Paliath Narendran

Personal Information

Home address	17 Crestwood Drive Clifton Park, NY 12065
Office address	Department of Computer Science University at Albany — State University of NY Albany, NY 12222
Phone numbers	(518)383-6720 (home) (518)442-3387 (work)
Citizenship:	United States
E-mail address:	pnarendran@albany.edu
Web page:	http://www.cs.albany.edu/˜dran/

Education

Ph.D. (1984)	Computer Science	Rensselaer Polytechnic Institute, Troy NY 12181. Thesis title: *Church-Rosser and Related Thue Systems.* Advisor: Robert McNaughton
M.Tech. (1980)	Computer Science	Indian Institute of Technology, Madras, India
B.Tech. (1978)	Electrical Engineering	Indian Institute of Technology, Madras, India

Professional Experience

Nov. 1983 to August 1988	Computer Science Branch General Electric Corporate Research and Development Schenectady, NY.
Sept. 1988 to August 1989	Visiting Research Associate Department of Computer Science University of Calgary Calgary, Alberta T2N 1N4
Sept. 1989 to August 1994	Visiting Associate Professor Department of Computer Science University at Albany — State University of NY Albany, NY 12222
Sept. 1994 to Jan. 2003	Associate Professor Department of Computer Science University at Albany — State University of NY Albany, NY 12222

Jan. 2003 to present	Professor Department of Computer Science University at Albany — State University of NY Albany, NY 12222

Research Interests

Automated reasoning, Formal specification and verification methods, Protocol analysis.

Publications

Journals:	47
Refereed Conference Papers:	69
Technical Reports:	12

Patents

[1] "Digital Circuit Design Verification," (with D. Musser and W. Premerlani) US Patent No. 4,872,126, October 3, 1989.

Grants and Awards

- Collaborative Research: Unification Laboratory: Increasing the Power of Cryptographic Protocol Analysis Tools (with D. Kapur, J. Meseguer and C. Lynch), National Science Foundation grant CNS-0905286, Sep 1, 2009—Aug 31, 2013, $239,085 (my share of the grant).
- Collaborative Research: Unification Laboratory for Cryptographic Protocol Analysis (with D. Kapur, J. Meseguer and C. Lynch), National Science Foundation grant CNS-0831209, Sep 1, 2008—Aug 31, 2009, $74,999 (my share of the grant). An additional supplement of $8,000 was awarded for supporting undergraduate research.
- Equational Unification for Cryptographic Protocol Analysis (with D. Kapur and C. Lynch), Office of Naval Research (ONR) grant subcontracted through ITT Industries, Inc., Fiscal Year 2002, $10,000 (my share of the grant).
- Collaborative Research on Semantic Unification and its Applications (with D. Kapur and C. Lynch), National Science Foundation grant CCR-0098095, Aug 15, 2001—July 31, 2004, $119,588 (my share of the grant).
- Equational Unification for Cryptographic Protocol Analysis (with D. Kapur and C. Lynch), Office of Naval Research (ONR) grant, Feb 15, 2001—Dec 31, 2001, $53,624 (my share of the grant).
- NYSUT Term Faculty Development Awards Program Travel Award, 1999.
- Equality Reasoning: Word and Unification Problems (with D. Kapur), National Science Foundation grant CCR-9712396, Sept 1, 1997—Aug 31, 1999, $161,887.
- Faculty Research Awards Program (FRAP), 1997-8. Project title: Hybrid Systems.
- Constraint-solving, Unification and Automated Reasoning and their application to Formal Verification Methods (with D. Kapur), National Research Council Travel award, Jan 1, 1997—Jan 31, 1998, $3,000.
- Research on Unification and Related Problems (with D. Kapur), NSF grant CCR-9404930, Dec 1, 1994—Nov 30, 1996, $61,853.
- Collaborative Research on Word & Unification Problems and Automated Reasoning (with D. Kapur), NSF grant INT-9401087, Aug 15, 1994—July 31, 1997, $22,743.

- Dean's Faculty Support Fund (DFSF), 1994-5.
- Faculty Research Awards Program (FRAP), 1994-5. Project title: Semantic Unification and Pattern Matching.
- NYSUT Term Faculty Development Awards Program Travel Award, 1993.
- Faculty Research Awards Program (FRAP), 1992-3. Project title: Formal Hardware Verification.
- NSF Travel Award CCR-9204363, Summer 1992.
- Faculty Research Awards Program (FRAP), 1990-1. Project title: Formal Hardware Verification.
- co-PI in NSF grant MIP-89-02558, 1989–92 (PI: Ganesh Gopalakrishnan).
- Air Force Contract F33615-85-C-1862, AFWAL, Wright-Patterson Air Force Base, Dayton, Ohio, 1986–1988. (I was instrumental in obtaining funding for Hardware Verification.)
- Investigator in NSF grant DCR-84-08461 (PI: Deepak Kapur).
- Investigator in NSF grant MCS-83-02123 (PI: Robert McNaughton).

Professional Activities

- Program Committee of the 1st International Conference on Information Systems Security and Privacy (ICISSP 2015), 2015.
- Program Committee of the 8th International Conference on Language and Automata Theory and Applications (LATA 2014), 2014.
- Program Committee of the 7th International Conference on Language and Automata Theory and Applications (LATA 2013), 2013.
- Program Committee of the Twenty-Second International Conference on Rewriting Techniques and Applications (RTA'11), 2011.
- Co-chair, Program Committee of SecReT'10, International Workshop on Security and Rewriting Techniques.
- Program Committee of SecReT'09, International Workshop on Security and Rewriting Techniques.
- Program Committee of the Nineteenth International Conference on Rewriting Techniques and Applications (RTA'08), 2008.
- Program Committee of the 3rd Annual Symposium on Information Assurance, Albany, NY, June 4–5, 2008.
- Program Committee of SecReT'07, International Workshop on Security and Rewriting Techniques.
- Visiting Research Associate of Institut National de Recherche en Informatique et en Automatique (INRIA) in Nancy, France in July 2006.
- Visiting professor at the Universite d'Orleans, June 2006.
- Program Committee of FTP-2005, the fifth International Workshop on First order Theorem Proving.
- Visiting professor at the Ecole Normale Superieure, Cachan, France, June 2004.
- Program Committee of the Second International Joint Conference on Automated Reasoning (IJCAR-2004).
- Visiting professor at the Universite d'Orleans, June 2003.
- Program Committee of FTP-2003, the fourth International Workshop on First order Theorem Proving.

- Program Committee of the 2003 IEEE Symposium on Logic in Computer Science (LICS-2003).
- Program Committee of 18th National Conference of the American Association for Artificial Intelligence (AAAI-02).
- Steering Committee of the International Workshops on First-Order Theorem Proving (FTP), 2001–2004.
- Program Committee of the 19th International Conference on Automated Deduction (CADE-19).
- Visiting Research Associate of Institut National de Recherche en Informatique et en Automatique (INRIA) in Nancy, France in July 2001.
- External member of Ph. D. Dissertation Committee for Zahir Maazouzi, Laboratoire d'Informatique Fondamentale d'Orleans (LIFO), Universite d'Orleans, June 2001.
- Visiting professor at the Universite d'Orleans, June 2001.
- Founding member of working group WG 1.6 (Term Rewriting) of the International Federation for Information Processing (IFIP).
- Program Committee of the 17th International Conference on Automated Deduction (CADE-17).
- Program Committee of the 19th conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS), 1999.
- Co-chair, Program Committee of the Tenth International Conference on Rewriting Techniques and Applications (RTA'99), 1999.
- Visiting professor at the Universite d'Orleans, June 1999.
- Visiting Research Associate of Institut National de Recherche en Informatique et en Automatique (INRIA) in Nancy, France in May–August 1997.
- July '96–July '99: Organizing Committee of the International Conference on Rewriting Techniques and Applications (RTA).
- Program Committee of the Eighth International Conference on Rewriting Techniques and Applications (RTA'97), 1997.
- Program Committee of the Seventh International Conference on Rewriting Techniques and Applications (RTA'96), 1996.
- Invited to give a tutorial on complexity issues in Automated Theorem Proving at the International Conference on Logic Programming and Automated Reasoning (LPAR'94), Kiev, Ukraine, July 1994.
- Visiting Scientist, University of Kaiserslautern, Germany, June 1995.
- Professeur Invité, University of Paris-Sud, Orsay, France, May 15–June 15, 1994.
- Program Committee of the Fifth International Conference on Rewriting Techniques and Applications (RTA'93), 1993.
- Consultant (Summer 1991), SRI International, Palo Alto, CA.
- Visiting Research Associate of Le Centre de Recherche en Informatique de Nancy (CRIN) in Nancy, France in July 1990.
- External member of Ph.D. Dissertation Committee for Wayne Snyder, Department of Computer Science, Univ. of Pennsylvania, Philadelphia, 1988.

University Service

Fall 13 & Spring 14	Co-Chair of the Omnibus Faculty Search Committee.
Fall 05–Spring 07:	Chair of the Faculty Search Committee.
Spring 04–Present:	Departmental Tenure and Promotion Committee.
Spring 02:	Ad hoc committee for selecting Departmental Chair.
Spring 00:	Co-organizer of *Perspectives on Computer Science: A Symposium in Honor of Richard Stearns,* June 5-6.
Fall 00 & Spring 01:	College Nominating Committee.
Fall 99–Present:	Undergraduate Curriculum Committee. (Chair, Fall 00 thru Fall 03)
Fall 99 & Spring 00:	College Academic Support Committee.
Fall 96:	Organized the Formal Methods and Automated Reasoning Day.
Spring 96:	Ad hoc committee for selecting Departmental Chair.
Fall 95–Spring 97:	College Academic Support Committee.
Fall 94–Fall 95:	Council on Libraries, and Information Systems and Computing (LISC).
Fall 94 & Spring 95:	College Academic Programs Committee.
Fall 94 & Spring 95:	College Diversity Committee.
Spring 94–Spring 97:	College of Arts and Sciences Council.
Spring 94:	College Student Grievance Committee.
Spring 94:	Chair, Graduate Curriculum Committee.
Fall 94–Present:	Graduate Admissions Committee.
Spring 94–Fall 95:	TA assignment Co-ordinator in the department.
Spring 94:	Student Recruitment—Contacting prospective students by telephone.
Spring 94:	Volunteer for the Hartmanis-Stearns Symposium, March 17-18.
Fall 93–Fall 03:	Colloquium Co-ordinator in the department.
Fall 93–Fall 95:	M.S. Comprehensive exam Co-ordinator.
Fall 91–Present:	Member, Graduate Curriculum Committee.
Fall 89–91:	Undergrad. Curriculum Committee.
Fall 89–Present:	Discrete Mathematics Exam Committee.
Fall 89–Present:	Graduate and Undergraduate Advising.

Ph.D Analytic exam committees:

Theory	Fall 89–Present
Math Foundations	Fall 92–Spring 97
Programming Languages	Fall 93–Present

Teaching

Courses taught

CSI 311	Principles of Programming Languages	Spring 01, Spring 02, Spring 03, Spring 08
CSI 404	Computer Organization	Fall 93, Fall 94, Fall 95, Fall 96, Fall 98, Fall 99, Summer 00
CSI 409	Automata and Formal Languages	Spring 92, Spring 93, Spring 96–Spring 00, Fall 00–Fall 16
CSI 421	Discrete Mathematics with Applications	Fall 91, Fall 92
CSI 426	Cryptography	Spring 04, Spring 05, Spring 07, Spring 09, Spring 11, Spring 14
CSI 519	Programming Languages	Spring 94–97, Spring 99 Spring 00–Spring 10, Fall 10–16
CSI 521	Discrete Mathematics with Applications	Fall 91, Fall 92
CSI 526	Cryptography	Spring 04, Spring 05, Spring 07, Spring 09, Spring 11, Spring 14
CSI 538	Computational Logic	Spring 06, Spring 10, Spring 13, Spring 15, Spring 16
CSI 601	Computability	Spring 90, Spring 91, Fall 93, Fall 94
CSI 620	Formal Hardware Verification	Fall 89, Fall 90, Fall 91
	Logic Programming	Spring 91
CSI 628	Cryptographic Protocols	Fall 04–Fall 09
CSI 630	Computational Logic	Spring 93
CSI 670	Topics in Specification and Verification	Spring 98, Fall 00, Fall 01, Fall 02, Fall 03

Doctoral Students

May 1989	Jonathan Stillman[1]	Title:	*Computational Problems in Equational Theorem Proving.*
May 1994	J.C. Hidalgo	Title:	*Algebraic Modelling of MOS Circuits.* Distinguished Dissertation Award, May 1994.
May 1997	Qing Guo	Title:	*Nilpotence, Bisimulation and the Unification Workbench.*
May 2005	Lida Wang	Title:	*Equational unification and its applications in formal verification of cryptographic protocols.* Distinguished Dissertation Award, May 2005.
May 2010	Ben Carle	Title:	*Beyond Regular: Pattern Matching with Extended Regular Expressions*
May 2012	Serdar Erbatur	Title:	*Unification Modulo Theories of Blind Signatures*
May 2012	Andrew Marshall	Title:	*Equational Unification: Algorithms And Complexity with Applications to Cryptographic Protocol Analysis*
May 2015	Kimberly Gero	Title:	*Deciding Static Inclusion for* Δ*-Strong and* $\omega\nabla$*-Strong Intruder Theories: Applications To Cryptographic Protocol Analysis*
May 2015	Peter Hibbs	Title:	*Unification Modulo Common List Functions*

[1] Jonathan Stillman's thesis work was carried out under my supervision. However, at the time of his thesis defense, I was not on the Computer Science faculty at the University at Albany and Professor Harry B. Hunt III was Stillman's official thesis advisor.

Masters Students

Spring 1994	Simona Babiceanu	Title:	“Semi-unification”
Spring 1996	Li Chou	Title:	“User Interface to the Unification Workbench”
Fall 1996	Qing Guo	Title:	“Second-order AC-matching”
Spring 1998	Kyungmin Kim	Title:	“A Java User Interface to the Unification Workbench”
Fall 2000	David Gosman	Title:	“Bottom-up Method for Proving Safety of Security Protocols”
Fall 2004	Rachel Pocino	Title:	“Producing an EPS graph of a plaintext tabular DFA”
Fall 2004	Michael Loegering	Title:	“Generation of Decimal Expansions of Irrational Numbers for Use in One-Time Pad Cryptography”
Spring 2006	Nrupi Patel	Title:	“On Factorizing Products of Large Primes”
Spring 2008	Gagandeep Jaswal	Title:	“Synchronized Regular Expressions”
Fall 2008	Hitesh Kumar	Title:	“Unification modulo a partial theory of exponentiation”
Spring 2009	Bibhu Mahapatra	Title:	“An Implementation of Tiden-Arnborg Algorithm for Unification modulo One-Sided Distributivity”
Fall 2009	Bingqiao Zhou	Title:	“Implementation of a Unification Algorithm modulo the Theory of *map*”
Spring 2010	Jingyi Lu	Title:	“An Implementation of an Algorithm for Set Partition Enumeration”
Spring 2010	Serdar Erbatur	Title:	“An Implementation of an Abelian Group Unification Algorithm”
Fall 2011	Kimberly Gero	Title:	“Elementary Unification Modulo List Length”
Spring 2012	Peter Hibbs	Title:	“Unification on Inverses Over Non-Commutative Group Operations”
Fall 2012	Christopher Bouchard	Title:	“Implementing Unification modulo Chaining”
Fall 2012	Swati Bhatt	Title:	“An Implementation of Forward Closure for Convergent Term Rewriting Systems”
Fall 2013	Andrew Pulver	Title:	“A Study of the Paterson-Wegman Algorithm and its Variants”

Publication List

Edited Conference Proceedings

[1] Rewriting techniques and applications : 10th international conference, RTA-99, Trento, Italy, July 1999, proceedings (Paliath Narendran, Michael Rusinowitch, eds.). *Lecture Notes in Computer Science* 1631, Springer, 1999.

Selected papers appear in a special issue of *Information and Computation,* volume 178 (2) 2002.

Journals

2014:

[1] “Unification modulo a 2-sorted Equational theory for Cipher-Decipher Block Chaining,” (with S. Anantharaman, C. Bouchard and M. Rusinowitch) *Logical Methods in Computer Science* 10(1) 2014.

2012:

[1] “Unification Modulo Homomorphic Encryption,” (with S. Anantharaman, H. Lin, C. Lynch and M. Rusinowitch) *Journal of Automated Reasoning* 48 135–158, 2012.

2011:

[1] “String rewriting and security analysis: An extension of a result of Book and Otto,” *Journal of Automata, Languages and Combinatorics* 16(2-4):75–90, 2011.

[2] “Unification over distributive exponentiation (sub)theories,” (with S. Erbatur, A.M. Marshall and D. Kapur) *Journal of Automata, Languages and Combinatorics* 16(2-4):109–140, 2011.

2005:

[1] “Closure Properties and Decision Problems of Dag Automata,” (with S. Anantharaman and M. Rusinowitch) *Information Processing Letters* 94 (5) 231–240, 2005.

2004:

[1] “Unification modulo *ACUI* plus distributivity Axioms,” (with S. Anantharaman and M. Rusinowitch) *Journal of Automated Reasoning* 33 (1) 1–28, 2004.

2003:

[1] “Deciding the confluence of ordered term rewrite systems,” (with H. Comon, R. Nieuwenhuis and M. Rusinowitch) *ACM Transactions on Computational Logic* 4(1), pages 33–55, 2003.

2001:

[1] “Unification of Concept Terms in Description Logics,” (with F. Baader) *J. Symbolic Computation,* 31 (3) 277–305, 2001.

2000:

[1] "Decidability and Complexity of SREU with one variable and related results," (with A. Degtyarev, Y. Gurevich, M. Veanes, and A. Voronkov) *Theoretical Computer Science* 243 (1-2) 167–184, 2000.

[2] "Unification and Matching modulo Nilpotence," (with Q. Guo and D. Wolfram) *Information and Computation* 162 (1-2): 3-23 (2000).

1998:

[1] "Equational unification, word unification and 2nd-order equational unification," (with F. Otto and D. Dougherty) *Theoretical Computer Science* 198, 1–47, 1998.

1997:

[1] "On the Unification Problem for Cartesian Closed Categories," (with F. Pfenning and R. Statman) *Journal of Symbolic Logic* 62 (2) June 1997, 636–647.

[2] "Single versus Simultaneous Equational Unification and Equational Unification for Variable-Permuting Theories," (with F. Otto) *Journal of Automated Reasoning* 19: 87–115, 1997.

1996:

[1] "Unification modulo ACI + 1 + 0," *Fundamenta Informaticae* 25 (1) 1996, 49–57.

[2] "Any Ground Associative-Commutative Theory has a Finite Canonical System," (with M. Rusinowitch) *Journal of Automated Reasoning* 17 (1) 1996, 131–143.

1994:

[1] "Codes modulo finite monadic and confluent Thue systems," (with F. Otto) *Theoretical Computer Science* 134, 1994, 175–188.

1993:

[1] "On Weakly Confluent Monadic String-Rewriting Systems," (with K. Madlener, F. Otto and L. Zhang) *Theoretical Computer Science* 113 (1993) 119-165.

[2] "An Algorithm for Finding Canonical Sets of Ground Rewrite Rules in Polynomial Time," (with J. Gallier, D. Plaisted, S. Raatz and W. Snyder) *JACM* 40 (1), Jan 1993, 1-16.

1992:

[1] "Complexity of Unification Problems with Associative-Commutative Operators," (with D. Kapur) *Journal of Automated Reasoning* 9 (2) 261–288, 1992.

[2] "Theorem Proving Using Equational Matings and Rigid E-Unification," (with J. Gallier, S. Raatz and W. Snyder) *JACM* 39 (2), April 1992, 377–429.

1991:

[1] "It is Undecidable whether a Finite Special String-Rewriting System Presents a Group," (with C. Ó'Dúnlaing and F. Otto) *Discrete Mathematics* 98 (1991) 153–159.

[2] "Automating Inductionless Induction using Test Sets," (with D. Kapur and H. Zhang) *Journal of Symbolic Computation* 11 (1991) 83-111.

[3] "Sufficient Completeness, Ground-Reducibility and Their Complexity," (with D. Kapur, D.J. Rosenkrantz and H. Zhang) *Acta Informatica* 28 (1991) 311-350.

[4] "Semi-unification," (with D. Kapur, D. Musser, and J. Stillman) *Theoretical Computer Science* 81 (1991) 169-187.

1990:

[1] "Rigid E-unification: NP-completeness and Applications to Theorem Proving," (with J. Gallier, D. Plaisted and W. Snyder) *Information and Computation* 87 1/2 (1990) 129-195.

[2] "On Ground-Confluence of Term Rewriting Systems," (with D. Kapur and F. Otto) *Information and Computation* 86 (1990) 14-31.

[3] "It is Decidable Whether a Monadic Thue System is Canonical Over a Regular Set," *Math. Systems Theory* 23 (1990) 245-254.

1989:

[1] "Some Polynomial-Time Algorithms for Finite Monadic Church-Rosser Thue Systems," (with F. Otto) *Theoretical Computer Science* 68 (1989) 319-332.

[2] "Cancellativity in Finitely Presented Semigroups," (with C. Ó'Dúnlaing) *Journal of Symbolic Computation* 7 (1989), 457-472.

1988:

[1] "Church-Rosser Languages," (with R. McNaughton and F. Otto) *Journal of the ACM* 35 (1988) 324-344.

[2] "Preperfectness is Undecidable for Thue Systems Containing only Length-Reducing Rules and a Single Commutation Rule," (with F. Otto) *Information Processing Letters* 29 (1988) 125-130.

[3] "Elements of Finite Order for Finite Weight-Reducing Thue Systems," (with F. Otto) *Acta Informatica* 25 (1988) 573-591.

[4] "Only Prime Superpositions need be considered in the Knuth-Bendix Procedure," (with D. Kapur and D.R. Musser) *Journal of Symbolic Computation* 6 (1988) 19-36.

1987:

[1] "On Sufficient-Completeness and Related Properties of Term Rewriting Systems," (with D. Kapur and H. Zhang) *Acta Informatica* 24 (1987) 395-415.

[2] "Special Monoids and Special Thue systems," (with R. McNaughton) *Journal of Algebra* 108 (1987) 248-255.

[3] "Complexity of Matching Problems," (with D. Benanav and D. Kapur) *Journal of Symbolic Computation* 3 (1987) 203-216.

1986:

[1] “The Problems of Cyclic Equality and Conjugacy for Finite Complete Rewriting Systems,” (with F. Otto) *Theoretical Computer Science* 47 (1986) 27-38.

[2] “On the Equivalence Problem for Regular Thue Systems,” *Theoretical Computer Science* 44 (1986) 237-245.

1985:

[1] “On Recursive Path Ordering,” (with M.S. Krishnamoorthy) *Theoretical Computer Science* 40 (1985) 323-328.

[2] “A Finite Thue System with Decidable Word Problem and Without Finite Equivalent Canonical System,” (with D. Kapur) *Theoretical Computer Science* 35 (1985) 337-344.

[3] “The Church-Rosser Property and Special Thue Systems,” (with D. Kapur, M.S. Krishnamoorthy and R. McNaughton) *Theoretical Computer Science* 39 (1985) 123-133.

[4] “The Knuth-Bendix Completion Procedure and Thue Systems,” (with D. Kapur) *SIAM Journal on Computing* 14 (4), Nov. 1985, 1052-1072.

[5] “Complexity of Certain Decision Problems about Congruential Languages,” (with C. Ó’Dúnlaing and H. Rolletschek) *Journal of Computer and System Sciences* 30 (3), 343–358, 1985.

[6] “Complexity Results on the Conjugacy Problem for Monoids,” (with F. Otto) *Theoretical Computer Science* 35 (1985) 227-243.

[7] “An O($|T|^3$) Algorithm for Testing the Church-Rosser Property of Thue Systems,” (with D. Kapur, M.S. Krishnamoorthy and R. McNaughton), *Theoretical Computer Science* 35 (1) (1985) 109-114.

1984:

[1] “The Undecidability of Preperfectness of Thue Systems,” (with R. McNaughton) *Theoretical Computer Science* 31 (1984) 165-174.

[2] “The Uniform Conjugacy Problem for Finite Church-Rosser Thue Systems is NP-complete,” (with F. Otto and K. Winklmann) *Information and Control* 63, 58-66, October/November 1984.

Conferences

2016:

[1] "Notes on Lynch-Morawska Systems," (with D. Hono, N. Galatage, K. Gero and A. Subburathinam) presented at the Unification Workshop (UNIF-2016), Porto, Portugal, June 26, 2016. Proceedings available at `http://users.mat.unimi.it/users/ghilardi/UNIF2016/UNIF16-abstracts.pdf`

[2] "Lynch-Morawska Systems on Strings," (with D. Hono and R. Veras) presented at the Unification Workshop (UNIF-2016), Porto, Portugal, June 26, 2016. Proceedings available at `http://users.mat.unimi.it/us`

2015:

[1] "Unification and matching in hierarchical combinations of syntactic theories," (with Serdar Erbatur, Deepak Kapur, Andrew M. Marshall, Catherine Meadows and Christophe Ringeissen) In *Frontiers of Combining Systems - 10th International Symposium, FroCoS 2015, Wroclaw, Poland, September 21-24, 2015, Proceedings*. pages 291–306, 2015.

2014:

[1] "On asymmetric unification and the combination problem in disjoint theories," (with Serdar Erbatur, Deepak Kapur, Andrew M. Marshall, Catherine Meadows and Christophe Ringeissen) In *Foundations of Software Science and Computation Structures - 17th International Conference, FOSSACS 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, April 5-13, 2014, Proceedings*, pages 274–288, 2014.

[2] "Theories of Homomorphic Encryption, Unification, and the Finite Variant Property," (with Fan Yang, Santiago Escobar, Catherine Meadows and Jose Meseguer) In *Proceedings of the 16th International Symposium on Principles and Practice of Declarative Programming (PPDP)*, Kent, Canterbury, United Kingdom, September 8-10, 2014, pages 123–133.

2013:

[1] "Hierarchical combination," (with Serdar Erbatur, Deepak Kapur, Andrew M. Marshall, and Christophe Ringeissen) In *Automated Deduction - CADE-24 - 24th International Conference on Automated Deduction, Lake Placid, NY, USA, June 9-14, 2013. Proceedings*, (Maria Paola Bonacina, editor.), pages 249–266.

[2] "Unication problems modulo a theory of until," (with Shreyaben Brahmakshatriya, Sushma Danturi and Kimberly A. Gero) In Konstantin Korovin and Barbara Morawska, editors, *27th International Workshop on Unification, UNIF 2013, Eindhoven, Netherlands, June 26, 2013*, volume 19 of *EPiC Series*, pages 22–29. EasyChair, 2013.

[3] "On forward closure and the finite variant property," (with Christopher Bouchard, Kimberly A. Gero and Christopher Lynch) In Pascal Fontaine, Christophe Ringeissen, and Renate A. Schmidt, editors, *FroCoS*, volume 8152 of *Lecture Notes in Computer Science*, pages 327–342. Springer, 2013.

[4] "Asymmetric unification: A new unification paradigm for cryptographic protocol analysis," (with Serdar Erbatur, Santiago Escobar, Deepak Kapur, Zhiqiang Liu, Christopher Lynch, Catherine Meadows, José Meseguer, Sonia Santiago, and Ralf Sasse) In *Automated Deduction - CADE-24 - 24th International Conference on Automated Deduction, Lake Placid, NY, USA, June 9-14, 2013. Proceedings*, (Maria Paola Bonacina, editor.), pages 231–248.

2012:

[1] "Unification modulo chaining," (with S. Anantharaman, C. Bouchard, and M. Rusinowitch) In *Language and Automata Theory and Applications*, LNCS 7183, pages 70–82. Springer, 2012.

[2] "Unification modulo synchronous distributivity," (with S. Anantharaman, S. Erbatur, C. Lynch, and M. Rusinowitch) In Bernhard Gramlich, Dale Miller, and Uli Sattler, editors, *IJCAR*, LNCS 7364, pages 14–29, Springer, 2012.

[3] "New Algorithms for Unification Modulo One-Sided Distributivity and Its Variants," (with A. Marshall) In Bernhard Gramlich, Dale Miller, and Uli Sattler, editors, *IJCAR*, LNCS 7364, pages 408–422, Springer, 2012.

[4] "Effective Symbolic Protocol Analysis via Equational Irreducibility Conditions" (with S. Erbatur, S. Escobar, D. Kapur, Z. Liu, C. Lynch, C. Meadows, J. Meseguer, S. Santiago and R. Sasse) In Sara Foresti, Moti Yung, and Fabio Martinelli, editors, *ESORICS*, LNCS 7459, pages 73–90. Springer, 2012.

2011:

[1] "Protocol Analysis in Maude-NPA Using Unification Modulo Homomorphic Encryption," (with S. Escobar, D. Kapur, C. Lynch, C. Meadows, J. Meseguer and R. Sasse) In: Proceedings of the 13th International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming (PPDP 2011), July 20-22, 2011, Odense, Denmark, 65–76.

[2] "Unification in Blind Signatures," (with S. Erbatur and C. Lynch) Presented at FTP-2011: International Workshop on First-Order Theorem Proving, July 2011.

2010:

[1] "Cap Unification: Application to Protocol Security modulo Homomorphic Encryption," (with Siva Anantharaman, Hai Lin, Christopher Lynch, and Michael Rusinowitch) In: Proceedings of ASIACCS, D. Feng, D. A. Basin, and P. Liu, editors, pages 192–203. ACM, 2010.

[2] "Unification modulo a partial theory of exponentiation," (with Deepak Kapur and Andrew Marshall) Presented at the 24th International Workshop on Unification (UNIF-2010), Edinburgh, Scotland, July 14, 2010. *Electronic Proceedings in Theoretical Computer Science* (EPTCS) 42, 12–23. `http://published.eptcs.org/`

[3] "On the Complexity of the Tiden-Arnborg Algorithm for Unification modulo One-Sided Distributivity," (with Andrew Marshall and Bibhu Mahapatra) Presented at the 24th International Workshop on Unification (UNIF-2010), Edinburgh, Scotland, July 14, 2010. *Electronic Proceedings in Theoretical Computer Science* (EPTCS) 42, 54–63. `http://published.eptcs.org/`

2009:

[1] "On extended regular expressions," (with B. Carle) presented at the Third International Conference on Language and Automata Theory and Applications (LATA-2009), Tarragona, Spain, April 2-8, 2009, Lecture Notes in Computer Science 5457, Springer (A.H. Dediu, A. Ionescu, C. Martin-Vide, eds.) 279–289.

[2] "Unification modulo Homomorphic Encryption," (with S. Anantharaman, H. Lin, C. Lynch and M. Rusinowitch) presented at the 7th International Symposium on FROntiers of COmbining Systems (FROCOS-2009), Trento, Italy, September 16-18th, 2009, Lecture Notes in Computer Science 5749, Springer (Silvio Ghilardi, Roberto Sebastiani, eds.) 100–116.

2008:

[1] "Unification and Matching Modulo Leaf-Permutative Equational Presentations," (with Thierry Boy de la Tour and Mnacho Echenim) presented at IJCAR 2008, Lecture Notes in Computer Science 5195 (A. Armando, P. Baumgartner and G. Dowek, eds.) 332–347.

[2] "Unification modulo Homomorphic Encryption is Decidable," (with S. Anantharaman, H. Lin, C. Lynch and M. Rusinowitch) presented at UNIF 2008, the 22nd International Workshop on Unification, Castle of Hegenberg, Austria, July 18, 2008. (Proceedings available on-line at: `http://www.score.cs.tsukuba.ac.jp/~mmarin/UNIF2008/UNIF_proceedings.pdf.`)

2007:

[1] "Intruders with caps," (with Siva Anantharaman and Michael Rusinowitch) Proceedings of the *Eighteenth International Conference on Rewriting Techniques and Applications,* (RTA-07), Paris, France, June 2007, Lecture Notes in Computer Science 4533, Springer (Franz Baader, ed.) 20–35.

[2] "On extended regular expressions," (with B. Carle and C. Scheriff) presented at the *Twenty-first International Workshop on Unification* (UNIF-2007), Paris, France, June 2007.

2006:

[1] "Unification modulo *ACUI* with collapsing homomorphisms," (with Pavithra Ramarathnam) Proceedings of the *Twentieth International Workshop on Unification* (UNIF-2006), pages 21–28, Seattle, Washington, June 2006.

2003:

[1] "*ACID*-Unification is NEXPTIME-Decidable," (with S. Anantharaman and M. Rusinowitch) Proceedings of the 28th International Symposium on Mathematical Foundations of Computer Science (MFCS 2003), pages 169–178, August 25–29, 2003.

[2] "Unification modulo ACUI with Homomorphisms/Distributivity," (with S. Anantharaman and M. Rusinowitch) Proceedings of the at the 19th International Conference on Automated Deduction (CADE-19), pages 442–457, Miami Beach, Florida, Jul 30–Aug 2, 2003.

[3] "Undecidability of unification over two theories of modular exponentiation," (with D. Kapur and L. Wang) Proceedings of the *Seventeenth International Workshop on Unification* (UNIF-2003), pages 39–50, Valencia, Spain, Jun 8, 2003.

[4] "An E-unification algorithm for analyzing protocols that use modular exponentiation," (with D. Kapur and L. Wang) Proceedings of the *Fourteenth International Conference on Rewriting Techniques and Applications,* (RTA-03), pages 165–179, Valencia, Spain, Jun 9–11, 2003.

2002:

[1] "A Unification Algorithm for the Group Diffie-Hellman Protocol," (with C. Meadows) Proceedings of the Workshop on Issues in the Theory of Security (WITS 2002), Portland, Oregon, Jan 2002.

2000:

[1] "The theory of total unary rpo is decidable," (with M. Rusinowitch) Proceedings of the First International on Compuational Logic (CL-2000), London, UK, July 2000, Lecture Notes in Computer Science 1861, Springer, 660–672.

1998:

[1] “Unification of Concept Terms in Description Logics,” (with F. Baader) Proceedings of the European Conference on Artificial Intelligence (ECAI-98), pages 331–335, Brighton, UK, August 1998.

[2] “RPO Constraint Solving is in NP,” (with M. Rusinowitch and R. Verma) Proceedings of the Annual Conference of the European Association for Computer Science Logic (CSL ’98), Brno, Czech Republic, August 1998, Lecture Notes in Computer Science 1584, Springer-Verlag, 385–398.

[3] “Decision Problems in Ordered Rewriting,” (with H. Comon, R. Nieuwenhuis and M. Rusinowitch) Proceedings of the Thirteenth Annual Symposium on Logic in Computer Science (LICS), Indianapolis, IN, June 1998, 276-286.

[4] “The Decidability of Simultaneous Rigid E-Unification with One Variable,” (with A. Degtyarev, Y. Gurevich, M. Veanes, and A. Voronkov) Proceedings of the *Ninth International Conference on Rewriting Techniques and Applications,* (RTA-98), pages 181–195, Tsukuba, Japan, March 1998.

[5] “Unification and Matching in Process Algebras,” (with Q. Guo, and S. Shukla) Proceedings of the *Ninth International Conference on Rewriting Techniques and Applications,* (RTA-98), pages 91–105, Tsukuba, Japan, March 1998. Lecture Notes in Computer Science 1379, Springer, 91–105.

1997:

[1] “The Word Matching Problem Is Undecidable In General Even For Finite Special String-Rewriting Systems That Are Confluent,” (with F. Otto) In: Proceedings of the 24th International Colloquium on Automata, Languages and Programming (ICALP’97), Bologna, Italy, July 1997, Lecture Notes in Computer Science 1256, Springer, 638–648.

1996:

[1] “On solving linear equations over polynomial semirings,” In: Proceedings of the Eleventh Annual Symposium on Logic in Computer Science (LICS) (E.M. Clarke, ed.), Rutgers University, NJ, July 1996, 466–472.

[2] “Unification and Matching modulo Nilpotence,” (with Q. Guo and D. Wolfram) presented at the 13th International Conference on Automated Deduction (CADE-13), Rutgers University, NJ, July-Aug 1996.

1995:

[1] “Some Independence Results for Equational Unification,” (with F. Otto and D. Dougherty) Presented at the Sixth International Conference on Rewriting Techniques and Applications (RTA ’95), Kaiserslautern, Germany, April 1995.

[2] “The All-Minors VCCS Matrix Tree Theorem, Half-resistors and Applications in Symbolic Simulation,” (with S. Chaiken) Presented at the *IEEE International Symposium on Circuits and Systems,* (ISCAS-95) Seattle, Washington, Vol. 2, 1239-1242, (1995).

1994:

[1] “Ground Temporal Logic — A Logic for Hardware Verification,” (with D. Cyrluk) Presented at the Conference on Computer-Aided Verification (CAV), Stanford, CA, June 21-24, 1994.

1993:

[1] “Computation of Signal Delays in RC Networks”, (with J.C. Hidalgo and S. Chaiken) Proceedings of The Fifth NASA Symposium on VLSI Design, New Mexico, November 1993.

[2] “On the Unification Problem for Cartesian Closed Categories,” (with F. Pfenning and R. Statman) Proceedings of the Eighth Annual Symposium on Logic in Computer Science (LICS), pages 57–63, Montreal, Canada, June 1993.

[3] “The Unifiability Problem in Ground AC Theories,” (with M. Rusinowitch) Proceedings of the Eighth Annual Symposium on Logic in Computer Science (LICS), pages 364–370, Montreal, Canada, June 1993.

1992:

[1] “Double Exponential Complexity of Computing a Complete Set of AC-Unifiers,” (with D. Kapur) In: Proceedings of the Seventh Annual Symposium on Logic in Computer Science (LICS), Santa Cruz, CA, 255-265, June 1992.

1991:

[1] “Any Ground Associative-Commutative Theory has a Finite Canonical System,” (with M. Rusinowitch) Proceedings of the Fourth International Conference on Rewriting Techniques and Applications (RTA-91), pages 423–434, Como, Italy, April 1991.

[2] “A Specialized Completion Procedure for Monadic String-Rewriting Systems Presenting Groups,” (with K. Madlener and F. Otto) In: Proceedings of the 18th International Colloquium on Automata, Languages and Programming (ICALP’91), Lecture Notes in Computer Science 510, Springer, 279–290, 1991.

1990:

[1] “Some Results on Equational Unification,” (with F. Otto) Proceedings of the 10th International Conference on Automated Deduction (CADE-10), Kaiserslautern, West Germany, July 1990.

1989:

[1] “It is Undecidable Whether the Knuth-Bendix Completion Procedure Generates a Crossed Pair,” (with J. Stillman) Proceedings of the 6th Annual Symposium on Theoretical Aspects of Computer Science (STACS), Paderborn, West Germany, February 1989.

[2] “On the Unification Problem for Cartesian Closed Categories,” (with F. Pfenning and R. Statman) Proceedings of the Workshop on Higher Order Logic, Banff, Alberta, September 24-27, 1989.

1988:

[1] “Finding Canonical Rewriting Systems Equivalent to a Finite Set of Ground Equations in Polynomial Time,” (with J. Gallier, D. Plaisted, S. Raatz and W. Snyder) Proceedings of the 9th International Conference on Automated Deduction (CADE-9), Argonne, Illinois, May 1988. Appears in LNCS 310, 182-196.

[2] “Formal Verification of the SOBEL Image Processing Chip,” (with J. Stillman) Proceedings of the 25th ACM/IEEE Design Automation Conference, Anaheim, California, June 1988. (An expanded version appears in in *Current Trends in Hardware Verification and Automated Theorem Proving,* (G. Birtwistle, P.A. Subrahmanyam, eds.), Springer-Verlag, NY, pp. 92-127.)

[3] "Rigid E-Unification is NP-complete," (with J. Gallier, D. Plaisted and W. Snyder) Proceedings of the Third Annual Symposium on Logic in Computer Science (LICS), Edinburgh, Scotland, July 1988.

1987:

[1] "Complexity of Homeomorphic Embedding," (with J. Stillman) Proceedings of the Fifth International Conference on Applied Algebra, Error-Correcting Codes, etc. (AAECC-5), Menorca, Spain, June 1987, Lecture Notes in Computer Science 356, Springer.

[2] "Elements of Finite Order for Finite Church-Rosser Thue Systems," (with F. Otto) Proceedings of the Fifth International Conference on Applied Algebra, Error-Correcting Codes, etc. (AAECC-5), Menorca, Spain, June 1987, Lecture Notes in Computer Science 356, Springer.

[3] "Hardware Verification in the Interactive VHDL Workstation," (with J. Stillman) Proceedings of the Workshop on Hardware Verification at Calgary, Alberta, Canada. Also appears in *VLSI Specification, Verification and Synthesis* (G. Birtwistle and P.A. Subrahmanyam, eds.), Kluwer Academic Publishers, Boston, 1988, 235-255.

[4] "BIDS: A Method for Specifying and Verifying Bidirectional Hardware Devices," (with D. Musser and W. Premerlani) Proceedings of the Workshop on Hardware Verification at Calgary, Alberta, Canada. Also appears in *VLSI Specification, Verification and Synthesis* (G. Birtwistle and P.A. Subrahmanyam, eds.), Kluwer Academic Publishers, Boston, 1988, 217-233.

1986:

[1] "Proof by Induction using Test Sets," (with D. Kapur and H. Zhang) Proceedings of the 8th Intl. Conference on Automated Deduction (CADE-8), Oxford, England, July 1986.

[2] "NP-completeness of the Set-Unification and Matching Problems," (with D. Kapur) Proceedings of the 8th Intl. Conference on Automated Deduction (CADE-8), Oxford, England, July 1986.

[3] "Complexity of Sufficient-Completeness," (with D. Kapur and H. Zhang) Proceedings of FSTTCS-86, New Delhi, India, December 1986.

1985:

[1] "A Path Ordering for Proving Termination of Term Rewriting Systems," (with D. Kapur and G. Sivakumar) Proceedings of the 10th Colloquium on Trees in Algebra and Programming, Berlin, Germany, March 1985, LNCS 185, 173–187.

[2] "An Equational Approach to Predicate Calculus," (with D. Kapur) In: Proceedings of the 9th International Joint Conference on Artificial Intelligence (Aravind Joshi, ed.), Los Angeles, CA, August 1985. Morgan Kaufmann, 1985, 1146–1153.

[3] "An Ideal-Theoretic Approach to Word Problems and Unification Problems over Finitely Presented Commutative Algebras," (with A. Kandri-Rody and D. Kapur) Proceedings of the Conference of Rewrite Rule Theory and Applications (RTA-85) at Dijon, France.

[4] "Reasoning about Three-Dimensional Space," (with D. Kapur, J.L. Mundy and D.R. Musser) Proceedings of the 1985 IEEE International Conference on Robotics and Automation in St. Louis, Missouri.

[5] "Cancellativity in Finitely Presented Semigroups," (with C. Ó'Dúnlaing) Proceedings of the workshop on Combinatorial Algorithms in Algebraic Structures held at Otzenhausen, West Germany, 1985.

[6] “Existence and Construction of a Grobner Basis for a Polynomial Ideal,” (with D. Kapur) Proceedings of the workshop on Combinatorial Algorithms in Algebraic Structures held at Otzenhausen, West Germany, 1985.

1984:

[1] “The Complexity of Testing whether a Polynomial Ideal is Non-trivial,” (with S. Agnarsson, A. Kandri-Rody, D. Kapur and B.D. Saunders) Proceedings of the *Third MACSYMA User’s Conference*, Schenectady, New York, July 1984.

1983:

[1] “The Knuth-Bendix completion procedure and Thue systems,” (with D. Kapur) Proceedings of the 3rd Conf on the *Foundations of Software Technology and Theoretical Computer Science* (FSTTCS), Bangalore, India, Dec 1983.

Technical Reports

2011:

[1] "Unification modulo Theories of Blind Signatures," (with Serdar Erbatur and Christopher Lynch) Technical Report SUNYA-CS-11-02, Department of Computer Science, University at Albany—SUNY, June 2011.

Available at: `ftp://ftp.cs.albany.edu/pub/tech-reports/2011/TR-SUNYA-CS-11-02.pdf`

2009:

[1] "On the Complexity of the Tiden-Arnborg Algorithm for Unification modulo One-Sided Distributivity," (with Andrew Marshall and Bibhu Mahapatra) Technical Report SUNYA-CS-09-01, Department of Computer Science, University at Albany—SUNY, 2009.

Available at: `ftp://ftp.cs.albany.edu/pub/tech-reports/2009/TR-CS-09-01.pdf`

2007:

[1] "Intruders with caps," (with Siva Anantharaman and Michael Rusinowitch) LIFO Technical Report RR **2007–02**, LIFO, Universite d'Orleans, Orleans, France.

2002:

[1] "*ACID*-Unification, Rewrite Reachability and Set Constraints," (with S. Anantharaman and M. Rusinowitch) LIFO Technical Report RR **2002–3**, Orleans, France.

1997:

[1] "The Decidability of Simultaneous Rigid E-unification with one variable," (with A. Degtyarev, Y. Gurevich, M. Veanes and A. Voronkov) UPMAIL Technical Report 139, March 1997, Uppsala University, Sweden.

1994:

[1] "Observations on Equational Rewriting," (with M. Subrahmaniam and Q. Guo) TR 94-2, Dept. of Computer Science, SUNY at Albany, Albany, NY 12222.

1992:

[1] "The Complexity of Two Simple Unifiability Problems," (with D.A. Wolfram) PRG-TR-32-92, Programming Research Group, Oxford University Computing Laboratory, Oxford, U.K.

1991:

[1] "Verification of a Hardware Scheme for Implementing a Least Recently Used Policy," (with J.C. Hidalgo) Dept. of Computer Science, SUNY at Albany, Albany, NY 12222.

1989:

[1] "Some Remarks on Second Order Unification," Dept. of Computer Science, University of Calgary, Calgary, Alberta, Canada T2N 1N4.

1988:

[1] “Formal Verification of the Sobel Image Processing Chip,” (with J. Stillman) submitted to AFWAL, Wright-Patterson Air Force Base, Ohio.

1987:

[1] “On the Membership Problem for some Grammars,” (with K. Krithivasan), CAR-TR-267, Center for Automation Research, University of Maryland, March 1987.

1986:

[1] “Report on a Proof-based Approach to Hardware Verification,” (with D. Musser and W. Premerlani) submitted to AFWAL, Wright-Patterson Air Force Base, Ohio.