Forschungsvorhaben mit Zeitplan für den Auslandsaufenthalt

Gerald Lüttgen*

07. Dezember 1994

1 Persönliche Schwerpunkte im Fach Informatik

Mein Forschungsschwerpunkt ist die formale *Analyse und Verifikation verteilter Systeme* mit Hilfe algebraischer, modallogischer und semantischer Methoden. Insbesondere habe ich in den Spezialgebieten *Prozeßkalküle*, *Modallogiken und Model Checking*, *Datenflußanalyse* und *formale und abstrakte Semantiken für Programmiersprachen* während meines Studiums theoretische und praktische Kenntnissse erworben. Tatsächlich fließen Ergebnisse aus allen genannten Gebieten in meine Diplomarbeit *"Kompositionelle Minimierung endlicher verteilter Systeme"* ein.

Im Rahmen meines Dissertationsvorhabens bei Herrn Prof. Steffen an der Universität Passau möchte ich untersuchen, inwieweit sich die Ergebnisse meiner Diplomarbeit auf Systeme mit *Prioritäten, stochastischem Verhalten* und *Realzeitaspekten* ausdehnen lassen. Dabei spielt neben der *Absraktion* als technisches Hilfsmittel bei der Modellierung von Systemen vor allem die oft unerläßliche Benutzerinteraktion eine wichtige Rolle, welche intuitiv sein soll und kein Detailwissen zugrundeliegender Techniken erfordern darf.

Meine Dissertation steckt in den Anfängen, so daß ich mich momentan in der Phase der Literaturrecherche befinde. Die Vielfalt der Veröffentlichungen über Erweiterungen der Standardmodellierungen verteilter Systeme erfordern eine sorgfältige Analyse, um festzustellen, ob sie für meine Zwecke geeignet sind.

Mein geplanter einjähriger Auslandsaufenthalt vom 01.04.95 bis zum 31.03.96 bei Herrn Prof. Rance Cleaveland an der North Carolina State University, USA, ist für meine Dissertation von zentraler Bedeutung. Herr Prof. Cleaveland ist einer der führenden Experten auf den für meine Dissertation bedeutsamen Spezialgebieten. Seine Expertise kann mir helfen, die bei meiner Literaturrecherche gewonnen Erkenntnisse von einer anderen Perspektive zu beleuchten, als dies hier an der Universität Passau möglich ist. Während in Passau die Prinzipien *Einfachheit* und *Kompositionalität* bei der Modellierung realer Systeme im Vordergrund stehen, werden an der North Carolina State University komplexe Techniken zur Behandlung realer Systeme untersucht. Diese beiden Sichtweisen sollen mir ermöglichen, meine Dissertation zu beschleunigen und wesentliche Teile während meines Aufenthalts anzufertigen.

*Adresse: Brixener Str. 30, 94036 Passau; Antrag: Doktorandenstipendium HSP II/AUFE

2 Themengebiet meiner Dissertation

Thema meiner Dissertation ist die adäquate Modellierung realer verteilter Systeme im Hinblick auf eine anschließende *(semi-) automatische Analyse* oder *Verifikation*. Im speziellen sollen Systeme mit Prioritäten, stochastischem Verhalten und Realzeitaspekten berücksichtigt werden.

Reale Systeme sind zu komplex, um sie mit Hilfe der vielfältig entwickelten Analyse- und Verifikationsmethoden untersuchen zu können. Obwohl viele Methoden den Gedanken der *Kompositionalität* aufgreifen, der es erlaubt, globale Systeme nur lokal betrachten zu müssen, sind sie dennoch meist für den Benutzer unverständlich. Um deren Handhabbarkeit in den Griff zu bekommen, müssen daher folgende Aspekte im Vordergrund stehen: *Abstraktion* und *Interaktion*.

Dabei ist nicht zu erwarten, daß die resultierenden Techniken und Methoden universell sind, sondern daß verschiedene Klassen von Systemen nur mit jeweils speziellen Techniken adäquat behandelt werden können. Insbesondere ist die Abstraktion ein sehr technisches Hilfsmittel, welches ein System aus der Benutzersicht nicht notwendigerweise vereinfacht. Trotzdem ist sie ein notwendiges Hilfsmittel, um die im vollen Kontext üblicherweise unentscheidbaren Problematiken auf ein entscheidbares oder besser sogar automatischen Methoden zugängliches *Abstraktionsniveau* zu reduzieren. Zwar erlauben derartige Abstraktionen keine vollständige, alle Aspekte erfassende Verifikation, sondern nur partielle oder approximative Aussagen. Trotzdem hat sich diese Technik als sehr vielversprechend gerade bei der Verifikation spezieller sicherheitskritischer Aspekte erwiesen. Diese Einschätzung wird um so treffender, je polymorpher die Systeme sind. Insbesondere gilt dies also für die in meinen Betrachtungen im Mittelpunkt stehenden Systeme mit Prioritäten, stochastischem Verhalten und Realzeitkomponenten. Doch gerade für den Benutzer ist es wichtig, daß ein Modell so einfach ist, daß er es versteht. Schließlich ist bekannt, daß Analyse- und Verifikationswerkzeuge im allgemeinen nicht ohne Benutzerinteraktion auskommen, da sich relevante Probleme oft nicht bis auf ein automatisch verifizierbares Maß abstrahieren lassen. Hier gilt es, Methoden für eine komfortable und intuitive Interaktion zu entwickeln, die eine Verifikation ohne Detailwissen über die dem Verifikationswerkzeug zugrundeliegenden Strategien ermöglichen.

Die Aspekte *Einfachheit* und *Benutzerinteraktion* sind bereits in meiner Diplomarbeit *"Kompositionelle Minimierung endlicher verteilter Systeme"* in einem eingegrenzten Szenario untersucht worden. Sie sollen jetzt systematisch auf die beschriebene allgemeinere, praxisrelevantere Situation ausgedehnt werden. Dazu sollen folgende Theorien und Methoden geeignet adaptiert werden:

- Prozeßkalküle mit Prioritäten, Wahrscheinlichkeiten und Realzeitaspekten
- Modularisierung von Systemen unter Verwendung objektorientierter Mechanismen
- Verhaltensbasierte Verifikationsmethoden basierend auf Quasiordnungen und Modallogiken (Model Checking)
- Abstrakte Interpretation als technisches Hilfsmittel bei der Modellierung von Systemen

3 Aufenthalt an der North Carolina State University

Der Aufenthalt an der North Carolina State University soll mir ermöglichen, meine Forschungen auf dem Themengebiet meiner Dissertation unter der Expertise von Herrn Prof. Cleaveland und seinen Mitarbeitern effizient voranzutreiben. Für mein Forschungsvorhaben habe ich mir bereits in Absprache mit Herrn Prof. Cleaveland und Herrn Prof. Steffen ein festes Zeitschema vorgenommen, welches die Forschungsziele quartalsweise absteckt.

Die Komplexität der Fragestellung macht zunächst weitgehende Literaturrecherchen notwendig, um die zahlreichen Artikel über Erweiterungen der Standardmodellierungen verteilter Systeme bzgl. Prioritäten, stochastischem Verhalten und Realzeitaspekten auszuwerten und auf ihre Tauglichkeit für das Promotionsvorhaben hin zu untersuchen. Diese Phase, in der ich mich bereits befinde, werde ich bis zum Antritt meines Besuchs an der North Carolina State University abschließen. Desweiteren stelle ich gerade zusammen mit Herrn Prof. Steffen und Frau Susanne Graf eine Journal-Version über die in meiner Diplomarbeit vorgestellten Methode zur kompositionellen Minimierung verteilter Systeme fertig.

Im Rahmen persönlicher Gespräche mit Herrn Prof. Cleaveland und seinen Mitarbeitern werde ich meine bei der Literaturrecherche gewonnenen Erkenntnisse diskutieren. Ich bin davon überzeugt, daß sich auf diese interaktive Weise am besten einschätzen läßt, wie das in meiner Diplomarbeit präsentierte Framework erweitert oder modifiziert werden muß, damit es den Anforderungen meiner Dissertation genügt. Gleichzeitig wollen wir einen „gemeinsamen Nenner“ für mein Forschungsvorhaben herstellen. Als zentrales Arbeitsergebnis im *ersten Quartal* ist die Fertigstellung eines gemeinsamen Papers von Prof. Cleaveland, Prof. Steffen und mir vorgesehen. Diese Arbeit beschäftigt sich mit einer interfacegestützten Verifikationsmethode basierend auf Quasiordnungen. Im Hinblick auf mein Dissertationsvorhaben soll dieses Projekt darüber Klarheit verschaffen, inwieweit eine Kombination bekannter Techniken, wie etwa *abstrakte Interpretation* und *Verifikation mittels Quasiordnungen*, sinnvoll möglich ist.

Aufgrund der gesammelten Erkenntnisse werde ich im *zweiten Quartal* die in meiner Diplomarbeit präsentierte Methode zur Minimierung verteilter Systeme so anpassen, daß sie flexibel und mächtig genug ist, damit sie auf adäquatere Modelle der Realität, die sich der Techniken von Prozeßkalkülen mit *Prioritäten, stochastischem Verhalten und Realzeitaspekten* bedienen, ausdehnen läßt. Dabei ist es wichtig, die genannten Aspekte *orthogonal* in die Methode zu integrieren. Insbesondere soll sich der Gedanke der *Kompositionalität* darin widerspiegeln. Dies unterstützt, daß in der Methode jeder einzelne Aspekt separat oder ggf. eine Kombination der Aspekte erfaßt werden kann. Weiterhin soll die Methode, welche eine Unterstützung des Benutzers verlangt, eine intuitive Benutzerinteraktion fördern, wie dies bereits in meiner Diplomarbeit berücksichtigt wurde. Im Hinblick auf die spätere Erweiterung der Methode werde ich mich insbesondere mit sogenannten *modalen Transitionssystemen* beschäftigen, welche sich zur Verifikation von Realzeitsystemen bzgl. geeigneter Quasiordnungen als besonders interessant erwiesen haben.

Im *dritten Quartal* werde ich beginnen, die entwickelte Methode bzgl. der zentralen Aspekte meiner Dissertation auszubauen. Zunächst sollen stochastische Modellierungsansätze und Prioritäten integriert werden. Da die Verifikationstechnik, in die meine Methode eingebettet ist, auf Quasiordnungen basiert, werde ich untersuchen, welche Quasiordnungen für diese Situation adäquat sind. Darüberhinaus gilt es ein *automatisches* Verfahren zu entwickeln, welches zu zwei gegebenen Modellen feststellt, ob diese in Quasiordnung zueinander stehen. Dieses sog. *Preorder-Checking* kann effizient mit Hilfe von *Model-Checking Verfahren* implementiert werden. Für elementare Systemmodelle, wie etwa der Prozeßkalkül CCS, hat die Frage nach einer

geeigneten Quasiordnung zu mehreren Lösungsansätzen geführt, wobei der von Prof. Cleaveland und Prof. Steffen publizierte Ansatz mit der Technik der Interfacespezifikationen zusammenpaßt, die in meiner Methode zur Minimierung von verteilten Systemen eine Schlüsselrolle spielt.

Im *letzten Quartal* meines Aufenthalts möchte ich meine erzielten Ergebnisse auf Systeme mit Realzeitaspekten ausdehnen. Weiterhin werde ich einen Vergleich zwischen der von mir entwickelten Methode und den an der North Carolina State University angewandten Techniken ziehen, um meinen Ansatz "Einfachheit statt Universalität" beurteilen zu können.

Für meine Dissertation ist die Synthese der Forschungsresultate von Herrn Prof. Cleaveland und Herrn Prof. Steffen von besonderer Wichtigkeit, damit ich sie zügig und effizient vorantreiben kann. Nach meinem Aufenthalt werde ich wieder in der Forschungsgruppe von Herrn Prof. Steffen an der Universität Passau eingegliedert und dort meine Dissertation fertigstellen.

(Gerald Lüttgen)

Literatur

[1] R. Cleaveland, M. Klein, and B. Steffen. Faster model checking for the modal mu-calculus. In Bochmann and Probst, editors, *Computer Aided Verification (CAV '92)*, volume 663 of *Lecture Notes in Computer Science*, pages 370–383, Montréal, June/July 1992. Springer-Verlag.

[2] R. Cleaveland, J. Parrow, and B. Steffen. The Concurrency Workbench: A semantics-based tool for the verification of finite-state systems. *ACM Transactions on Programming Languages and Systems*, 15(1):36–72, January 1993.

[3] R. Cleaveland and B. Steffen. A preorder for partial process specifications. In J.C.M. Baetan and J.W. Klop, editors, *CONCUR '90*, volume 458 of *Lecture Notes in Computer Science*, pages 141–151, Amsterdam, August 1990. Springer-Verlag.

[4] R. Cleaveland and B. Steffen. When is 'partial' adequate? A logic-based proof technique using partial specifications. In *Fifth Annual Symposium on Logic in Computer Science (LICS '90)*, pages 440–449, Philadelphia, June 1990. Computer Society Press.

[5] R. Cleaveland and B. Steffen. A linear-time model-checking algorithm for the alternation-free modal mu-calculus. In K.G. Larsen and A. Skou, editors, *Computer Aided Verification (CAV '91)*, volume 575 of *Lecture Notes in Computer Science*, pages 48–58, Aalborg, Denmark, July 1991. Springer-Verlag.

[6] U. Celikkan and R. Cleaveland. Computing diagnostic tests for incorrect processes. In *Proceedings of the IFIP Symposium on Protocol Specification, Testing and Verification*, pages 263–278, Lake Buena Vista, Florida, June 1992. North-Holland.

[7] U. Celikkan and R. Cleaveland. On computing diagnostic information for preorder checking. In Bochmann and Probst, editors, *Computer Aided Verification (CAV '92)*, volume 663 of

Lecture Notes in Computer Science, pages 370–383, Montréal, June/July 1992. Springer-Verlag.

[8] R. Cleaveland. Tableau-based model checking in the propositional mu-calculus. *Acta Informatica*, 27(8):725–747, September 1990.

[9] R. Cleaveland. Analyzing concurrent systems using the Concurrency Workbench. In P.E. Lauer, editor, *Functional Programming, Concurrency, Simulation and Automated Reasoning*, volume 693 of *Lecture Notes in Computer Science*, pages 129–144. Springer-Verlag, 1993.

[10] R. Cleaveland. An operational semantics of value-passing. In *Proceedings of the North American Process Algebra Workshop*, Cornell University Technical Report TR 93-1369, Ithaca, New York, August 1993.

[11] R. Cleaveland and M.C.B. Hennessy. Priorities in process algebras. In *Third Annual Symposium on Logic in Compter Science (LICS '88)*, pages 193–202, Edinburgh, Scotland, July 1988. Computer Society Press.

[12] R. Cleaveland and M.C.B. Hennessy. Priorities in process algebra. *Information and Computation*, 87(1/2):58–77, July/August 1990.

[13] R. Cleaveland and J. Riely. Testing-based abstractions for concurrent systems. In B. Jonsson and J. Parrow, editors, *CONCUR '94*, volume 836 of *Lecture Notes in Computer Science*, pages 417–432, Uppsala, Sweden, August 1994. Springer-Verlag.

[14] R. Cleaveland, S. Smolka, and A. Zwarico. Testing preorders for probabilistic processes. In W. Kuich, editor, *Automata, Languages and Programming (ICALP '92)*, volume 623 of *Lecture Notes in Computer Science*, pages 708–719, Vienna, July 1992. Springer-Verlag.

[15] R. Cleaveland and D. Yankelevich. An operational framework for value-passing processes. In *21st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (PoPL '94)*, pages 326–338, Portland, Oregon, January 1994. Computer Society Press.

[16] R. Cleaveland and A. Zwarico. A theory of testing for real time. In *Sixth Annual Symposium on Logic in Computer Science (LICS '91)*, pages 110–119, Amsterdam, July 1991. Computer Society Press.

[17] A. Fredette and R. Cleaveland. A generalized approach to real-time schedulability analysis. In *Proceedings of the Workshop on Real-Time Operating Systems and Software*, pages 98–103, New York, NY, May 1993.

[18] A. Fredette and R. Cleaveland. RTSL: A language for real-time schedulability analysis. In *Proceedings of the Real-Time Systems Symposium*, pages 274–283, Durham, NC, December 1993. Computer Society Press.

[19] V. Natarajan, L. Christoff, I. Christoff, and R. Cleaveland. Priorities and abstraction in process algebra, 1994. To appear in Proceedings of *Foundations of Software Technology and Theoretical Computer Science*.

[20] S. Yuen, R. Cleaveland, Z. Dayar, and S. Smolka. Fully abstract characterizations of testing preorders for probabilistic processes. In B. Jonsson and J. Parrow, editors, *CONCUR '94*, volume 836 of *Lecture Notes in Computer Science*, pages 497–512, Uppsala, Sweden, August 1994. Springer-Verlag.

[21] R. Cleaveland, S.P. Iyer, and D. Yankelevich. Abstractions for preserving all CTL^* formulae. 1994. Submitted to CAV'94.

[22] R. Bryant. Graph-based algorithms for boolean function manipulation. *IEEE Transactions on Computation*, 35(8), 1986.

[23] E.M. Clarke, O. Grumberg, and D. Long. Model checking and abstraction. In *Proceedings of XIX POPL*, 1992.

[24] P. Cousot and R. Cousot. Abstract interpretation: A unified lattice model for static analysis of programs by construction and approximation of fixpoints. In *Conference Record of the 4th ACM Symposium on Principles of Programming Languages*, 1977.

[25] D. Dams, O. Grumberg, and R. Gerth. Abstract interpretation of reactive systems: Abstractions preserving $\forall CTL^*$, $\exists CTL^*$ and CTL^*, 1993. Submitted to IEEE PROCOMONET.

[26] S. Graf and C. Loiseaux. Program verification using compositional abstraction. In *Proceedings FASE/TAPSOFT*, 1993.

[27] S. Graf and B. Steffen. Using interface specifications for compositional reduction. In *Proceedings of the International Workshop on Computer-Aided Verification '90*, volume 531. Springer Lecture Notes in Computer Science, 1990.

[28] C.A.R. Hoare. *Communicating Sequential Processes.* Prentice Hall International, 1985.

[29] J. B. Kam and J. D. Ullman. Monotone data flow analysis frameworks. *Acta Informatica*, 7:309–317, 1977.

[30] K.G. Larsen. Modal specifications. In *Proceedings of Workshop on Automatic Verification Methods for Finite State Systems*, Springer Lecture Notes in Computer Science, 407, 1990.

[31] K. G. Larsen, B. Steffen, and Carsten Weise. A constraint oriented proof methodology based on modal transition systems. To appear in the BRICS Notes Series, October 1994.

[32] K. G. Larsen and B. Thomsen. Compositional proofs by partial specification of processes. *Proc. IEEE Symp. Logic in Computer Science*, 1988.

[33] K.G. Larsen and L. Xinxin. Compositionality through an operational semantics of contexts. In *ICALP '90*, volume 443, 1990.

[34] G. Lüttgen. Kompositionelle Minimierung endlicher verteilter Systeme. *Diplomarbeit an der RWTH Aachen*, 1994.

[35] T. Margaria, A. Claßen, and B. Steffen. Computer aided tool synthesis in META–Frame. GI/ITG Workshop on *"Anwendung formaler Methoden beim Entwurf von Hardwaresystemen"*, March 1995.

[36] R. Milner. A calculus for communicating systems. *Springer Lecture Notes in Computer Science*, 92, 1980.

[37] R. Milner. *Communication and Concurrency.* Prentice Hall, 1989.

[38] B. Steffen. Characteristic formulae. In *ICALP '89, Stresa (Italy)*, volume 372, 1989.

[39] B. Steffen. Finite model checking and beyond. To appear in the BRICS Notes Series, October 1994.

[40] B. Steffen and A. Ingólfsdóttir. Characteristic formulae for CCS with divergence. *Information and Computation*, 110, 1994.

[41] C. Stirling and D. J. Walker. Local model checking in the modal mu-calculus. In *CAAP '89*, volume 351, 1989.

[42] R. van Glabbeek, S.A. Smolka, B. Steffen, and C.M.N. Tofts. Reactive, generative, and stratified models of probabilistic processes. In *Proceedings of the International Conference on Logic in Computer Science'90, Philadelphia*, pages 130–141, 1990.