Constructive mathematics without choice

Fred Richman
Florida Atlantic University
Boca Raton, FL 33431

Abstract

What becomes of constructive constructive mathematics without the axiom of (countable) choice? Using illustrations from a variety of areas, it is argued that it becomes better.

Despite the apparent unanimity among schools of constructive mathematics with respect to the acceptance of the countable axiom of choice, I believe it to be one of the central problems, or mysteries, of constructive mathematics. The axiom may be written as

$$\forall m\,\exists n\,P(m,n) \Longrightarrow \exists \alpha\,\forall m\,P(m,\alpha_n) \tag{CC}$$

where P is a binary predicate, m and n are in N, and $\alpha \in \mathsf{N}^{\mathsf{N}}$.

Brouwer's choice sequences constitute one approach to this problem. Such sequences may be thought of as finite sequences that have the potential of going on indefinitely. That is, they embody the hypothesis of CC (or even the axiom of dependent choices): the ability to go on.. We could say that Brouwer solved the problem of CC by defining the conclusion to be the hypothesis.

Other justifications of CC, including some by intuitionists, consider how we could know that the hypothesis was true, and conclude that we would have to possess an infinite sequence α as in the conclusion. We could say that this solves the problem of CC by defining the hypothesis to be the conclusion.

I would like to suggest that the way to approach the problem is in accordance with Bishop's fourth principle of constructivism, that meaningful

---

[0] 1981 Mathematics Subject Classification. Primary 03F65, 03E25
Key words and phrases. axiom of choice, constructive mathematics.

distinctions deserve to be maintained [2, page 5]. That is, we should reject CC.

It's not a question of whether you *believe* in CC or not—it is a question of whether you prefer doing mathematics with CC or without CC. I will argue that the mathematics becomes better if you reject this axiom, in much the same way that the mathematics becomes better if you reject the law of excluded middle. In particular, one consequence (or cause) of the acceptance of CC is the predominance of sequences in constructive practice. When we reject CC we find ourselves forced to formulate our theorems in nonsequential terms, which in many cases are more natural.

Three case studies are considered: the Hilbert syzygy theorem, the theory of trace-class operators on a Hilbert space, and the fundamental theorem of algebra.

1 The Hilbert syzygy theorem

This theorem was a watershed in my thinking about countable choice. The first time I had even thought to question countable choice was when Wim Ruitenburg asked if we would use it in our book, *A course in constructive algebra*. We agreed that there were already enough problems to face, so we made no systematic effort to eliminate choice from our arguments. I didn't worry too much about it until I was explaining a constructive Hilbert syzygy theorem to an audience of algebraists.

The (abstract) Hilbert syzygy theorem relates the projective dimension of modules over a ring R to modules over the ring of polynomials $R[X]$. A module P is *projective* if whenever you have a diagram

$$\begin{tikzcd} & P \arrow[d] \\ A \arrow[r] & B \end{tikzcd}$$

where $A \to B$ is onto, you can lift to a map $P \to A$. The simplest nontrivial example of a projective module is the ring R viewed as a module over itself. This is a free module on one generator—to define a map from R to another R-module, you just have to say where 1 goes. It is easy to see that finite-rank free modules (direct sums of finitely many copies of R) are also projective. An example of an infinite-rank free R-module is $R[X]$, which is free on the generators 1, X, X^2, ….

Free modules are projective in the presence of the full axiom of choice. Note that the axiom of choice says that every set is projective in the category of sets (just interpret the diagram above as a diagram of sets and functions). To show that $R[X]$ is projective requires some form of countable choice.

The **projective dimension** of a module A is 0, written $\mathsf{pd}\, A = 0$, if A is projective. Inductively, we say that $\mathsf{pd}\, B \leq n + 1$ if $B \cong P/A$, where P is projective and $\mathsf{pd}\, A \leq n$.

The abstract Hilbert syzygy theorem says that

> $\mathsf{pd}\, A \leq n$ for all R-modules A, if and only if $\mathsf{pd}\, A \leq n + 1$ for all $R[X]$-modules A

The concrete theorem has to do with the projective dimension of finitely presented modules over $k[X_1, \ldots, X_n]$ where k is a (discrete) field. A module is finitely presented if it can be written as the quotient a finite-rank free module by a finitely generated submodule. Passing from the abstract to the concrete is already a problem for $n = 0$ because not every module over a field is free, nor is every free module projective. I pointed this out to my audience, noting that the full axiom of choice implies the law of excluded middle. So I had to restrict the class of R-modules that occur in the abstract theorem. The natural choice is finitely presented modules, the modules of interest in the concrete case.

Because the proof used the fact that $R[X]$ is projective, I had to explain to my audience, and myself, that although the full axiom of choice was unacceptable, the countable axiom of choice was okay. This is a tough sell. Accordingly, I was motivated to look for a choice-free development.

In fact, avoiding countable choice leads to a better treatment. One is led to the conclusion that the real theorem is about **flat** dimension, a much more tractable concept than projective dimension from a constructive point of view. The difference is illustrated by considering modules over the ring Z of integers, that is, abelian groups. In the presence of the full axiom of choice, a Z-module is projective if and only if it is free. Flat Z-modules are exactly the torsion-free abelian groups—groups in which the only element of finite order is the identity. The additive group of rational numbers is an example of a flat Z-module that is not free.

It is easy to prove that all free modules, and all projective modules, are flat. In addition, every module over a field is flat. Replacing “projective” by “flat”, the abstract Hilbert syzygy theorem becomes

> fd $A \leq n$ for all R-modules A, if and only if fd $A \leq n + 1$ for all $R[X]$-modules A

(see [6]). One need not restrict to finitely presented modules A, as seems to be the case for projective dimension. Moreover, if the ring R is coherent, then the projective dimension of a finitely presented module is the same as its flat dimension, so the concrete Hilbert syzygy theorem follows immediately from this version of the abstract theorem.

2 Trace-class operators

Bishop defined a Hilbert space to be separable, and remarked in the preface to [1] that he was avoiding "pseudogenerality." With this convention, a closed subspace of a Hilbert space need not be a Hilbert space. Separable Hilbert spaces have orthonormal bases, but you use countable choice to prove this. Indeed, without countable choice, the separability hypothesis is generally rather useless. This is a side benefit of rejecting countable choice: you eliminate separability hypotheses from your theorems.

A basis is essentially an aligned family of **frames**—finite sets of orthogonal unit vectors. By concentrating on frames in general, and not on some particular aligned family, we get basis-free approaches. As an example, we consider trace-class operators.

In most treatments of trace-class operators, one assumes that the operator T has an adjoint, or at least an absolute value (a positive operator $|T|$ such that $\langle |T|\, x, |T|\, x \rangle = \langle Tx, Tx \rangle$ for all x). Then one takes a basis $e_1, e_2, \ldots$ of the Hilbert space and considers the sum

$$\sum_{i=1}^{\infty} |\langle |T|\, e_i, e_i \rangle|$$

If this sum converges, then T is of **trace class**. Of course one must show that the definition is independent of the particular basis.

Without countable choice we must formulate a definition that does not involve a basis, unless we want to restrict ourselves to Hilbert spaces that have bases. One might have wanted a basis-free definition of trace class in any event, but rejecting countable choice makes it imperative. In an analogous situation, anyone might prefer direct (or constructive) proofs, but rejection of the law of excluded middle requires them.

One suitable definition for an operator T to be of trace class is for the supremum

$$\|T\|_1 = \sup \sum_{i=1} |\langle Te_i, f_i\rangle|$$

to exist, where $e_1, \ldots, e_n$ and $f_1, \ldots, f_n$ range over orthonormal sets of size n, and n ranges over the positive integers [7]. So T is of trace class if a certain set of real numbers has a supremum. This elegant, basis-free definition comes about as a direct consequence of rejecting countable choice.

We can also pick out the singular values of the operator T from the expression for $\|T\|_1$. If we let $\|T\|_1^{(n)}$ denote the supremum for fixed n, then the n-th singular value is given by

$$\sigma_n = \|T\|_1^{(n)} - \|T\|_1^{(n-1)}$$

provided that the two suprema exist. (It is true, but not obvious, that if $\|T\|_1$ exists, then so does each $\|T\|_1^{(n)}$.)

3 Completeness

Hilbert spaces are complete. What does that mean? One uses countable choice to show that the Cauchy reals are sequentially complete [9, page 267 N.B.]. This indicates that Cauchy reals are the wrong notion in the absence of countable choice. In general, we rely on CC to show that the sequential completion of a metric space is sequentially complete. So sequential completeness is a concept of dubious value in the absence of CC.

We can define real numbers to be located Dedekind cuts in the rational numbers, but for an arbitrary metric space we need a more general notion. The idea is that an element of the completion $\hat{X}$ of a metric space X is something you can approximate with elements of X. Technically, to specify an element θ of $\hat{X}$, you construct, for each positive rational number r, a nonempty subset S_r which is to consist of r-approximations to θ. The defining property is if that $x \in S_r$ and $y \in S_t$, then $d(x, y) \leq r + t$. There is a natural isometry of X into $\hat{X}$, and X is complete if this isometry is onto.

We will use this notion of a completion to describe the fundamental theorem of algebra in a choiceless environment.

4 The fundamental theorem of algebra

It came as a bit of a surprise to find out that the fundamental theorem of algebra requires countable choice in the absence of the law of excluded middle. At least that is the case for complex numbers based on Dedekind reals. For complex numbers based on Cauchy reals, Ruitenburg [8] showed that the fundamental theorem of algebra holds.

For complex numbers based on Dedekind reals there is already a problem with square roots, that is, with the polynomial $X^2 - a$. The problem is with small values of a, and is a reflection of the fact that the function X^2 does not admit a continuous cross-section in a neighborhood of zero. If we ever find out that a is nonzero, then we have to choose between the two square roots of a. With the law of excluded middle, we could simply consider the two cases $a = 0$ and $a \neq 0$ separately. In fact, the following weak countable choice principle [3], which is implied both by CC and by LEM, suffices:

> Given a sequence A_n of nonempty sets, at most one of which is not a singleton, then there is a choice sequence $a_n \in A_n$.

What is the story without choice? Let $M_n(\mathbb{C})$ denote the set of n-multisets of complex numbers, with a metric given by

$$\inf_{\sigma \in S_n} \sup_i |r_i - s_{\sigma i}| .$$

We identify two elements r and s of $M_n(\mathbb{C})$ when the distance between them is zero. One can show that the correspondence between the element $r_1, \ldots, r_n$ of $M_n(\mathbb{C})$ and the coefficients of the polynomial $(X - r_1) \cdots (X - r_n)$ is uniformly continuous on bounded subsets (in both directions).

Given a monic polynomial $p(X)$ of degree n, we can construct Gaussian numbers $r_1, \ldots, r_n$ that approximate the n roots of $p(X)$ in the sense that $(X - r_1) \cdots (X - r_n)$ is close to $p(X)$. What we are constructing is an element of the completion $\widehat{M}_n(\mathbb{Q}[i])$, where $\mathbb{Q}[i]$ denotes the Gaussian numbers. It is natural to call this element the **spectrum** of $p(X)$.

Note that the spectrum need not necessarily be in $M_n(\mathbb{C})$, which is a subset of $\widehat{M}_n(\mathbb{Q}[i])$ in a natural way. An element of $M_n(\mathbb{C})$ constructed from $p(X)$ in this way is a complete set of roots for $p(X)$, the multiset of a complete factorization. The spectrum of $p(X)$ only allows us to find polynomials near $p(X)$ that admit complete factorizations. In practice, this is what algorithms that implement the fundamental theorem of algebra do—for a given ε, they construct an n-multiset of Gaussian numbers that approximate the roots of $p(X)$ within ε.

References

[1] **Bishop, Errett**, Foundations of constructive analysis, McGraw-Hill, 1967.

[2] ————————, "Schizophrenia in contemporary mathematics," in Errett Bishop: Reflections on him and his research, Contemp. Math. 39 (1985) AMS.

[3] **Bridges, Douglas, Fred Richman and Peter Schuster**, A weak countable choice principle, Proc. Amer. Math. Soc. (to appear)

[4] **Mines, Ray, Fred Richman and Wim Ruitenburg**, A course in constructive algebra, Springer-Verlag 1988

[5] **Richman, Fred**, The fundamental theorem of algebra: a constructive development without choice, Pac. J. Math. (to appear)

[6] ————————, Flat dimension and the Hilbert syzygy theorem, New Zealand J. Math., 26 (1997), 263–273.

[7] **Richman, Fred, Douglas Bridges and Peter Schuster**, Trace-class operators, preprint, www.math.fau.edu/Richman/html/docs.htm

[8] **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.

[9] **Troestra, Anne S., and Dirk van Dalen**, Constructivism in mathematics: an introduction, North-Holland 1988