Formal Verification of Business Process Models and Notations.

LRE, EPITA Toulouse

Field : Computer Science
Research Unit : LRE, EPITA
Working Place : EPITA Toulouse
Qualification : Master's degree or Engineer's degree in computer science.
Contact : Souheib Baarir (souheib.baarir@epita.fr) and Quentin Peyras (quentin.peyras@epita.fr).

1 Context

Business process modeling is a valuable framework that allows companies and organizations to exert greater control over their processes. In the field of process notation, Business Process Model and Notation (BPMN) is among the most popular. Various initiatives have proposed formal semantics for BPMN, including a recent first-order logic formalization presented in [HBP+22]. Using this formalization, it is possible to translate the semantics into a specification language for verification purposes. Verification is important as it enables formal checking of critical properties of BPMN, such as dead transitions (transitions that are never taken), deadlocks (the process is blocked and cannot perform a transition), and livelocks (the process is stuck in a loop preventing it from completing its task). Moreover, time constraints are of utmost importance in BPMN [HBPQ21], and thus, must be taken into account for verification purposes. Therefore, the formalization must include the semantics of time-related constructs, allowing for quantitative verification in addition to qualitative verification. In [HBP+22], the authors encode the resulting semantics in TLA+ [LMTY02], a well-known specification language, and use the TLA+ model-checker, TLC, to verify properties related to BPMN. While this formalization shows promise, it does not cover all aspects of BPMN semantics, such as unbound data, multi-instance constructs or variable duration for tasks, leaving room for future research.

2 Proposed approach

There are several ways to expand the formalization of BPMN. One possibility is to verify BPMN with unbound data, meaning data is initialized with any value. This can be achieved through the use of symbolic verification techniques. Additionally, it is necessary to address multi-instance constructs. This can be accomplished by assigning identifiers to differentiate each instance of processes and activities and by typing these identifiers with the type of their corresponding process or activity. One way to achieve this is by introducing a bag that retains the type of each identifier. Alternatively, sorted first-order logic can be utilized for the formalization of the type system on identifiers. Regarding time constraints, one possibility is to extend the parameterization of the model by allowing variable time durations for tasks or timeouts. This can be achieved by replacing the fixed values for time-constraints with time intervals or variables. Then, the satisfaction of some properties of the

model could depend on the values of these variables. Indentifying such constraints from the model is also an interesting track to follow.

3 Supervision

This PhD will be supervised by Souheib Baarir (HDR) and Quentin Peyras and conducted within the LRE at EPITA Toulouse.

4 Application procedure

Send the following documents to quentin.peyras@epita.fr :

- a CV ;
- a motivation letter ;
- academic transcripts (L3, M1, M2) ;
- a letter of recommandation is preferred.

Références

[HBP+22] Sara Houhou, Souheib Baarir, Pascal Poizat, Philippe Quéinnec, and Laïd Kahloul. A first-order logic verification framework for communication-parametric and time-aware bpmn collaborations. *Information Systems*, 104 :101765, 2022.

[HBPQ21] Sara Houhou, Souheib Baarir, Pascal Poizat, and Philippe Quéinnec. A Direct Formal Semantics for BPMN Time-Related Constructs. In *ENASE 2021 - 16th International Conference on Evaluation of Novel Approaches to Software Engineering*, pages 138–149, online, Czech Republic, April 2021.

[LMTY02] Leslie Lamport, John Matthews, Mark Tuttle, and Yuan Yu. Specifying and verifying systems with tla+. In *Proceedings of the 10th workshop on ACM SIGOPS European workshop*, pages 45–48, 2002.