Platonism, Constructivism, and Computer Proofs vs. Proofs by Hand*

Yuri Gurevich†

Introduction

In one of Krylov's fables, a small dog Moska barks at the elephant who pays no attention whatsoever to Moska. This image comes to my mind when I think of constructive mathematics versus "classical" (that is mainstream) mathematics. In this article, we put a few words into the elephant's mouth. The idea to write such an article came to me in the summer of 1995 when I came across a fascinating 1917 bet between the constructivist Hermann Weyl and George Polya, a classical mathematician. An English translation of the bet (from German) is found below.

Our main objection to the historical constructivism is that it has not been sufficiently constructive. The constructivists have been obsessed with computability and have not paid sufficient attention to the feasibility of algorithms. However, the constructivists' criticism of classical mathematics has a point. Instead of dismissing constructivism offhand, it makes sense to come up with a positive alternative, an antithesis to historical constructivism. We believe that we have found such an alternative. In fact, it is well known and very popular in computer science: the principle of separating concerns.

Many classical mathematicians and computer scientists have been never exposed to constructivism. By way of motivating 20th century constructivism, we recall, in Section 1, the foundational crisis at the beginning of 20th century. In Section 2, constructivism is introduced. That is where the Weyl/Polya bet appears. Section 3 is devoted to positive contributions of constructivism. The ensuing discussion, in Section 4, touches on various related issues. In the final Section 5, we criticize the historical constructivism.

*In "Current Trends in Theoretical Computer Science: Entering the 21st Century", editors Paun, Rozenberg and Salomaa, World Scientific, 2001. The article was first published in 1995 [Gu2] but the introduction was added later.

†Microsoft Research, Redmond, WA 98052, USA.

1 Paradoxes and the related foundational crisis

Quisani: Is constructivism relevant to computer science?

Author: Some prominent computer scientists think so.

Q: What do you think?

A: I am more skeptical about constructivism in general.

Q: Why?

A: What do you know about constructivism?

Q: Next to nothing. I believe that constructivists reject non-constructive proofs, but I do not understand why. A non-constructive proof can be illuminating and, in some cases, may guide you to a constructive one.

A: History gives us a reason to be cautious about non-constructive proofs. Do you believe that mathematical objects, like the set $\mathcal{R}$ of real numbers, actually exist? Maybe, $\mathcal{R}$ is a product of your imagination. Maybe $\mathcal{R}$ is a product of our civilization.

Q: $\mathcal{R}$ isn't just a product of my imagination; people discussed $\mathcal{R}$ before I was born. And I do not believe that $\mathcal{R}$ is only a product of our civilization. If there are other sufficiently intelligent beings elsewhere in the universe, they surely have similar ideas about $\mathcal{R}$. There is something objective about $\mathcal{R}$. One may say it exists. It does not exist in the same sense as this table does; you cannot touch it. On the other hand, it cannot be destroyed. In that sense its existence is more powerful.

A: You are a typical mathematical Platonist.

Q: What do you mean?

A: Working in mathematics, one develops a strong feeling of dealing with objective reality. As in archaeology, one digs and discovers things and does not create them in any way. One feels, as you do, that mathematical objects really exist and have existed before anyone discovers them. That is mathematical Platonism[1].

Q: Are you saying that all mathematicians are Platonists?

A: No, some mathematicians are not Platonists, and there is a number of anti-Platonist schools in the philosophy of mathematics [Be]. The debate on the nature of mathematical objects is an important part of the history of mathematics. You

[1]It is not assumed of course that a mathematical Platonist adheres to the philosophy of Plato and believes for example that material things are reflections of ideas. In that sense, a mathematical Platonist is not necessarily a Platonist (just as a red herring is not necessarily a herring, and a hot dog is usually not a dog). Nevertheless, the term "mathematical Platonist" is sometimes abbreviated to "Platonist" in the rest of this section.

will find an interesting recent battle in [CC] where Platonism is attacked by a neurobiologist. The modern form of mathematical Platonism is based on the notion of set and is relatively recent. The notion of set was introduced by Georg Cantor (1845–1918) only in the 1870s. He also developed the first theory of sets.

Q: Met with a grandiose applause I guess.

A: Not quite. "Cantor's discoveries, starting around 1873 and slowly expanding to an autonomous branch of mathematics, had at first met with distrust and even with open antagonism on the part of most mathematicians and with indifference on the part of almost all philosophers" [FB]. In particular, Leopold Kronecker (1823–1891) remarked that "God made the integers, all the rest is the work of man". "It was only in the early nineties that set theory became fashionable and began, rather suddenly, to be widely applied in analysis and geometry" [FB].

Q: Still, most mathematicians are Platonists, is that right?

A: I think so.

Q: Somehow we independently grow to become Platonists.

A: I do not think it is always independent. To an extent, we learn the attitude. I remember, in a geometry class, my teacher wanted to prove the congruence of two triangles. Let's take a third triangle, she said, and I asked where do triangles come from. I worried that there may be no more triangles there. Those were hard times in Russia, and we were accustomed to shortages.

Q: What did she say?

A: She looked at me for a while and then said: "Shut up". But eventually I got the idea that you don't have to build a triangle when you need one; all possible triangles exist ahead of time.

Q: Why did you bring the issue of mathematical Platonism? Is there anything wrong with mathematical Platonism?

A: The unrestrained set-theoretic Platonism leads to paradoxes (known also as antinomies) of set theory.[2] I continue quoting from the book [FB] by Abraham Fraenkel and Yehoshua Bar-Hillel: "But at this very moment, when Cantor's daring vision seemed finally to have reached its triumphant climax, when his achievements had just received their final systematic touch, he met the first of those antinomies. This happened in 1895".

Probably the most famous of set-theoretic paradoxes was discovered by Bertrand Russell in 1902. Let R be the collection of sets that do not contain themselves. In other words, for any set X, $X \in R \leftrightarrow X \notin X$. Now ask if R contains itself and you have $R \in R \leftrightarrow R \notin R$.

[2]The two terms are not completely synonymous. A paradox is a statement that seems contradictory. An antinomy is a contradiction. Some logicians speak about set-theoretic paradoxes, some about set-theoretic antinomies, and some use the two terms interchangeably.

Q: This is fascinating. How did Cantor react to paradoxes?

A: Cantor didn't lose faith in his theory. "A Platonist isn't compelled to believe in the existence of anything anyone imagines (especially if the imagination turns out to be contradictory)" [Bl]. Paradoxes just guide us toward better understanding of the objectively existing world of sets.

Q: How did other mathematicians react to paradoxes?

A: Most mathematicians did not worry but "Russell's antinomy came as a veritable shock to those few thinkers who occupied themselves with foundational problems at the turn of the century. Dedekind ... stopped for some time the publication of his essay, the fundaments of which he regarded as shattered. Still more tragic was Frege's fate: he had just put the final touches on his chief work, after decades of tiresome effort, when Russell wrote him about his discovery. In the last sentence of the appendix, Frege admits that one of the foundations of his edifice had been shaken by Russell" [FB].

Q: I do not understand why most mathematicians did not worry.

A: A typical reaction was that the contradictions were found on the fringes of mathematical universe, far from where we work. We don't quantify over all sets in our papers. One should sharpen the notion of set, what is and what is not a set. Russell's argument shows only that R is not a legal set.

Q: I am not sure I buy the argument about fringes. A fringe area of today may be a part of the kernel tomorrow. How was the crisis resolved?

A: Some people argue that the crisis has not been resolved. But a number of solutions have been suggested. By far the most popular solution is the so called ZFC, the Zermelo-Fraenkel set theory with the axiom of choice. ZFC is an axiomatic system based on first-order logic which provides a restricted number of operations to construct new sets from the given ones. It is widely believed to be safe; no known paradoxes apply to it. And it allows one to do all the usual mathematics.

Q: What is a set from ZFC point of view?

A: Intuitively there is a cumulative hierarchy of sets. Start from a well-defined collection of atoms that are not sets, and construct sets by stages. Finite stages are followed by transfinite:

$$0, 1, 2, \ldots, \omega, \omega + 1, \ldots \ .$$

At each stage, construct all possible sets composed of atoms and sets constructed on the previous stages.

Q: How many stages are there?

A: Intuitively the construction goes forever. That is why collections like the collection of all sets or Russell's collection R cannot exist in the cumulative hierarchy. Every set is a material for constructing additional sets and in particular for constructing larger sets.

Q: If I understood you correctly, ZFC is a first-order theory. It follows that if it has one infinite model then it has many infinite models.

A: You are right. If ZFC is consistent, it has many models. There is no particular model of ZFC that is preferred by all.

Q: Are there interesting statements that distinguish between different models of ZFC.

A: Yes. You might have heard about the Continuum Hypothesis of Cantor (briefly CH). It asserts that there are no cardinalities between the cardinality of natural numbers and that of real numbers. (Cantor proved that the cardinality of reals exceeds that of natural numbers.) Kurt Gödel proved that if ZFC is consistent then it has models where CH holds [Go1]. Paul Cohen proved that if ZFC is consistent than it has models where CH fails [Co].

Q: It sounds like the notion of a set depends on a chosen model of ZFC.

A: That is a possible point of view.

Q: It sounds formalistic to me because of the stress on ZFC and consistency.

A: Fortunately most mathematician can afford not to worry about that. What they do does not depend on the choice of ZFC model.

Q: I guess Cantor believed that sets exist independently of our models.

A: I think so.

Q: What about that point of view? Did it die with Cantor?

A: No. The most famous defender of it is probably Gödel: "... there exists, I believe, a satisfactory foundation of Cantor's set theory in its whole original extent and meaning ... It might seem at first that the set-theoretic paradoxes would doom to failure such an undertaking, but closer examination shows that they cause no trouble at all. They are a very serious problem, not for mathematics, however, but rather for logic and epistemology" [Go2]. Pointing out that sets of interest to mathematicians usually belong to the cumulative hierarchy described above, Gödel continued: "This concept of set ... according to which a set is something obtainable from the integers (or some other well-defined objects) by iterated application ... of the operation 'set of' ... has never led to any antinomy whatsoever; that is, the perfectly 'naive' and uncritical working with this concept of set has so far proved completely self-consistent" [Go2].

Q: Did Gödel think that the continuum hypothesis was either true or false?

A: I think so. "For if the meanings of the primitive terms of set theory as explained ... are sound, it follows that the set-theoretical concepts and theorems describe some well-determined reality, in which Cantor's conjecture must be either true or false. Hence its undecidability from the axioms being assumed today can only mean that these axioms do not contain a complete description of that reality" [Go2].

Q: Suits me.

2 Constructivism

A: The Dutch mathematician Brouwer thought though that the set-theoretic paradoxes were only the tip of an iceberg. The problem was much deeper: the logic of finite domains was improperly used for infinite ones. In particular, Brouwer rejected the law of the excluded middle $\alpha \vee \neg\alpha$ and the double negation law $(\neg\neg\alpha) \to \alpha$.

Q: I do not see any connection between these laws and the distinction between finite and infinite, and what is wrong with these laws anyway?

A: Before I plunge into all that, let me mention that the constructivist camp is not monolithic. There is a consensus that mathematics should be constructive, but there is no consensus on what does this exactly mean. There are several constructivist schools. Brouwer's own brand of constructivism is called intuitionism because he insisted that mathematics should be build on intuitively clear principles. "However, although intuitive clarity is, according to the position of the intuitionists, the principal and only criterion of mathematical truth, it is just this criterion which, in the opinion of many mathematicians, is often not satisfied by both the philosophical premises and the concrete mathematical theories of intuitionism" [Ku]. I am most familiar with the Russian constructivist school and this may be reflected somewhat in the following explanations and comments. The Russian school was led by A. A. Markov whose philosophy was quite clear.

Now, to your question. Consider a property P of natural numbers and let $\alpha_P = (\exists n)P(n)$. Is the statement α_P true or false? Let us assume that there is an algorithm that, given a natural number n, computes the truth value of $P(n)$. If instead of the set $\mathcal{N}$ of all natural numbers, we had only natural numbers < 10, we could examine every single number $n < 10$ and this way verify or refute the statement $(\exists n < 10)P(n)$. But we cannot examine all natural numbers because such an examination would never end. For some P, there may exist alternative methods of deciding the truth value of α_P, but in general we cannot verify or refute α_P; in that sense the statement $\alpha_P \vee \neg\alpha_P$ is not necessarily true.

Q: Form a set $\bar{P} = \{n : P(n)\}$. Either $\bar{P}$ is empty or it isn't. In the first case α_P is false, and in the second case it is true.

A: The constructivist might not object to forming the set $\bar{P}$; the question is what does it mean. In the case of numbers < 10, you can mentally walk through the sequence $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ and select those numbers that satisfy P and put them into an imaginary sack or write them down. A similar process would last forever in the case of the set $\mathcal{N}$ of all natural numbers. The constructivist thinks about your $\bar{P}$ as a potential rather than actual, completed totality.

By the way, your second sentence is an instance of the law of the excluded middle and your third sentence has an implicit assumption that a non-empty set necessarily has an element which is an instance of the double negation law. Since constructivists reject both laws, they would regard your argument as hopelessly classical, that is in line with classical (rather than constructive) logic. "Classical" mathematicians often find it hard to deal with potential totalities.

Q: Isn't the totality of all sets a potential totality for a ZFC Platonist?

A: You may have a point there.

Q: I guess the set $\mathcal{N}$ itself is non-completed from the constructivist point of view.

A: That's right.

Q: Then where do natural numbers come from? Do you need a creator constantly at work?

A: Constructivists usually accept the existence of each individual natural number (though Van Dantzig asked if $10^{10^{10}}$ is a finite number); it is the concept of a completed set of all natural numbers that is under attack. One extreme constructivist view, known as ultra-intuitionism, is represented by Esenin-Volpin who doubts even the uniqueness of the series of natural numbers. Compare, he told me once, the potentially infinite series of seconds starting from some fixed moment and the potentially infinite series of world wars.

Q: A Platonist like me would not ask Van Dantzig's question. Even if his number exceeds the number of elementary particles in the universe, one can easily construct a set of sets that has this cardinality. Can you give me an example where the constructivist's point of view is plausible and different from the classical one?

A: I will try. Consider the task of constructing an algorithm that prints 0 if Riemann's Hypothesis holds and prints 1 otherwise.

Q: I know nothing about Riemann's Hypothesis.

A: All you have to know at this point is that this famous hypothesis has not been proved or disproved. Constructivists often used Fermat's Last Theorem for such examples but it was proved recently [Wi].

Q: Let me see. If Riemann's Hypothesis holds then the desired algorithm just prints 0, and if the hypothesis fails then it prints 1. It follows that there is an algorithm for the task. In fact, one of the two trivial algorithms will do.

A: The constructivist will not accept your argument. In constructive mathematics, in order to establish $\alpha \vee \beta$ you have to prove α or to prove β. This is not unnatural. Notice that you don't really have a definite algorithm for the task. In particular, you do not know which of the two trivial algorithms suits the task. Furthermore, any algorithm for the task will solve Riemann's Hypothesis.

Q: Interesting. Is constructive mathematics very different from classical?

A: It is. Many classical theorems fail in the constructive world. One example is Bolzano-Weierstrass Theorem: Every bounded nonempty set of real numbers has a least upper bound. An algorithm constructed by Specker produces a bounded increasing sequence of rational numbers which has no least upper bound in constructivist's real line [Sp]. Classically speaking, the least upper bound of Specker's sequence is not computable.

Q: Are you going to explain the computability of a real number?

A: For the sake of brevity, let us drop the issue of the computability of reals and consider the following weaker form of Bolzano-Weierstrass Theorem that deals only with natural numbers:

(*) Every infinite sequence of zeros and ones has a least upper bound.

Even this fails in the constructive world.

Q: But what does the constructive version of (*) mean exactly? Translate it to classical mathematics.

A: One possible translation of (*) is this:

(**) There exists an algorithm A that, given an algorithm f from natural numbers to $\{0,1\}$, computes $\sup\{f(n) : n \in \mathcal{N}\}$.

A statement of the form $(\forall x \in D_1)(\exists y \in D_2)\varphi(x,y)$ means for the constructivist[3] that there exists an algorithm f from D_1 to D_2 such that, for all x in D_1, $\varphi(x, f(x))$ is true.

Q: I see a possible problem with (**). *A priori* chosen algorithm A may by unable to analyze f. Of course it can generate numbers $f(0), f(1), f(2)$, *etc.* and wait until a one is generated, but it cannot wait forever. Thus it may be unable to distinguish between an algorithm that generates an infinite sequence of zeros and an algorithm that generates a one after generating a very long finite sequence of zeros.

A: That is right. Suppose that A witnesses (**). Do you see how to use A to prove or disprove Fermat's Last Theorem?

[3]At least if the constructivist is of Markov's school and the given description of domain D_1 is simple in an appropriate sense [Ku].

Q: I think I do. Order all quadruples (x, y, z, n) of positive integers somehow.

A: I do not think that somehow is good enough here.

Q: OK, then order them first by $\max\{x, y, z, n\}$ and then lexicographically. There is an algorithm f from natural numbers to $\{0, 1\}$ such that $f(k) = 1$ if and only if the kth quadruple (x, y, z, n) witnesses Fermat's Last Theorem, that is $x^n + y^n = z^n$ and $n > 2$. It follows that $A(f) = 0$ if and only if Fermat's Last Theorem holds.

A: Good.

Q: Since Fermat's Last Theorem has been confirmed, I wonder if my proof can be modified to use Riemann's Hypothesis instead of Fermat's Last Theorem.

A: Yes, this is possible. Recall that a Diophantine equation is an equation of the form $P(x_1, \ldots, x_r) = 0$ where P is a polynomial with integer coefficients and the variables range over integers. Given a Diophantine equation $P(x_1, \ldots, x_r) = 0$, order all r-tuples of integers first by the maximum absolute value and then lexicographically. Clearly there is an algorithm f_P from natural numbers to $\{0, 1\}$ such that $f_P(k) = 1$ if and only if the kth r-tuple of integers satisfies the equation. Hence $A(f_P) = 0$ if and only if the equation $P(x_1, \ldots, x_r) = 0$ is unsolvable.

By a theorem of Davis, Matiyasevich and Robinson, there is a particular Diophantine equation $R(x_1, \ldots, x_r) = 0$ which is unsolvable if and only if Riemann's Hypothesis holds [DMR]. It follows that $A(f_R) = 0$ if and only if Riemann's Hypothesis holds. Thus A should be a very clever algorithm indeed.

Q: Can you disprove (**) outright?

A: We have almost done that. Let me remind you that the following famous decision problem (Hilbert's Tenth Problem)

Instance: An arbitrary Diophantine equation.
Question: Is the equation solvable?

is undecidable [Ma].

Q: Let me see. Given an algorithm A that satisfies (**), we want to construct an algorithm A' for Hilbert's Tenth Problem. I got it. You have mentioned an algorithm f_P above. In fact, there is an algorithm F such that $F(P)$ is the desired f_P for every integer polynomial P. The desired A' is the composition of F and A: $A'(P) = A(F(P)) = A(f_P) = 1$ if and only if the equation $P(\bar{x}) = 0$ is solvable.

A: Good.

Q: Are there surprising positive theorems in constructive mathematics?

A: Yes. A famous theorem of Russian constructivism is Tseitin's continuity Theorem: Every real-valued function of a real argument is continuous [Ku, page

165].[4] The notion of function used here is a natural generalization of the notion of recursive function to the case when the arguments and values are constructive reals, and the continuity is constructive continuity which is stronger than classical continuity. In Brouwer's analysis, quite different from the analysis of Russian constructivists, you have Brouwer's Continuity Theorem: Every function from a closed real interval to $\mathcal{R}$ is uniformly continuous [TV, page 307].

Q: Interesting, very interesting. What was the reaction of the mainstream of mathematical community to constructive mathematics and constructivists' criticism of classical mathematics?

A: Mostly indifference.

Q: That must be frustrating for the constructivists.

A: Of course. I recall though that in 1960s Russian constructivists were enthusiastic and hoped that mainstream mathematicians would eventually understand that classical mathematics may be a sort of cheating: a proof that an equation has a solution may give us no clue how to actually find this solution, and so on. They expected that the advent of computers will make mathematicians more conscious about algorithms and will raise their interest in constructive mathematics. In 1995, I "discovered" in ETH[5] the following fascinating document[6] involving two famous mathematicians.

> *Between* G. Polya *and* H. Weyl *a bet is made according to the following conditions and concerning the following two theorems of contemporary mathematics:*
>
> *(1) Every bounded set of real numbers has the least upper bound.*
>
> *(2) Every infinite set of real numbers contains a countable subset.*
>
> Weyl *predicts the following:*
>
> *Within the next 20 years, i.e. by the end of 1937,* Polya *himself or the majority of authoritative mathematicians will concede that the notions of "number", "set", and "countable", which enter into these theorems and on which we generally rely today, are totally vague and that it is just as impossible to ask about the truth and falsity of (1) and (2) as, for example, about the truth of the principal theses of* Hegel*'s philosophy of nature.*

[4] In fact, Tseitin proved a stronger theorem: Every mapping from a complete separable metric space into a separable metric space is continuous. A special but important case of this theorem was discovered independently by Kreisel, Lacombe and Shoenfield. The references can be found in [Ku] and [TV].

[5] Swiss Institute of Technology

[6] As far as I know, [Gu2] contains the first English publication of the document.

POLYA *himself or the majority of authoritative mathematicians will recognize that the theorems (1) and (2) are wrong according to a reasonably possible, clear interpretation of their literal meaning (be it the case that different interpretations will still be available, or be it the case that already a consensus will have been reached upon one). Or if, in the mentioned period of time, one managed to find a clear interpretation of these two theorems in which at least one of them is true, then a creative achievement was necessary, by which the foundations of mathematics took a new and original turn, thereby providing the notions of a number and of a set with a new content about which we have no idea today.*

WEYL *is the winner if his prediction proves correct, otherwise* POLYA *is the winner.*

If after the determined period the two parties do not agree who is the winner then the set of all full professors of mathematics, different from the two parties to the bet, at the ETH and the universities of Zürich, Göttingen and Berlin shall act as judges. Their decision will be made by a majority of votes; in case of equality of votes the bet shall be considered a tie.

The losing party promises to publish the conditions of the bet and the fact that he has lost it, as an advertisement in the Jahresberichte of the Deutsche Mathematiker Vereinigung at his expense.

Zürich, February 9, 1918.

Q: Can one find Weyl's ad in the Jahresberichte?

A: No. Weyl did admit losing the bet but, with Polya's permission, did not publish any ad in Jahresberichte [Po].

3 Good things about constructivism

Q: Before you criticize constructivism, tell me if you find anything good about it?

A: Yes, I do.

1 Historically, the intuitionistic critique of classical mathematics contributed to clarifying important issues like the necessity of clear separation of mathematics and metamathematics or the nature of axiomatic method.

Q: Was there any controversy about the axiomatic method? Everybody seems to like it.

A: Brouwer criticized the method in his doctoral thesis (1907). Here is how Evert W. Beth summarized the critique in [Be]: "Axiomaticians are reproached with establishing merely verbal edifices without paying due attention to the construction of a corresponding system of mathematical entities. Moreover, they are charged with inconsistency in that they falsely accept the consistency of an axiom system as a guarantee of the existence of a system of mathematical entities fulfilling the axioms, while at the same time they appeal to the existence of intuitively constructed system of mathematical entities in their proofs of consistency."

Q: I am not sure I understand this completely but one phrase has caught my attention: "They falsely accept the consistency of an axiom system as a guarantee of the existence of a system of mathematical entities fulfilling the axioms". In other words, a consistent axiomatic system may have no model. This is certainly false in the case of first-order logic. Just use the completeness and (if the number of axioms is infinite) the compactness theorems.

A: The axiomatic method is not restricted to first-order logic, but even in the case of first-order logic, Brouwer has a point: It is possible that every model of a consistent system of axioms is necessarily very complex. The consistency will not guarantee you a model if your application admits only finite models, or only finitely generated models, or only computable models, *etc.* Besides, the completeness and compactness theorems for first-order logic were proved much later.

2 Brouwer wanted to wake up mathematicians to foundational problems. He succeeded to an extent.

3 Constructive mathematics can be seen as classical mathematics with restricted tools and in that sense achievements of constructive mathematics are also achievements of classical mathematics. Recall Tseitin's Continuity Theorem mentioned above (every constructive function of a real argument is continuous) for instance. In some areas of mathematics, like finite combinatorics, there is little difference between the constructive and classical approaches. Members of a broader Russian constructivist school proved impressive theorems of direct interest to mainstream mathematicians. One example is early results of G. S. Tseitin on computational complexity. Another example is Matiyasevich's negative solution of Hilbert's Tenth Problem.

4 Constructive logic, a byproduct of constructivism, has found numerous applications in computer science, *e.g.* in type theory, and also in classical mathematics. One does not have to be a constructivist to use constructive logic, and it appears, possibly in a disguise, in very unexpected places. For example, Cohen's forcing (called strong forcing nowadays), the key notion in his proof that the negation of Cantor's Continuum Hypothesis is consistent with ZFC [Co] is intimately related to constructive logic (though Cohen does not mention that as far as I remember); see also [Fi].

5 There is also that ever growing gap between pure mathematics and applications. Constructivists worry about it. Listen to the famous American constructivist Errett Bishop: "Mathematics flourishes as never before. Its scope is immense, its quality high. Mathematicians flourish as never before. Their profession is respectable, their salaries good ... And yet there is dissatisfaction in the mathematical community. The pure mathematician is isolated from the world, which has little need of his brilliant creations. He suffers from alienation which is seemingly inevitable: he has followed the gleam and it has led him out of this world" [Bi].

Q: Did the constructivists succeed in narrowing the gap?

A: The emphasis on constructions and computations has been certainly useful. I think that there is a real danger in sciences of over-abstracting into the rarefied atmosphere of irrelevance. Unfortunately, the constructivists' criticism of classical mathematics tended to throw the baby out with the bath water, and the constructivists created a kind of very pure mathematics of their own.

4 Computer proofs vs. proofs by hand

Q: You have not mentioned that constructive proofs buy you peace of mind. Imagine that you have two hardware chips for the same task. The correctness of one was verified constructively and the correctness of the other was verified classically, say within ZFC. Would you pay more for the constructively verified chip?

A: Probably not. It is true that, as far as we know, ZFC may be inconsistent, but the chance that the chip fails because of the inconsistency of ZFC is very remote indeed. The physical laws used in the construction of the chip may be not absolute either. We have plenty but still only so much evidence in favor of those laws. I would pay more attention to which of the two proofs is more transparent, what kind of testing did the chips go through, to what extent the tedious details of the proofs were checked by computer programs, how reliable are those programs, and so on.

However, there is a somewhat related pro-constructivism argument that has been taken more seriously. Imagine that you need to program an algorithm that, given a natural number x produces a natural number y so that a decidable condition $\psi(x, y)$ is satisfied. I speak about natural numbers for simplicity. It may be the case for example that x is a directed graph and y is a string. A proof of $(\forall x)(\exists y)\psi(x, y)$ in constructive logic yields[7] a program for computing y from x which is a provably correct implementation of the specification. This idea in one form or another

[7] *E.g.* via classical Kleene's realizability or more modern type-theoretical modified realizability

inspired many; in particular it is an inspiration for the proof system Coq developed in INRIA Roquencourt near Paris.

Q: It sounds great. You don't have to program and then try to prove the correctness of a piece of $C++$ code. Just prove $(\forall x)(\exists y)\psi(x,y)$, get your program and don't worry about verification. How difficult it is to extract a program from the proof?

A: In certain cases, proofs and programs correspond very closely to each other. For example, any proof of a formula φ in the minimal constructive logic of implication yields an expression (program) of type φ in the appropriate typed combinatory calculus, and the other way around.

Q: I have no idea what you are talking about.

A: Consider[8] a typed calculus with two constants K and S satisfying the equations $Kxy = x$ and $Sxyz = (xz)(yz)$ for all x, y, z. The convention of associating to the left is used here, so that $Kxy = (Kx)(y)$ and $Sxyz = ((Sx)(y))(z)$.

Q: In what sense is the calculus typed?

A: A type is associated with each variable.

Q: Is there any simple semantics of the calculus?

A: Given some initial types, construct new types by induction: If α and β are types then $\alpha \to \beta$ is a type. An element of type $\alpha \to \beta$ is a function from type α to type β. Now consider the universe of all elements of all the types.

Q: How are K and S interpreted?

A: In fact, for every pair (α, β) of types, we have a constant $K_{\alpha,\beta}$ interpreted as an element of type

$$\alpha \to (\beta \to \alpha)$$

such that $K_{\alpha,\beta}xy = x$ for all elements x, y of types α, β respectively. Similarly, for every triple (α, β, γ) of types, we have a constant $S_{\alpha,\beta,\gamma}$ interpreted as an element of type

$$(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$$

such that $S_{\alpha,\beta,\gamma}xyz = (xz)(yz)$ for all elements z, y, x of types $\alpha, \alpha \to \beta$ and $\alpha \to (\beta \to \gamma)$ respectively.

Q: I understand what you have said but do not have any feel for the calculus.

A: That is OK for our purposes here. The calculus can be seen as a rudimentary functional programming language. The two displayed type expressions happen to be the two axioms for the minimal constructive logic of implication. The only

[8] The reader uninterested in the details of the example may skip this **A** and the four following **A**'s and resume with **A:** You seem suspicious.

derivation rule of that logic, *modus ponens*, corresponds naturally to the composition of functions: if x is of type α and y is of type $\alpha \to \beta$, then $y(x)$ is of type β. Any proof of a formula φ in the logic yields an expression (program) of type φ in the combinatory calculus, and the other way around.
For example, the proof

$$\begin{array}{l} \alpha \to (\beta \to \alpha) \\ (\alpha \to (\beta \to \alpha)) \to ((\alpha \to \beta) \to (\alpha \to \alpha)) \\ (\alpha \to \beta) \to (\alpha \to \alpha) \end{array}$$

of the formula $\varphi = ((\alpha \to \beta) \to (\alpha \to \alpha))$ generates the sequence

$$K_{\alpha,\beta},\ S_{\alpha,\beta,\alpha},\ S_{\alpha,\beta,\alpha}(K_{\alpha,\beta})$$

of expressions where the final expression is of type φ.

This is a special case of the so-called Curry-Howard correspondence described for example in [Si].

Q: How far has this correspondence between proofs and formulas been extended?

A: You seem suspicious.

Q: I guess I am. Recall that I am a professional programmer and only an amateur logician. To me, the combinatory calculus does not look like a programming language. It seems that the correspondence is really between two logical systems.

A: You may have a point there. The correspondence has not been extended anywhere near real-life programming languages.

Q: What about the quality of the algorithms extracted from the proofs?

A: People working in the field tell me that the programs extracted from proofs tend to be slow. One reason for the slowness is that the program verifies not only the final result but also various intermediate results. It isn't obvious how to free the program from unnecessary verification. In fact, people do a bit of reverse engineering and analyze known faster programs to see which proofs can generate them or at least similar faster programs.

Q: It would be great though to have a fully automated system for proving theorems and extracting algorithms. Actually it would be great to have a fully automated system just for proving theorems.

A: I think that such a system can be useful only for very limited tasks. Trying to prove a theorem, I like to use whatever logic it takes to prove the theorem. The natural proof of the theorem may be outside the system. Furthermore, it may be the case that any proof of the theorem within the system is much more complex. The theorem may not be even provable in the system.

It takes creativity, ingenuity and the intimate knowledge of the application field to prove meaningful theorems and to design good algorithms. Do you believe that a fully automated theorem proving system can do that for you?

Q: I doubt it. It had better be an interactive system, so that the computer does only more routine parts.

A: I agree. One reasonable way to go is to split the process into two stages. First, prove your theorem using any mathematics that helps; do not restrict yourself to any fixed formal system. Second, if necessary, use computers to check your proof. Notice that the second task is not trivial. A whole new scientific discipline may be needed. Let me call it Pedantics. A better pedanticist ("pedant" sounds negative) has a system with a more liberal front end, so that it is not too painful to rewrite your informal proof into their formal language.

Q: In other words, first prove your theorem by hand and then go to a pedanticist.

A: You can use computers on the first stage as well, for example to deal with tedious details. An interactive system like PVS [ORSV] may be useful. By the way, mathematicians use computers more and more in their proofs. The solution of the Four Color Problem [AH, RSST] is a good example. Certainly computer scientists should take advantage of computers.

Q: I heard that some mathematicians doubt that the Four Color Problem has been really proved.

A: I do not think that there are still serious doubts about the result. It is curious though to have a proof which needs another proof to show that the first proof is correct. To convince a human reader, a proof should create right images in reader's head, it should be transparent, and thus it is not surprising that mathematicians find computer proofs less convincing. It surprises me more that so many computer scientists scorn proofs by hand and accept computer proofs only.

Q: But mathematicians make errors.

A: Surely they do. That is the reason for the second stage.

Q: Can a human comprehend a program with a million of lines of code?

A: I think that this may be possible if the program is the result of a reasonable design process. The design may involve a whole hierarchy of programs of various abstraction levels where some programs refine various parts of others. A human can keep in mind only so many details, but the top level program, the total architecture, and each particular refinement may be amenable to human analysis.

Q: What about a proof that the final program lives up to the top level specification.

A: Use a mathematical modeling system which allows you to model all those programs on their natural abstraction levels. For each refinement, the informal correctness argument should give rise to a mathematical proof of correctness.

Q: Oh, I see. You want me to use your abstract state machines.

A: I surely do, but this is not the point. Let us return to constructivism.

5 An antithesis to constructivism

Q: What do you think is wrong with constructivism?

A: There are two basic issues with the historical constructivism. One is the ideological restriction of logic and mathematics. The other is the feasibility of constructions. Ironically the historical constructivism has not been sufficiently constructive.

Q: Do you have an antithesis to constructivism?

A: Well, my antithesis to constructivism would be the pragmatic principle of separating concerns.

Q: What do you mean?

A: Suppose you need to know whether, for every object x of a type X, there is an object y of a type Y such that some condition $K(x, y)$ is satisfied. It may be the case, that a mere existence of the desired y is sufficient for your purpose. Then try to prove just the existence of y. For example, you may assume $\neg(\forall x)(\exists y)K(x, y)$ and try arrive to a contradiction.

It may happen of course that knowing $(\forall x)(\exists y)K(x, y)$ is insufficient. You need to know whether there is a function f with $K(x, f(x))$ for all x which is Borel, or arithmetical, or recursive, whatever. Go ahead and investigate that. Notice that recursivity is only of possible issues. The historical constructivism is obsessed with recursivity.

It may also happen that you need to construct an appropriate y from a given x in a practical sense. Having an impractical algorithm for constructing y may useless.

Q: Did the constructivists believe that non-constructive methods are really irrelevant?

A: I am not knowledgeable enough to discuss their beliefs but the history of mathematics demonstrates very clearly the usefulness and relevance of non-constructive methods. Many mathematicians were appalled by the proposals of constructivists to restrict their tools.

Q: Can you give me a simple example of the relevance of non-constructive methods?

A: Recall our discussion on zero-one laws [Gu1] and in particular on the zero-one law for the first-order properties of graphs. We were interested in finite graphs but used the infinite random graph as a clean and simple limit case.

Q: I understand that the constructivists devoted most attention to the mathematical analysis.

A: That is true. Nevertheless the classical analysis is clearer than its constructive counterpart(s), and its non-constructive (or seemingly non-constructive) theorems and methods have been used for developing modern efficient numerical methods.

Q: Was constructive mathematics relevant to the development of modern efficient numerical methods?

A: I don't think so.

Q: Why wasn't it? I understand that banning of non-constructive methods can be detrimental. But the emphasis on constructions and computations could be a counterbalance.

A: To be fair, we should remember that there were only few constructivists. It is plausible that a greater constructivist community would contribute heavily to developing efficient numerical methods. To this end, they would have to overcome the fixation on the notion of recursivity. Notice also that a constructive proof of $(\forall x)(\exists y)\varphi(x,y)$ does not guarantee a feasible algorithm for constructing y from x. And algorithms may be impractical indeed. An algorithm can run years and years on input $x = 2$; it is like climbing a tree and claiming to be closer to the moon.

Q: It may be important though to know whether y is computable from x. If you prove that there is no algorithm for the purpose then you know that there is no feasible algorithm for the job either.

A: True.

Q: Maybe, when the notion of algorithm was introduced, some people thought that every natural decision problems has a feasible decision algorithm. As an undergrad, I had a similar illusion about the convergence of numerical series. Later I was surprised to see series converging so slowly that they are useless for approximating the limit.

A: I think you are right. By the way, it is often the case in applications that the decision problem of interest is obviously decidable. The problem is only to find a feasible algorithm. For example, many problems are NP, that is solvable in nondeterministic polynomial time, and therefore exponential-time solvable.

Q: Is there a polynomial-time version of constructive mathematics?

A: The thought has occurred to constructivists [Kr] but they did not do much work in this direction.[9]

Q: I wonder why. Polynomial-time algorithms are supposed to be feasible.

[9] A work has been done also on polynomial-time bounded versions of constructive logics; see [GSS] in this connection.

A: An algorithm that runs in time say n^{72} is not feasible. It is natural polynomial-time solvable problems that so often happen to be feasible. The first polynomial-time algorithm for such a problem may be not feasible at all, but then people construct more and more feasible algorithms and finally the problem may be proved to be solvable in time $n \log(n)$ or even linear time.

Q: But maybe the complexity analysis is irrelevant. You speak about worst-case complexity. An algorithm with bad worst-time behavior may run fast on average or on inputs of interest.

A: The average-case analysis is harder but the overall picture should be similar. The case of inputs of interest is too elusive for a theoretical investigation. It may be the case that an algorithm of high complexity is satisfactory on inputs of interest. I would not bet on that though. Complexity analysis is only a guidance, but it is worth to be taken seriously.

Q: You want the constructivists worry about feasibility?

A: Yes, feasibility is the real issue. It seems to me that the constructivist movement lost the pioneering spirit. In computer science, constructivists did not play the role one could expect them to play. They remained largely satisfied with constructivity on the level of recursive functions and did not refine the notion of construction sufficiently. Of course that task is very hard and the constructive community was never very large. Still, they could have been the ones to pioneer computational complexity theory. They could have been the first to criticize the existing complexity theory for ignoring too often the feasibility issue.

Q: But the feasibility concept is hard. It is hard to define in theoretical terms what is feasible.

A: True, but this is also a challenge. Maybe a new constructivism will arise to meet the challenge.

Acknowledgment

Andreas Blass, Egon and Donatella Börger, Martin Davis, Vladik Kreinovich, Boris Kushner, Gregory Mints, Jan Smith, Vladimir Uspensky and Dirk van Dalen contributed many useful comments to [Gu2]. Clemens Cap translated the Polya/Weyl bet. [Gu2] was written in July and August 1995 when I was visiting Paris (LITP) and Aarhus (BRICS) respectively. I am very grateful for the help and hospitality.

References (slightly annotated):

[**AH**] Kenneth Appel and Wolfgang Haken, "Every planar map is four colorable", Bull. Amer. Math. Soc. 82 (1976), no. 5, 711–712.

There is also a more recent book of the same authors and with the same title: Contemporary Mathematics, Volume 98, American Mathematical Society, 1989.

[**Be**] Evert W. Beth, "The Foundations of Mathematics: A Study in the Philosophy of Science", North-Holland, 1959.

[**Bi**] Errett Bishop, "Foundations of Constructive Analysis", McGraw-Hill, 1967.

[**Bl**] Andreas Blass, Private communication, August 1995.

[**CC**] Jean-Pierre Changeux and Alain Connes, "Matière à pensée", Odile Jacob, 1989.

[**Co**] Paul Cohen, "Set Theory and the Continuum Hypothesis", Benjamin, 1966.

A great exposition of Gödel's proof of the consistency of ZFC + CH and a much less readable exposition of Cohen's own result. A more accessible exposition of the Cohen's theorem is found *e.g.* in [Sh]. (More recent expositions tend to avoid strong forcing because it doesn't obey classical logic.)

[**DMR**] Martin Davis, Yuri Matiyasevich and Julia Robinson, "Hilbert's tenth problem. Diophantine equations: Positive aspects of negative solutions", Proceedings of Symposia in Pure Mathematics 28, American Mathematical Society, Providence, RI, 1976, 323–378.

[**FB**] Abraham A. Fraenkel and Yehoshua Bar-Hillel, "Foundations of Set Theory", North-Holland, 1958.

[**Fi**] Melvin Chris Fitting, "Intuitionistic logic, model theory and forcing", Amsterdam, North-Holland Pub. Co., 1969.

[**GSS**] Jean-Yves Girard, Andre Scedrov and Philip J. Scott, "Bounded linear logic: a modular approach to polynomial-time computability", Theor. Comput. Sci. Theoretical Computer Science 97:1, 1992, 1–66.

[**Go1**] Kurt Gödel, "Consistency-Proof for the Generalized Continuum Hypothesis", Proc. of Amer. National Academy of Sciences, vol. 25, 1939.

A more accessible exposition is found *e.g.* in [Co].

[**Go2**] Kurt Gödel, "What is Cantor's continuum problem?", in "Philosophy of Mathematics", eds. P. Benacerraf and H. Putnam, Cambridge University Press, 1983, 470–485.

[**Gu1**] Yuri Gurevich, "Zero-One Laws", Bulletin of the European Assoc. for Theor. Computer Science, No. 46 (Feb. 1992), 90–106.

[**Gu2**] Yuri Gurevich, "Platonism, Constructivism, and Computer Proofs vs. Proofs by Hand", Bulletin of European Association for Theoretical Computer Science, Oct. 1995, 145–166.

[**Kl**] Stephen Cole Kleene, "Introduction to Metamathematics", Van Nostrand, 1952 (and North Holland 1971).

[**Kr**] Vladik Kreinovich, "Remark on the Margins of Kushner's Book: On the Constructive Mathematical Analysis Restricted to Polynomial Time Algorithms", Manuscript (in Russian), Leningrad, 1973.

[**Ku**] Boris A. Kushner "Lectures on Constructive Mathematical Analysis", Translations of Mathematical Monographs, vol. 60, American Mathematical Society, Providence, Rhode Island, USA, 1984. The original published by Nauka, Moscow in 1973.

[**Ma**] Yuri V. Matiyasevich, "Hilbert's Tenth Problem", MIT Press, 1993.

[**ORSV**] S. Owre, J. Rushby, N. Shankar and F. von Henke, "Formal Verification for Fault-tolerant Architectures: Prolegomena to the Design of PVS". In: *IEEE Transactions on Software Engineering*, vol. 21, no. 2, February 1995, 107–125.

[**Po**] G. Polya, "Eine Erinnerung an Hermann Weyl", Math. Zeitschrift (126), 1972, 296–298.

[**RSST**] Neil Robertson, Daniel P. Sanders, Paul D. Seymour and Robin Thomas, "The Four Colour Theorem", J. of Combinatorial Theory, Ser. B, 70:1, 2–44 (1997).

A cleaner proof (comparative to [AH]) of the Four Color Theorem that also uses a computer in an essential way.

[**Sh**] Joseph R. Shoenfield, "Mathematical Logic", Addison-Wesley, 1967.

[**Si**] Harry Simmons, "Logic and Computation: Taking the Curry-Howard Correspondence Seriously", Manuscript, Computer Science Dept., Manchester University, UK, 1993.

[**Sp**] Ernst Specker, "Nicht konstruktiv beweisbare Sätze der Analysis", J. Symbolic Logic 14 (1949), 145–158.

[**TV**] Anne S. Troelstra and Dirk van Dalen, "Constructivism in Mathematics: An Introduction", Volumes 1 and 2, North-Holland, 1988.

[**vD**] Dirk van Dalen, "Why Constructive Mathematics?", Kluwer Dordrecht, in print.

According to the author, the paper is in part a reaction to my criticism that constructivism is not sufficiently constructive.

[**Wi**] Andrew Wiles, "Modular elliptic curves and Fermat's Last Theorem", Annals of Mathematics 141:3, May 1995, 443–551.

The theorem of relevance to us is this:

Theorem 0.5. Suppose that $u^p + v^p + w^p = 0$ with $u, v, w \in \mathcal{Q}$ and $p \geq 3$, then $uvw = 0$.

Here $\mathcal{Q}$ is the field of rational numbers and p is a positive integer.