

Spreads and choice in constructive mathematics

Fred Richman
Florida Atlantic University
Boca Raton, FL 33431

21 June 2001

Abstract

An approach to choice-free mathematics using spreads: If constructing a point satisfying property P requires choice, replace this problem by that of constructing a nonempty set of elements satisfying P . Then construct a spread, without choice, whose elements satisfy P . The theory is developed and several examples are given.

1 Constructing points without choice

There are many situations in (constructive) mathematics where you want to construct a point, say a real or complex number, with certain characteristics. The three problems I want to consider are

- constructing a complex number that satisfies a given nonconstant polynomial over the complex numbers—the fundamental theorem of algebra
- constructing a point in a given set of positive measure, and
- constructing a point in the intersection of a given countable family of open dense subsets of a complete metric space—the Baire category theorem.

For each of these problems, the traditional solutions appeal to countable choice, or rather to the stronger *axiom of dependent choices*. This appeal does not seem to be removable, although Ruitenburg [5] has proved the fundamental theorem of algebra, without using choice, when the coefficients are given by pairs of *Cauchy* real numbers (limits of *sequences* of rational numbers). In the absence of choice we must distinguish between Cauchy real numbers and the more general Dedekind real numbers. The former have not been shown to be Cauchy complete (without using choice), which makes them a little unsatisfactory—the reason we constructed the reals in the first place was because the rationals were not complete!

In [3] the problem posed by the fundamental theorem of algebra is solved by redefining what a solution is. Instead of trying to approximate a single root of the polynomial, we approximate the set of roots—the spectrum. The spectrum is an element σ in the completion of the set of n -multisets of Gaussian numbers. We can measure the distance from any complex number to σ although we may not be able to construct a complex number whose distance to σ is 0 (an element of σ). We will see how this may be interpreted in terms of spreads in Theorem 3. For now, we note that attention is shifted from constructing a point with a certain property to constructing a nonempty set of points with that property. We then redefine what we mean by a “nonempty set of points.”

We will illustrate these ideas by solving Problem 1 in the chapter on integration in [1] without using choice. In this problem we are given a sequence J_n of intervals such that the sum of the lengths $\sum |J_n|$ converges to a number that is less than the length of another interval I , and are required to construct a point in I that is not in any J_n . Our solution will be to construct a spread, in the sense of [2], such that any infinite path in that spread defines a point of the desired kind. The bad news is that, without countable choice, we cannot prove the existence of such a path. Perhaps that’s because we are thinking only of *lawlike* paths. Brouwer’s choice sequences are one way to get around this problem. Constructing a suitable spread is essentially the same as showing that there is a choice sequence with the required property. Alternatively, a spread can be thought of as a nondeterministic algorithm for constructing the desired point.

2 Spreads

A **tree** is a partially ordered set T with a least element 0 such that for each $t \in T$ the set $\{s \in T : s \leq t\}$ is a finite chain. Denote by $|t|$ the **level** of t , the natural number describing how far t is from the root 0 . The least element is supposed to be a convenience, but it might be more of a nuisance. We denote $T \setminus \{0\}$ by T^+ .

Let M be a metric space and T a tree. A (**uniform Cauchy**) M -**spread** on T consists of a sequence $\varepsilon_1 \geq \varepsilon_2 \geq \dots$ of real numbers decreasing to 0 , called the **regulator** (of convergence) of the spread, and a function from T to subsets α_t of M so that

- the diameter of α_t is at most $\varepsilon_{|t|}$, for $t > 0$,
- if $s < t$, then $\alpha_s \supset \alpha_t$,
- α_0 is nonempty (inhabited), and
- if α_s is nonempty, then α_t is nonempty for some $t > s$.

A Cauchy sequence c_n gives rise to a spread α on \mathbf{N} by setting $\alpha_n = \{c_n, c_{n+1}, \dots\}$.

These spreads differ in two respects from the spreads in Heyting [2, page 34]. The branching in the tree T is arbitrary, rather than being indexed by the natural numbers at each node, and we do not assume that each node is either admissible or not—in our case, t is admissible if α_t is nonempty. Troelstra and van Dalen [6, page 186] use essentially the same definition of a tree (*spread law*) as Heyting does, but Heyting includes in a spread a *complementary law* which assigns to each node a mathematical object, as we have done here with α_t .

If x is any element of M , then defining $\alpha_t = \{x\}$ for all nonzero $t \in T$, and $\varepsilon_n = 0$, gives a uniform Cauchy spread—a **constant spread** which we will denote by x . More generally, if X is any nonempty subset of M , then we can form a (constant) spread α representing X by letting $T^+ = X \times \mathbf{N}^+$, with $(x, m) < (y, n)$ if $x = y$ and $m < n$, and $\alpha_t = \{x\}$ for $t = (x, m)$. Thus the notion of a spread can be thought of as a generalization of the notion of a nonempty subset of M . In fact, it is not hard to see that it generalizes the notion of a nonempty subset of the *completion* of M . In particular, the completion of M itself can be considered to be an M -spread, as in the traditional intuitionistic view of the continuum \mathbf{R} as a \mathbf{Q} -spread.

Let α and β be M -spreads on trees S and T , respectively. The **distance** between α and β is given by

$$d(\alpha, \beta) = \sup_n \inf_{|s|, |t|=n} d(\alpha_s, \beta_t)$$

so $d(\alpha, \beta) \leq r$ if, for each n and $\delta > 0$, there exist $s \in S$ and $t \in T$ with $|s| = |t| = n$ and $d(\alpha_s, \beta_t) \leq r + \delta$. The quantity $d(\alpha, \beta)$ need not be a (located) real number; it is a generalized real number in the sense of [4]. Similarly, the distance between α and a subset X of M is given by

$$d(\alpha, X) = \sup_n \inf_{|s|=n} d(\alpha_s, X)$$

which is equal to the distance between α and the spread representing X . In particular, using either formula, the distance between a point $x \in M$ and α is given by

$$d(\alpha, x) = \sup_n \inf_{|s|=n} d(\alpha_s, x).$$

If $d(\alpha, x)$ is a real number for each x in M , then we say that α is **located**. Note that $d(\alpha, x) \leq d(\alpha_t, x) + \varepsilon_{|t|}$.

We can define operations of addition and subtraction of **R**-spreads α and β by

$$\alpha_t \pm \beta_t = \{a \pm b : a \in \alpha_t \text{ and } b \in \beta_t\}.$$

The result is a spread $\alpha \pm \beta$, taking the regulator to be the termwise sum of the regulators of α and β . Define $\alpha < \beta$ to mean that there exist n in \mathbf{N} and $\delta > 0$ in \mathbf{R} so that $b - a \geq \delta$ whenever $a \in \alpha_t$ and $b \in \beta_t$ and $|t| = n$. Define $\alpha \leq \beta$ to mean that $\alpha < \beta + \delta$ for all $\delta > 0$.

By a closed interval we mean a set of the form $[u, v] = \{x \in \mathbf{R} : u \leq x \leq v\}$. An **R**-spread α is **contained in** a closed interval $[u, v]$, written $\alpha \in [u, v]$, if $u \leq \alpha \leq v$. In general, we say that α is **contained in** a closed subset C of M if $d(\alpha, x) \geq d(C, x)$ for each $x \in M$. The reader can check that these two definitions of “contained in” agree for $C = [u, v]$. A spread is **bounded** if it is contained in a bounded closed subset of M .

3 Problem 1

We illustrate these ideas on Problem 1 of the integration chapter of [1]. Let $|I|$ denote the length of an interval I of real numbers.

Theorem 1 *Let I be a closed interval and J_n a sequence of nonempty intervals such that $\sum |J_n|$ converges to a number that is less than $|I|$. Then there is a spread α contained in I such that $d(y, \alpha) > 0$ for each $y \in \bigcup J_n$.*

Proof. Let $e \leq |I| - \sum |J_n|$ be a positive rational number. If we expand the J_n to open intervals $J'_n = \{x \in R : d(x, J_n) < e/2^{n+2}\}$, then $|J'_n| = |J_n| + e/2^{n+1}$ is the sum of two convergent sequences, and $e/2 \leq |I| - \sum |J'_n|$, so the hypotheses are still met. Thus we may assume that the J_n are open.

Let T be the tree of finite sequences of the symbols L and R . For $t \in T$, define I_t inductively by $I_0 = I$, and, if $I_t = [a, b]$, then $I_{tL} = [a, (a+b)/2]$ and $I_{tR} = [(a+b)/2, b]$. Define the regulator to be $\varepsilon_i = (1/2)^i |I|$. Note that $|I_t| = \varepsilon_{|t|}$. Set

$$\alpha_t = \{x \in I_t \setminus \bigcup_{i=1}^{|t|} J_i : \sum_{n=1}^{\infty} |J_n \cap I_t| < |I_t|\}.$$

Note that $\sum_{n=1}^{\infty} |J_n \cap I_t|$ converges because $|J_n \cap I_t| \leq |J_n|$, and that if α_t is nonempty, then $\alpha_t = I_t \setminus \bigcup_{i=1}^{|t|} J_i$. In particular, $\alpha_0 = I_0 = I$ is nonempty. As $|I_t| = |I_{tL}| + |I_{tR}|$ and $|J_n \cap I_t| = |J_n \cap I_{tL}| + |J_n \cap I_{tR}|$ we have

$$|I_t| - \sum_{n=1}^{\infty} |J_n \cap I_t| = |I_{tL}| - \sum_{n=1}^{\infty} |J_n \cap I_{tL}| + |I_{tR}| - \sum_{n=1}^{\infty} |J_n \cap I_{tR}|$$

from which it follows that if $\sum_n |J_n \cap I_t| < |I_t|$, then either $\sum_n |J_n \cap I_{tL}| < |I_{tL}|$ or $\sum_n |J_n \cap I_{tR}| < |I_{tR}|$. That is, if α_t is nonempty, then either α_{tL} or α_{tR} is nonempty.

Suppose $y \in J_m$. As J_m is open, $y \pm \delta \in J_m$ for some $\delta > 0$. So if $|t| \geq m$, then $d(y, \alpha_t) \geq \delta$, whence $d(y, \alpha) \geq \delta$. ■

Notice that the tree T constructed in this proof is a complete binary tree, but the subtree of interest, $\{t \in T : \alpha_t \text{ is nonempty}\}$, the set of *admissible* nodes in the terminology of [2], is not detachable as required in both [2] and [6].

Gabriel Stolzenberg points out that Theorem 1 is interesting even when J_n is a singleton for each n . If $J_n = \{r_n\}$ for some enumeration r_n of the rational numbers, then the theorem asserts the existence of an irrational number in I , or rather a spread representing a “nonempty set” of irrational

numbers. In this case, $|J_n| = e2^{-n-1}$ and we may assume that I has rational endpoints and pick $e = |I|$. Then $|I_t| = e2^{-|t|} = 2|J_{|t|}|$, so

$$\sum_{i=1}^n |J_i| = e(1 - 2^{-n})/2 < e/2 = \sum_{i=1}^{\infty} |J_i|$$

whence $\sum_{i=n+1}^{\infty} |J_i| = e2^{-n-1}$. To construct an infinite path in the spread α , and so construct an irrational number in I , proceed as follows. The nodes t such that

$$\sum_{m=1}^{|t|} |J_m \cap I_t| < |I_t|/2 = e2^{-|t|-1}$$

form a detachable subset S of T because all the intervals have rational endpoints. If $t \in S$, then

$$\sum_{n=1}^{\infty} |J_n \cap I_t| < |I_t|/2 + e2^{-|t|-1} = |I_t|$$

so α_t is nonempty. Moreover,

$$|I_t| - \sum_{n=1}^{|t|} |J_n \cap I_t| - |J_{|t|+1} \cap I_t| = |I_{tL}| - \sum_{n=1}^{|tL|} |J_n \cap I_{tL}| + |I_{tR}| - \sum_{n=1}^{|tR|} |J_n \cap I_{tR}|$$

and, because $t \in S$,

$$|I_t|/2 < |I_t| - \sum_{n=1}^{|t|} |J_n \cap I_t|$$

so

$$\begin{aligned} 0 &< |J_{|t|}| - |J_{|t|+1}| \leq |I_t|/2 - |J_{|t|+1} \cap I_t| \\ &< |I_{tL}| - \sum_{n=1}^{|tL|} |J_n \cap I_{tL}| + |I_{tR}| - \sum_{n=1}^{|tR|} |J_n \cap I_{tR}| \end{aligned}$$

from which it follows that either tL or tR is in S . Thus we can construct an infinite path by staying in S and, for example, going left except when we have to go right.

The situation is a different if r_n is an arbitrary sequence of *real* numbers rather than an enumeration of the rational numbers. Then we are dealing with Cantor's theorem that the real numbers are uncountable. In that case is not so clear how to construct an infinite path in α without appealing to choice.

4 The fundamental theorem of algebra

In [3] the **spectrum** of a nonconstant monic polynomial $p(x)$ of degree n is defined to be the limit of the multisets of complex numbers $\mathbf{r} = \{r_1, \dots, r_n\}$ such that $p(x)$ is approximately equal to $p_{\mathbf{r}}(x) = (x - r_1) \cdots (x - r_n)$. The spectrum σ defines a nonnegative function $d(z, \sigma)$ on the complex numbers—the limit of the distance functions $d(z, \mathbf{r}) = \inf_i |z - r_i|$. If $p(x)$ factors completely, then σ can be represented as a multiset of complex numbers (the roots of p); otherwise it is just an object that can be approximated by multisets of complex numbers.

We want to axiomatize (most of) the essential properties of the function $d(z, \sigma)$.

A **locater** is a function $f : M \rightarrow [0, \infty)$ such that

- $f(y) \leq f(x) + d(x, y)$. This is a Lipschitz condition of order 1, and it makes f uniformly continuous.
- If $f(y) < u$, then there exists x with $d(x, y) < u$ and $f(x)$ arbitrarily small.

(Functions with an additional property were called *locations* in [3] and were identified with points in the completion of M .) If, in addition, f is bounded away from zero on the complement of some bounded subset of M , we say that f is **bounded**.

If L is a nonempty located subset of M , then $d(x, L)$ is a locater. This, of course, is the prototype locater. The converse can be proved, if M is complete, using the axiom of dependent choices. If L , in addition, is bounded, then $d(x, L)$ is bounded away from zero on the complement of the bounded subset $\{z \in M : d(z, L) < 1\}$.

Theorem 2 *Let f be a locater on a complete metric space M . Given the axiom of dependent choices, the set $L = f^{-1}(0)$ is a located subset of M such that $f(y) = d(y, L)$ for all $y \in M$.*

Proof. Let u be a positive real number. If there is $x \in L$ such that $d(x, y) < u$, then $f(y) \leq f(x) + d(x, y) < u$ (without choice). We will show that, conversely, if $f(y) < u$, then there is $x \in L$ such that $d(x, y) < u$. Hence L is located and $d(y, L) = f(y)$.

Choose v so that $f(y) < v < u$. Let $x_0 = y$ and choose x_1 so that $d(x_1, x_0) < v$ and $f(x_1) < (u - v)/2$. For $i > 0$, inductively choose x_{i+1} such that

$$\begin{aligned} d(x_{i+1}, x_i) &< (u - v)/2^i \\ f(x_{i+1}) &< (u - v)/2^{i+1} \end{aligned}$$

The x_i form a Cauchy sequence. Let x be its limit. Then $x \in L$ because L is closed and $f(x_i) < (u - v)/2^{i+1}$, so $d(x, L) = 0$. Moreover,

$$d(y, x) = d(x_0, x) \leq \sum_{i=0}^{\infty} d(x_{i+1}, x_i) < v + (u - v) = u.$$

■

It's not hard to see that $d(z, \sigma)$ is a bounded locator because σ is a limit of the bounded located sets \mathbf{r} . Similarly if α is a bounded located spread, then $d(z, \alpha)$ is a bounded locator because

$$d(z, \alpha) = \sup_n \inf_{|s|=n} d(\alpha_s, z) = \sup_n d\left(\bigcup_{|s|=n} \alpha_s, z\right)$$

and $d(\bigcup_{|s|=n} \alpha_s, z)$ is a locator. We need to check that $d(y, \alpha) \leq d(x, \alpha) + d(x, y)$, but that inequality is preserved by suprema. We must also verify that if $d(y, \alpha) < u$, then there exists x with $d(x, y) < u$ and $d(x, \alpha)$ arbitrarily small. If $d(y, \alpha) < u$, then $d(\bigcup_{|s|=n} \alpha_s, y) < u$ for all n , so there exists x such that $d(x, y) < u$ and $d(x, \bigcup_{|s|=n} \alpha_s)$ is arbitrarily small, hence $d(x, \alpha)$ is arbitrarily small.

To see that $d(z, \alpha)$ is a *bounded* locator, choose a bounded closed set B containing α . Then $d(z, \alpha) \geq d(z, B)$ for every complex number z , so the function $d(z, \alpha)$ is bounded away from zero on the complement of the bounded set $\{z : d(z, B) < 1\}$.

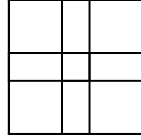
Theorem 3 *Let f be a bounded locator on the complex numbers. Then there is a bounded located complex-valued spread α so that the $d(\alpha, z) = f(z)$ for all z .*

Proof. Let S be a square of width e so that $f(y) \geq \delta > 0$ outside S . Let S^c denote the (metric) complement of S . We first show that

$$\text{if } f(x) \leq \delta/2, \text{ then } d(x, S^c) \geq \delta/2. \quad (**)$$

Indeed, if $y \in S^c$, then $\delta \leq f(y) \leq f(x) + d(x, y)$, so $d(x, y) \geq \delta/2$.

Choose θ in $(1/2, 1)$ so that $(\theta - 1/2)e < \delta/2$ and choose q so that $0 < q < (\theta - 1/2)$. Consider the tree T of all finite sequences from $\{1, 2, 3, 4\}$. To each node t we inductively associate a square S_t of width $e_t = \theta^{|t|}e$. The root node is the empty sequence 0, and we set $S_0 = S$. Having constructed S_t , cover S_t with four squares $S_{t1}, S_{t2}, S_{t3}, S_{t4}$ of width θe_t , each with a corner in common with S_t . Here is the picture.



The width of the two central strips where the S_{t_i} overlap is $2(\theta - 1/2)e_t$.

Next we show that if $f(x) \leq \delta/2$, then for each n there exists t at level n such that $d(x, S_t^c) > qe_t$. This is true for $n = 0$ by (***) and the choice of θ and q . The general statement follows by induction upon observing that if $d(x, S_t^c) > qe_t$, then $d(x, S_{t_i}^c) > qe_{t_i}$ for some $i = 1, 2, 3, 4$.

The condition that means, intuitively, that S_t contains a point of f in its interior is

$$f(x) < d(x, S_t^c) \text{ for some point } x \in S_t. \quad (*)$$

If $f(x) < u < d(x, S_t^c)$, then there exists y such that $f(y)$ is arbitrarily small and $d(x, y) < u$, so $d(y, S_t^c) \geq d(x, S_t^c) - u > f(y)$. Thus if (*) holds for t , then it holds with $f(x)$ arbitrarily small.

There exists x such that $f(x) < \delta/2$, so $d(x, S^c) \geq \delta/2 > f(x)$. Hence Condition (*) holds for $t = 0$. Moreover, if it holds for t , then it holds for one of $t1, t2, t3, t4$. Our spread is defined by setting

$$\alpha_t = \{y \in S_t : (*) \text{ holds for } t\},$$

that is, $\alpha_t = S_t$ if (*) holds for t , and α_t is empty otherwise (not to say that either the condition holds or it doesn't). The regulator of the spread is $\varepsilon_n = \theta^n e$.

If α_t is nonempty, then $\alpha_t = S_t$. Moreover, $f(x)$ is arbitrarily small for some point $x \in S_t$. Now

$$f(y) \leq f(x) + d(x, y) \leq f(x) + d(S_t, y) + \sqrt{2}\theta^{|t|}e,$$

so $f(y) \leq d(S_t, y) + \sqrt{2}\theta^{|t|}e$ for all t such that α_t is nonempty, whence $f(y) \leq d(\alpha, y)$.

Conversely, if $f(y) < u$, then we need to find t at level n so that $d(S_t, y) < u$ and α_t is nonempty. Because $f(y) < u$, there exists x with $d(x, y) < u$ and $f(x) < q\theta^n e$. As $f(x) \leq \delta/2$, there exists t at level n so that $d(x, S_t^c) > q\theta^n e$, so $d(x, S_t^c) > f(x)$. That's the condition for α_t to be nonempty, and $d(S_t, y) < u$ because $x \in S_t$ and $d(x, y) < u$. ■

If σ is the spectrum of a polynomial p , then we can let $f(z) = d(z, \sigma)$ in this theorem. Then α and σ are equivalent insofar as they represent objects that can be described by how they are located with respect to the complex numbers. In the presence of choice, α and σ can be thought of as equal sets: $\{z : d(z, \alpha) = 0\}$ and $\{z : d(z, \sigma) = 0\}$. The spectrum σ has more structure because, in the presence of choice, it is a multiset not just a set. The multiplicities get lost when we pass to α because α is constructed from the function $d(z, \sigma)$ alone.

Nothing about the structure of the complex numbers is used in Theorem 3 other than the metric space structure of \mathbf{R}^2 . The proof goes through, *mutatis mutandis*, for \mathbf{R}^n as well.

5 The Baire category theorem

The Baire category theorem [1, Page 93] says that if M is a complete metric space, and U_n is a sequence of dense open sets, then the intersection $\bigcap_{n=1}^{\infty} U_n$ is dense. It suffices to show that the intersection is nonempty because we can get the stronger theorem by replacing M by the closure of an open ball B in M , and U_n by $U_n \cap B$.

If S is a subset of M , and $r > 0$, we let

$$B_r(S) = \{x \in M : d(x, S) < r\}.$$

We are not assuming that S is located: To say $d(x, S) < r$ is equivalent to saying that there exists $s \in S$ such that $d(x, s) < r$. We say that S is **well contained** in S' if $B_r(S) \subset S'$ for some $r > 0$. This extends the usage in [1, Page 130] to arbitrary sets S .

Theorem 4 *If M is a nonempty complete metric space, and U_n is a sequence of dense open sets, then there exists an M -spread α such that α_t is well contained in $U_{|t|}$ for every t .*

Proof. The tree T consists of finite sequences of pairs $(c_1, r_1), \dots, (c_m, r_m)$ such that

- $c_i \in M$,
- $0 < r_i \leq 1/i$,
- $B_{r_i}(c_i)$ is well contained in U_i ,
- $d(c_i, c_{i+1}) + r_{i+1} < r_i$.

Set $\alpha_0 = M$ and $\alpha_t = B_{r_m}(c_m)$ where $t = ((c_1, r_1), \dots, (c_m, r_m))$. We must show that if $0 < r \leq 1/m$ and $B_r(c)$ is well contained in U_m , then there exists c' and $0 < r' \leq 1/(m+1)$ so that $d(c, c') + r' < r$ and $B_{r'}(c')$ is well contained in U_{m+1} . Let $c' \in U_{m+1}$ be within $r/2$ of c and choose $\delta > 0$ so that $B_\delta(c')$ is well contained in $B_r(c)$. Let $r' = \min(r/2, \delta)$. ■

Because α_t is well contained in $U_{|t|}$ for every t , any infinite path in α gives a point in the intersection of all the U_n .

References

- [1] BISHOP, ERRETT AND DOUGLAS BRIDGES, *Constructive analysis*, Springer-Verlag 1980.
- [2] HEYTING, AREND, *Intuitionism, an introduction*, North-Holland 1956
- [3] RICHMAN, FRED, The fundamental theorem of algebra: a constructive development without choice, *Pacific J. Math.* **196** (2000), 213-230.
- [4] _____, Generalized real numbers in constructive mathematics, *Indagationes Mathematicae*, **9** (1998), 595–606.
- [5] RUITENBURG, WIM B. G., Constructing roots of polynomials over the complex numbers. *Computational aspects of Lie group representations and related topics* (Amsterdam, 1990), 107–128, CWI Tract, **84**, Math. Centrum, Centrum Wisk. Inform., Amsterdam, 1991.
- [6] TROELSTRA, ANNE S., AND DIRK VAN DALEN, *Constructivism in mathematics: an introduction*, North-Holland, 1988.