Gödel's incompleteness theorem (1931), one of the most important results of mathematical logic, can be roughly described as saying that no axiom system is sufficient to resolve all mathematical problems. This immediately leads to the question of what specific mathematical theorems cannot be proved using natural axioms encoutered in practice. Perhaps the best-known example was given in 1963 by Paul Cohen, who showed that the continuum hypothesis, a statement concerning the possible sizes of infinite subsets of the real number line, cannot be proved or disproved on the basis of the commonly accepted axioms of mathematics, the so-called Zermelo-Fraenkel axioms. However, the very formulation of the continuum hypothesis mentions rather unusual and enigmatic objects. On the other hand, from the perspective of everyday mathematics, the Zermelo-Fraenkel axioms are extremely powerful. To understand what theorems of more down-to-earth mathematics require proofs that invoke very abstract, unexpected or even doubtful objects, one has to study weaker axiom systems. As an example of the effects of such study, we may mention a result obtained in 1977 by J. Paris and L. Harrington, who exhibited a principle of finite combinatorics that cannot be proved without reference to at least some infinite objects, for instance to so-called transfinite ordinal numbers.

The project will deal with provability in some axiom systems suitable for investigating theorems from combinatorics and the theory of computation. Part of our work will concern two well-known combinatorial results: Ramsey's Theorem for pairs and Hindman's Theorem. The former says that if we are given an infinite supply of points and some of them are connected by edges, then there is an infinite set of points in which either each pair of points is connected or no pairs are; this generalizes similar weaker statements about finite graphs. Hindman's Theorem has a slightly more complicated statement linking Ramsey-like ideas with the properties of addition on the natural numbers. The strength of axioms needed to prove Hindman's Theorem remains a mystery after many years of study: all proofs known up to now, including proofs of apparently weaker versions of the theorem, require axioms much stronger than those needed to prove the Paris-Harrington principle, but on the other hand, it is still not excluded that all consequences of the theorem in finite combinatorics have purely elementary proofs. We intend to study the problem whether proving Hindman's Theorem and its restrictions genuinely requires nonelementary reasoning. The case of Ramsey's Theorem for pairs is a bit different: even though the proof of the theorem itself requires the use of relatively complex infinite sets, it was shown recently that many consequences of the theorem have proofs that are essentially calculations on the natural numbers (cf. a May 24, 2016 article in Quanta Magazine). The practical significance of this result is not yet clear: for instance, it is unknown whether the more elementary proofs of consequences of Ramsey's Theorem are not astronomically large compared to the original proofs. This will be one of the issues investigated as part of the project.

Related questions concern the strength of axioms needed to prove some results of theoretical computer science, in particular theorems stating the existence of algorithms solving certain computational tasks. A result of this kind due to M. Rabin (1969) was known for having only remarkably advanced and abstract proofs. Recently, we showed together with a group of collaborators that this was unavoidable: Rabin's Theorem cannot be proved without invoking sets with very complicated, almost circular definitions. Interestingly, Rabin's algorithm itself is rather elementary; the advanced axioms are needed to prove its correctness, and indeed the correctness of any algorithm solving the specific problem. We would now like to obtain a more precise characterization of the axioms needed to prove Rabin's Theorem, and to find other examples of theorems from computer science that cannot be proved without using objects that would seem to lie well outside the range of interests of computer science. Perhaps surprisingly, this will also require analyzing the logical strength of some variants of Ramsey's Theorem.

A separate part of the project will be devoted to the study of provability in axiom systems that are part of so-called bounded arithmetic. These systems are very weak and some statements known to be unprovable in them express apparently "obvious" combinatorial principles, such as the pigeonhole principle: „if $n+1$ pigeons are placed in n holes, then at least one hole will contain more than one pigeon". Research on bounded arithmetic is connected to the study of algorithms solving a crucial problem known as satisfiability: „given a logical formula, can we assign values to variables in the formula so that the whole formula becomes true?" Simplifying somewhat, one could say that each important result on unprovability in bounded arithmetic leads to the example of a formula that some specific algorithm cannot deal with in reasonable time. At the moment, we can only provide such examples for very simple algorithms, but these include the most popular algorithms used in practice – such as, for instance, the one underlying the recently discovered solution to the Boolean Pythagorean triples (cf. the August 2017 issue of Communications of the ACM). Our aim is to enlarge the pool of available examples, mostly related to systems that incorporate some mechanisms for counting.