Abstract. Model checking of real-time systems with respect to Duration Calculus (DC) specifications requires the translation of DC formulae into automata-based semantics. This task is difficult to automate. The existing algorithms provide a limited DC coverage and do not support compositional verification. We propose a translation algorithm that advances the applicability of model checking tools to real world applications. Our algorithm significantly extends the subset of DC that can be handled. It decomposes DC specifications into sub-properties that can be verified independently. The decomposition bases on a novel distributive law for DC. We implemented the algorithm as part of our tool chain for the automated verification of systems comprising data, communication, and real-time aspects. Our translation facilitated a successful application of the tool chain on an industrial case study from the European Train Control System (ETCS).

1 Introduction

Verification of embedded hardware and software systems requires reasoning about data, communication, and real-time aspects. Duration Calculus (DC) represents these dimensions in one formalism. As a fundamental concept, it offers the use of data variables with possibly infinite data domains that are interpreted over dense real-time intervals.

To apply the automata theoretic approach of Vardi and Wolper [VW86] for model checking DC, we need to translate DC formulae into automata. This is a difficult task and it has been shown in [ZHS93] that it cannot be solved in general. Translation algorithms into automata-based semantics are known for restricted classes of DC only [Rav94, BLR95, Pan02, Frä04]. But they are not compositional and consider neither infinite data domains nor communication.

We identify a new class of DC formulae, called test formulae, that can be translated into automata, also referred to as test automata in this paper. Test
formulae (1) significantly extend the previously known classes and (2) take communication aspects and infinite data domains into account. Our expressiveness results suggest that the new class is among the richest for which satisfiability with respect to an automaton is decidable under a dense time interpretation.

Translations of DC suffer from an exponential blow up of the resulting automata in the number of operators. To overcome this problem, we provide an algorithm that decomposes a formula into sub-formulae that are translated independently. It allows for an efficient verification as it reduces the size of the automata. The decomposition is realised using a new operator for the DC that permits a distributive law of linear complexity.

We implemented our translation algorithm as part of a tool chain and provide evidence that it can handle industrial problems. We verify the emergency treatment of the European Train Control System (ETCS) [ERT02]. Our approach is the first that permits model checking of a comprehensive ETCS fragment considering communication, data, and real-time. Therefore, we bridge the gap between theoretical results and their practical applications. Due to our model's parameters and infinite data types, we apply the abstraction refinement model checker ARMC [Ryb06].

To summarise our contributions, we identify a novel class of DC formulae and give a translation algorithm into enhanced timed automata [AD94]. Since a direct translation leads to an exponential blow up of the automata, we give a normal form for our novel class to decompose given properties. The normal form is realised using a new distributive law of linear complexity based on a new operator for the DC. We implemented the algorithm and applied our tool chain to verify real-time properties of the ETCS case study.

The paper is organised as follows. After a short introduction to our case study, we recall the DC and the applied automaton model, phase event automata (PEA), in Sect. 2. The class of test formulae, the new operator, and the normal form are presented in Sect. 3. Based upon these results, Sect. 4 gives the test automata semantics and states its correctness. The case study and our model checking results are sketched in Sect. 5. Section 6 reviewing related work and suggesting future investigations, concludes the paper.

1.1 Motivating Example

![Fig. 1. Consecutive trains](image)

The emerging European Train Control System (ETCS) is an international standard [ERT02] that shall replace national train control systems to ensure cross-border interoperability and to improve railway safety as well as track utilisation. In the final ETCS implementation level, the existing national trackside systems for detection of train speed, location, and integrity will not be used anymore. Instead, data values required for a moving train are ascertained in cooperation of the train’s on-board ETCS unit with a radio block centre (RBC) that