BRICS Research Series, Abstracts, 1994

July 9, 2003

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

References

[RS-94-48] *PostScript*, *DVI.*
Jens Chr. Godskesen and Kim G. Larsen.
Synthesizing Distinguishing Formulae for Real Time Systems.
December 1994.
21 pp. Extended abstract appears in Wiedermann and Hjek, editors, *Mathematical Foundations of Computer Science: 20th International Symposium*, MFCS '95 Proceedings, LNCS 969, 1995, pages 519–528.
Abstract: This paper describes a technique for generating diagnostic information for the *timed* bisimulation equivalence and the *timed* simulation preorder. More precisely, given two (parallel) networks of regular real–time processes, the technique will provide a logical formula that differentiates them in case they are not timed (bi)similar. Our method may be seen as an extension of the algorithm by Čerāns for deciding timed bisimilarity in that information of time–quantities has been added sufficient for generating distinguishing formulae. The technique has been added to the automatic verification tool EPSILON and applied to various examples.

[RS-94-47] *PostScript*, *DVI.*
Kim G. Larsen, Bernhard Steffen, and Carsten Weise.
A Constraint Oriented Proof Methodology based on Modal Transition Systems.
December 1994.
13 pp.
Abstract: In this paper, we present a constraint-oriented state-based proof methodology for concurrent software systems which exploits compositionality and abstraction for the reduction of the verification problem under investigation. Formal basis for this methodology are Modal Transition Systems allowing loose state-based specifications, which can be refined by successively adding constraints. Key concepts of our method are *projective views*, *separation of proof obligations*, *Skolemization* and *abstraction.* The method is even applicable to real time systems.

[RS-94-46] *PostScript, DVI.*

Amos Beimel, Anna Gl, and Mike Paterson.

Lower Bounds for Monotone Span Programs.

December 1994.

14 pp. Appears in *36th Annual Symposium on Foundations of Computer Science*, FOCS '95 Proceedings, 1995, pages 674–681.

Abstract: The model of span programs is a linear algebraic model of computation. Lower bounds for span programs imply lower bounds for contact schemes, symmetric branching programs and for formula size. Monotone span programs correspond also to linear secret-sharing schemes. We present a new technique for proving lower bounds for monotone span programs. The main result proved here yields quadratic lower bounds for the size of monotone span programs, improving on the largest previously known bounds for explicit functions. The bound is asymptotically tight for the function corresponding to a class of 4-cliques.

[RS-94-45] *PostScript.*

Jrgen H. Andersen, Kre J. Kristoffersen, Kim G. Larsen, and Jesper Niedermann.

Automatic Synthesis of Real Time Systems.

December 1994.

17 pp. Appears in Flp and Gcseg, editors, *22nd International Colloquium on Automata, Languages, and Programming*, ICALP '95 Proceedings, LNCS 944, 1995, pages 535–546.

Abstract: This paper presents a method for automatically constructing real time systems directly from their specifications. The model–construction problem is considered for implicit specifications of the form:

$$(A_1 \mid \ldots \mid A_n \mid X) \ \mathsf{sat}\ S$$

where S is a real time (logical) specification, $A_1 \ldots A_n$ are given (regular) timed agents and the problem is to decide whether there exists (and if possible exhibit) a real time agent X which when put in parallel with $A_1 \ldots A_n$ will yield a network satisfying S. The method presented proceeds in two steps: first, the implicit specification of X is transformed into an equivalent direct specification of X; second, a model for this direct specification is constructed (if possible) using a direct model construction algorithm. A prototype implementation of our method has been added to the real time verification tool EPSILON.

[RS-94-44] *PostScript.*

Sten Agerholm.

A HOL Basis for Reasoning about Functional Programs.

December 1994.

PhD thesis. viii+224 pp.

Abstract: Domain theory is the mathematical theory underlying denotational semantics. This thesis presents a formalization of domain theory in the Higher Order Logic (HOL) theorem proving system along with a mechanization of proof functions and other tools to support reasoning about the denotations of functional programs. By providing a fixed point operator for functions on certain domains which have a special undefined (bottom) element, this extension of HOL supports the definition of recursive functions which are not also primitive recursive. Thus, it provides an approach to the long-standing and important problem of defining non-primitive recursive functions in the HOL system.

Our philosophy is that there must be a direct correspondence between elements of complete partial orders (domains) and elements of HOL types, in order to allow the reuse of higher order logic and proof infrastructure already available in the HOL system. Hence, we are able to mix domain theoretic reasoning with reasoning in the set theoretic HOL world to advantage, exploiting HOL types and tools directly. Moreover, by mixing domain and set theoretic reasoning, we are able to eliminate almost all reasoning about the bottom element of complete partial orders that makes the LCF theorem prover, which supports a first order logic of domain theory, difficult and tedious to use. A thorough comparison with LCF is provided.

The advantages of combining the best of the domain and set theoretic worlds in the same system are demonstrated in a larger example, showing the correctness of a unification algorithm. A major part of the proof is conducted in the set theoretic setting of higher order logic, and only at a late stage of the proof domain theory is introduced to give a recursive definition of the algorithm, which is not primitive recursive. Furthermore, a total well-founded recursive unification function can be defined easily in pure HOL by proving that the unification algorithm (defined in domain theory) always terminates; this proof is conducted by a non-trivial well-founded induction. In such applications, where non-primitive recursive HOL functions are defined via domain theory and a proof of termination, domain theory constructs only appear temporarily.

[RS-94-43] *PostScript*, *DVI*.

Luca Aceto and Alan S. A. Jeffrey.

A Complete Axiomatization of Timed Bisimulation for a Class of Timed Regular Behaviours (Revised Version).

December 1994.

18 pp. Appears in *Theoretical Computer Science* vol. 152(2) pages 251–268, December 1995.

Abstract: One of the most satisfactory results in process theory is Milner's axiomatization of strong bisimulation for regular CCS. This result holds for open terms with finite-state recursion. Wang has shown that timed bisimulation can also be axiomatized, but only for closed terms without recursion. In this paper, we provide an axiomatization for timed bisimulation of open terms with finite-state recursion.

[RS-94-42] *PostScript*, *DVI*.

Dany Breslauer and Leszek Gąsieniec.

Efficient String Matching on Coded Texts.
December 1994.
20 pp. Appears with the title *Efficient String Matching on Packed Texts* in Galil and Ukkonen, editors, *Combinatorial Pattern Matching: 6th Annual Symposium*, CPM '95 Proceedings, LNCS 937, 1995, pages 27–40 and in *RAIRO Informatique Thorique et Applications*, 30(6):521–544, 1996.

Abstract: The so called "four Russians technique" is often used to speed up algorithms by encoding several data items in a single memory cell. Given a sequence of n symbols over a constant size alphabet, one can encode the sequence into $O(n/\lambda)$ memory cells in $O(\log \lambda)$ time using $n/\log \lambda$ processors.

This paper presents an efficient CRCW-PRAM string-matching algorithm for coded texts that takes $O(\log\log(m/\lambda))$ time making only $O(n/\lambda)$ operations, an improvement by a factor of $\lambda = O(\log n)$ on the number of operations used in previous algorithms. Using this string-matching algorithm one can test if a string is square-free and find all palindromes in a string in $O(\log\log n)$ time using $n/\log\log n$ processors.

[RS-94-41] *PostScript*, *DVI*.
Peter Bro Miltersen, Noam Nisan, Shmuel Safra, and Avi Wigderson.
On Data Structures and Asymmetric Communication Complexity.
December 1994.
17 pp. Appears in *The Twenty-seventh Annual ACM Symposium on Theory of Computing*, STOC '95 Proceedings, 1995, pages 103–111. Appears also in *Journal of Computer and System Sciences*, 57(1):37–49, 1998.

Abstract: In this paper we consider two party communication complexity when the input sizes of the two players differ significantly, the "asymmetric" case. Most of previous work on communication complexity only considers the total number of bits sent, but we study tradeoffs between the number of bits the first player sends and the number of bits the second sends. These types of questions are closely related to the complexity of static data structure problems in the cell probe model. We derive two generally applicable methods of proving lower bounds, and obtain several applications. These applications include new lower bounds for data structures in the cell probe model. Of particular interest is our "round elimination" lemma, which is interesting also for the usual symmetric communication case. This lemma generalizes and abstracts in a very clean form the "round reduction" techniques used in many previous lower bound proofs.

[RS-94-40] *PostScript*, *DVI*.
Luca Aceto and Anna Inglfsdttir.
CPO Models for GSOS Languages — Part I: Compact GSOS Languages.
December 1994.
70 pp. An extended abstract of the paper appears in: *Proceedings of*

CAAP '95, LNCS 915, 1995, pages 439–453. Full version also appears in *Information and Computation*, 129(2):107–141, September 1996.

Abstract: In this paper, we present a general way of giving denotational semantics to a class of languages equipped with an operational semantics that fits the GSOS format of Bloom, Istrail and Meyer. The canonical model used for this purpose will be Abramsky's domain of synchronization trees, and the denotational semantics automatically generated by our methods will be guaranteed to be fully abstract with respect to the finitely observable part of the bisimulation preorder. In the process of establishing the full abstraction result, we also obtain several general results on the bisimulation preorder (including a complete axiomatization for it), and give a novel operational interpretation of GSOS languages.

[RS-94-39] *PostScript*, *DVI*.
Ivan B. Damgrd, Oded Goldreich, and Avi Wigderson.
Hashing Functions can Simplify Zero-Knowledge Protocol Design (too).
November 1994.
18 pp.

Abstract: In *Crypto93*, Damgrd showed that any constant-round protocol in which the verifier sends only independent, random bits and which is zero-knowledge against the *honest* verifier can be transformed into a protocol (for the same problem) that is zero-knowledge *in general*. His transformation was based on the interactive hashing technique of Naor, Ostrovsky, Venkatesan and Yung, and thus the resulting protocol had very large round-complexity.

We adopt Damgrd's methods, using ordinary hashing functions, instead of the abovementioned interactive hashing technique. Typically, the protocols we derive have much lower round-complexity than those derived by Damgrd's transformation. As in Damgrd's transformation, our transformation preserves statistical/perfect zero-knowledge and does not rely on any computational assumptions. However, unlike Damgrd's transformation, the new transformation is not applicable to argument systems or to proofs of knowledge.

[RS-94-38] *PostScript*, *DVI*.
Ivan B. Damgrd and Lars Ramkilde Knudsen.
Enhancing the Strength of Conventional Cryptosystems.
November 1994.
12 pp.

Abstract: We look at various ways of enhancing the strength of conventional cryptosystems such as DES by building a new system which has longer keys and which uses the original system as a building block. We propose a new variant of two-key triple encryption which is not vulnerable to the meet in the middle attack by van Oorschot and Wiener. Under an appropriate assumption

on the security of DES, we can prove that our system is at least as hard to break as single DES.

[RS-94-37] *PostScript*, *DVI*.
Jaap van Oosten.
Fibrations and Calculi of Fractions.
November 1994.
21 pp. Appears in *Journal of Pure and Applied*, 146(1):77–102, 2000.
Abstract: Given a fibration $\mathcal{E} \to \mathcal{B}$ and a class Σ of arrows of $\mathcal{B}$, one can construct the free fibration (on $\mathcal{E}$ over $\mathcal{B}$ such that all reindexing functors over elements of Σ are equivalences.

In this work I give an explicit construction of this, and study its properties. For example, the construction preserves the property of being fibrewise discrete, and it commutes up to equivalence with fibrewise exact completions. I show that mathematically interesting situations are examples of this construction. In particular, subtoposes of the effective topos are treated.

[RS-94-36] *PostScript*, *DVI*.
Alexander A. Razborov.
On provably disjoint **NP***-pairs.*
November 1994.
27 pp.
Abstract: In this paper we study the pairs (U, V) of disjoint **NP**-sets representable in a theory T of Bounded Arithmetic in the sense that T proves $U \cap V = \emptyset$. For a large variety of theories T we exhibit a natural disjoint **NP**-pair which is complete for the class of disjoint **NP**-pairs representable in T. This allows us to clarify the approach to showing independence of central open questions in Boolean complexity from theories of Bounded Arithmetic initiated in [1]. Namely, in order to prove the independence result from a theory T, it is sufficient to separate the corresponding complete **NP**-pair by a (quasi)poly-time computable set. We remark that such a separation is obvious for the theory $\mathcal{S}(S_2) + \mathcal{S}\Sigma_2^b - PIND$ considered in [1], and this gives an alternative proof of the main result from that paper.

[1] A. Razborov. Unprovability of lower bounds on circuit size in certain fragments of Bounded Arithmetic. To appear in *Izvestiya of the RAN*, 1994.

[RS-94-35] *PostScript*.
Gerth Stlting Brodal.
Partially Persistent Data Structures of Bounded Degree with Constant Update Time.
November 1994.
24 pp. Appears in *Nordic Journal of Computing*, 3(3):238–255, 1996.
Abstract: The problem of making bounded in-degree and out-degree data structures partially persistent is considered. The node copying method of Driscoll *et al.* is extended so that updates can be performed in *worst-case* constant time on the pointer machine model. Previously it was only known to be possible in

amortised constant time [Driscoll89]. The result is presented in terms of a new strategy for Dietz and Raman's dynamic two player pebble game on graphs. It is shown how to implement the strategy and the upper bound on the required number of pebbles is improved from $2b + 2d + O(\sqrt{b})$ to $d + 2b$, where b is the bound of the in-degree and d the bound of the out-degree. We also give a lower bound that shows that the number of pebbles depends on the out-degree d.

[RS-94-34] *PostScript*, *DVI.*
Henrik Reif Andersen, Colin Stirling, and Glynn Winskel.
A Compositional Proof System for the Modal μ-Calculus.
October 1994.
18 pp. Appears in *Ninth Annual IEEE Symposium on Logic in Computer Science*, LICS '94 Proceedings, 1994, pages 144–153. Superseeded by BRICS Report RS-98-40.
Abstract: We present a proof system for determining satisfaction between processes in a fairly general process algebra and assertions of the modal μ-calculus. The proof system is compositional in the structure of processes. It extends earlier work on compositional reasoning within the modal μ-calculus and combines it with techniques from work on local model checking. The proof system is sound for all processes and complete for a class of finite-state processes.

[RS-94-33] *PostScript*, *DVI.*
Vladimiro Sassone.
Strong Concatenable Processes: An Approach to the Category of Petri Net Computations.
October 1994.
40 pp. Workshop version appears in Engberg, Larsen and Mosses, editors, *6th Nordic Workshop on Programming Theory*, NWPT '6 Proceedings, BRICS Notes Series NS-94-6, December 1994, 1994, pages 385–399 with the title *An Approach to the Category of Net Computations*. Revised version appears in Mosses, Nielsen and Schwartzbach, editors, *Theory and Practice of Software Development: 6th International Conference Joint Conference CAAP/FASE*, TAPSOFT '95 Proceedings, LNCS 915, 1995, pages 334–348 with the title *On the Category of Petri Net Computations*.
Abstract: We introduce the notion of *strong concatenable process* for Petri nets as the least refinement of non-sequential (concatenable) processes which can be expressed abstractly by means of a *functor* $\mathcal{Q}[\_]$ from the category of Petri nets to an appropriate category of symmetric strict monoidal categories with free non-commutative monoids of objects, in the precise sense that, for each net N, the strong concatenable processes of N are isomorphic to the arrows of $\mathcal{Q}[N]$. This yields an axiomatization of the causal behaviour of Petri nets in terms of symmetric strict monoidal categories.

In addition, we identify a *coreflection* right adjoint to $\mathcal{Q}[\_]$ and we characterize its replete image in the category of symmetric monoidal categories, thus yielding an abstract description of the category of net computations.

[RS-94-32] *PostScript*, *DVI*.
Alexander Aiken, Dexter Kozen, and Ed Wimmers.
Decidability of Systems of Set Constraints with Negative Constraints.
October 1994.
33 pp. Appears in *Information and Computation*, 122(1):30-44, October 1995.

Abstract: Set constraints are relations between sets of terms. They have been used extensively in various applications in program analysis and type inference. Recently, several algorithms for solving general systems of positive set constraints have appeared. In this paper we consider systems of mixed positive and negative constraints, which are considerably more expressive than positive constraints alone. We show that it is decidable whether a given such system has a solution. The proof involves a reduction to a number-theoretic decision problem that may be of independent interest.

[RS-94-31] *PostScript*, *DVI*.
Noam Nisan and Amnon Ta-Shma.
Symmetric Logspace is Closed Under Complement.
September 1994.
8 pp.

Abstract: We present a Logspace, many-one reduction from the undirected st-connectivity problem to its complement. This shows that $SL = co - SL$.

[RS-94-30] *PostScript*.
Thore Husfeldt.
Fully Dynamic Transitive Closure in Plane Dags with one Source and one Sink.
September 1994.
26 pp. Appears in Spirakis, editor, *Third Annual European Symposiumon on Algorithms*, ESA '95 Proceedings, LNCS 979, 1995, pages 199–212.

Abstract: We give an algorithm for the Dynamic Transitive Closure Problem for planar directed acyclic graphs with one source and one sink. The graph can be updated in logarithmic time under arbitrary edge insertions and deletions that preserve the embedding. Queries of the form 'is there a directed path from u to v?' for arbitrary vertices u and v can be answered in logarithmic time. The size of the data structure and the initialisation time are linear in the number of edges.

The result enlarges the class of graphs for which a logarithmic (or even polylogarithmic) time dynamic transitive closure algorithm exists. Previously, the only algorithms within the stated resource bounds put restrictions on the topology of the graph or on the delete operation. To obtain our result, we use a new characterisation of the transitive closure in plane graphs with one source and one sink and introduce new techniques to exploit this characterisation.

We also give a lower bound of $\Omega(\log n/\log\log n)$ on the amortised complexity of the problem in the cell probe model with logarithmic word size. This is the first dynamic directed graph problem with almost matching lower and upper bounds.

[RS-94-29] *PostScript*, *DVI*.
Ronald Cramer and Ivan B. Damgrd.
Secure Signature Schemes Based on Interactive Protocols.
September 1994.
24 pp. Appears in Coppersmith, editor, *Advances in Cryptology: 15th Annual International Cryptology Conference*, CRYPTO '95 Proceedings, LNCS 963, 1995, pages 297–310.

Abstract: A method is proposed for constructing from interactive protocols digital signature schemes secure against adaptively chosen message attacks. Our main result is that practical secure signature schemes can now also be based on computationally difficult problems other than factoring, such as the discrete logarithm problem.

More precisely, given only an interactive protocol of a certain type as a primitive, we can build a (non-interactive) signature scheme that is secure in the strongest sense of Goldwasser, Micali and Rivest (GMR): not existentially forgeable under adaptively chosen message attacks. There are numerous examples of primitives that satisfy our conditions, e.g. Feige-Fiat-Shamir, Schnorr, Guillou-Quisquater, Okamoto and Brickell-Mc.Curley.

In fact, the existence of one-way group homomorphisms is a sufficient assumption to support our construction. As we also demonstrate that our construction can be based on claw-free pairs of trapdoor one-way permutations, our results can be viewed as a generalization of the GMR signature scheme.

[RS-94-28] *PostScript*, *DVI*.
Oded Goldreich.
Probabilistic Proof Systems.
September 1994.
19 pp.

Abstract: Various types of *probabilistic* proof systems have played a central role in the development of computer science in the last decade. In this exposition, we concentrate on three such proof systems — *interactive proofs*, *zero-knowledge proofs*, and *probabilistic checkable proofs* — stressing the essential role of randomness in each of them.

This exposition is an expanded version of a survey written for the proceedings of the International Congress of Mathematicians (*ICM94*) held in Zurich in 1994. It is hope that this exposition may be accessible to a broad audience of computer scientists and mathematians.

[RS-94-27] *PostScript*, *DVI*.

Torben Braner.

A Model of Intuitionistic Affine Logic from Stable Domain Theory (Revised and Expanded Version).

September 1994.

19 pp. Full version of paper appearing in Abiteboul and Shamir, editors, *Automata, Languages and Programming: 21st International Colloquium*, ICALP '94 Proceedings, LNCS 820, 1994, pages 340–351. This report is a revised and expanded version of DAIMI IR-118.

Abstract: Girard worked with the category of coherence spaces and continuous stable maps and observed that the functor that forgets the linearity of linear stable maps has a left adjoint. This fundamental observation gave rise to the discovery of Linear Logic. Since then, the category of coherence spaces and linear stable maps, with the comonad induced by the adjunction, has been considered a canonical model of Linear Logic. Now, the same phenomenon is present if we consider the category of pre dI domains and continuous stable maps, and the category of dI domains and linear stable maps; the functor that forgets the linearity has a left adjoint. This gives an alternative model of Intuitionistic Linear Logic. It turns out that this adjunction can be factored in two adjunctions yielding a model of Intuitionistic Affine Logic; the category of pre dI domains and affine stable functions. It is the goal of this paper to show that this category is actually a model of Intuitionistic Affine Logic, and to show that this category moreover has properties which make it possible to use it to model convergence/divergence behaviour and recursion.

[RS-94-26] *PostScript*, *DVI*.

Sren Riis.

Count(q) versus the Pigeon-Hole Principle.

August 1994.

3 pp. Appears in *Archive for Mathematical Logic* 36(3):157–188 (1997) (expanded to a selfcontained paper).

Abstract: For each $p \leq 2$ there exist a model $\mathbb{M}^*$ of $I\Delta_0(\alpha)$ which satisfies the Count(p) principle. Furthermore if p contain all prime factors of q there exist $n, r \in \mathbb{M}^*$ and a bijective map $f \in \mathrm{Set}(\mathbb{M}^*)$ mapping $\{1, 2, ..., n\}$ onto $\{1, 2, ..., n + q^r\}$.

A corollary is a complete classification of the Count(q) versus Count(p) problem. Another corollary solves an open question by M. Ajtai.

[RS-94-25] *PostScript*, *DVI*.

Sren Riis.

Bootstrapping the Primitive Recursive Functions by 47 Colors.

August 1994.

5 pp. Improved version appears in *Decrete Mathematics* 169(1–3):269–272 (1997) under the title *Bootstrapping the Primitive Recursive Functions by Only 27 Colors*.

Abstract: I construct a concrete coloring of the 3 element subsets of *IN*. It has the property that each homogeneous set

$\{s_1, s_2, ..., s_u\}, u \geq s_1$ has its elements spread so much apart that $F_\omega(s_i) < s_{i+1}$ for $i = 1, 2, ..., s_1$. It uses only 47 colors. This is more economical than the approximately 160000 colors used by Ketonen and Solovay.

[RS-94-24] *PostScript*, *DVI*.
Sren Riis.
A Fractal which violates the Axiom of Determinacy.
August 1994.
3 pp.

Abstract: By use of the axiom of choice I construct a symmetrical and elf similar subset $A \subseteq [0,1] \subseteq IR$. hen by an elementary strategy stealing argument it is shown hat A is not determined. The (possible) existence of ractals like A clarifies the status of the controversial xiom of Determinacy.

[RS-94-23] *PostScript*, *DVI*.
Sren Riis.
Finitisation in Bounded Arithmetic.
August 1994.
31 pp. Manuscript presented at The Tenth Workshop on the Mathematical Foundations of Programming Semantics, Kansas, USA, 1994.

Abstract: I prove various results concerning un-decidability in weak fragments of Arithmetic. All results are concerned with $S^1_2 \subseteq T^1_2 \subseteq S^2_2 \subseteq T^2_2 \subseteq ....$ a hierarchy of theories which have already been intensively studied in the literature. Ideally one would like to separate these systems. However this is generally expected to be a very deep problem, closely related to some of the most famous and open problems in complexity theory.

In order to throw some light on the separation problems, I consider the case where the underlying language is enriched by extra relation and function symbols. The paper introduces a new type of results. These state that the first three levels in the hierarchy (i.e. S^1_2, T^1_2 and S^2_2) are never able to distinguish (in a precise sense) the "finite" from the "infinite". The fourth level (i.e. T^2_2) in some cases can make such a distinction. More precisely, elementary principles from finitistical combinatorics (when expressed solely by the extra relation and function symbols) are only provable on the first three levels if they are valid when considered as principles of general (infinitistical) combinatorics. I show that this does not hold for the fourth level.

All results are proved by forcing.

[RS-94-22] *PostScript*, *DVI*.
Torben Braner.
A General Adequacy Result for a Linear Functional Language.
August 1994.
39 pp. Presented at *Mathematical Foundations of Programming Semantics: 10th International Conference*, MFPS '94. Strongly re-

vised version accepted for publication in a special issue of *Theoretical Computer Science* devoted the proceedings of MFPS '94.

Abstract: A main concern of the paper will be a Curry-Howard interpretation of Intuitionistic Linear Logic. It will be extended with recursion, and the resulting functional programming language will be given operational as well as categorical semantics. The two semantics will be related by soundness and adequacy results. The main features of the categorical semantics are that convergence/divergence behaviour is modelled by a strong monad, and that recursion is modelled by "linear fixpoints" induced by CPO structure on the hom-sets. The "linear fixpoints" correspond to ordinary fixpoints in the category of free coalgebras w.r.t. the comonad used to interpret the "of course" modality. Concrete categories from (stable) domain theory satisfying the axioms of the categorical model are given, and thus adequacy follows in these instances from the general result.

[RS-94-21] *PostScript*, *DVI*.
Sren Riis.
Count(q) does not imply Count(p).
July 1994.
55 pp. Appears in *Annals of Pure and Applied Logic* 90(1–3):1–56 (1997).

Abstract: I solve a conjecture originally studied by M.Ajtai. It states that for different primes q, p the matching principles Count(q) and Count(p) are logically independent. I prove that this indeed is the case. Actually I show that Count(q) implies Count(p) exactly when each prime in p also is a factor in q.

[RS-94-20] *PostScript*, *DVI*.
Peter D. Mosses and Martn Musicante.
An Action Semantics for ML Concurrency Primitives.
July 1994.
21 pp. Appears in Naftalin, Denvir and Bertran, editors, *Industrial Benefit of Formal Methods: First International Symposium of Formal Methods Europe*, FME '94 Proceedings, LNCS 873, 1994, pages 461–479.

Abstract: This paper is about the recently-developed framework of action semantics. The pragmatic qualities of action semantic descriptions are particularly good, which encourages their use in industrial-scale applications where semantic descriptions are needed, e.g., compiler development.

The paper has two main aims: to demonstrate the remarkable extensibility of action semantic descriptions, and to illustrate the action semantics treatment of concurrency. These aims are achieved simultaneously, by first giving the description of a sequential (ML-like) programming language fragment, and then extending the described language with some concurrency primitives (taken from CML). The action semantic description of the sequential part of the language *does not change at all* when the concurrency primitives are added, it merely gets augmented by

the description of the new features!

[RS-94-19] *PostScript.*
Jens Chr. Godskesen, Kim G. Larsen, and Arne Skou.
Automatic Verification of Real–Timed Systems Using EPSILON.
June 1994.
8 pp. Appears in Voung and Chanson, editors, *Fourteenth International IFIP Symposium on Protocol Specification, Testing and Verification*, PSTV '94 Proceedings, 1994, pages 323–330.

Abstract: In this paper we report on an application and extension of the theory of *Timed Modal Specifications* (TMS) and its associated verification tool EPSILON. The novel feature with which EPSILON has been extended is the ability to automatically generate *diagnostic information* in cases of erroneous refinement steps.

[RS-94-18] *PostScript, DVI.*
Sten Agerholm.
LCF Examples in HOL.
June 1994.
16 pp. Revised version appears in *The Computer Journal*, 38(2): 121–130, 1995. Also in Melham and Camilleri, editors, *Higher Order Logic Theorem Proving and Its Applications: 7th International Workshop*, HOLTPA '94 Proceedings, LNCS 859, 1994, pages 1–16.

Abstract: The LCF system provides a logic of fixed point theory and is useful to reason about non-termination, arbitrary recursive definitions and infinite types as lazy lists. It is unsuitable for reasoning about finite types and strict functions. The HOL system provides set theory and supports reasoning about finite types and total functions well. In this paper a number of examples are used to demonstrate that an extension of HOL with domain theory combines the benefits of both systems. The examples illustrate reasoning about infinite values and non-terminating functions and show how mixing domain and set theoretic reasoning eases reasoning about finite LCF types and strict functions. An example presents a proof of the correctness and termination of a recursive unification algorithm using well-founded induction.

[RS-94-17] Allan Cheng.
Local Model Checking and Traces.
June 1994.
30 pp. Please refer to the revised version BRICS-RS-95-39.

Abstract: We present a *CTL*-like logic which is interpreted over labeled asynchronous transition systems. The interpretation reflects the desire to reason about these only with respect their progress fair behaviours. For finite systems we provide a set of tableau rules and prove soundness and completeness with respect to the given interpretation of our logic. We also provide a model checking algorithm which solves the model checking problem in deterministic polynomial time in the size of the formula and the labelled asynchronous transition system. We then consider different extensions of the logic with modalities expressing concurrent behaviour and investigate how this affects the decidability of the satisfiability problem.

[RS-94-16] Lars Arge.
External-Storage Data Structures for Plane-Sweep Algorithms.
June 1994.
37 pp. Revised version appears in Akl, Dehne, Sack and Santoro, editors, *Algorithms and Data Structures: 4th Workshop*, WADS '95 Proceedings, LNCS 955, 1995, pages 334–345. Please refer to the revised and extended version BRICS-RS-96-28.
Abstract: In this paper we develop a technique for transforming an internal memory datastructure into an external storage data structure suitable for plane-sweep algorithms. We use this technique to develop external storage versions of the range tree and the segment tree. We also obtain an external priority queue. Using the first two structures, we solve the orthogonal segment intersection, the isothetic rectangle intersection, and the batched range searching problem in the optimal number of I/O-operations. Unlike previously known I/O-algorithms the developed algorithms are straightforward generalizations of the ordinary internal memory plane-sweep algorithms. Previously almost no dynamic data structures were known for the model we are working in.

[RS-94-15] Mogens Nielsen and Glynn Winskel.
Petri Nets and Bisimulations.
May 1994.
36 pp. Please refer to the revised and corrected version BRICS-RS-95-4.
Abstract: Several categorical relationships (adjunctions) between models for concurrency have been established, allowing the translation of concepts and properties from one model to another. The purpose of the present paper is twofold: firstly to present a central example of such a relationship (a coreflection between asynchronous transition systems and Petri nets), and secondly to illustrate its use by transferring to nets a general concept of bisimulation.

[RS-94-14] *PostScript.*
Nils Klarlund.
The Limit View of Infinite Computations.
May 1994.
16 pp. Appears in Jonsson and Parrow, editors, *Concurrency Theory: 5th International Conference*, CONCUR '94 Proceedings, LNCS 836, 1994, pages 351–366.
Abstract: We show how to view computations involving very general liveness properties as limits of finite approximations. This computational model does not require introduction of infinite nondeterminism as with most traditional approaches. Our results allow us directly to relate finite computations in order to infer properties about infinite computations. Thus we are able to

provide a mathematical understanding of what simulations and bisimulations are when liveness is involved.

In addition, we establish links between verification theory and classical results in descriptive set theory. Our result on simulations is the essential contents of the Kleene-Suslin Theorem, and our result on bisimulation expresses Martin's Theorem about the determinacy of Borel games.

[RS-94-13] *PostScript*, *DVI*.
Glynn Winskel.
Stable Bistructure Models of PCF.
May 1994.
26 pp. *Preliminary draft.* Invited lecture for MFCS '94. Appears in Prvara, Rovan and Ruzicka, editors, *Mathematical Foundations of Computer Science: 19th International Symposium*, MFCS '94 Proceedings, LNCS 841, 1994, pages 177–197.

Abstract: Stable bistructures are a generalisation of event structures to represent spaces of functions at higher types; the partial order of causal dependency is replaced by two orders, one associated with input and the other output in the behaviour of functions. They represent Berry's bidomains. The representation can proceed in two stages. Bistructures form a categorical model of Girard's linear logic consisting of a linear category together with a comonad. The comonad has a co-Kleisli category which is equivalent to a cartesian-closed full subcategory of Berry's bidomains. A main motivation for bidomains came from the full abstraction problem for Plotkin's functional language PCF. However, although the bidomain model incorporates both the Berry stable order and the Scott pointwise order, its PCF theory (those inequalities on terms which hold in the bidomain model) does not include that of the Scott model. With a simple modification we can obtain a new model of PCF, combining the Berry and Scott orders, which does not have this inadequacy.

[RS-94-12] Glynn Winskel and Mogens Nielsen.
Models for Concurrency.
May 1994.
144 pp. Appears as a chapter in the *Handbook of Logic and the Foundations of Computer Science*, vol. 4, pages 1–148, Oxford University Press, 1995.

Abstract: This report surveys a range of models for parallel computation to include interleaving models like transition systems, synchronisation trees and languages (often called Hoare traces in this context), and models like Petri nets, asynchronous transition systems, event structures, pomsets and Mazurkiewicz traces where concurrency is represented more explicitly by a form of causal independence. The presentation is unified by casting the models in a category-theoretic framework. One aim is to use category theory to provide abstract characterisations of constructions like parallel composition valid throughout a range of different models and to provide formal means for translating between dif-

ferent models.

A knowledge of basic category theory is assumed, up to an acquaintance with the notion of adjunction.

[RS-94-11] *PostScript*.
Nils Klarlund.
A Homomorphism Concept for ω-Regularity.
May 1994.
16 pp. Appears in Pacholski and Tiuryn, editors, *European Association for Computer Science Logic: 8th Workshop*, CSL '94 Selected Papers, LNCS 933, 1995, pages 471–485.

Abstract: The Myhill-Nerode Theorem (that for any regular language, there is a canonical recognizing device) is of paramount importance for the computational handling of many formalisms about finite words.

For infinite words, no prior concept of homomorphism or structural comparison seems to have generalized the Myhill-Nerode Theorem in the sense that the concept is both language preserving and representable by automata.

In this paper, we propose such a concept based on Families of Right Congruences (Maler and Staiger 93), which we view as a recognizing structures.

We also establish an exponential lower and upper bound on the change in size when a representation is reduced to its canonical form.

[RS-94-10] *PostScript*.
Jakob L. Jensen, Michael E. Jrgensen, and Nils Klarlund.
Monadic Second-order Logic for Parameterized Verification.
May 1994.
14 pp.

Abstract: Much work in automatic verification considers families of similar finite-state systems. But an often overlooked property is that sometimes a single finite-state system can be used to describe a parameterized, infinite family of systems. Thus verification of unbounded state spaces can take place by reduction to finite ones.

The purpose of this article is to introduce Monadic Second-order Logic as a practical means of carrying out such reductions. The logic is a highly succinct alternative to the use of regular expressions. We have built a tool that acts as a decision procedure and translator to DFAs.

The potential applications are numerous. We discuss text processing, Boolean circuits, and distributed systems. Our main example is an automatic proof of properties for the "Dining Philosophers with Encyclopedia" example by Kurshan and MacMillan. We establish these properties for the parameterized case *without* the use of induction.

[RS-94-9] *PostScript*, *DVI*.
Gordon Plotkin and Glynn Winskel.

Bistructures, Bidomains and Linear Logic.
May 1994.
16 pp. Appears in Abiteboul and Shamir, editors, *Automata, Languages and Programming: 21st International Colloquium*, ICALP '94 Proceedings, LNCS 820, 1994, pages 352–363.

Abstract: Bistructures are a generalisation of event structures to represent spaces of functions at higher types; the partial order of causal dependency is replaced by two orders, one associated with input and the other output in the behaviour of functions. Bistructures form a categorical model of Girard's classical linear logic in which the involution of linear logic is modelled, roughly speaking, by a reversal of the roles of input and output. The comonad of the model has associated co-Kleisli category which is equivalent to a cartesian-closed full subcategory of Berry's bidomains.

[RS-94-8] *PostScript*, *DVI.*
Javier Esparza and Mogens Nielsen.
Decidability Issues for Petri Nets.
May 1994.
23 pp. Appears in *Journal of Information Processing and Cybernet. EIK*, 30:143–160, 1994.

Abstract: This is a survey of some decidability results for Petri nets, covering the last three decades. The presentation is structured around decidability of specific *properties*, various behavioural *equivalences* and finally the model checking problem for *temporal logics.*

[RS-94-7] *PostScript*, *DVI.*
Andr Joyal, Mogens Nielsen, and Glynn Winskel.
Bisimulation from Open Maps.
May 1994.
42 pp. Appears in LICS '93 special issue of *Information and Computation*, 127(2):164–185, June 1986.

Abstract: An abstract definition of bisimulation is presented. It enables a uniform definition of bisimulation across a range of different models for parallel computation presented as categories. As examples, transition systems, synchronisation trees, transition systems with independence (an abstraction from Petri nets) and labelled event structures are considered. On transition systems the abstract definition readily specialises to Milner's strong bisimulation. On event structures it explains and leads to a revision of history-preserving bisimulation of Rabinovitch and Traktenbrot, Goltz and van Glabeek. A tie-up with open maps in a (pre)topos, as they appear in the work of Joyal and Moerdijk, brings to light a promising new model, presheaves on categories of pomsets, into which the usual category of labelled event structures embeds fully and faithfully. As an indication of its promise, this new presheaf model has "refinement" operators, though further work is required to justify their appropriateness and understand their relation to previous attempts. The general approach yields a logic, generalising Hennessy-Milner logic, which is characteristic for the generalised notion of bisimulation.

[RS-94-6] *PostScript*, *DVI*.
Mogens Nielsen and Christian Clausen.
Bisimulations, Games, and Logic.
April 1994.
37 pp. Full version of paper appearing in Karhumki, Maurer and Rozenberg, editors, *Results and Trends in Theoretical Computer Science: Colloquium in Honor of Arto Salomaa*, RTTCS '94 Selected Papers, LNCS 812, 1994, pages 289–305.
Abstract: In a recent paper by Joyal, Nielsen, and Winskel, bisimulation is defined in an abstract and uniform way across a wide range of different models for concurrency. In this paper, following a recent trend in theoretical computer science, we characterize their abstract definition game-theoretically and logically in a non-interleaving model. Our characterizations appear as surprisingly simple extensions of corresponding characterizations of interleaving bisimulation.

[RS-94-5] *PostScript*, *DVI*.
Peter D. Mosses.
Unified Algebras and Abstract Syntax.
March 1994.
21 pp. Appears in Ehrig and Orejas, editors, *Recent Trends in Data Type Specification, 9th Workshop on Specification of Abstract Data Types*, RTDTS '92 Selected Papers, LNCS 785, 1994, pages 280–294.
Abstract: We consider the algebraic specification of abstract syntax in the framework of unified algebras. We illustrate the expressiveness of unified algebraic specifications, and provide a grammar-like notation for specifying abstract syntax, particularly attractive for use in semantic descriptions of full-scale programming languages.

[RS-94-4] *PostScript*, *DVI*.
Nils Klarlund and Michael I. Schwartzbach.
Graphs and Decidable Transductions based on Edge Constraints.
February 1994.
19 pp. Appears in Tison, editor, *Trees in Algebra and Programming: 19th International Colloquium*, CAAP '94 Proceedings, LNCS 787, 1994, pages 187–201.
Abstract: We give examples to show that not even **c-edNCE**, the most general known notion of context-free graph grammar, is suited for the specification of some common data structures.

To overcome this problem, we use monadic second-order logic and introduce *edge constraints* as a new means of specifying a large class of graph families. Our notion stems from a natural dichotomy found in programming practice between ordinary pointers forming spanning trees and auxiliary pointers cutting across.

Our main result is that for certain transformations of graphs definable in monadic second-order logic, the question of whether a graph family given by a specification $\mathcal{A}$ is mapped to a family given by a specification $\mathcal{B}$ is decidable. Thus a decidable Hoare logic arises.

[RS-94-3] *PostScript*, *DVI*.
Uffe H. Engberg and Glynn Winskel.
Linear Logic on Petri Nets.
February 1994.
54 pp. Appears in Bakker, de Roever and Rozenberg, editors, *A Decade of Concurrency: Reflections and Perspectives, REX School/Symposium*, REX '94 Proceedings, LNCS 803, 1994, pages 176–229.

Abstract: This article shows how individual Petri nets form models of Girard's intuitionistic linear logic. It explores questions of expressiveness and completeness of linear logic with respect to this interpretation. An aim is to use Petri nets to give an understanding of linear logic and give some appraisal of the value of linear logic as a specification logic for Petri nets. This article might serve as a tutorial, providing one in-road into Girard's linear logic via Petri nets. With this in mind we have added several exercises and their solutions. We have made no attempt to be exhaustive in our treatment, dedicating our treatment to one semantics of intuitionistic linear logic.

Completeness is shown for several versions of Girard's linear logic with respect to Petri nets as the class of models. The strongest logic considered is intuitionistic linear logic, with $\otimes$, $\multimap$, $\&$, $\oplus$ and the exponential ! ("of course"), and forms of quantification. This logic is shown sound and complete with respect to *atomic nets* (these include nets in which every transition leads to a nonempty multiset of places). The logic is remarkably expressive, enabling descriptions of the kinds of properties one might wish to show of nets; in particular, negative properties, asserting the impossibility of an assertion, can also be expressed. A start is made on decidability issues.

[RS-94-2] *PostScript*, *DVI*.
Alexander E. Andreev.
Complexity of Nondeterministic Functions.
February 1994.
47 pp.

Abstract: The complexity of a nondeterministic function is the minimum possible complexity of its determinisation. The entropy of a nondeterministic function, F, is minus the logarithm of the ratio between the number of determinisations of F and the number of all deterministic functions.

We obtain an upper bound on the complexity of a nondeterministic function with restricted entropy for the worst case.

These bounds have strong applications in the problem of algorithm derandomization. A lot of randomized algorithms can be converted to deterministic ones if we have an effective hitting set

with certain parameters (a set is hitting for a set system if it has a nonempty intersection with any set from the system).

Linial, Luby, Saks and Zuckerman (1993) constructed the best effective hitting set for the system of k-value, n-dimensional rectangles. The set size is polynomial in $k(\log n)/\epsilon$.

Our bounds of nondeterministic functions complexity offer a possibility to construct an effective hitting set for this system with almost linear size in $k(\log n)/\epsilon$.

[RS-94-1] *PostScript.*

Glynn Winskel.

Semantics, Algorithmics and Logic: Basic Research in Computer Science. BRICS Inaugural Talk.

February 1994.

8 pp.

Abstract: This is a transcript of a talk at the inauguration of BRICS, Basic Research in Computer Science, Centre of the Danish Research Foundation, on 2 February 1994 at the Steno museum, University of Aarhus, Denmark.