25th Conference Applications of Logic in Philosophy and the Foundations of Mathematics, Szklarska Poręba, May 2020

An abstract of the invited lectures by Mirna Džamonja

Set theory and constructive mathematics

What is meant by set theory in these notes is the set theory axiomatised by the axioms of ZFC, using classical 1st order logic.

ZFC is commonly described as non-constructive, mostly because of the Axiom of Choice which states that there is a choice function for every family of non-empty sets, without constructing a witness to this existential statement. ZFC, especially the Axiom of Choice, gives many examples of quite disastrous counter-example to the any intuition about constructability. The most striking, perhaps, is the Banach-Tarski paradox, which allows one to take a ball B in R^3 and decompose it into 5 pieces, which then can be put together to form two copies of B. Another example is usually taken to be the Diaconescu/Goodman-Myhill theorem which shows that AC implies the law of the excluded middle.

In constructive type theory, there is no excluded middle. Hence, we conclude that not only ZFC is not constructive, but it moreover inimical to constructive mathematics.

Our thesis will be that this is not the case, since this statement strongly depends on what we take to be constructive mathematics. We are going to take a different point of view than that taken by classical constructive mathematics (which is not a uniquely defined notion).

In this view, we consider AC to be a positive statement. It says that whatever set one has, there is a way to see this set as a line with no infinite decreasing sequences, a line that is well-ordered. This avoids anarchy and is viewed positively in, for example, computer sciences, where one studies well quasi-orders and takes them to be the heart of termination arguments. This idea can indeed be traced to Turing in 1949 and has featured prominently in computer science ever since. So AC is natural, it increases the limits of computation and it manifests itself in the study of ordinals.

The Law of Excluded Middle LEM is even more natural. Even in type theory one can formulate it as a judgement. For example, in Voïevodski's simplical model of homotopy type theory with the univalence axiom, which is laudable for its connection with Coq's theorem proving abilities, LEM can be added on the level of propositions and AC on the level of sets, still obtaining a model of HoTT with Univalence.

It seems to us that these more recent ideas of constructability indicate that we should revisit the engrained opinion that ZFC and constructive mathematics are inimical. We can start by asking what 'constructive mathematics' actually means. A closer look at this question leads to the observation that although there are several reasonable candidates for this notion that have been considered since 1930s, the view of what that notion should be has not been uniquely settled. One can also identify various motivations, not always congruent and some no longer relevant , which have determined such definitions.

We feel that in the modern world which is digitalised, to define what is constructive we should start from what constructive means to us and today. It seems that the answer goes back to Turing and Church, which basically states that what is constructive is that which can be done by a computer.

Having settled that, where does such a definition leave set theory? Our thesis on this is that set theory may gain new knowledge through the connection with computing and vice versa. Turing and Church were interested in the concept of computability, but the times have changed and computers can do much more: they can help us reason.

It may come as a surprise to some, but there is already a close connection of set theory to computing. Part of it is expressed through the work on the proof verifier Isabelle (HOL), which allows the law of excluded middle and can re-prove many theorems in set theory. Lawrence Paulson reproved Gödel's Incompleteness Theorems in Isabelle and proved the independence of AC from the axioms of ZF (2003). This is surprising since the popular type theoretic theorem provers do not work on the basis of classical logic. However, Isabelle does and it can handle important theorems in set theory. As part of our thesis, we may ask what kind of questions in logic and set theory could be approached by this theorem prover.

In principle, everything that can be proved in set theory can also be proved in Isabelle, but the point is how to find such proofs. Even though it has become usual to associate combinatorial set theory to questions about cardinals, questions about ordinals form part of set theory where much has to be discovered and where it seems that help of a computer assistant might have a huge impact. This is specifically true of ordinal partition relations. For example, it is still an open question, worth 1000$ on the Erdös list, to completely characterise countable ordinals α such that $\alpha \rightarrow (\alpha, 3)$. The reason that the computer might help is that the existing results are very technical and almost undoable by a human. New progress by the existing methods is hard to envisage.

Our idea is to move on this question by building libraries of ordinal partitions in Isabelle so to be able to prove further results mechanically. This is a project with Paulson and Angeliki Koutsoukou-Argyraki. So far, we have been able to recover results including Specker's theorem and the theorems by Erdös and Milner.

We shall report on this project and will discuss some other areas where the interaction between set theory and computing could be of interest.