

# Invited Talk: Solving String Constraints, Starting from the Beginning and from the End

Philipp Rümmer

## Abstract

The recent years have seen a wealth of research on string solvers, i.e., SMT solvers that can check satisfiability of quantifier-free formulas over a background theory of strings and regular expressions. String solvers can be applied in different verification algorithms, for instance in symbolic execution to check path feasibility, in software model checking to take care of implication checks; a prime application area is security analysis for languages like JavaScript and PHP, for instance to discover vulnerability to injection attacks. To process constraints from those domains, it is necessary for string solvers to handle a delicate combination of (theoretically and practically) challenging operations: concatenation in word equations, to model assignments in programs; regular expressions or context-free grammars, to model properties or attack patterns; string length, to express string manipulation in programs; transduction, to express sanitisation, escape operations, and replacement operations in strings; and others. This talk will give a general introduction to string solving, and then present a solver architecture based on the concept of pre-image computation that is simple, yet turns out to be complete for an expressive fragment of string constraints. The architecture has been implemented in our solver OSTRICH (and is the result of joint work with many people).