as soon question its validity as the average physicist would the existence of gravity. In turn the philosopher might point out that physics is an empirical science, thus there is little save tradition preventing gravity from disappearing at any moment. Still, physicists, philosophers, and mathematicians alike seem happy to leave their possessions lying about unanchored.

This paper seeks to acquaint those that know the theorems of mathematics as unquestionably true with those who still have questions. It seeks to expose that this most elegantly complex, fundamental and abstract field contains some that seek to make proof more difficult by rejecting contradiction; Some that demand that mathematics be anchored in a certain intuition about the natural numbers; That there has always been, and remains, a fringe to mathematics with roots in the idea that the use of proof by contradiction is akin to alchemy.

> *The belief in the universal validity of the principle of the excluded third in mathematics is considered by the intuitionists as a phenomenon of the history of civilization of the same kind as the former belief in the rationality of π, or in the rotation of the firmament about the earth.*
>
> *Brouwer [1]*

What follows herein is a modest attempt to give insight into the heretical intuitionist mind. We will attempt to gain a peek into the mechanisms of its madness by developing the framework necessary to construct a fundamental theorem of calculus.

1 From Numbers to Mathematics

Constructive mathematics is built upon the positive integers as an unquestionably fundamental base.

> *The primary concern of mathematics is number, and this means the positive integers. We feel about number in the way Kant felt about space. The positive integers and their arithmetic are presupposed by the very nature of our intelligence and, we are tempted to believe, by the very nature of intelligence in general. The development of the theory of the positive integers from the concept of the unit, the concept of adjoining a unit, and the process of mathematical induction carries complete conviction.*
>
> Bishop [2]

In building our constructive framework we must create new mathematical objects out of those we have created before through finite methods. The positive integers exist before we begin, and from our intuitive notions about them we will now work our way through the real numbers and into calculus.

2 Existence and Contradiction

In order to build a notion of existence onto the natural numbers we will associate existential statements with predicates on binary sequences. Through this we will gain support for the rejection of some of the more dubious logical constructs admitted by classical mathematics. (This section follows and summarizes the more thorough treatment by Bridges [1].)

A *sequence* is a rule which associates to each positive integer n a mathematical object, a_n. The object a_n is called the *nth term* of the sequence. We take a, a binary sequence, and consider the following statements:

$$P(a) \ : \ a_n = 1 \text{ for some } n, \tag{1}$$
$$\neg P(a) \ : \ a_n = 0 \text{ for all } n, \tag{2}$$
$$P(a) \vee \neg P(a) \ : \ \text{Either } P(a) \text{ or } \neg P(a), \tag{3}$$
$$\forall (P(a) \vee \neg P(a)) \ : \ \text{For all } a, \text{ either } P(a) \text{ or } \neg P(a). \tag{4}$$

We note that showing that neither A nor B can be false is not sufficient to prove $A \vee B$ constructively. A constructive proof of $P(a) \vee \neg P(a)$ must provide a finite method showing that $a_n = 0$ for all n, or computing a positive integer n such that $a_n = 1$.

As an example we could define the sequence

$$
\begin{aligned}
a_n = 0 \quad & \text{if every even integer } j \text{ such that } 2 < j \leq n \\
& \text{is the sum of two primes,} \\
= 1 \quad & \text{otherwise,}
\end{aligned}
$$

for which a constructive proof of $P(a) \vee \neg P(a)$ would give a finite routine for deciding Goldbach's conjecture. Since we lack such routine, we say that a above is a constructive counterexample to (4). That is, a constructive counterexample is evidence that some statement does not admit a constructive proof.

More abstractly, a constructive counterexample to some statement A is proof that A implies some principle that is unacceptable in our constructive framework. Two such principles follow under the names given to them by Bishop.

> **The limited principle of omniscience (LPO):** If (a_n) is a binary sequence, then either there exists n such that $a_n = 1$, or else $a_n = 0$ for each n.
>
> **The lesser limited principle of omniscience (LLPO):** If (a_n) is a binary sequence containing at most one 1, then either $a_{2n} = 0$ for each n, or else $a_{2n+1} = 0$ for each n.

LPO is equivalent to (4), and thus a constructive proof of it would give finite method for deciding many unsolved problems in mathematics. This provides substantial support of our exclusion of **LPO** from constructive mathematics. Additionally, the principle of the excluded middle implies **LPO** and is therefore rejected from our constructive framework.

It may be of interest that the rejected **LLPO** is equivalent to each of the following statements:

$$
\begin{aligned}
[-1, 1] &= [-1, 0] \cup [0, 1] \\
\text{For each } r \in \mathbb{R},\ &\text{either } r \leq 0 \text{ or } r \geq 0. \\
\text{For } r, s \in \mathbb{R}, rs = 0 &\Longrightarrow r = 0 \text{ or } s = 0.
\end{aligned}
$$

In the context of constructive mathematics we call some statement A **simply existential** if we can construct a binary sequence a as above such that A holds if and only if there exists some n such that $a_n = 1$. For some simply existential statements A and B our aforementioned principles take on the forms:

$$\begin{aligned} \text{LPO} &: A \vee \neg A, \\ \text{LLPO} &: \neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B. \end{aligned}$$

Since $A \wedge B$ is simply existential if A and B are, we can also extend LLPO by induction to

$$\neg(A_1 \wedge \ldots \wedge A_n) \Leftrightarrow \neg A_1 \vee \ldots \vee \neg A_n.$$

Two other rejected principles, stated for some simply existential statement, A, are the **the weak limited principle of omniscience**

$$\text{WLPO} : \neg A \vee \neg\neg A,$$

and **Markov's Principle**

$$\text{MP} : \neg\neg A \Leftrightarrow A.$$

Both are commonly used for constructive counterexamples. Before moving on we note that LPO $\Rightarrow$ WLPO $\Rightarrow$ LLPO.

3 Set and Functions

To construct some set, S, we must first explain how to construct its elements using objects already in our system, and then describe an equality relation for those elements. Our notion of equality must satisfy the usual properties of an equivalence relation. We will then define functions as rules assigning elements of some image set to elements of some domain set. The definitions and proofs contained in this section are taken from Bishop's original 1967 treatise [2].

We will use the standard notation $x \in S$, to denote that x is an element of S. Once we have a set S, we can define the subset

$$\{x : x \in S, x \text{ has property } P\}$$

provided that we can perform constructions on the elements of S that can be proven to satisfy the requirements of the property P. The intersection of two subsets of S based on properties P and Q is defined to be the set

$$\{x : x \in S, x \text{ has properties } P \text{ and } Q\}.$$

We now define an *operation* from a set A to a set B as a rule f which assigns an element $f(a) \in B$ to each element $a \in A$. We require that this rule gives us a specific and finite way to construct $f(a)$ from the method used to construct a.

As per usual we call A the *domain* of f. If $f(a_1) = f(a_2)$ whenever $a_1 = a_2$ for $a_1, a_2 \in A$, then f is called a *function*. We note that a function whose domain is $\mathbb{Z}^+$ is a sequence as previously defined.

Functions can be composed as per the usual definition and are associative if the compositions are well defined. If $g(f(a)) = a$ for some a in the domain of f and $f(g(b)) = b$ for b in the domain of g, then f is a bijection and g is its inverse.

4 The Rationals and Reals

The construction of the rational numbers from the integers is done in the usual fashion. In order to then further construct the real numbers we define them as regular sequences of rational numbers. Notions of equality and order are then constructed. Or course this will involve rejecting some classical and seemingly essential aspects of what it means to be a real number. Again our proofs and definitions follow those of Bishop [2].

We define the rational numbers, $\mathbb{Q}$ as expressions of the form p/q for $p, q \in \mathbb{Z}$ and $q \neq 0$. The rational numbers p/q and r/s are equal if $ps = qr$. The integer n is identified with the rational number $n/1$. It is easy to see that we have a valid equivalence relation and elements based on the integers, thus $\mathbb{Q}$ is a valid constructive set.

Definition 4.1: A sequence $\{x_n\}$ of rational numbers is *regular* if

$$|x_m - x_n| \leq m^{-1} + n^{-1} \text{ for } m, n \in \mathbb{Z}^+.$$

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

$$|x_n - y_n| \leq 2n^{-1} \text{ for } n \in \mathbb{Z}^+.$$

We denote the set of real numbers by $\mathbb{R}$ and point out that we have essentially followed the standard completion of the real numbers by Cauchy sequences of rational numbers.

The reflexivity and symmetry of the above relation are obvious. To see that it is indeed transitive, and thus an equivalence relation as required, we introduce the following lemma.

Lemma 4.2 *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*

$$|x_n - y_n| \leq j^{-1} \text{ for } n \geq N_j.$$

Proof: If $x = y$ then the above holds with $N_j \equiv 2j$.

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

$$\begin{aligned} |x_n - y_n| &\leq |x_n - x_m| + |x_m - y_m| + |y_m - y_n| \\ &\leq (n^{-1} + m^{-1}) + j^{-1} + (n^{-1} + m^{-1}) \leq 2n^{-1} + 3j^{-1} \end{aligned}$$

Since this holds for all $j \in \mathbb{Z}^+$, our equality relation on the real numbers is an equivalence relation.

We call the rational number x_n the *nth rational approximation* to the real number $x \equiv \{x_n\}$. We also associate each real number $x \equiv \{x_n\}$ with an integer K_x such that

$$|x_n| < K_x \text{ for } n \in \mathbb{Z}^+.$$

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

We now straightforwardly describe how arithmetic applies to the real numbers by acting on their rational approximations. We present the following statements without proof for the sake of space.

Definition 4.3: 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 an rational number. We define

$$
\begin{array}{ll}
(a) & x+y \equiv \{x_{2n}+y_{2n}\}_{n=1}^{\infty}, \\
(b) & xy \equiv \{x_{2kn}y_{2kn}\}_{n=1}^{\infty}, \\
(c) & \max\{x,y\} \equiv \{\max\{x_n,y_n\}\}_{n=1}^{\infty}, \\
(d) & -x \equiv \{-x_n\}_{n=1}^{\infty}, \\
(e) & \min\{x,y\} \equiv -\max\{-x,-y\} \\
(f) & |x| \equiv -\max\{x,-x\} \\
(g) & \alpha^* \equiv \{\alpha,\alpha,\alpha,\ldots\}.
\end{array}
$$

Proposition 4.4: *The sequences in the above definition are real numbers.*

Proposition 4.5: *For arbitrary real numbers x, y and z and rational nubmers α and β,*

$$
\begin{array}{ll}
(a) & x+y=y+x, \quad xy=yx, \\
(b) & (x+y)+z=x+(y+z), \quad x(yz)=(xy)z, \\
(c) & x(y+z)=xy+xz, \\
(d) & 0^*+x=x, 1^*\cdot x=x, \\
(e) & x-x=0^*, \\
(f) & |xy|=|x||y|, \\
(g) & (\alpha+\beta)^*=\alpha^*+\beta^*, (\alpha\beta)^*=\alpha^*\beta^*, \text{ and } (-\alpha)^*=-\alpha^*.
\end{array}
$$

Thus we have defined arithmetic with the real numbers obeying the same rules as that of the rational numbers. We already have an equality relation on $\mathbb{R}$, and now introduce several ordering relations and the subsets they define.

Definition 4.6: A real number $x \equiv \{x_n\}$ is said to be *positive* if

$$x_{n_0} > n_0^{-1}$$

for some $n \in \mathbb{Z}^+$. A real number $x \equiv \{x_n\}$ is said to be *nonnegative* if

$$x_n \geq -n^{-1} \text{ for } n \in \mathbb{Z}^+.$$

We define the sets $\mathbb{R}^+$ and $\mathbb{R}^{0+}$ as the positive reals and nonnegative reals respectively.

Lemma 4.7 *A real number $x \equiv \{x_n\}$ is positive if and only if there exists a positive integer N such that*

$$x_n \geq N^{-1} \text{ for } n \geq N.$$

A real number $x \equiv \{x_n\}$ is nonnegative if and only if for each $m \in \mathbb{Z}^+$ there exists a positive integer N_m such that

$$x_n \geq -m^{-1} \text{ for } n \geq N_m.$$

For a proof of the above see [2]. It should be noted that to speak of some real number $\{x_n\}$ as an element of $\mathbb{R}^+$ is an abuse of the language. An element of $\mathbb{R}^+$ consists of some real number $\{x_n\}$ and a positive integer n such that $x_n > n^{-1}$. We will continue to speak of positive real numbers loosely, but the existence of the accompanying positive integer is to be tacitly assumed.

Letting $\mathbb{R}^*$ represent either $\mathbb{R}^+$ or $\mathbb{R}^{0+}$, we give the following proposition and leave the simple proofs to the reader.

Proposition 4.8: *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 ordering relations on $\mathbb{R}$.

Definition 4.9: Let x and y be real numbers. We define

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

and

$$x \geq y (y \leq x) \text{ if } x - y \in \mathbb{R}^{0+}.$$

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

If $x < y$ or $x = y$ then $x \leq y$. The converse is in fact not valid. That is, given some $x \leq y$ we cannot necessarily construct some equality relation between x and y by Lemma 4.2, or show that $x - y \in \mathbb{R}^+$.

Finally we have the following rules for manipulating our inequalities on the real numbers. The proofs of which follow simply from Proposition 4.8.

Proposition 4.10: *For all real number $x, y, z,$ and t,*

$$
\begin{array}{rl}
(a) & x < z \text{ whenever } x < y \text{ and } y \leq z \text{ or } x \leq y \text{ and } y < z, \\
(b) & x \leq z \text{ whenever } x \leq y \text{ and } y \leq z, \\
(c) & x + y \leq z + t \text{ whenever } x \leq z \text{ and } y \leq t, \\
(d) & x + y < z + t \text{ whenever } x \leq z \text{ and } y < t, \\
(e) & xy \leq zy \text{ whenever } x \leq z \text{ and } y \geq 0^*, \\
(f) & xy < zy \text{ whenever } x < z \text{ and } y > 0^*, \\
(g) & -x > -y \text{ if } x < y, \\
(h) & -x \geq -y \text{ if } x \leq y, \\
(i) & \max\{x, y\} \geq x, \\
(j) & \min\{x, y\} \leq x, \\
(k) & x = y \text{ if } x \leq y \text{ and } y \leq x, \\
(l) & |x| \geq 0^*, \\
(m) & |x + y| \leq |x| + |y|.
\end{array}
$$

One property of the relation $<$ that we will noticeably avoid is antisymmetry. This negatively asserts that at most one of the relations $x < y$ or $y < x$ is true. Its place is taken by (k) above.

5 Convergence and Continuity

Having constructed sequences and the real numbers with accompanying relations of equality and order, we now forge ahead into calculus. Boldly ignoring the apparent difficulty of constructing the infinitesimal, we will see that our notions of limits and continuity follow surprisingly naturally from our treatment of the reals as regular sequences of rational numbers. We continue to follow Bishop [2] directly.

Definition 5.1: A sequence $\{x_n\}$ of real numbers (not to be confused with a real number $x \equiv \{x_n\}$) *converges* to a real number x_0 if for each $k \in \mathbb{Z}^+$ there exists $N_k \in \mathbb{Z}^+$ with

$$|x_n - x_0| \leq k^{-1} \text{ for } n \geq N_k.$$

We then write

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

Definition 5.2: A sequence $\{x_n\}$ of real number is a *Cauchy sequence* if for each $k \in \mathbb{Z}^+$ there exists $M_k \in \mathbb{Z}^+$ such that

$$|x_m - x_n| \leq k^{-1} \text{ for } m, n \geq M_k.$$

Other useful results obtained by Bishop by way of proofs that are too lengthy to detail here include:

> **Theorem 5.3** *A sequence $\{x_n\}$ of real numbers converges if and only if it is a Cauchy sequence*
>
> **Proposition 5.4** *Assume that $x_n \to x_0$ as $n \to \infty$, and $y_n \to y_0$ as $n \to \infty$. Then*
>
> (a) $x_n + y_n \to x_0 + y_0$ as $n \to \infty$,
>
> (b) $x_n y_n \to x_0 y_0$ as $n \to \infty$,
>
> (c) $\max\{x_n, y_n\} \to \max\{x_0, y_0\}$ as $n \to \infty$,
>
> (d) $x_0 = c$ whenever $x_n = c$ for all n,
>
> (e) $x_n^{-1} \to x_0^{-1}$ as $n \to \infty$ whenever $x_0 \neq 0$ and $x_n \neq 0$ for all $n \geq N_0$ for some N_0,
>
> (f) $x_0 \leq y_0$ if $x_n \leq y_n$ for all n.

That is, real numbers constructed as limits are well behaved when we work with their approximations.

It is convenient to extend our definition of the real numbers to include the elements $-\infty$ and ∞. To construct an element of this extended set $\mathbb{R}_\infty$ we simply choose a real number, or choose ∞ or $-\infty$. Our ordering relation is then extended by defining $-\infty < \infty$, $-\infty < x$, and $x < \infty$ for all real numbers x.

For each $a \in \mathbb{R}_\infty$ we can now define

$$\begin{aligned}
(-\infty, a) &\equiv \{x : x \in \mathbb{R}, x < a\},\\
(-\infty, a] &\equiv \{x : x \in \mathbb{R}, x \leq a\},\\
(a, \infty) &\equiv \{x : x \in \mathbb{R}, a < x\},\\
[\,a, \infty) &\equiv \{x : x \in \mathbb{R}, a \leq x\}.
\end{aligned}$$

For each a and b in $\mathbb{R}_\infty$ we define

$$\begin{aligned}(a,b) &\equiv (a,\infty)\cap(-\infty,b),\\ (a,b] &\equiv (a,\infty)\cap(-\infty,b],\\ [\,a,b) &\equiv [\,a,\infty)\cap(-\infty,b),\\ [\,a,b] &\equiv [\,a,\infty)\cap(-\infty,b].\end{aligned}$$

An interval defined as above is *bounded* if both of its endpoints are finite. An interval I is *nonvoid* if $x \in I$ for some $x \in \mathbb{R}$, and *closed* if it contains both of its endpoints. A closed, bounded, nonvoid interval is *compact.*

Definition 5.5: A real-valued function f defined on a compact interval I is *continuous* on I if for each $\varepsilon > 0$ there exists $\omega(\varepsilon) > 0$ such that $|f(x) - f(y)| \leq \varepsilon$ whenever $x, y \in I$ and $|x - y| \leq \omega(\varepsilon)$. The operation $\varepsilon \mapsto \omega(\varepsilon)$ is called a *modulus of continuity* for f.

A real-valued function f on an arbitrary interval J is *continuous* on J if it is continuous on every compact subinterval I or J.

Theorem 5.6. *Let the subset A of $\mathbb{R}$ have the property that for each $\varepsilon > 0$ there exist a n_0 and finitely many $\{y_1, \ldots, y_{n_0}\}$ of points of A such that for each x in A at least one of the numbers $|x - y_1|, \ldots, |x - y_{n_0}|$ is less than ε. (Such a set A is called totally bounded.) Then supremum A and infimum A exist.*

Proof: For each positive integer k choose points $y_1, \ldots, y_{n_k}$ in A such that for each x in A at least one of the numbers $|x - y_1|, \ldots, |x - y_{n_k}|$ is less that k^{-1}. For some value of m, $1 \leq m \leq n_k$, we have

$$y_m \geq \max\,\{y_1, \ldots, y_n\} - k^{-1}.$$

Write $x_k \equiv y_m$. If x is any point in A, we have $|x - y_i| < k^{-1}$ for some value of i, $1 \leq i \leq n$. Hence

$$x - x_k = x - y_i + y_i - y_m < k^{-1} + k^{-1} = 2k^{-1}.$$

Thus the sequence $\{x_n\}$ of elements of A has the property that $x - x_k < 2k^{-1}$ for all $x \in A$ and all $k \in \mathbb{Z}^+$. In particular, $|x_j - x_k| < 2j^{-1} + 2k^{-1}$ for all j and k. Therefore $\{x_k\}$ is a Cauchy sequence, whose limit we call x_0. For all $x \in A$,

$$x - x_0 = \lim_{k\to\infty}(x - x_k) \leq \lim_{k\to\infty} 2k^{-1} = 0.$$

Therefore x_0 is an upper bound for A, and since $x_0 = \lim_{k\to\infty} x_k$ it is the supremum. The proof that the infimum exists is similar.

Corollary 5.7: *If $f : [a,b] \to \mathbb{R}$ is a continuous function on a compact interval, then the quantities*

$$\sup f \equiv \sup \{f(x) : x \in [a,b]\}$$

and

$$\inf f \equiv \inf \{f(x) : x \in [a,b]\}$$

(called, respectively, the supremum and the infimum of f on the interval $[a,b]$) exist.

Proof: Let $\varepsilon > 0$ be given. Choose real numbers $a = a_0 \leq a_1 \leq \ldots \leq a_n = b$ such that $a_{i+1} - a_i \leq \omega(\varepsilon)$ for $0 \leq i \leq n-1$, where ω is a modulus of continuity for f. Then, for each x in $[a,b]$, we have $|x - a_i| \leq \omega(\varepsilon)$, and therefore $|f(x) - f(a_i)| \leq \varepsilon$, for some i. Since ε is arbitrary, it follows that the set $\{f(x) : x \in [a,b]\}$ is totally bounded. Therefore $\sup f$ and $\inf f$ exist, by Theorem 5.6.

6 The Intermediate Value Theorem

We now present the constructive statement of the Intermediate Value Theorem reproduced directly from the rewrite of Bishop's 1967 text by Douglas Bridges [3].

The Intermediate Value Theorem. *Let f be a continuous function defined on an interval I, and let a, b be points of I with $f(a) < f(b)$. Then for each y in $[f(a), f(b)]$ and each $\varepsilon > 0$, there exists x in $[\min\{a,b\}, \max\{a,b\}]$ such that $|f(x) - y| < \varepsilon$.*

Proof: Since f is continuous, we have $a \neq b$. We may assume that $a < b$. Consider y in $[f(a), f(b)]$ and $\varepsilon > 0$. Let

$$m \equiv \inf\{|f(x) - y| : a \leq x \leq b\},$$

which exists by the above. We suppose that $m > 0$ and show this to be impossible. We then have that $f(a) - y \leq -m$ and $f(b) - y \geq m$. Letting ω be a modulus of continuity for f on $[a,b]$, we choose points $a = x_0 \leq x_1 \leq \ldots \leq x_n = b$ such that $x_{k+1} - x_k \leq \omega(m)$ for $0 \leq k \leq n-1$. Then for such k we have

$$|f(x_{k+1}) - y - (f(x_k) - y)| = |f(x_{k+1}) - f(x_k)| \leq m.$$

Since $|f(x) - y| \geq m$ for all x in $[a, b]$, it follows that the quantities $f(x_k) - y$ and $f(x_{k+1}) - y$ are either both positive or both negative. Therefore the quantities $f(x_i) - y$, for $(0 \leq i \leq n)$ are either all positive or all negative. Hence $f(a) - y$ and $f(b) - y$ are either both positive or both negative. This contradiction ensures that the possibility $m > 0$ is ruled out, so that $m < \varepsilon$, and the desired conclusion follows.

References

[1] Bridges, Douglas, *Varieties of Constructive Mathematics,* (1987) ISBN 0-521-31802-5.

[2] Bishop, Erret, *Foundations of Constructive Analysis,* (1967) McGraw-Hill.

[3] Bishop, Erret, *Constructive Analysis,* (1985) ISBN 3-540-15066-8.