Abstract:

Recursive programs even over finite data domains are infinite state due to the unboundedness of the call stack. While sequential recursive programs can be modeled and verified via pushdown systems, verification in the presence of concurrency, which is undecidable in general, remains an interesting and challenging problem. The focus of my research so far has been to address this problem via different techniques: under-approximations, accelerations and via regular abstractions. In this talk I will present one of our result on regular abstractions.

A regular abstraction is the approximation of an infinite state system as a finite automaton. For instance, one may approximate the behaviors (as a language) of a recursive program/pushdown system by its downward closure (i.e. the collection of all subwords of words in the language) and this is always a regular language. One may also disregard the order of letters in the words and consider the Parikh-image of the language. Again for recursive programs/ pushdown systems, this is representable by a finite state automaton.

I will explain the main ideas behind our results on computing regular abstractions for automata equipped with a counter. While such representations for pushdown systems involves an exponential blowup, we will see that the situation is significantly better for counter systems. It is polynomial for both upward and downward closures and quasi-polynomial for parikh image abstraction.

I will then show how to use the above result to carry out verification of quantitative properties for procedural programs. Our Quantitative logic provides the ability to express arithmetic constraints over the execution times of procedure invocations. In this logic one may express properties such as “within the execution of each invocation of a procedure P, the time spent in executing invocations of procedures Q and R is less than 15%”.

Time permitting, I will also explain a second application of our result: in deciding the control state reachability problem for an under-approximation (bounded-stage runs) of concurrent recursive programs communicating via shared memory.