Available online at www.sciencedirect.com
ScienceDirect
Computer Networks 51 (2007) 439–455
Computer Networks
www.elsevier.com/locate/comnet

A template-based approach for the generation of abstractable and reducible models of featured networks

A. Miller *, M. Calder, A.F. Donaldson

Department of Computing Science, University of Glasgow, Glasgow G12 8QQ, Scotland, United Kingdom

Available online 22 September 2006

Responsible Editor: H. Rudin

Abstract

We investigate the relationship between symmetry reduction and inductive reasoning when applied to model checking networks of featured components. Popular reduction techniques for combatting state space explosion in model checking, like abstraction and symmetry reduction, can only be applied effectively when the natural symmetry of a system is not destroyed during specification. We introduce a property which ensures this is preserved, *open symmetry*. We describe a template-based approach for the construction of open symmetric Promela specifications of featured systems. For certain systems (*safely featured parameterised systems*) our generated specifications are suitable for conversion to abstract specifications representing any size of network. This enables feature interaction analysis to be carried out, via model checking and induction, for systems of any number of featured components. In addition, we show how, for *any* balanced network of components, by using a graphical representation of the features and the process communication structure, a group of permutations of the underlying state space of the generated specification can be determined easily. Due to the open symmetry of our Promela specifications, this group of permutations can be used directly for symmetry reduced model checking.

The main contributions of this paper are an automatic method for developing open symmetric specifications which can be used for generic feature interaction analysis, and the novel application of symmetry detection and reduction in the context of model checking featured networks.

We apply our techniques to a well known example of a featured network – an email system.

Keywords: Model checking; Feature interaction; Induction; Abstraction; Symmetry reduction

1. Introduction

Model checking [14,36,38] is a popular automated approach for investigating the behaviour of computer networks. A system is specified using a modelling language, and a state space (or *model*) generated. The state space is explored to check properties that are expected to hold for the original system. In particular, model checking is a useful technique for carrying out *feature interaction* analysis on networks of featured components. However, model checking suffers from the well known state space explosion problem: the size of the state space grows exponentially with the number of components.

* Corresponding author.
E-mail address: alice@dcs.gla.ac.uk (A. Miller).

1389-1286/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2006.08.009

Approaches for combatting state space explosion often involve abstraction to replace sets of states with state representatives. One method, induction, is used to construct an (abstract) state space which encapsulates the behaviour of systems of *any* size. This method is useful for ensuring that properties which hold for small, finite systems, still hold when any number of new components are added to the system. However, if a property does not hold for the abstract state space, no general result can be inferred (and no meaningful counter-example generated).

For large, finite systems, symmetry reduction is an alternative reduction technique which can be used to reduce the size of the state space – sometimes dramatically. Symmetry reduction involves finding a group of permutations of the state space which preserve the property to be checked, and using it to build a (smaller) *quotient* state space. The property will hold for the quotient state space if and only if it holds for the original state space.

In previous work [9,37] we have used an abstraction/induction approach to model and analyse parameterised networks of featured components, for networks of any size. Our approach relies upon restricting the behaviour of the components to be *open symmetric*. Open symmetry requires that for any statement in the specification that refers to a literal component id, all symmetrically equivalent statements are present in the component specification.

We have also developed an approach, for balanced networks of unfeatured components, to detect the symmetry present in a system using a graphical representation of the process communication structure – the *static channel diagram* (*SCD*) [17,19]. The SCD is generated automatically from a Promela specification of the system, and a suitable automorphism group of the state space ($G \subseteq \mathrm{Aut}(\mathscr{M})$) is obtained from the automorphism group of the SCD ($\mathrm{Aut}(SCD)$). Although $\mathrm{Aut}(SCD)$ can be found easily and automatically, some elements of $\mathrm{Aut}(SCD)$ are not *valid*: they do not belong to $\mathrm{Aut}(\mathscr{M})$. Thus it is necessary to remove all invalid elements of $\mathrm{Aut}(SCD)$ to obtain a suitable automorphism group G. This involves checking the validity of the group generators against the Promela specification itself. If the model could be ensured to be open symmetric however, all elements of $\mathrm{Aut}(SCD)$ would be valid with respect to the model, and we would only need to check the validity of the generators against the property to be verified. This would be faster and in many cases would mean that we could use $G = \mathrm{Aut}(SCD)$ directly for symmetry reduced model checking.

While conducting our previous work on abstraction/induction and symmetry detection we have been struck by strong parallels between the approaches used. For example, in both cases the techniques are less effective (or do not apply at all) if components are not open symmetric. We have become increasingly aware that the tools we have developed for constructing models suitable for abstraction/induction, could be used to construct finite models of networks of featured components to which symmetry reduction can be applied.

In this paper we show how, for any *balanced* network of featured components we can use a template-based approach to generate Promela specifications which are, by construction, open symmetric. For *safely featured parameterised systems* the generated specifications are suitable for applying our induction approach.

In addition, we introduce a new graphical representation of the specification – a *feature configuration diagram* (*FCD*) and show that the automorphism group of the FCD induces an automorphism group of the underlying state space, for any balanced system. This allows for immediate application of symmetry reduction methods, without the need to check for symmetry validity. We present a tool – the *featured specification generator* (*FSG*) to implement our approach, and we present experimental results for an email system. This extension of our earlier work is the first time we have applied symmetry detection methods to networks of featured components.

Our methods are illustrated via two example networks: a telephone network, in which all components are of the same type, and an email network in which there are two types of component – client components and a mailer component. However, it is important to point out that our techniques are applicable to networks consisting of multiple component types.

2. Background

2.1. Systems and specifications

Consider a system of communicating components. A specification of the system consists of a set of processes (each describing a component) together with a set of channels. Processes can be separated into different types according to the type of component they represent (e.g., *client* component or *server* component).