Towards Model-Based Engineering: A Constraint-Based Approach

Dissertation
zur Erlangung des Doktorgrades
am Department Informatik der Universität Hamburg

vorgelegt von

Rüdiger Lunde

aus Buxtehude

Hamburg 2006

Genehmigt vom Department Informatik der Universität Hamburg

auf Antrag von	Prof. Dr. Bernd Neumann
und	Prof. Dr.-Ing. Wolfgang Menzel

Hamburg, den 31. Mai 2006

Prof. Dr. Winfried Lamersdorf
Leiter Department Informatik

Berichte aus der Informatik

Rüdiger Lunde

Towards Model-Based Engineering: A Constraint-Based Approach

Shaker Verlag
Aachen 2006

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the internet at http://dnb.ddb.de.

Zugl.: Hamburg, Univ., Diss., 2006

Printed in Germany.

ISBN-10: 3-8322-5279-7
ISBN-13: 978-3-8322-5279-3
ISSN 0945-0807

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen
Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9
Internet: www.shaker.de • e-mail: info@shaker.de

Zusammenfassung

Formalisierte Modelle haben heute ihren Weg in fast alle Phasen des Konstruktionsprozesses technischer Systeme gefunden. Beginnend mit der breiten Einführung von CAD-Programmen haben modellbasierte Entwicklungswerkzeuge die Arbeit von Ingenieuren revolutioniert. Doch obwohl modellbasierte Techniken zur Bewältigung einer Fülle von Aufgaben eingesetzt werden, ist die Wiederverwendbarkeit von Modellen wegen existierender Beschränkungen und Barrieren auf der Repräsentations- und Berechnungsebene immer noch sehr eingeschränkt. Folglich bedarf die Modellerzeugung in hohem Maß manueller Eingriffe, was zunehmend die Arbeitszeit von Ingenieuren verschlingt und fehleranfällig ist.

In dieser Arbeit wird die Eignung von Techniken aus dem Forschungsgebiet der modellbasierten Diagnose zur Unterstützung des Konstruktionsprozesses untersucht. Ziel ist es, die prozessübergreifende Wiederverwendbarkeit von Modellen und Analyseverfahren zu verbessern, wobei zwei spezielle Phasen im Mittelpunkt des Interesses stehen: Zuverlässigkeitsanalyse und Diagnose. Es wird ein constraintbasierter Ansatz vorgestellt, der stark von der klassischen General Diagnostic Engine (GDE) inspiriert wurde.

Die diskutierten Erweiterungen und Varianten werden durch die speziellen Anforderungen aus dem gewählten Anwendungsbereich motiviert. So erlaubt es die Kombination von lokalen Konsistenztechniken mit Intervallarithmetik, Wertebereichsteilungsverfahren und Netzwerkzerlegung, die Vollständigkeit des Schlussfolgerungsverfahrens zu verbessern. Der vorgestellte Constraint-Löser erweitert den aus dem Bereich kontinuierlicher Constrainterfüllungsprobleme (CSP) bekannten Branch&Prune-Algorithmus um einen Netzwerkzerlegungsschritt und eine einfache ATMS-Schnittstelle. Für zwei praktisch relevante Klassen von Netzwerkzerlegungen, nämlich ‘unabhängig lösbare Zerlegungen’ und ‘sequentiell lösbare Zerlegungen’, wird die Korrektheit des Lösungsalgorithmus bewiesen. Darüber hinaus werden effiziente Verfahren zur Berechnung solcher Zerlegungen im Detail diskutiert. Zur Verbesserung der Effizienz der Abhängigkeitsverfolgung wird ein Austausch des ATMS durch eine neue Komponente vorgeschlagen, den so genannten ‘Value Manager’. Im Gegensatz zu konventionellen Reason Maintenance Systemen steuert der Value Manager durch den Einsatz von Datenreduktionstechniken aktiv den Ressourcenverbrauch. Außerdem kommen leistungsfähige Fokussierungsverfahren und Datenpufferung zum Einsatz.

Die Anwendbarkeit der vorgestellten Konzepte auf typische Problemstellungen aus Automobilbau und Luftfahrt wird mit Hilfe von Experimenten, basierend auf einer Referenzimplementierung, nachgewiesen. Die dokumentierten Resultate unterstreichen die Effizienz der vorgestellten Algorithmen, insbesondere im Hinblick auf hybride Constraint-Netzwerke, die sowohl kontinuierliche als auch diskrete Wertebereiche enthalten.

Abstract

By now, formalized models have found their way into almost every step of the engineering process. Model-based development tools have revolutionized engineer's work, beginning with the introduction of CAD systems. But although model-based techniques are used for a multiplicity of engineering tasks, the reuse of models is still very limited due to barriers on representational or computational levels. As a consequence, model generation is still a predominantly manual task and hence tends to be error-prone and time-consuming.

This thesis studies the applicability of techniques from the field of model-based diagnosis to support the engineering process with a focus on the reuse of models in two phases: reliability analysis and diagnosis. A constraint-based approach is presented, which is strongly inspired by the general diagnostic engine.

To cope with the specific requirements of the chosen application focus, several extensions and modifications are discussed. Inference completeness is improved by combining local consistency techniques with interval arithmetics, domain splitting and network decomposition. A new constraint solver is presented which extends the branch&prune algorithm known from continuous constraint satisfaction problem solving by a network decomposition step and a simple ATMS interface. Two classes of decompositions, namely 'independently solvable decompositions' and 'sequentially solvable decompositions', are defined and the correctness of the solver with respect to them is proven. Efficient algorithms to compute such decompositions are discussed in detail. Dependency tracking efficiency is improved by replacing the ATMS by a new component which we call 'value manager'. In contrast to classical reason maintenance systems, the value manager actively controls resource consumption by applying data reduction techniques. Additionally, it incorporates strong focusing and data buffering.

The applicability of the concepts to typical engineering problems from the automotive and the aviation domains is shown by experiments based on a reference implementation. The presented results emphasize the efficiency of the discussed algorithms, especially with respect to hybrid constraint networks comprising discrete as well as continuous variable domains.

Acknowledgements

First of all, I thank Prof. Dr. Bernd Neumann for his guidance throughout the three years of this PhD project. His valuable comments helped me to focus on important aspects during the different phases. I especially liked his compact way of writing emails.

I also thank my colleagues from ROSE and Sörman for the good working atmosphere and inspiring discussions. Among them, I especially thank Dr. Georg Strobl for his support and encouragement, Frank Seifart for proof-reading and a lot of interesting questions, and Klaus Thorwart for his remarks on network decomposition. The work was partly funded by R.O.S.E. Informatik GmbH and Sörman Information & Media AB, and I am really grateful for the permission to publish these results.

A special thanks goes to my friend Wolfgang Jekeli. During the final phase of the thesis, he provided many helpful comments and suggestions for improvements. Most of all, I thank my wife Prof. Dr. Karin Lunde. Without her understanding, patience, and encouragement, this work would not have been possible. Besides her considerable indirect support, she also directly contributed to this thesis by improving my English writing.

Finally, I wish to thank my parents Sigrid and Friedrich Lunde for their love and support. In gratitude and with joy I dedicate this thesis to them.

Contents

1 Introduction **1**

1.1 The Vision of Model-Based Engineering . . . 1
1.2 Two Applications . . . 4
1.2.1 Diagnosis of an Automotive Electrical System . . . 4
1.2.2 Reliability Analysis of a Fly-by-Wire System . . . 6
1.3 A Constraint-Based Approach . . . 8
1.4 The Reasoning Framework . . . 10
1.5 The Aim of This Thesis . . . 11

2 Basic Definitions and Concepts **13**

2.1 Interval Propagation Based Constraint Solving . . . 13
2.1.1 Constraint Networks . . . 13
2.1.2 Constraint Solving . . . 14
2.1.3 Local Propagation . . . 16
2.1.4 Interval Arithmetic . . . 18
2.2 Reason Maintenance Systems . . . 20

3 Integrating Domain Splitting and Network Decomposition **22**

3.1 The Branch&Prune Algorithm . . . 23
3.1.1 Basic Properties of the Algorithm . . . 24
3.1.2 Improving Efficiency by Network Decomposition . . . 26
3.2 Graph Notions . . . 27
3.3 Network Decomposition Based on Independent Solvability . . . 29
3.3.1 Independently Solvable Decompositions . . . 29
3.3.2 Production Rules for Independently Solvable Decompositions . . . 33
3.3.3 Implementation Issues . . . 36
3.4 Network Decomposition Based on Sequential Solvability . . . 37
3.4.1 Sequentially Solvable Decompositions and Related Classes of Decompositions . . . 38
3.4.2 Production Rules for Generating Sequentially Solvable Decompositions 48
3.4.3 Strategies for Generating Sequentially Solvable Decompositions . . . 55
3.4.4 Implementation Issues . . . 59
3.5 Controlling Domain Splitting . . . 62
3.6 Relaxing the Requirements for Domain Reduction Accuracy . . . 65
3.6.1 Focusing on Variables of Interest . . . 65
3.6.2 Pragmatic Abortion Criteria . . . 73
3.7 An ATMS Interface . . . 74

4 The Value Manager Architecture 78
4.1 Dependency Tracking by Means of a RMS . . . 78
4.2 Aspects of Efficiency with Respect to Numeric Constraint Problems . . . 79
4.2.1 Storage Consumption . . . 79
4.2.2 Label Completeness . . . 81
4.3 Key Concepts of the Value Manager Architecture . . . 83
4.3.1 Consequences on the Value Manager's View of Data . . . 84
4.3.2 Consequences on Label Completeness . . . 85
4.3.3 Consequences on the Communication Interface . . . 85
4.4 Services Provided by the Value Manager . . . 86
4.4.1 Focusing and Data Reduction Strategies . . . 87
4.4.2 Supporting Inference Selection . . . 90
4.4.3 Disjunction Handling . . . 92
4.4.4 Supporting Parallel Computing . . . 94
4.5 Implementation Issues . . . 94
4.5.1 Classes and Responsibilities . . . 94
4.5.2 Communication between Value Manager and Problem Solver . . . 96
4.5.3 Efficiency Issues . . . 96

5 Experimental Results 99
5.1 Diagnosing an Automotive Electrical System . . . 100
5.1.1 Experiment: Impact of the Decomposition Strategy on Performance . . 100
5.1.2 Experiment: Impact of the Split Variable Selection on Performance . . 104
5.2 Generating an FMEA for an Automotive Electrical System . . . 104
5.2.1 Experiment: Impact of the Value Manager on Simulation Performance . 105
5.2.2 Experiment: Data Reduction within the Value Manager . . . 106
5.2.3 Experiment: Impact of Variables of Interest on Simulation Performance 107
5.3 Analyzing the Reliability of a Fly-by-Wire-System . . . 108
5.3.1 Experiment: Impact of the Dependency Tracking on Simulation Performance . . . 109
5.3.2 Experiment: Influence of Conflict Handling on Search Space Reduction 109

6 Conclusion 111

References 115