Computational Complexity and Brouwer's Continuum

Robert L. Constable
Cornell University
USA

February 26, 2020

Abstract

The key feature of Brouwer's intuitionistic mathematics is its treatment of the *continuum* of real numbers. That type includes real numbers given by computable sequences of rationals in the style of the 1985 book by Bridges and Bishop, *Constructive Analysis*. It also includes real numbers given by *free choice sequences of point cores*. It is natural to assign a *computational complexity* cost in the style of Hartmanis and Stearns to real numbers given by algorithms. However, free choice sequences *are not given by algorithms*. On the other hand, in order for a choice sequence to define a real number, the elements of the sequence must be increasingly better rational approximations to the number. There is a cost parameterized by the natural numbers to computing these rational approximations. That is one measure for the computational complexity of the real numbers given by free choice.

This short article establishes a framework for formalizing and investigating this notion of complexity for computing with Brouwer's continuum. The fundamental principle about the intuitionistic continuum is the *Continuity Principle*. This is perhaps the central principle of Brouwer's mathematics, showing that his real numbers are not enumerable, i.e. countable, and it contradicts classical real analysis. It allows us to compute with Brouwer's real numbers.

1 Background on Intuitionism

Brouwer's 1907 doctoral thesis was entitled *On the Foundations of Mathematics.* In it he claimed that mathematics is *not a part of logic*. He believed that a formal language is not essential to mathematics. Computer scientists interested in intuitionism claim that a formal language is necessary to enable computers to help us perform certain mathematical acts, including *formal* *proofs* about free choice sequences.

Computer science has brought many of Brouwer's ideas on logic and mathematics to life by *implementing them* in proof assistants. Elements of his logic were formalized in our book *Implementing Mathematics*[15], *IM* for short. Since the publication of the that book, in 1986, the *Nuprl proof assistant* has implemented not only intuitionistic logic but also elements of Brouwer's work on analysis and topology. These results have been applied to problems in computer science, mathematics, applied mathematics and to logic itself. L.E.J.Brouwer has even made significant contributions to computer science, a subject that did not exist for most of his life, from 1881 to 1966.

In 1986 at Cornell, a dozen members of the PRL research group wrote a book entitled *Implementing Mathematics with the Nuprl Proof Development System* [15]. In that book and in further formal work, we implemented significant elements of Errett Bishop's book *Foundations of Constructive Analysis* [8]. Computers could execute our formal proofs to accomplish tasks in real analysis. We followed Bishop in adopting many of Brouwer's ideas, especially in formalizing intuitionistic logic. Our book is frequently cited even today, 34 years later, in part because of the success of this methodology.[1]. We will examine in these notes the case for *implementing as much of intuitionistic mathematics as possible*. Brouwer claims that its full range cannot be implemented, only certain elements can be formalized. We will examine this border.

Dr.Mark Bickford has formalized in Nuprl significant parts of the Bishop and Bridges book, and we obtained permission from the publishers, Springer Verlag, to link results in that book to his formalization. This combination created an interesting *new paradigm for publishing mathematics*, see http://www.nuprl.org/MathLibrary/ConstructiveAnalysis/.

Using the *Nuprl proof assistant* [15] we have implemented not only intuitionistic logic but also elements of Brouwer's discoveries in analysis and topology [6, 23, 22, 24, 5]. We have applied these results to problems in computer science, mathematics, applied mathematics and to logic itself. In due course these concepts and theorems will be implemented in other proof assistants as more connections are established to computer science. In this and related ways, L.E.J.Brouwer has made significant contributions to computer science, a subject that did not exist in his life time.

2 Implementing Elements of Intuitionistic Mathematics

The Cornell Nuprl proof assistant implements *intuitionistic type theory* enhanced with concepts developed and implemented in Nuprl since 1984, e.g quotient types, dependent intersection, recursive types and novel types documented in the 1986 book on the theory and its implementation

[1]The Nuprl book is available on the PRL web page at: http://www.nuprl.org/book/

[15]. As far as we know, there is no other proof assistant that has formalized and implemented Brouwer's intuitionistic mathematics enhanced with the types mentioned above. We have called this theory *enhanced intuitionistic type theory.*

Recently we defined this theory in the Coq proof assistant [1]. When we are exploring possible new types and rules we verify their consistency using Coq. We call this a *dual-prover technology.* That methodology was independently advocated by the late Field's Medalist Vladimir Voevodsky. All of the Nuprl results are available at the library and web page of the proof assistant, www.nuprl.org.

We present some of these concepts using the approach called the *semantics of evidence* [14]. As of 2020 Nuprl remains the only proof assistant that implements the *full range* of *Brouwer's intuitionistic mathematics.* This implementation was made possible by the pioneering work of Kleene and Vesley in their book *The Foundations of Intuitionistic Mathematics* and the work of the PRL group over the past six years to implement these ideas. Many of the key articles were published in the *Logic in Computer Science* (LICS) conference and related venues.

These notes build on our experience transforming the logic of the Nuprl proof assistant from *constructive* mathematics in the style of Bishop and Bridges [9] to implementing Brouwer's *intuitionistic* mathematics [18, 26, 10, 11, 17, 12, 25, 20, 19, 21], especially including his essential *Continuity Principle*, *free choice sequences* and elements of the *Creating Subject* arguments [2]. As far as we know, Nuprl is to date the only proof assistant that implements and applies this range of intuitionistic mathematics. We have reported in the proceedings of the *Logic in Computer Science* (LICS) meetings and in other publications [7, 23] on the course of our four year long transformation of the Nuprl proof assistant's logic from constructive mathematics to intuitionistic mathematics. Many of the conference papers and the Nuprl book are available at: www.nuprl.org.

3 Calculus and the Real Numbers in Nuprl

In Chapter 2 page 15 Bishop and Bridges [9] define the notion of an *operation.* They say that an operation is a *finite mechanical procedure.* They write $f : (A \to B)$ to indicate that f maps elements from the set A into set B. If the operation f respects the equality on the set A, i.e. if $a = b$ in A implies $f(a) = f(b)$ then f is called a *function.* This wording is essentially the same as used by logicians. They define a *sequence* as a function whose domain is the set of positive integers. Recall their definition of the real numbers repeated here.

Definition 2.1: A sequence of rational numbers q_n is *regular* if $|q_m - q_n| \leq 1/m + 1/n$ for all m, n positive natural numbers. A *real number* is a regular sequence of rationals. We call q_n the nth *approximation* to the real number.

Two real numbers x_n, y_n are *equal* iff $|x_n - y_n| \leq 2/n$. The type of real numbers just defined is denoted by $\mathbb{R}$. It is easy to see that equality on real numbers is an equivalence relation.

It is noteworthy that Brouwer proposed a wider notion of real numbers. He allows them to be given by *free choice sequences* [11, 13]. The choices used to generate the sequence need not be given by a rule or an *algorithm*. The rational approximations can be "freely chosen".

3.1 Brouwer's real numbers, his Continuity Principle, and Bar Induction

Brouwer uses the notion of a *point core* to define his real numbers. His basic format for a real number is progressively smaller nested intervals of rational numbers. This rendering is suggestive where the endpoints of the intervals are rational numbers. The definition evokes the idea of a "point core" looking like this:

$$[\,[\,[\,[\,[\,[\,[\,[\,[\,\cdot\,]\,]\,]\,]\,]\,]\,]\,]\,]$$

The matching brackets determine rational intervals of the continuum. Brouwer believed that our *intuition of time* gave us the conceptual basis for exploring the mathematical continuum. Weyl [27] was also interested in connections between the mathematical continuum and the time/space continuum.

Brouwer's *Continuity Principle* is expressed this way in Nuprl [22]. The downward arrow, $\downarrow$, tells us that the computational content of the proposition following the arrow is hidden, thus not available for computation. This is not a completely faithful implementation of Brouwer's notion because we cannot necessarily find the natural number k. We need to search for it.

Continuity Principle:

$$\forall F : \mathbb{R} \Rightarrow \mathbb{N}. \downarrow \forall f : \mathbb{R}.\exists k : \mathbb{N}.\forall g : \mathbb{R}.(g = fin(\mathbb{R})_k) \Rightarrow (F(g) = F(f)).$$

The downward pointing arrow, $\downarrow$, tells us that the proof does not explicitly give the value k, we need to search for it.

Two real numbers are *separated*, $x \neq y$ if and only if $x < y$ or $y < x$.

The arithmetic operations on reals are easy to define, and they make intuitive sense. Here are the definitions. We call x_n the n-th approximation to the real number.

1. $x + y = (x_{2n}) + (y_{2n})$ for each natural number n.
2. $x \times y = (x_{2kn}) \times (y_{2kn})$ for all n.
3. $max(x, y) = max(x_n, y_n)$ for all n.
4. $-x = (-x_n)$ for all n.
5. $\alpha^\star = (\alpha, \alpha, \alpha, ...)$.

Proposition Each of the above five sequences of rational numbers defines a real number. We associate with each real number x an integer K_x called the *canonical bound* for x. We define it as the least integer K_x such that the absolute value of the n_{th} approximation is less than K_x.

Definition A real number (x_n) is *positive*, writing $\mathbb{R}^+$, if $x_n \geq 1/n$ for some positive n. A real is *nonnegative*, say $x_n \epsilon \mathbb{R}^{0+}$ if and only if $x_n \geq -n^{-1}$ for n a positive integer.

Here is an important theorem about real numbers that is similar to Cantor's theorem. It shows that if we have an *enumeration* of reals, say (a_n) and two reals x_0 and y_0 such that $x_0 < y_0$, then we can find a real number x such that $x_0 \leq x \leq y_0$ moreover, $x \neq a_n$ for all positive integers n.

Theorem 2.19. Let (a_n) be a sequence of real numbers, and let x_0 and y_0 be real numbers such that $x_0 < y_0$. Then we can find a real number x such that $x_0 \leq x \leq y_0$ and $x \neq a_n$ for all natural numbers n.

The proof of **Theorem** 2.19 on page 27 of Bishop and Bridges is formalized in Nuprl by Mark Bickford. The verbatim account from Bishop and Bridges is given in the part of their book which is posted on-line at the Nuprl web site. The url for the book is given above in the abstract. Here is an English language version of the theorem.

Theorem 2.19 in English: Given a sequence of real numbers $a_1, a_2, a_3, ...$ and given a proper non-empty closed interval of the reals, we can effectively find another real number x in this interval, different from all of the a_i.

This is a constructive version of *Cantor's Theorem* that *the real numbers are uncountable* in the sense that we can find a real number a not on this list. Brouwer gave a very different proof that the intuitionistic reals are uncountable. We look at that next.

Brouwer created an account of the continuum of the intuitionistic reals using his concept of a *universal spread*. Spreads are trees with infinitely many branches from each node and all of whose branches are infinite in length. The universal spread allows the paths in the tree to be given by *arbitrary free choices* as well as by rules. The universal spread contains *all possible* sequences of natural numbers, some given by *laws* and some created *freely*. The spread has an *uncountable* number of nodes. Indeed, the universal spread is the basis for Brouwer's notion of the continuum. He provides a simple argument that the universal spread is uncountable. So we conclude that the continuum is uncountable without employing a diagonalization argument.[2]

We list some properties of the universal spread to start building up our knowledge of this central concept in Brouwer's intuitionism. The elements of a spread are sequences of natural numbers. They can be given by a rule describing for any natural number n the n-th element of the sequence. They can also be given by free choice, the n-th element is freely chosen, say by a *creating subject*. Some sequences might be *finite* because there is no means given for extending them further. The *choice law* determines the spread. Indeed Brouwer did not think of the spread as the collection of its elements but as the law determining how the choices are made.

Brouwer created an account of the continuum and the intuitionistic reals using his concept of a *universal spread*. Spreads are trees with infinitely many branches from each node and all of whose branches are infinite in length. The universal spread allows the paths in the tree to be given by *arbitrary free choices* as well as by rules. The universal spread contains *all possible* sequences of natural numbers, some given by *laws* and some created *freely*. The spread has an *uncountable* number of nodes. Indeed, the universal spread is the basis for Brouwer's notion of the continuum. He provides a simple argument that the universal spread is uncountable. So we conclude that the continuum is uncountable without employing a diagonalization argument.[3]

We list some properties of the universal spread to start building up our knowledge of this central concept in Brouwer's intuitionism. The elements of a spread are sequences of natural numbers. They can be given by a rule describing for any natural number n the n-th element of the sequence. They can also be given by free choice, the n-th element is freely chosen, say by a *creating subject*. Some sequences might be *finite* because there is no means given for extending them further. The *choice law* determines the spread. Indeed Brouwer did not think of the spread as the collection of its elements but as the law determining how the choices are made.

There is a special spread called the *universal spread* consisting of all infinite sequences of natural

[2] Joan Rand Moschovakis provides a YouTube presentation of free choice sequences with the title: "A Logical Look at Kripke's idea of free choice sequences".

[3] Joan Rand Moschovakis provides a YouTube presentation of free choice sequences with the title: "A Logical Look at Kripke's idea of free choice sequences".

numbers, $\mathbb{N}$. We denote this spread as $\triangle$. The choice law for this universal spread allows *any choice* of a natural number at each step of creating an element, i.e. a sequence. The universal spread includes *all sequences of natural numbers* no matter how they are created, by law or free choice. Brouwer showed that $\triangle$ is uncountable by essentially the argument we give now.

In order for a function, say α to be defined on any spread, the value it takes on each sequence as input must be determined by an initial segment of that sequence, say the values up to number y. This function α must take the same value on any sequence that has the same initial segment, say a function β. But we can arrange that at a larger value, say $y+1$, $\alpha(y+1) \neq \beta(y+1)$. This means it is impossible to map $\triangle$ onto $\mathbb{N}$ in a one-to-one way. Consequently, the universal spread $\triangle$ is not enumerable. It is uncountable. Brouwer proved this without using diagonalization.

The *intuitionistic continuum* is a special spread. We describe it now. I relies on the notion of point cores that we defined above.

It is not practical to draw the universal spread as a tree because of the large branching factor. The root must connect directly to all natural numbers and so must the interior nodes. We can't diagram that as a tree, although a spread is usually shown that way. It can also be seen as a co-recursive type.

The *intuitionistic continuum* $\Re$ is a special spread. We describe it now. It relies on the notion of point cores that we defined above.

It is not practical to draw the universal spread as a tree because of the large branching factor. The root must connect directly to all natural numbers and so must the interior nodes. We can't diagram that as a tree, although a spread is usually shown that way. It can also be seen as a co-recursive type.

Theorem: $\neg(\forall x : \Re.(x \neq 0 \Rightarrow x < 0 \vee x > 0))$.

Proof: We need a proposition A that is known not to be *testable*. Brouwer meant that we do not have a proof of $(\neg A \vee \neg\neg A)$. We could take A to be $P = NP$. This is a famous open problem in computer science about polynomial time computation done *deterministically*, i.e. in P or *non-deterministically*, i.e. in NP. We do not know whether $P = NP$ or $(P \neq NP)$. This proposition is *non-testable* as of July 2019. So we know $(P = NP) \vee (P \neq NP)$. This is the same as $\neg(P \neq NP) \vee (P \neq NP)$. Next we define a choice sequence r of rational numbers with these three properties.

- As long as by the time we choose $r(n)$ the creating subject has not found evidence for either $P = NP$ or $(P \neq NP)$, define $r(n)$ to be 0. That is $((P \neq NP) \wedge (\neg(P \neq NP))) \Rightarrow (r = 0)$.

- If between the choice of $r(m-1)$ and $r(m)$, the creating subject has found evidence for $P = NP$, then choose $r(n)$ for all $n > m$ to be 2^{-m}.

- If between $r(m-1)$ and $r(m)$ the creating subject has evidence for $(P \neq NP)$, then choose $r(n) = -(2^{-m})$ for all $n \geq m$.

  We can see that r is a real number since it converges. Furthermore, we defined it to satisfy $(r = 0) \Leftrightarrow ((P \neq NP) \wedge \neg(P \neq NP)$. So the creating subject knows $r \neq 0$.

  So the creating subject can reason that *there never was evidence for* $P = NP$, and indeed, none for $(P \neq NP)$. So $P = NP$ has been tested. By symmetry, if $r > 0$, i.e.$\neg(r \leq 0)$, then there is never evidence of $(P \neq NP)$, hence $\neg(P \neq NP)$.

  Hence $P = NP$ *has been tested*, contradicting the assumption that it has not been tested. Therefore we know that $r < 0 \vee r > 0$ cannot be proved. Qed

4 Conclusion: What the Future May Hold

Computer science, as a relatively young discipline is making considerable progress in helping mathematicians and computer scientists solve open problems and discover new ones. Proof assistants are a critical technology in this kind of research. That fact was very well understood by the Fields Medalist Vladimir Voevodsky who turned to computer science to help validate his ideas in homotopy theory. In particular he sought assistance in proving what he called his *Univalence Axiom*. This axiom is critical to understanding equality in homotopy theory. His conjecture was confirmed at Cornell by Mark Bickford working with Voevodsky using the Nuprl proof assistant [4]. The PRL research group has been enriching and applying the Nuprl proof assistant since 1985 [15], for over thirty four years with at least 30 PhD students working on and with the system along with a strong technical support staff including Richard Eaton, Anne Trostle, and Sarah Sernaker.

The Nuprl developers and researchers now use a *dual prover architecture* with the Coq proof assistant [3]. Coq is used to insure that the Nuprl rules are formally sound and that extensions of Nuprl preserve soundness. This capability helps extend the scope of Nuprl's reasoning power, applications, and discoveries.

Hermann Weyl's 1918 book in German, *Das Continuum* [27], was another approach by a highly respected mathematician to understand the continuum more deeply. Initially Weyl was very sympathetic to Brouwer's ideas, but he became interested in what is called *predicative* mathematics. His work has not made the same deep and broad impact as Brouwer's.

We end with a comment on the role of *Artificial Intelligence* (AI) in proof assistants. Stephen Hawking [16] said the following in a popular article on AI : *"Success in creating AI would be the biggest event in human history."* Computer science is well on its way to creating ever stronger AI methods. We already see benefits of progress in AI over the past five years in helping formalize elements of intuitionistic mathematics. I believe that a small one of them is an elegant result by Mark Bickford on the continuum, *Connectedness of the continuum in intuitionistic mathematics*, which Nuprl helped him discover and formalize.

References

[1] Abhishek Anand and Vincent Rahli. Towards a formally verified proof assistant. In *International Conference on Interactive Theorem Proving*, pages 95–197, 2014.

[2] Mark Van Atten. The Creating Subject, the Brouwer-Kripke schema and infinite proofs. *https://halshs.archives-ouvertes.fr/halshs-01781435*, 2018.

[3] Yves Bertot and Pierre Castéran. *Interactive Theorem Proving and Program Development; Coq'Art: The Calculus of Inductive Constructions*. Texts in Theoretical Computer Science. Springer-Verlag, 2004.

[4] Mark Bickford. Formalizing category theory and presheaf models of type theory in Nuprl. *arXiv e-prints*, 2018.

[5] Mark Bickford. Brouwer's fixed point theorem in intuitionistic mathematics. Technical report, 2020.

[6] Mark Bickford, Liron Cohen, Robert L. Constable, and Vincent Rahli. Computability beyond Church-Turing via choice sequences. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '18, pages 245–254, New York, NY, USA, 2018. ACM.

[7] Mark Bickford, Liron Cohen, Robert L. Constable, and Vincent Rahli. Computability Beyond Church-Turing via Choice Sequences. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS18, pages 245–254, New York, NY, USA, 2018. ACM.

[8] E. Bishop. *Foundations of Constructive Analysis*. McGraw Hill, NY, 1967.

[9] E. Bishop and D. Bridges. *Constructive Analysis*. Springer, New York, 1985.

[10] L.E.J. Brouwer. Intuitionisme en Formalisme. *Clausen, Amsterdam*, 1912.

[11] L.E.J. Brouwer. Über Definitionsbereiche von Funktionen. *Mathematische Annalen*, 97:60–75, 1927.

[12] L.E.J Brouwer. *Brouwer's Cambridge Lectures on Intuitionism*. Cambridge University Press, 1981.

[13] L.E.J. Brouwer. Intuitionism and formalism. In P. Benacerraf and H. Putnam, editors, *Philosophy of mathematics: selected writings*. Cambridge University Press, 1983.

[14] Robert L. Constable. The semantics of evidence (also appeared as Assigning Meaning to Proofs). *Constructive Methods of Computing Science*, F55:63–91, 1989.

[15] Robert L. Constable, Stuart F. Allen, H. M. Bromley, W. R. Cleaveland, J. F. Cremer, R. W. Harper, Douglas J. Howe, T. B. Knoblock, N. P. Mendler, P. Panangaden, James T. Sasaki, and Scott F. Smith. *Implementing Mathematics with the Nuprl Proof Development System*. Prentice-Hall, NJ, 1986.

[16] Stephen Hawking. *Brief Answers*. John Murray, UK, 2018.

[17] A. Heyting, editor. *L. E. J. Brouwer Collected Works*, volume 1. North-Holland, Amsterdam, 1975.

[18] S. C. Kleene and R. E. Vesley. *Foundations of Intuitionistic Mathematics*. North-Holland, 1965.

[19] Joan Rand Moschovakis. A Classical view of the Intuitionistic Continuum. *Ann. Pure Appl. Logic*, 81(1-3):9–24, 1996.

[20] Joan Rand Moschovakis. The logic of Brouwer and Heyting. In *Logic from Russell to Church*, pages 77–125. 2009.

[21] Joan Rand Moschovakis and Garyfallia Vafeiadou. Intuitionistic mathematics and logic. Technical report, EU Common Fund, 1999.

[22] Vincent Rahli and Mark Bickford. Validating Brouwer's Continuity Principle for numbers using named exceptions. *Mathematical Structures in Computer Science*, 28:942–990, 2018.

[23] Vincent Rahli, Liron Cohen, Mark Bickford, and Robert Constable. Bar induction is compatible with constructive type theory. *Journal of the ACM (JACM)*, 66(2):13:1–13:35, April 2019.

[24] Vincent Rahli, Liron Cohen, Mark Bickford, and Robert Constable. Bar induction is compatible with constructive type theory. *Journal of the ACM (JACM)*, 66(2):13:1–13:35, April 2019.

[25] Anne Sjerp Troelstra. *Metamathematical Investigation of Intuitionistic Mathematics*, volume 344 of *Lecture Notes in Mathematics*. Springer-Verlag, 1973.

[26] Mark van Atten. *On Brouwer*. Wadsworth Philosophers Series. Thompson/Wadsworth, Toronto, Canada, 2004.

[27] Hermann Weyl. *The Continuum*. Dover, New York, 1987.