

Lecture Notes in Computer Science

1179

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Advisory Board: W. Brauer D. Gries J. Stoer

Joxan Jaffar Roland H.C. Yap (Eds.)

Concurrency and Parallelism, Programming, Networking, and Security

Second Asian Computing Science Conference
ASIAN'96
Singapore, December 2-5, 1996
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Joxan Jaffar

Roland H.C. Yap

National University of Singapore

Department of Information and Computer Science

Lower Kent Ridge, Singapore 119260

E-mail: {joxan,ryap}@iscs.nus.sg

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Concurrency and parallelism, programming, networking, and security : proceedings / Second Asian Computing Science Conference, ASIAN '96, Singapore, December 2 - 5, 1996.
Joxan Jaffar ; Roland H. C. Yap (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1996
(Lecture notes in computer science ; Vol. 1179)
ISBN 3-540-62031-1

NE: Jaffar, Joxan [Hrsg.]; Asian Computing Science Conference <2, 1996, Singapore>; GT

CR Subject Classification (1991): F.3, F.2, D.1, D.3, C.2, I.2

ISSN 0302-9743

ISBN 3-540-62031-1 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer - Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1996
Printed in Germany

Typesetting: Camera-ready by author
SPIN 10550201 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

This conference ASIAN'96 represents the second in the hopefully long and successful series of ASIAN'XX conferences. The inaugural conference, last year in Thailand, served to bring world-class computer science to the regional academic community. Its basic strategy was to use themes representing areas of focus (algorithms, concurrency, and knowledge), to have a visible international program committee, and to have prominent invited speakers. With the partnership of INRIA, France, and UNU/IIST, Macau, ASIAN'95 was realized by the Asian Institute of Technology, Thailand.

This year in Singapore, ASIAN'96 serves to continue the tradition. The themes now are programming, concurrency/parallelism, networking, and security. The program committee is international, our keynote speaker is David Harel (Weizmann Institute, Israel), and our invited speakers are Jean-Chrysostome Bolot (INRIA, France), Gert Smolka (DFKI-Saarbrücken, Germany), and Doug Tygar (Carnegie Mellon University, USA).

We received a surprising 169 submitted papers. Of these, 90 papers came from Asia and the rest were mainly from Australia and New Zealand (19 papers), Europe (45 papers), and North America (14 papers). The breakdown of submissions from Asia is as follows: Japan (30), India (23), Korea (8), China (7), Hong Kong (7), Singapore (6), Macau (3), Taiwan (3), Vietnam (2), and Philippines (1). The submission and review process was conducted mainly electronically. The committee meeting was also held mainly electronically over a period of four days. Almost all papers had at least two reviews; most had three or more. Eventually, we accepted 31 papers, and in addition, 14 posters.

We are once again indebted to our main partners, INRIA of France and UNU/IIST of Macau. Once again, the Singapore office of CICC (Japan) came through with valuable support. Last year, the European Commission was a sponsor and this year their support has been requested. New support this year was obtained from ILOG (Singapore) for efforts in constraint programming. Last but not least, our home departments in the Asian Institute of Technology and the National University of Singapore also provided valuable support.

October 1996

Joxan Jaffar, NUS & IBM Watson, USA
Roland H.C. Yap, NUS

Steering Committee

Dines Bjørner (UNU/IIST, Macau)
 Shigeki Goto (Waseda U., Japan)
 Joxan Jaffar (NUS/IBM)
 Gilles Kahn (INRIA, France)
 Kanchana Kanchanasut (AIT, Thailand)
 Jean-Jacques Lévy (INRIA, France)
 R.K. Shyamasundar (TIFR Bombay, India)

Program Committee

Martín Abadi (SRC, DEC, USA)
 Eliezer A. Albacea (U. of Philippines)
 Anuchit Anuchitanukul (Bank of Thailand & AIT)
 Kim Bruce (Williams College, USA)
 Rance Cleaveland (NCSU, USA)
 Dang Van Hung (UNU/IIST, Macau)
 Li Gong (JavaSoft, USA)
 Shigeki Goto (Waseda U., Japan)
 Seif Haridi (SICS, Sweden)
 Nevin Heintze (Bell Labs, USA)
 Pascal van Hentenryck (Brown U., USA)
 Jieh Hsiang (NTU, Taiwan)
 Kyoki Imamura (Kyushu IT, Japan)
 Joxan Jaffar, *Program Chair* (NUS/IBM)
 Tomasz Janowski (UNU/IIST, Macau)
 Gilles Kahn (INRIA, France)
 Lam Kwok-Yan (NUS, Singapore)
 John Lamping (Xerox PARC, USA)
 Peter Lee (CMU, USA)
 Jean-Jacques Lévy (INRIA, France)
 Chidchanok Lursinsap (Chulalongkorn U. & AIT)
 Michael Maher (Griffith U., Australia)
 Hideo Miyahara (Osaka U., Japan)
 Gustaf Neumann (Essen U., Germany)
 Phillip Wadler (U. of Glasgow, UK)
 Vijay Saraswat (ATT Research, USA)
 S. Sudarshan (IIT, Bombay)
 R. Sureswaran (USM, Malaysia)
 Doug Tygar (CMU, USA)
 Belawati Widjaja (U. of Indonesia)
 Roland H.C. Yap, *Local Arrangements Chair* (NUS)

List of Referees

A.L. Ananda	M. Gelfond	K. Kunen	A. Sattar
J. Andrews	L. George	T.W. Lam	S. Seshadri
C.H. Ang	A. Ghose	T.Y. Leong	R. Setiono
D.N. Anh	R. Givan	W.K. Leow	H. Shen
G. Antoniou	D. Gollmann	T.W. Ling	T. Shinohara
K. Baba	A. Gordon	B. Liu	R. Shyamasundar
C. Baral	V. Gupta	P. Long	A. Srinivasan
T. Basaruddin	C. Hall	H.-J. Lu	M.E. Stickel
P. Bernus	M. Hanus	K.T. Lua	P. Stuckey
G.M. Bierman	D. Harel	A. Malhotra	C. Sun
D. Billington	J. Harland	L. Maranget	H. Sunahara
S. Blackburn	E. Harris	K. Marriott	K.K. Sung
J.-C. Bolot	K. Harumoto	T. Masuzawa	M.H. Sørensen
A. Brodsky	M. Henson	S. Michaylov	H. Takada
S. Brookes	T. Henzinger	D. Miller	K.-L. Tan
B. Carlson	T. Higashino	T. Miyazaki	Y.C. Tay
B. Carpenter	M. Higuchi	O. de Moor	M. Thomas
B. Chazelle	H. Hirota	L. Naish	F. Tip
C.L. Chee	W. Hsu	S. Nusser	H.-C. Tu
I.-J. Chiang	G.-S. Huang	J. O'Donnell	D.N. Turner
W.-N. Chin	P. Hudak	H. Ohsaki	T. Ushio
K.W. Chong	L. Hui	Y. Oie	N. Wakamiya
T.S. Chua	H. Ichikawa	C. Okasaki	U. Waldmann
W. Conen	M. Indrika	D. Oliva	M. Wallace
J.N. Crossley	M. Inoue	L. Ong	J. Wang
M. Dalrymple	P. Iyer	B.C. Ooi	W.F. Wong
V. DePaiva	S. Jain	J. Palsberg	Q. Xu
A. Deutsch	S. Jarzabek	P.K. Pandya	N. Yamai
F. Dridi	T. Kaneko	E. Poll	M. Yamashita
P.M. Dung	D. Kapur	W. Prasetya	S. Yasutome
J. Field	P. Kellock	N. Raja	C.K. Yuen
K. Fisher	B. Kernighan	A. Ramer	W. Zadrozny
C. Fournet	S.C. Khoo	J. Rao	L.X. Zhang
M. Fromherz	R. Klapsing	E. Ravindran	I. Zukerman
K.-E. Fujita	E. Koepfen	M. Reid-Miller	
H. Fukuoka	K. Korb	J.G. Riecke	
H. Ganzinger	K.N. Kumar	B.-H. Ryu	

Table of Contents

Algorithms

Randomized Parallel List Ranking for Distributed Memory Multiprocessors <i>F. Dehne, S.W. Song</i>	1
Suffix Arrays for Multiple Strings: A Method for On-line Multiple String Searches <i>F. Shi</i>	11
Relations Among Parallel and Sequential Computation Models <i>H. Vollmer</i>	23

Constraints and Logic Programming

The Expressive Power of "Possible-is-Certain" Semantics <i>S. Greco, D. Saccà</i>	33
Using Stochastic Methods to Guide Search in CLP: A Preliminary Report <i>J.H.M. Lee, H.F. Leung, P.J. Stuckey, V.W.L. Tam, H.W. Won</i>	43
Backtrackable State with Linear Affine Implication and Assumption Grammars <i>P. Tarau, V. Dahl, A. Fall</i>	53
Declarative Debugging in Constraint Logic Programming <i>A. Tessier</i>	64

Distributed Systems

An Improved Logging and Checkpointing Scheme for Recoverable Distributed Shared Memory <i>T. Park, S.B. Cho, H.Y. Yeom</i>	74
Distributed Concurrency Control in Real-time Cooperative Editing Systems <i>C. Sun, Y. Yang, Y. Zhang, D. Chen</i>	84

Variable Timestamp-Based Distributed Deadlock Detection and Resolution	96
<i>H. Wu, W.-N. Chin</i>	

Formal Systems

Lambda-Definable Term Rewriting Systems	106
<i>S. Byun, R. Kennaway, R. Sleep</i>	
Sets as Anti-Chains	116
<i>C.A. Gunter, T.-H. Ngair, D. Subramanian</i>	
A Typed Lambda Calculus of Objects	129
<i>L. Liquori, G. Castagna</i>	
Intensionality versus Extensionality and Primitive Recursion	142
<i>P. Valarcher</i>	
On the Bounded Theories of Finite Trees	152
<i>S. Vorobyov</i>	

Networking and Security

Broadcasting in Star Graphs with Byzantine Failures	162
<i>Y. Hamada, A. Mei, F. Bao, Y. Igarashi</i>	
Blind Threshold Signatures Based on Discrete Logarithm	172
<i>W.-S. Juang, C.-L. Lei</i>	
Computation of the k -Error Linear Complexity of Binary Sequences with Period 2^n	182
<i>T. Kaida, S. Uehara, K. Imamura</i>	
Symbolic Rights and Vouchers for Access Control in Distributed Object Systems	192
<i>V. Nicomette, Y. Deswarte</i>	
The Heuristics for the Constrained Multicast Routing	204
<i>Z.-B. Xu, B.-T. Yang</i>	
On Design and Analysis of a New Block Cipher	213
<i>X. Yi</i>	

Programming and Systems

CHESSEBOARD: A Synergy of Object-Oriented Concurrent Programming and Program Layering	223
<i>T. Elrad, B. Sheen, N.V. Nastasic</i>	
A Computational Approach to Flattening Nested Data Parallelism in Functional Languages	234
<i>G. Keller, M. Simons</i>	
Concurrent Object-Oriented Programming in Tempo++	244
<i>R. Ramirez</i>	
A Universal Scripting Framework or Lamda: The Ultimate “little language”	254
<i>O. Shivers</i>	
Design and Application of a Light-Weight Persistency Mechanism	266
<i>M. Theißinger</i>	

Specification and Verification

Hierarchical Verification Using Verification Diagrams	276
<i>I.A. Browne, Z. Manna, H.B. Sipma</i>	
A Dynamic Evolution for the Specification of Distributed Systems	287
<i>I.A. Hamid, F. Khendek</i>	
Formal Verification and Evaluation of Execution Time in the Envelope Theory	299
<i>S. Igarashi, M. Shio, T. Shirogane, T. Mizutani</i>	
Design of Controllers for Linear Hybrid Systems	309
<i>R. Majumdar, R.K. Shyamasundar</i>	
Checking Linear Duration Invariants by Linear Programming	321
<i>X. Li, D.V. Hung</i>	

Posters

Conjunctive Vector Representations for Set Valued Feature Descriptions..	333
<i>M. Carl</i>	
Constructive Negation in Definite Constraint Logic Programs	335
<i>V. Chandru, S. Roy, R. Subrahmanyam</i>	
Multilevel Master-Slave Parallel Programming Models	337
<i>H.-C. Chen, A. Lim, N.A. Warsi</i>	
Improving the X.509 Protocol for ATM Networks	339
<i>S.-C. Chuang</i>	
InterMUD Communications (IMC) Protocol with Extensions to VRMLise MultiUser Domains (MUDs)	341
<i>F.K. Chan, J. Seng, L.-S. Ooi, J.-K. Tan, K. Mok, T.W. Tan</i>	
ALPS-HI: An Annotated Logic Programming System with Hypothetical Implications	343
<i>K. Goshi, J. Cheng, K. Ushijima</i>	
Constructing More Relevant Models	345
<i>L. He, Y. Chao, Y. Simajiri, H. Seki, H. Itoh</i>	
Formal Analysis for Continuous Systems Controlled by Programs	347
<i>S. Igarashi, T. Mizutani, T. Shirogane, M. Shio</i>	
Implementation Tuning of a Dataflow Language on a Stock Parallel Machine with Visualization Tools	349
<i>S. Kusakabe, K. Inenaga, K. Nishimura, M. Amamiya</i>	
Overall System for Secure Wireless Mobile Networks	351
<i>A. Li, O. Bukhres</i>	
Materialized View Adaptation in Distributed Databases	353
<i>M. Mohania, G. Dong</i>	
Coupling Object-Orientation & Deduction - A Modelling Perspective	355
<i>E. Ravindran, S.C. Hui</i>	
An Integer Programming-Based Nurse Rostering System	357
<i>J. Thornton, A. Sattar</i>	

Synthesizing Parallel Divide-and-Conquer Algorithms Using the List Interleave Operator	359
<i>R. Voicu</i>	

Keynote Lecture

Some Thoughts on Statecharts, 13 Years Later	361
<i>D. Harel</i>	

Invited Lectures

End-to-end Behavior of the Internet: Measurements, Analysis, and Applications	362
<i>J.-C. Bolot</i>	
The Oz Programming Language and System	377
<i>G. Smolka</i>	
Cryptographic Postage Indicia	378
<i>J.D. Tygar, B.S. Yee, N. Heintze</i>	

Author Index	393
--------------------	-----