Effective computations in predicative mathematics

According to Alexander Grothendieck mathematical research is about understanding things as they are, and therefore, this activity is on the same level as exposition of mathematics and teaching. He described his work as the process of creation of new worlds, where the problems to be solved could naturally live and easily be solved. Some problems seem to be difficult, only because we are looking at them from the perspective of a wrong world. The worlds he built are nowadays known as Grothendieck toposes.

This philosophy also manifests itself in the recent work on nominal sets and sets with atoms. The idea of treating mathematical structures as living inside an alternative universe rather than the usual universe led to a vast simplification of methods and proofs of some known theorems. Consequently, it shed light on previously unnoticeable phenomena. A similar motivation underlied the work on foundations for automata theory in sets with atoms. Sets with atoms serve as an alternative to the usual set theory foundations for mathematics, where some infinite, though highly symmetric sets, behave in a finitistic way. Therefore, one can try to carry over classical analysis and algorithms from finite structures to some infinite structures. Recent results show that this is indeed possible and leads to many practical applications: automata over infinite alphabets, model checking, constraint satisfaction solving programming languages[1], to name a few. The aim of the proposed project from this perspective is in the spirit of the philosophy of Alexander Grothendieck: to find a better explanation and exposition of mathematics, such that new theorems immediately appear, and uncover unexploited area of mathematics triggering research in new directions. Furthermore, the project will result with a theory unifying various branches of mathematics and computer science, preventing the process of rediscovering previously known results. This project has, however, more objectives.

This project lies in the Pasteur's quadrant — it is an application-inspired basic research, which can be directly used to solve real-world problems: especially targeting mission and safety critical systems. The reliability of information systems is one of the most important and difficult concern in the system design process. Failures in mission and safety critical systems may cause long term environmental damages, human deaths or even annihilation of whole civilizations. For example, in 1980 North American Aerospace Defense Command reported that USA was under attack and started preparation for a nuclear counter attack. Fortunately, it was quickly recognized that the report was caused by NORAD systems failure. Three years later, Soviet early warning satellites reported incoming five United States ballistic missiles. Officer in charge Stanislav Petrov, suspecting an error in computer systems, decided to break official procedures and did not lunch the nuclear missiles, preventing the full-scale nuclear war between USA and USSR. Later investigation showed that the system malfunctioned. In the period of 1985-1987 the Therac-25 medical device was involved in several cases where massive overdoses of radiation were given to patients resulting in six deaths. The device malfunctioned due to concurrent programming errors causing a race condition. In 2004 a new computer system was deployed to the Child Support Agency in United Kingdom. The software had more than 500 bugs resulting in overpay 1900000 people and underpay about 700000 people.

Model checking techniques help verification of systems and systems' models by automatising this process and giving formal proofs that the system works properly, or producing explicit counterexamples to the system correctness. Unfortunately, the classical model checking can deal with finite systems only, and as such may be applied to hardware design processes, but not directly to computer software (although, some truncations of computer systems to finite state machines can be checked by such tools). The reason for this limitation is that adding to finite systems additional expressive power, which is needed to model full computer systems, makes the process of verification ineffective (i.e. strongly undecidable). Nonetheless, recent results show that some infinite systems can be treated as finite from the perspective of alternative mathematics, and checked effectively. Our project will result with a more general view on alternative mathematics yielding new techniques for model checking.

[1] A working implementation of $N\lambda$, a functional programming language capable of processing infinite structures with atoms, is available through the web-site: `https://www.mimuw.edu.pl/~szynwelski/nlambda/`.