Contract Specification and Verification: Experience with the Symboleo Language

Daniel Amyot

School of Electrical Engineering and Computer Science,
University of Ottawa, Canada
damyot@uottawa.ca

Abstract. Legal contracts specify the terms and conditions that apply to business transactions. Contracts are commonly expressed in natural language and contain many legal requirements that are often ambiguous, incomplete, and possibly inconsistent. Smart contracts are programs intended to partially automate, monitor, and control the execution of legal contracts to ensure compliance with relevant terms and conditions. This presentation focuses on the formal specifications of legal contracts that can enable automated analysis and can support the generation of smart contract programs that monitor legal contracts. To that end, the Symboleo textual language was recently proposed, where contracts consist of collections of obligations and powers that define a legal contract's compliant executions. Symboleo also offers execution time operations such as subcontracting, assignment, and substitution. The concepts underlying Symboleo are inspired from an existing legal ontology (UFO-L) with specialized contract concepts, with semantics described in terms of logical axioms on statecharts that describe the lifetimes of contracts, obligations, powers, and other concepts. An encoding of Symboleo specifications in the nuXmv language, including a library of trusted modules capturing basic Symboleo concepts, enables the formal verification of properties of a contract, expressed in temporal logic (i.e., in LTL or CTL). Examples and experiences from two domains (food supply chain and transactive energy markets) will be discussed, together with ongoing work on contract monitoring and other challenges.

Short bio. Daniel Amyot is Professor at the School of Electrical Engineering and Computer Science of the University of Ottawa. His research interests include software engineering, scenario-based and goal-based requirements engineering, business process modelling and mining, regulatory compliance, smart contracts, and healthcare informatics. Daniel led the standardization of the User Requirements Notation at the International Telecommunication Union (from 2002 to 2013) and is now heavily invested in the development of Symboleo for specifying, verifying, and monitoring (smart) legal contracts. He was general chair of the RE Conference in 2015 and program co-chair in 2018. Daniel is on the editorial boards of SoSyM, REJ, and EMSE. He holds a Ph.D. in Computer Science from the University of Ottawa (2001) and is a Senior Member of IEEE.