Towards an Optimal Generation of Zones Graph Relating Timed Bisimulation Relation and Distribution

Matmat Riadh, MISC Laboratory, Abdelhamid Mehri Constantine 2 University, Constantine, Algeria
Kitoumi Ilham, MISC Laboratory, Abdelhamid Mehri Constantine 2 University, Constantine, Algeria
Saidouni Djamel Eddine, MISC Laboratory, Abdelhamid Mehri Constantine 2 University, Constantine, Algeria

ABSTRACT

The timed automata are extensively used in different fields of formal validation in particular the model checking one. In this paper the authors are interested by a class of TA called durational actions timed automata (daTA) and the zones graph which represents an exact finite state abstraction based on what called Zones. The authors present a novel approach to construct a zone graph, based on the maximality semantics called maximality-based zone graph (MZG) by a local construction approach and they define timed maximality bisimulation relation for real-time model based on the maximality semantics. The authors propose a new method for distributed state space generation of maximality-based zone graph based on DHT structure. They also describe an implementation of this construction (DTaMaZG tool). The experiments given at the end of this article has shown good results especially when comparing with other works that have already proceed in the distributed generation of MLTS (Maximality based Labeled Transition Systems).

KEYWORDS

Distributed Hash Tables, Durational Actions Timed Automata, Maximality Based Zone Graph, Maximality Semantics, Real-time Systems, State Space Explosion, Timed Maximality Bisimulation Relation

INTRODUCTION

The development of critical systems, such as systems whose failure can have catastrophic consequences, requires the use of reliable design methods based on formal approaches. These later allow the precise description of systems and their desired properties, as well as reasoning about them. The systems are modeled in a language with clear mathematically defined syntax and semantics, like logics, automata and process algebra.

In this paper we are interested by a subclass of timed automata model, named timed automata with durational actions (daTA). The daTA model (Belala et al., 2013; Guellati et al., 2014) are a form of timed automata that admit a more natural representation of action durations and advocates carrying true concurrency, which are realistic assumptions for specifying real-time systems. It’s based on maximality semantics.

Indeed, in real world systems, actions are not instantaneous, but have durations. This realistic characteristic is important in many cases in addition to the maximality semantics has been proved necessary and sufficient both for the refinement process and duration of actions (Saidouni & Courtiat, 2003).
One of the most automated tool in formal verification is Model Checking (Holzmann, 1991), where a finite state space of a system is constructed and the desired correctness properties are checked against it. Generation phase consists on exploring all possible reached states from the initial state. Actually, a large part of real-life systems are made up of many interacting components, for which state space can be huge and eventually cannot fit in memory or even be, it will be too large for being explored entirely. This leads to the so called state space explosion problem, which is known to be the most limiting and decreasing factor of this technique.

Several approaches have been developed to cope with this issue, such as symbolic state space encoding using binary decision diagram (BDD) (Drechsler & Becker, 1998; Heyman et al., 2000), other method have taken benefits from some equivalence relations to reduce the state space of the model, like: partial order reduction (Godefroid & Wolper, 1994), bisimulation relation (Blom & Orzan, 2005), alpha-equivalence relation (Bouneb & Saidouni, 2009) and aggregation (Saidouni et al., 2011). As recent researches are based on the use of parallel and distributed computations, many papers presenting distributed model checking algorithms mention the importance of a good state space partitioning method. A good partitioning scheme can efficiently reduce the problem of the combinatorial state space explosion (Garavel et al., 2001; Barnat et al., 2001; Bingham et al., 2010; Voros et al., 2011), all these approaches consist on the use of a cluster or a network of workstations and each machine explores a part of the state space. However, they bear differences on the memory architecture used; either shared or distributed one, the data structure selected to store states, and the way states are distributed over machines of the network.

In this paper, our contributions are of interest for the formal verification domain and more especially for the distributed Model Checking. In its first step, Model Checking consists on generating the full state space: starting from the initial state, computes all its successors, repeats the process for all the newly discovered states until achieving exploration; there is no more state to explore. The fundamental interest of this proposal is the construction of distributed state space in the context of the maximality semantics based on zones using distributed hash tables structure.

We propose a novel approach to construct a zone graph, based on the maximality semantics called Maximality-based Zone Graph (MZG) and we define Timed Maximality Bisimulation Relation (TMBR) for real-time model based on the maximality semantics.

Inspired from the file sharing service in Peer to Peer systems (Saroiun et al., 2002), we propose a new algorithm for distributed state space generation of the Maximality-based Zone Graph using distributed hash table as a data structure for storing the set of states generated locally by the correspondent processor and for performing a quick look-up of states that have already been explored and the more important is to avoid exploring any state more than once.

So that, we aim at better construct the full state space of systems to enhance the problem of combinatorial state space explosion and achieve a good load balancing between processors of the network. Besides, this approach is very interesting for the community of graphs, since it handles the generation of graphs in a distributed environment on the fly while generating it.

An implementation of the proposed algorithms has been done. Furthermore, we illustrate the results by means a case study of Automatic teller machine system.

Paper outlines. Section 2 recalls some basic definitions about durational actions timed automata model. Section 3 proposes the definition of Maximality-based Zone Graph. Section 4 presents and discusses the basic proposed algorithm for the on the fly distributed generation of Maximality-based Zone Graph. In Section 5, we provide our measurements and experimental results. Finally, Section 6 concludes the paper and gives some perspectives.
Programmability and Scalability on Multi-Core Architectures
www.igi-global.com/chapter/programmability-scalability-multi-core-architectures/36412?camid=4v1a

Collaborative Services for Fault Tolerance in Hierarchical Data Grid
www.igi-global.com/article/collaborative-services-for-fault-tolerance-in-hierarchical-data-grid/104761?camid=4v1a