Counting models in formal verification

Filip Mazowiecki

The research and development we propose lies in the highly visible area of computer science: *formal verification*. It spans the spectrum from developing mathematical theories to implementing software tools. The objectives of this action are driven by current challenges and opportunities of computing devices. As they become more pervasive and more powerful, their design architectures and modes of operation are increasingly concurrent. The structure of the concurrency is often not fixed, and involves unboundedly many components, placing highly complex demands on formal verification.

In this project we analyse fundamental properties of certain models in formal verification. The common theme of the models is that they are used to count various properties. This is very useful as it captures properties like time, concurrency, probabilities, or duplicates that allow to express many problems arising in formal verification. Unfortunately, models that can count become significantly more complex and the decision problems are intractable or even undecidable. The goal of this project is to study expressiveness and complexity of different variants of the models to understand the properties that they can capture. Primarily, we are interested in two models: *Petri nets* and *weighted automata*.

Petri nets are an established model of concurrency with extensive applications in modelling and analysis of software, business processes and others. Having an elegant definition this model is also appealing in theoretical aspects. In this project we will focus on *workflow nets* a class of Petri nets that allows to model business processes. Specifically, they allow to formally represent workflow procedures in Workflow Management Systems (WFMSs). Such a mathematical representation enables the algorithmic formal analysis of their behaviour. This is particularly relevant for large organisations that seek to manage the workflow of complex business processes. Such challenges have received, and continue to receive, intense academic attention, e.g. via a discipline coined as *process mining* and pioneered by Wil van der Aalst. The aim of the project is to focus on important variants of workflow nets that have not received proper theoretical analysis. Primarily, we want to focus on the theoretical aspect of these problems. But building on that analysis we hope to develop new tools.

Weighted automata, introduced in the 1960s by Schützenberger, are a quantitative version of finite state automata for computing functions over words. Weighted automata are a fundamental model that occurs in surprisingly many contexts: from theoretical mathematical models of linear sequences and dynamic systems to practical applications in machine learning. The problems proposed in this project occur naturally as the communities work on similar models but on different questions. Formally, weighted automata are an extension of *linear recurrence sequences* (LRS), a robust class of functions often introduced to undergraduates. A typical example is the Fibonacci sequence, defined by the recurrence $F_{n+2} = F_{n+1} + F_n$. Weighted automata generalise this idea, allowing to count or measure properties of certain objects. In this project we will focus on the fundamental problems like equivalence or determinisation, which allow to simplify models. Finally, a part of the project is devoted to build new bridges between weighted automata and the previous model of *Petri nets*.