Enhanced Coinduction
Rot, J.C.

Citation

Version: Not Applicable (or Unknown)
License: Leiden University Non-exclusive license
Downloaded from: https://hdl.handle.net/1887/35814

Note: To cite this publication please use the final published version (if applicable).
Curriculum vitae

- Born in Amsterdam 1987
- High school 1999 – 2005
  Atheneum College Hageveld, Heemstede
- BSc Computer Science 2007 – 2010
  Leiden University
- MSc Computer Science (cum laude) 2010 – 2011
  Leiden University
- PhD student 2012 – 2015
  Leiden University
- Post-doctoral researcher 2015 – …
  Laboratoire de l’Informatique du Parallélisme (LIP), ENS Lyon
Acknowledgements

In the last years I had the pleasure of learning and researching in an inspiring, exciting and very friendly environment. I am grateful to many people for being a part of this; in particular Henning Basold, Stijn de Gouw, Jan van Rijn and Jonathan Vis. I want to thank Marcello Bonsangue, Frank de Boer and Jan Rutten for getting (and keeping) me excited about research and for their kindness. This thesis has been improved based on detailed comments on previous versions, by Bart Jacobs, Helle Hansen and Henning Basold. In the last years I have worked together with many people, which, for me, has always been one of the best parts of doing research. I am convinced this is the case because I have had the chance of working with excellent people. I want to single out Bartek Klin, who hosted me during an inspiring research period in Warsaw.

I am grateful to my family—in the first place for their support and care. To Job, for sharing his brilliant thoughts and listening carefully. Finally I thank Hanna, for supporting me in every possible way, and reminding me of what is valuable in life.
Coinductie, de duale van inductie, is een fundamenteel principe voor het definiëren van oneindige objecten, en het bewijzen van eigenschappen van zulke objecten. Het belangrijkste voorbeeld van coinductie in de informatica is bisimulatie, een algemene karakterisatie van equivalentie tussen systemen met oneindig of circulair gedrag, met een concrete bewijsmethode. Coinductieve technieken verschaffen nuttige bewijsprincipes voor verschillende onderzoeksgebieden zoals de theorie van concurrency, de studie van oneindige datastructuren en de automaten-theorie.

De brede toepasbaarheid en toenemende interesse in coinductieve technieken zijn gebaseerd op de theorie van coalgebra’s. Dit is een wiskunde-theorie waarin we eigenschappen van toestandsgebaseerde modellen van berekening kunnen begrijpen en bewijzen op een hoog abstractieniveau, en deze eigenschappen vervolgens toepassen op concrete systemen. De theorie van coalgebra’s geeft een structureel en algemeen perspectief op bisimulatie en coinductie, met een canonieke karakterisatie van equivalentie en bijbehorende bewijsprincipes.

In dit proefschrift ontwikkelen we technieken die coinductief redeneren vereenvoudigen en verbeteren. We gebruiken hiervoor de theorie van coalgebra’s, om algemeen toepasbare methoden te verkrijgen. In het eerste deel van het proefschrift introduceren we verbeteringen van coinductieve bewijsprincipes, en in het tweede gedeelte van coinductieve definitieprincipes.

We introduceren een coalgebraïsche theorie van verbeterde bewijstechnieken voor bisimilariteit, in Hoofdstuk 4. Onze theorie generaliseert de zogeheten up-to-technieken, die geïntroduceerd zijn door Milner en Sangorgi om het redeneren over processen te vereenvoudigen, van processen naar een breed scala aan toestandsgebaseerde systemen, zoals (niet)deterministische automaten, systemen die oneindige rijtjes representeren en transitiesystemen met kwantitatieve informatie. In Hoofdstuk 2 passen we deze technieken toe om te redeneren over formele talen. In Hoofdstuk 5 worden onze bewijsprincipes verder gegeneraliseerd, op basis van een algemeen perspectief op coinductieve predicaten, zoals geïntroduceerd door Hermida en Jacobs. Met deze generalisatie verkrijgen we verbeterde bewijsprincipes voor willekeurige coinductieve predicaten, wat we toepassen om nieuwe methoden te verkrijgen voor het redeneren over simulatie van transitiesystemen, taal inclusie van automaten met kwantitatieve informatie, en divergentie van processen.

Coinductieve definitietechieken zijn geschikt voor het definiëren en bestuderen van de semantiek van talen. Turi en Plotkin hebben getoond dat men een
compositional semantics can be obtained through the interaction between syntax (modeled by algebra's) and observations (modeled by coalgebra's) to be specified by means of a so-called distributive law. In Chapter 6, we see how such distributive laws can be integrated with recursive equations, so as to simplify the specification of languages. The most important result from this chapter is that the interpretation of a specification, which can contain recursive equations of a certain form, is compositional, and that the proof principles from previous chapters can be used.

Distributive laws can be useful to study coinductive defined languages, but they are sometimes difficult to describe. In Chapter 7, we show how distributive laws can be presented as quotient of other distributive laws, which are easy to present using existing techniques. We apply our technique to derive simple distributive laws for the semantics of operations on infinite sequences and context-free grammars.
Titles in the IPA Dissertation Series since 2009


M. de Mol. *Reasoning about Functional Programs: Sparkle, a proof assistant for Clean*. Faculty of Science, Mathematics and Computer Science, RU. 2009-02


M.J. van Weerdenburg. *Efficient Rewriting Techniques*. Faculty of Mathematics and Computer Science, TU/e. 2009-06


J.A.G.M. van den Berg. *Reasoning about Java programs in PVS using JML*. Faculty of Science, Mathematics and Computer Science, RU. 2009-11


M.R. Czenko. *TuLiP - Reshaping Trust Management*. Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2009-16

T. Chen. *Clocks, Dice and Processes*. Faculty of Sciences, Division of Mathematics and Computer Science, VUA. 2009-17

R.S.S. O’Connor. Incompleteness & Completeness: Formalizing Logic and Analysis in Type Theory. Faculty of Science, Mathematics and Computer Science, RU. 2009-19

B. Ploeger. Improved Verification Methods for Concurrent Systems. Faculty of Mathematics and Computer Science, TU/e. 2009-20

T. Han. Diagnosis, Synthesis and Analysis of Probabilistic Models. Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2009-21

R. Li. Mixed-Integer Evolution Strategies for Parameter Optimization and Their Applications to Medical Image Analysis. Faculty of Mathematics and Natural Sciences, UL. 2009-22

J.H.P. Kwisthout. The Computational Complexity of Probabilistic Networks. Faculty of Science, UU. 2009-23

T.K. Cocx. Algorithmic Tools for Data-Oriented Law Enforcement. Faculty of Mathematics and Natural Sciences, UL. 2009-24

A.I. Baars. Embedded Compilers. Faculty of Science, UU. 2009-25

M.A.C. Dekker. Flexible Access Control for Dynamic Collaborative Environments. Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2009-26


C.J. Boogerd. Focusing Automatic Code Inspections. Faculty of Electrical Engineering, Mathematics, and Computer Science, TUD. 2010-01

M.R. Neuhäußer. Model Checking Nondeterministic and Randomly Timed Systems. Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2010-02

J. Endrullis. Termination and Productivity. Faculty of Sciences, Division of Mathematics and Computer Science, VU. 2010-03

T. Staijen. Graph-Based Specification and Verification for Aspect-Oriented Languages. Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2010-04

Y. Wang. Epistemic Modelling and Protocol Dynamics. Faculty of Science, UvA. 2010-05

J.K. Berendsen. Abstraction, Prices and Probability in Model Checking Timed Automata. Faculty of Science, Mathematics and Computer Science, RU. 2010-06

A. Nugroho. The Effects of UML Modelling on the Quality of Software. Faculty of Mathematics and Natural Sciences, UL. 2010-07

A. Silva. Kleene Coalgebra. Faculty of Science, Mathematics and Computer Science, RU. 2010-08

J.S. de Bruin. Service-Oriented Discovery of Knowledge - Foundations, Implementations and Applications. Faculty of Mathematics and Natural Sciences, UL. 2010-09

D. Costa. Formal Models for Component Connectors. Faculty of Sciences, Division of Mathematics and Computer Science, VUA. 2010-10

M.M. Jaghoori. Time at Your Service: Schedulability Analysis of Real-Time and Distributed Services. Faculty
of Mathematics and Natural Sciences, UL. 2010-11

R. Bakhshi. **Gossiping Models: Formal Analysis of Epidemic Protocols.** Faculty of Sciences, Department of Computer Science, VUA. 2011-01

B.J. Arnoldus. **An Illumination of the Template Enigma: Software Code Generation with Templates.** Faculty of Mathematics and Computer Science, TU/e. 2011-02

E. Zambon. **Towards Optimal IT Availability Planning: Methods and Tools.** Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2011-03

L. Astefanoaei. **An Executable Theory of Multi-Agent Systems Refinement.** Faculty of Mathematics and Natural Sciences, UL. 2011-04

J. Proença. **Synchronous coordination of distributed components.** Faculty of Mathematics and Natural Sciences, UL. 2011-05

A. Moralı. **IT Architecture-Based Confidentiality Risk Assessment in Networks of Organizations.** Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2011-06

M. van der Bijl. **On changing models in Model-Based Testing.** Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2011-07

C. Krause. **Reconfigurable Component Connectors.** Faculty of Mathematics and Natural Sciences, UL. 2011-08

M.E. Andrés. **Quantitative Analysis of Information Leakage in Probabilistic and Nondeterministic Systems.** Faculty of Science, Mathematics and Computer Science, RU. 2011-09

M. Atif. **Formal Modeling and Verification of Distributed Failure Detectors.** Faculty of Mathematics and Computer Science, TU/e. 2011-10

P.J.A. van Tilburg. **From Computability to Executability – A process-theoretic view on automata theory.** Faculty of Mathematics and Computer Science, TU/e. 2011-11

Z. Protic. **Configuration management for models: Generic methods for model comparison and model co-evolution.** Faculty of Mathematics and Computer Science, TU/e. 2011-12

S. Georgievska. **Probability and Hiding in Concurrent Processes.** Faculty of Mathematics and Computer Science, TU/e. 2011-13

S. Malakuti. **Event Composition Model: Achieving Naturalness in Runtime Enforcement.** Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2011-14

M. Raffelsieper. **Cell Libraries and Verification.** Faculty of Mathematics and Computer Science, TU/e. 2011-15

C.P. Tsirogiannis. **Analysis of Flow and Visibility on Triangulated Terrains.** Faculty of Mathematics and Computer Science, TU/e. 2011-16

Y.-J. Moon. **Stochastic Models for Quality of Service of Component Connectors.** Faculty of Mathematics and Natural Sciences, UL. 2011-17

R. Middelkoop. **Capturing and Exploiting Abstract Views of States in OO Verification.** Faculty of Mathematics and Computer Science, TU/e. 2011-18

M.F. van Amstel. **Assessing and Improving the Quality of Model Transformations.** Faculty of Mathematics and Computer Science, TU/e. 2011-19

H.J.S. Basten. *Ambiguity Detection for Programming Language Grammars*. Faculty of Science, UvA. 2011-21

M. Izadi. *Model Checking of Component Connectors*. Faculty of Mathematics and Natural Sciences, UL. 2011-22

L.C.L. Kats. *Building Blocks for Language Workbenches*. Faculty of Electrical Engineering, Mathematics, and Computer Science, TUD. 2011-23

S. Kemper. *Modelling and Analysis of Real-Time Coordination Patterns*. Faculty of Mathematics and Natural Sciences, UL. 2011-24


A. Middelkoop. *Inference of Program Properties with Attribute Grammars, Revisited*. Faculty of Science, UU. 2012-02


F. Heidarian Dehkordi. *Studies on Verification of Wireless Sensor Networks and Abstraction Learning for System Inference*. Faculty of Science, Mathematics and Computer Science, RU. 2012-06


H. Rahmani. *Analysis of Protein-Protein Interaction Networks by Means of Annotated Graph Mining Algorithms*. Faculty of Mathematics and Natural Sciences, UL. 2012-09


L.J.P. Engelen. *From Napkin Sketches to Reliable Software*. Faculty of Mathematics and Computer Science, TU/e. 2012-11

F.P.M. Stappers. *Bridging Formal Models – An Engineering Perspective*. Faculty of Mathematics and Computer Science, TU/e. 2012-12

W. Heijstek. *Software Architecture Design in Global and Model-Centric Software Development*. Faculty of Mathematics and Natural Sciences, UL. 2012-13

C. Kop. *Higher Order Termination*. Faculty of Sciences, Department of Computer Science, VUA. 2012-14
A. Osaiweran. Formal Development of Control Software in the Medical Systems Domain. Faculty of Mathematics and Computer Science, TU/e. 2012-15

W. Kuijper. Compositional Synthesis of Safety Controllers. Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2012-16


B. Lijnse. TOP to the Rescue – Task-Oriented Programming for Incident Response Applications. Faculty of Science, Mathematics and Computer Science, RU. 2013-04

G.T. de Koning Gans. Outsmarting Smart Cards. Faculty of Science, Mathematics and Computer Science, RU. 2013-05

M.S. Greiler. Test Suite Comprehension for Modular and Dynamic Systems. Faculty of Electrical Engineering, Mathematics, and Computer Science, TUD. 2013-06

L.E. Mamane. Interactive mathematical documents: creation and presentation. Faculty of Science, Mathematics and Computer Science, RU. 2013-07

M.M.H.P. van den Heuvel. Composition and synchronization of real-time components upon one processor. Faculty of Mathematics and Computer Science, TU/e. 2013-08


M.J.M. Roeloffzen. Kinetic Data Structures in the Black-Box Model. Faculty of Mathematics and Computer Science, TU/e. 2013-14


C. de Gouw. Combining Monitoring with Run-time Assertion Checking. Fac-
ulty of Mathematics and Natural Sciences, UL. 2013-17

J. van den Bos. *Gathering Evidence: Model-Driven Software Engineering in Automated Digital Forensics.* Faculty of Science, UvA. 2014-01


T.M. Ngo. *Qualitative and Quantitative Information Flow Analysis for Multi-threaded Programs.* Faculty of Electrical Engineering, Mathematics and Computer Science, UT. 2014-05

A.W. Laarman. *Scalable Multi-Core Model Checking.* Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2014-06

J. Winter. *Coalgebraic Characterizations of Automata-Theoretic Classes.* Faculty of Science, Mathematics and Computer Science, RU. 2014-07

W. Meulemans. *Similarity Measures and Algorithms for Cartographic Schematization.* Faculty of Mathematics and Computer Science, TU/e. 2014-08

A.F.E. Belinfante. *JTorX: Exploring Model-Based Testing.* Faculty of Electrical Engineering, Mathematics & Computer Science, UT. 2014-09

A.P. van der Meer. *Domain Specific Languages and their Type Systems.* Faculty of Mathematics and Computer Science, TU/e. 2014-10

B.N. Vasilescu. *Social Aspects of Collaboration in Online Software Communities.* Faculty of Mathematics and Computer Science, TU/e. 2014-11

F.D. Aarts. *Tomte: Bridging the Gap between Active Learning and Real-World Systems.* Faculty of Science, Mathematics and Computer Science, RU. 2014-12


M. Helvensteijn. *Abstract Delta Modeling: Software Product Lines and Beyond.* Faculty of Mathematics and Natural Sciences, UL. 2014-14

P. Vullers. *Efficient Implementations of Attribute-based Credentials on Smart Cards.* Faculty of Science, Mathematics and Computer Science, RU. 2014-15

F.W. Takes. *Algorithms for Analyzing and Mining Real-World Graphs.* Faculty of Mathematics and Natural Sciences, UL. 2014-16

M.P. Schraagen. *Aspects of Record Linkage.* Faculty of Mathematics and Natural Sciences, UL. 2014-17

G. Alpár. *Attribute-Based Identity Management: Bridging the Cryptographic Design of ABCs with the Real World.* Faculty of Science, Mathematics and Computer Science, RU. 2015-01
A.J. van der Ploeg.  *Efficient Abstractions for Visualization and Interaction.* Faculty of Science, UvA. 2015-02

R.J.M. Theunissen.  *Supervisory Control in Health Care Systems.* Faculty of Mechanical Engineering, TU/e. 2015-03

T.V. Bui.  *A Software Architecture for Body Area Sensor Networks: Flexibility and Trustworthiness.* Faculty of Mathematics and Computer Science, TU/e. 2015-04

A. Guzzi.  *Supporting Developers’ Teamwork from within the IDE.* Faculty of Electrical Engineering, Mathematics, and Computer Science, TUD. 2015-05


S. Dietzel.  *Resilient In-network Aggregation for Vehicular Networks.* Faculty of Electrical Engineering, Mathematics and Computer Science, UT. 2015-07

E. Costante.  *Privacy throughout the Data Cycle.* Faculty of Mathematics and Computer Science, TU/e. 2015-08

S. Cranen.  *Getting the point — Obtaining and understanding fixpoints in model checking.* Faculty of Mathematics and Computer Science, TU/e. 2015-09

R. Verdult.  *The (in)security of proprietary cryptography.* Faculty of Science, Mathematics and Computer Science, RU. 2015-10

J.E.J. de Ruiter.  *Lessons learned in the analysis of the EMV and TLS security protocols.* Faculty of Science, Mathematics and Computer Science, RU. 2015-11


S. Picek.  *Applications of Evolutionary Computation to Cryptology.* Faculty of Science, Mathematics and Computer Science, RU. 2015-14


J.C. Rot.  *Enhanced coinduction.* Faculty of Mathematics and Natural Sciences, UL. 2015-18