Heinrich Heine Universität Düsseldorf

Heinrich-Heine-Universität Düsseldorf 40204 Düsseldorf
Dekanat der Mathematisch-Naturwissenschaftlichen Fakultät

An alle
hauptamtlichen Professoren/innen
und Privatdozenten/innen
des Faches Informatik der
Mathematisch-Naturwissenschaftlichen Fakultät

Mathematisch-Naturwissenschaftliche Fakultät

Dekanat

Promotionsangelegenheiten
Universitätsstraße 1
40225 Düsseldorf
Telefon: +49 (0)211 81 15092
E-Mail: promotionmnf@hhu.de

19.09.2022

Promotionsverfahren von **Herrn M.Sc. Philipp Körner**
Auslage der Dissertation und Gutachten sowie Termin der mündlichen Prüfung
Anlage: Einseitige Zusammenfassung der Dissertation

Sehr geehrte Damen und Herren,

in dem oben genannten Promotionsverfahren wird die Annahme der Dissertation

On Executing State-Based Specifications and Partial Order Reduction for High-Level Formalisms

von den Berichterstattenden Prof. Dr. M. Leuschel und Dr. A. Idani beantragt. Sie kann zusammen mit den Gutachten in der Zeit

vom 24.09.2022 bis 11.10.2022

eingesehen werden. Bitte wenden Sie sich zur Einsicht an das Promotionsbüro (promotionmnf@hhu.de).

Einsprüche gegen diese Dissertation können nur zwei Tage nach der vorgenannten Frist geltend gemacht werden. Erfolgt kein Einspruch, so gilt die Dissertation als angenommen (§ 7 Ziffer (5) PO).

Sofern die Dissertation angenommen wird, findet die mündliche Prüfung am

14.10.2022 um 12:30 Uhr

im **Hörsaal 5B** statt. Als Prüferinnen bzw. Prüfer sind vorgesehen:
Prof. Dr. J. Rothe, Prof. Dr. S. Conrad und Prof. Dr. E. Wanke.

Die Öffentlichkeit ist bei der Befragung zugelassen.

Mit freundlichen Grüßen
im Auftrag

Athina von Essen

On Executing State-Based Specifications and Partial Order Reduction for High-Level Formalisms

Philipp Körner

This thesis is a selection of my co-authored manuscripts on state-based formal methods tools and applications. A focus lies on the B Method and the animator, constraint solver and model checker ProB.

The *first part* explores the opportunities that stem from executing state-based specifications. Three approaches are investigated:

Firstly, *embedding the tool* ProB into Java programs and interacting with it using a high-level API that exposes animation, constraint solving and model checking techniques: This technique enables a variety of applications, and has been successfully utilised in a timetable planning tool and a demonstrator in the railway domain.

Secondly, *treating imperative code* as a specification and attempting verification using the model checker CBMC: While technically feasible, verification *after* implementation comes with a variety of pitfalls and fixing located errors is quite cumbersome at this stage.

Finally, *embedding the B language* into Clojure in order to programmatically generate (parts of) and solve constraints or animate and model check constructed B machines: this approach treats specifications as plain data. Following the ideas of Lisp, this enables tools that analyse and transform specifications as well as the creation of domain-specific languages (DSLs).

The *second part* of this thesis re-visits an implementation of a state space reduction technique, partial order reduction (POR), in ProB. Anecdotally, we had little success with exploiting POR techniques for real-world models. Using a large collection of B machines, we put numbers to our impressions and find that, indeed, in the vast majority of cases, POR does not yield any reduction.

Motivated by a grand challenge we set ourselves, — a model of an interlocking system that *should* be susceptible to POR techniques, yet does not exhibit any reduction — we identify two idioms that hinder POR for higher-level specifications. The first idiom, usage of parameterised operations, often can be eliminated by unrolling a single operation into many, one for each possible parameter value. The second idiom, usage of high-level data structures such as sets or functions, often can be addressed by replacing sets with a bitvector encoding, or using constraint solvers to determine independence of operations.