**Ph.D. in Information Technology**
**Thesis Defense**

**February 9th, 2022**
**at 14:00**
**online by Teams**

**Michele CHIARI** – XXXIV Cycle

## Temporal Logic and Model Checking for Operator Precedence Languages: Theory and Applications

Supervisor: Prof. **Dino Mandrioli**

**Abstract:**

The ubiquity of computer systems in every industrial sector poses demanding challenges, including the verification of adherence of mission- and safety-critical systems to their requirements. Model checking is one of the most successful techniques developed for this objective. It consists of the formal specification of the system's requirements by means of a logic formalism, the generation of a model of the system by using an operational or denotational formalism, and the automatic and exhaustive verification of the adherence of the latter to the former.

The capabilities of this process depend on the choice of such formalisms. Different kinds of temporal logic are most often used for specifying requirements, both because of their ease in reasoning about the system's behavior along time, and because of the efficient model-checking algorithms they allow for. In terms of expressiveness, however, temporal logics such as LTL, CTL, and CTL* are limited to requirements expressible as regular languages. This can be a daunting limitation when the system to be verified is a procedural program. Procedures, or functions, are ubiquitous in the most popular programming languages. The matching between their calls and returns cannot be expressed by regular languages, so temporal logics limited to them cannot express requirements related to procedure execution.

This thesis develops a model-checking framework based on Operator Precedence Languages (OPLs). OPLs are a subclass of Deterministic Context-Free Languages, and are significantly more expressive than regular languages. Being suitable for describing the syntax of real-world programming languages, they can dramatically extend the properties expressible in system specifications. In particular, they enable verification of procedural programs with exceptions, which state-of-the-art logics cannot do. In this thesis, we present two temporal logics capable of expressing OPL properties. The first one, OPTL, is a first attempt at this task, for which we develop a model-checking procedure. Unfortunately, OPTL still has some limitations in terms of expressiveness. Thus, we introduce a

better logic, POTL, for which we prove equivalence to First-Order Logic, and develop and implement an automata-theoretic model-checking procedure. The resulting tool shows promising results when executed on case studies.

**PhD Committee**
Prof. **Letizia Tanca**, Politecnico di Milano
Prof. **Manfred Droste**, Università di Lipsia
Prof. **Adriano Peron**, Universita' di Napoli