BRICS Research Series, Abstracts, 2006

June 1, 2007

This document is also available as *PostScript* and *DVI*.

References

[RS-06-19] *PostScript*, *PDF*, *DVI*.
Michael David Pedersen.
Logics for The Applied π Calculus.
December 2006.
viii+111 pp.

Abstract: In this master's thesis we present a modal logic for Applied π which characterises observational equivalence on processes. The motivation is similar to that of Applied π itself, namely generality: the logic can be adapted to a particular application simply by defining a suitable equational theory on terms.

As a first step towards the logic for Applied π, a strong version of static equivalence on frames is introduced in which term reductions are observable in addition to equality on terms. We argue that the strong version is meaningful in applications and give two refined definitions based on the notion of cores introduced in work by Boreale et al. for the Spi calculus. The refined definitions are useful because they do not involve universal quantification over arbitrary terms and hence are amenable to a logical characterisation. We show that the refined definitions coincide with the original definition of strong static equivalence under certain general conditions.

A first order logic for frames which characterises strong static equivalence and which yields characteristic formulae is then given based on the refined definitions of strong static equivalence. This logic facilitates direct reasoning about terms in a frame as well as indirect reasoning about knowledge deducible from a frame. The logic for Applied π is then obtained by adding suitable Hennessy-Milner style modalities to the logic for frames, hence facilitating reasoning about both static and dynamic properties of processes. We finally demonstrate the logic with an application to the analysis of the Needham-Schroeder Public Key Protocol.

[RS-06-18] Małgorzata Biernacka and Olivier Danvy.
A Syntactic Correspondence between Context-Sensitive Calculi and Abstract Machines.

dec 2006.

iii+39 pp. Extended version of an article to appear in TCS. Revised version of BRICS RS-05-22.

Abstract: We present a systematic construction of environment-based abstract machines from context-sensitive calculi of explicit substitutions, and we illustrate it with ten calculi and machines for applicative order with an abort operation, normal order with generalized reduction and call/cc, the lambda-mu-calculus, delimited continuations, i/o, stack inspection, proper tail-recursion, and lazy evaluation. Most of the machines already exist but they have been obtained independently and are only indirectly related to the corresponding calculi. All of the calculi are new and they make it possible to directly reason about the execution of the corresponding machines.

[RS-06-17] *PostScript*, *PDF*, *DVI*.

Olivier Danvy and Kevin Millikin.

A Rational Deconstruction of Landin's J Operator.

December 2006.

ii+37 pp. Revised version of BRICS RS-06-4. A preliminary version appears in the proceedings of IFL 2005, LNCS 4015:55–73.

Abstract: Landin's J operator was the first control operator for functional languages. It was specified with an extension of the SECD machine, which was the first abstract machine for functional languages. We present a family of compositional evaluation functions corresponding to this extension of the SECD machine, using a series of elementary transformations (transformation into continuation-passing style (CPS) and defunctionalization, chiefly) and their left inverses (transformation into direct style and refunctionalization). To this end, we modernize the SECD machine into a bisimilar one that operates in lock step with the original one but that (1) does not use a data stack and (2) uses the caller-save rather than the callee-save convention for environments. We then characterize the J operator in terms of CPS and in terms of delimited-control operators in the CPS hierarchy. As a byproduct, we also present a reduction semantics for applicative expressions with the J operator, based on Curien's original calculus of explicit substitutions. This reduction semantics mechanically corresponds to the modernized version of the SECD machine and to the best of our knowledge, it provides the first syntactic theory of applicative expressions with the J operator.

The present work is concluded by a motivated wish to see Landin's name added to the list of co-discoverers of continuations. Methodologically, however, it mainly illustrates the value of Reynolds's defunctionalization and of refunctionalization as well as the expressive power of the CPS hierarchy (a) to account for the first control operator and the first abstract machine for functional languages and (b) to connect them to their successors.

[RS-06-16] *PostScript*, *PDF*.

Anders Møller.
Static Analysis for Event-Based XML Processing.
October 2006.
16 pp.
Abstract: Event-based processing of XML data - as exemplified by the popular SAX framework - is a powerful alternative to using W3C's DOM or similar tree-based APIs. The event-based approach is particularly superior when processing large XML documents in a streaming fashion with minimal memory consumption.

This paper discusses challenges and presents some considerations for creating program analyses for SAX applications. In particular, we consider the problem of statically guaranteeing that a given SAX application always produces only well-formed and valid XML output.

[RS-06-15] *PostScript*, *PDF*, *DVI*.
Dariusz Biernacki, Olivier Danvy, and Kevin Millikin.
A Dynamic Continuation-Passing Style for Dynamic Delimited Continuations.
October 2006.
ii+28 pp. Revised version of BRICS RS-05-16.
Abstract: We put a pre-existing definitional abstract machine for dynamic delimited continuations in defunctionalized form, and we present the consequences of this adjustment.

We first prove the correctness of the adjusted abstract machine. Because it is in defunctionalized form, we can refunctionalize it into a higher-order evaluation function. This evaluation function, which is compositional, is in continuation+state passing style and threads a trail of delimited continuations and a meta-continuation. Since this style accounts for dynamic delimited continuations, we refer to it as 'dynamic continuation-passing style' and we present the corresponding dynamic CPS transformation. We show that the notion of computation induced by dynamic CPS takes the form of a continuation monad with a recursive answer type and we present a new simulation of dynamic delimited continuations in terms of static ones as well as new applications of dynamic delimited continuations.

The significance of the present work is that the computational artifacts surrounding dynamic CPS are not independent designs: they are mechanical consequences of having put the definitional abstract machine in defunctionalized form.

[RS-06-14] *PostScript*, *PDF*, *DVI*.
Giorgio Delzanno, Javier Esparza, and Jiří Srba.
Monotonic Set-Extended Prefix Rewriting and Verification of Recursive Ping-Pong Protocols.
July 2006.
31 pp. To appear in ATVA '06.
Abstract: Ping-pong protocols with recursive definitions of agents,

but without any active intruder, are a Turing powerful model. We show that under the environment sensitive semantics (i.e. by adding an active intruder capable of storing all exchanged messages including full analysis and synthesis of messages) some verification problems become decidable. In particular we give an algorithm to decide control state reachability, a problem related to security properties like secrecy and authenticity. The proof is via a reduction to a new prefix rewriting model called Monotonic Set-extended Prefix rewriting (MSP). We demonstrate further applicability of the introduced model by encoding a fragment of the ccp (concurrent constraint programming) language into MSP.

[RS-06-13] *PostScript*, *PDF*, *DVI*.
Jiří Srba.
Visibly Pushdown Automata: From Language Equivalence to Simulation and Bisimulation.
July 2006.
21 pp. To appear in CSL '06.

Abstract: We investigate the possibility of (bi)simulation-like preorder/equivalence checking on the class of visibly pushdown automata and its natural subclasses visibly BPA (Basic Process Algebra) and visibly one-counter automata. We describe generic methods for proving complexity upper and lower bounds for a number of studied preorders and equivalences like simulation, completed simulation, ready simulation, 2-nested simulation preorders/equivalences and bisimulation equivalence. Our main results are that all the mentioned equivalences and preorders are EXPTIME-complete on visibly pushdown automata, PSPACE-complete on visibly one-counter automata and P-complete on visibly BPA. Our PSPACE lower bound for visibly one-counter automata improves also the previously known DP-hardness results for ordinary one-counter automata and one-counter nets. Finally, we study regularity checking problems for visibly pushdown automata and show that they can be decided in polynomial time.

[RS-06-12] *PostScript*, *PDF*, *DVI*.
Kristian Støvring.
Higher-Order Beta Matching with Solutions in Long Beta-Eta Normal Form.
June 2006.
13 pp. To appear in *Nordic Journal of Computing*, 2006.

Abstract: Higher-order matching is a special case of unification of simply-typed lambda-terms: in a matching equation, one of the two sides contains no unification variables. Loader has recently shown that higher-order matching up to beta equivalence is undecidable, but decidability of higher-order matching up to beta-eta equivalence is a long-standing open problem.

We show that higher-order matching up to beta-eta equivalence is decidable if and only if a restricted form of higher-order matching up to beta equivalence is decidable: the restriction is that

solutions must be in long beta-eta normal form.

[RS-06-11] *PostScript*, *PDF*.
Kim G. Larsen, Ulrik Nyman, and Andrzej Wasowski.
An Interface Theory for Input/Output Automata.
June 2006.
40 pp. Appears in Misra, Nipkow and Sekerinski, editors, *Formal Methods: 14th International Symposium*, FM '06 Proceedings, LNCS 4085, 2006, pages 82–97.

Abstract: Building on the theory of interface automata by de Alfaro and Henzinger we design an interface language for Lynch's Input/Output Automata, a popular formalism used in the development of distributed asynchronous systems, not addressed by previous interface research. We introduce an explicit separation of assumptions from guarantees not yet seen in other behavioral interface theories. Moreover we derive the composition operator systematically and formally, guaranteeing that the resulting compositions are always the weakest in the sense of assumptions, and the strongest in the sense of guarantees. We also present a method for solving systems of relativized behavioral inequalities as used in our setup and draw a formal correspondence between our work and interface automata. Proofs are provided in an appendix.

[RS-06-10] *PostScript*, *PDF*.
Christian Kirkegaard and Anders Møller.
Static Analysis for Java Servlets and JSP.
June 2006.
23 pp. Full version of paper presented at SAS '06.

Abstract: We present an approach for statically reasoning about the behavior of Web applications that are developed using Java Servlets and JSP. Specifically, we attack the problems of guaranteeing that all output is well-formed and valid XML and ensuring consistency of XHTML form fields and session state. Our approach builds on a collection of program analysis techniques developed earlier in the JWIG and XACT projects, combined with work on balanced context-free grammars. Together, this provides the necessary foundation concerning reasoning about output streams and application control flow.

[RS-06-9] Claus Brabrand, Robert Giegerich, and Anders Møller.
Analyzing Ambiguity of Context-Free Grammars.
April 2006.
19 pp.

Abstract: It has been known since 1962 that the ambiguity problem for context-free grammars is undecidable. Ambiguity in context-free grammars is a recurring problem in language design and parser generation, as well as in applications where grammars are used as models of real-world physical structures. However, the fact that the problem is undecidable does not mean that there are no useful *approximations* to the problem.

We observe that there is a simple linguistic characterization of the grammar ambiguity problem, and we show how to exploit this to conservatively approximate the problem based on local regular approximations and grammar unfoldings. As an application, we consider grammars that occur in RNA analysis in bioinformatics, and we demonstrate that our static analysis of context-free grammars is sufficiently precise and efficient to be practically useful.

[RS-06-8] *PostScript*, *PDF*.
Christian Kirkegaard and Anders Møller.
Static Analysis for Java Servlets and JSP.
April 2006.
22 pp.
Abstract: We present an approach for statically reasoning about the behavior of Web applications that are developed using Java Servlets and JSP. Specifically, we attack the problems of guaranteeing that all output is well-formed and valid XML and ensuring consistency of XHTML form fields and session state. Our approach builds on a collection of program analysis techniques developed earlier in the JWIG and XACT projects, combined with work on balanced context-free grammars. Together, this provides the necessary foundation concerning reasoning about output streams and application control flow.

[RS-06-7] *PostScript*, *PDF*, *DVI*.
Petr Jančar and Jiří Srba.
Undecidability Results for Bisimilarity on Prefix Rewrite Systems.
April 2006.
20 pp. Presented at *FoSSaCS 2006*, LNCS 3921:277–291.
Abstract: We answer an open question related to bisimilarity checking on labelled transition systems generated by prefix rewrite rules on words. Stirling (1996, 1998) proved the decidability of bisimilarity for normed pushdown processes. This result was substantially extended by Sénizergues (1998, 2005) who showed the decidability for regular (or equational) graphs of finite out-degree (which include unnormed pushdown processes). The question of decidability of bisimilarity for a more general class of so called Type -1 systems (generated by prefix rewrite rules of the form $R \xrightarrow{a} w$ where R is a regular language) was left open; this was repeatedly indicated by both Stirling and Sénizergues. Here we answer the question negatively, i.e., we show undecidability of bisimilarity on Type -1 systems, even in the normed case. We complete the picture by considering classes of systems that use rewrite rules of the form $w \xrightarrow{a} R$ and $R_1 \xrightarrow{a} R_2$ and show when they yield low undecidability (Π^0_1-completeness) and when high undecidability (Σ^1_1-completeness), all with and without the assumption of normedness.

[RS-06-6] *PostScript*, *PDF*, *DVI*.
Luca Aceto, Willem Jan Fokkink, Anna Ingólfsdóttir, and Bas Luttik.

A Finite Equational Base for CCS with Left Merge and Communication Merge.
March 2006.
22 pp.
Abstract: Using the left merge and communication merge from ACP, we present an equational base for the fragment of CCS without restriction and relabelling. Our equational base is finite if the set of actions is finite.

[RS-06-5] *PostScript*, *PDF*, *DVI.*
Kristian Støvring.
Extending the Extensional Lambda Calculus with Surjective Pairing is Conservative.
March 2006.
18 pp. To appear in *Logical Methods in Computer Science*. Supersedes RS-05-35.
Abstract: We answer Klop and de Vrijer's question whether adding surjective-pairing axioms to the extensional lambda calculus yields a conservative extension. The answer is positive. As a byproduct we obtain the first "syntactic" proof that the extensional lambda calculus with surjective pairing is consistent.

[RS-06-4] *PostScript*, *PDF*, *DVI.*
Olivier Danvy and Kevin Millikin.
A Rational Deconstruction of Landin's J Operator.
February 2006.
ii+26 pp. To appear in the post-reviewed proceedings of the 17th International Workshop on the *Implementation and Application of Functional Languages* (IFL'05), Dublin, Ireland, September 2005.
Abstract: Landin's J operator was the first control operator for functional languages, and was specified with an extension of the SECD machine. Through a series of meaning-preserving transformations (transformation into continuation-passing style (CPS) and defunctionalization) and their left inverses (transformation into direct style and refunctionalization), we present a compositional evaluation function corresponding to this extension of the SECD machine. We then characterize the J operator in terms of CPS and in terms of delimited-control operators in the CPS hierarchy. Finally, we present a motivated wish to see Landin's name added to the list of co-discoverers of continuations.

[RS-06-3] *PostScript*, *PDF*, *DVI.*
Małgorzata Biernacka and Olivier Danvy.
A Concrete Framework for Environment Machines.
February 2006.
ii+29 pp. To appear in the *ACM Transactions on Computational Logic*. Supersedes BRICS RS-05-15.
Abstract: We materialize the common understanding that calculi with explicit substitutions provide an intermediate step between an abstract specification of substitution in the lambda-calculus and its concrete implementations. To this end, we go back to

Curien's original calculus of closures (an early calculus with explicit substitutions), we extend it minimally so that it can also express one-step reduction strategies, and we methodically derive a series of environment machines from the specification of two one-step reduction strategies for the lambda-calculus: normal order and applicative order. The derivation extends Danvy and Nielsen's refocusing-based construction of abstract machines with two new steps: one for coalescing two successive transitions into one, and the other for unfolding a closure into a term and an environment in the resulting abstract machine. The resulting environment machines include both the Krivine machine and the original version of Krivine's machine, Felleisen et al.'s CEK machine, and Leroy's Zinc abstract machine.

[RS-06-2] *PDF.*
Mikkel Baun Kjærgaard and Jonathan Bunde-Pedersen.
A Formal Model for Context-Awareness.
February 2006.
26 pp.
Abstract: There is a definite lack of formal support for modeling real- istic context-awareness in pervasive computing applications. The Conawa calculus presented in this paper provides mechanisms for modeling complex and interwoven sets of context-information by extending ambient calculus with new constructs and capabilities. In connection with the calculus we present four scenarios which are used to evaluate Conawa. The calculus is a step in the direction of making formal methods applicable in the area of pervasive computing.

[RS-06-1] *PostScript*, *PDF*, *DVI.*
Luca Aceto, Taolue Chen, Willem Jan Fokkink, and Anna Ingólfsdóttir.
On the Axiomatizability of Priority.
January 2006.
25 pp.
Abstract: This paper studies the equational theory of bisimulation equivalence over the process algebra BCCSP extended with the priority operator of Baeten, Bergstra and Klop. It is proven that, in the presence of an infinite set of actions, bisimulation equivalence has no finite, sound, ground-complete equational axiomatization over that language. This negative result applies even if the syntax is extended with an arbitrary collection of auxiliary operators, and motivates the study of axiomatizations using conditional equations. In the presence of an infinite set of actions, it is shown that, in general, bisimulation equivalence has no finite, sound, ground-complete axiomatization consisting of conditional equations over the language studied in this paper. Finally, sufficient conditions on the priority structure over actions are identified that lead to a finite, ground-complete axiomatization of bisimulation equivalence using conditional equations.