Automating Correctness Verification of Artifact-Centric Business Process Models*

Diana Borrego, Rafael M. Gasca, and María Teresa Gómez-López

Department of Computer Languages and Systems, University of Seville, Spain
{dianabn,gasca,maytegomez}@us.es
http://www.idea.us.es/

1 Resumen

Traditionally, business processes are modelled as activity-centric business process models in which activities are focused on and data just serve as inputs and outputs of some services. They follow the imperative principles, implying that the workflow of the activities can be defined at design time. But for some types of problems, it is easier to represent how the data are modified during the process execution instead of the activities that execute the data evolution.

For this reason, the artifact-centric methodology (data-centric approach) has emerged as a new paradigm to support business process management, where business artifacts appeared for the necessity of enrich the business process model with information about data providing a way for understanding the interplay between data and process. Artifacts are business-relevant objects that are created, evolved, and (typically) archived as they pass through a business, combining both data aspects and process aspects into a holistic unit.

Artifact-centric modelling establishes data objects (called artifacts) and their lifecycles as focus of the business process modelling. This type of modelling is inherently declarative: the control flow of the business process is not explicitly modelled, but follows from the lifecycles of the artifacts.

The lifecycle represents how the state of an artifact may evolve over the time. The different activities change the state of the artifact and the values of the data associated to each artifact; these may be manual or automatic. The evolution of the artifacts implies a change of the state and the values of the data, until a goal state of an artifact is reached. One of the reasons why the artifact-centric paradigm facilitates the process description is the capacity to model the relations between objects with different cardinalities, not only 1-to-1 relations. This modeling capabilities are not entirely supported in activity-centric scenarios. For instance, BPMN 2.0 (currently wide accepted activity-centric notation) allows to easily represent multi-instance activities and pools (processes), but with some

* Original paper: Automating Correctness Verification of Artifact-Centric Business Process Models. Published in Journal of Information and Software Technology (IF: 1.046, Q2 in two categories). Vol. 62, Issue C, Pages 187-197, June 2015. DOI: 10.1016/j.infsof.2015.02.010

limitations: (i) relations between different processes can only be expressed as hierarchies, where a process can invoke multiple instances of its subprocess; (ii) the return value of an executed sub-process instance is only accessible when its execution finishes, not allowing the interaction of another process during the execution; and (iii) the definition of Data Objects, Data Inputs, Data Outputs, Sets, and Data Associations in BPMN 2.0 allows to specify collections of elements, but it does not permit data instance differentiation or to include the relation between the data objects between them.

When more than one artifact is involved in the process, it is possible that a combination of services and data values violate the policies of the business. In order to avoid this situation at runtime, it is possible to detect some of these possible errors even at design time. Specifically, the errors derived from an incorrect design of the model. In spite of the unknown runtime data in the design time phase, our proposal is able to perform a data verification of the models by means of the use of mandatory domains of values, which can be obtained from previous executions and/or knowledge from experts. Making use of this information, it is possible to determine the existence of certain errors in the structural and data perspectives of the model before it is deployed.

The paper develops a fully automated approach for verifying the correctness of artifact-centric models at design time, including the state relation between the artifacts of the model (handling 1-to-N and N-to-M associations between artifacts), and the data values that define the relations between them. To develop the automatic verification, services are formally modeled using pre and postconditions over the data associated to the artifacts' states. To analyse the correctness of the model, it is necessary to study when the services can be executed. A service can be executed if the evolution of the lifecycle of the artifact arrives at the service and its precondition is satisfied. Upon completion, the service delivers data that satisfies its postconditions. The no satisfiability of a pre or postcondition can cause that the lifecycle gets stuck at a service and fails.

Two correctness notions are distinguished (reachability and weak termination), and novel verification algorithms are developed to check them. In more detail, our proposal consists of various phases: (a) preprocessing is applied to detect basic data anomalies; (b) the artifact union graph is translated into a CSP formulation in order to automatize the verification, avoiding its manual performance which is time-consuming and error-prone; (c) the CSP formulation models the lifecycle of the artifacts with pre and postconditions of the services and the numerical data managed, analysing the possible interaction among the different artifacts; and (d) in case of an error, feedback is provided by determining the states which are nor reachable and/or weak-terminable. The approach is complete, so it always generates accurate feedback in case of an error.

To the best of our knowledge, this paper presented the first verification approach for artifact-centric business process models that integrates pre and postconditions, which define the behavior of the services, and numerical data verification when the model is formed of more than one artifact. The approach can detect errors not detectable with other approaches.