Eesti teaduse tippkeskus / Estonian Centre of Excellence in Research
Töökindlate Arvutisüsteemide Uurimise Keskus / Centre for Dependable Systems
Põhitulemused / Main results 2003–2007

We divide the results of the centre into two categories: research results and advances in the internationalization and attraction of young researchers to computer science and engineering research.

Research results

Mathematical foundations and programming language theory

A series of papers were produced on the category theory of structured recursion and corecursion and of effectful and context-dependent computation. A number of (co)recursion schemes for initial algebras and final coalgebras were shown to be an instance of one scheme parameterized by a comonad and distributive law encapsulating the (co)recursive call pattern of the scheme. A general account of structured recursion was given in terms of recursive coalgebras, generalizing recursions schemes for initial algebras. Categorical account were given for type-based termination, also known as circular proofs, and for the fold-build theory of initial algebras which is the basis of the program transformation known as shortcut deforestation (Uustalu, Vene, Kabanov, with colleagues).

An explicit construction of the coproduct of two ideal monads was developed as a means for constructing a monad for a combination of two effects. An account was developed of partiality from nontermination as a monadic effect. Comonads were shown to useful for modelling context-dependent computations such as causal or general dataflow computation and purely synthesized and general attributed evaluation (tree labelling). An categorical analysis of various types of tree transducers was given (Uustalu, Vene, with colleagues).

A static analyzer for detecting potential data races in the multithreaded C code called Goblint was developed. The implemented analysis is sound on a “safe” subset of C and sufficiently efficient to be used for race-detection of multithreaded programs up to about 25 thousand lines of code. It uses a global invariant approach to avoid the state space explosion problem and is both context- and path-sensitive. The Goblint analyzer is open source and is available at http://goblint.at.mt.ut.ee/ (Vene, Vojdani).

A method of typesystematic description of program analyses and optimizations was proposed for the setting of proof-carrying code. It allows for simple relational soundness and improvement proofs of the analyses and optimizations and for automatic transformation of program proofs along transformation of programs. The method was demonstrated both for a high-level language and a JVML-like stack-based low-level language. For the stack-based language novel analyses and optimizations were proposed that finetune the usage of the operand stack; the key analyses are birectional (Uustalu, Saabas).

A method of synthesizing simulation code from Stateflow system descriptions was developed based on a denotational semantics of Stateflow (Toom).

Soundness of program slicing was proved with respect to nonstandard, nonwellfounded small-step and big-step semantics (Nestra).

The papers and drafts of Uno Kaljulaid on semigroups and automata were edited and published in the form of a book (Penjam, Peetre).

Genetic programming and evolutionary algorithms were applied to inductive synthesis of programs and learning of finite-state machines (Penjam, Sanko, Spitšakova).

Size reduction and minimality issues of finite automata were studied. A method was presented for size reduction of multitape automata. Also, transition minimality issues of bideterministic automata were studied. Bideterministic automata were shown to be transition-minimal NFAs and the necessary and sufficient conditions presented for a bideterministic automaton to be uniquely transition-minimal among NFAs. More generally, bideterministic automata were shown to be transition-minimal epsilon-NFAs (Tamm).

Formal methods in software engineering

The two-level load balancing method for robotic assembly lines was elaborated and its convergence proved (Vain, Jääger).

A finite model building technique was proposed that is used in automated theorem prover Gandalf. This technique assists in solving the decidability problem of assertions stated in 1st order predicate calculus (Tammet).

State isomorphism based symmetry reduction technique has been developed that exploits symmetries of the model (state graph isomorphism) to reduce the effects of state space explosion in explicit state reachability analysis.

The implementation is based on McKay's linearisation approach. The method is implemented in model-testing toolkit called NModel (by Margus Veanes et al, MS Research Redmond) (Ernits).

A new method for calculating reachability in state models has been proposed. The method combines iterated search refinement method with bit state hashing. The key idea is to use collisions in bitstate hash table to randomly filter the search space, thus resulting in bit-state pruning. The method has proven to be efficient in several practical domains like scheduling, hardware synthesis, pre-set test trace generation using MC. It has been shown that the method can be easily implemented on massively parallel computation architectures that reduces criticality of the scaling factor (Ernits).

A method for synthesis of test purpose directed reactive planning testers for nondeterministic systems was developed and its superiority regarding competitive testing methods (random walk, anti-ant) has been demonstrated (Vain, Ernits, Kull, Raiend).

A robot swarm (distributed) coordination algorithm was developed that assumes asynchronous wireless communication between distributed agents over local and passive data carriers (RFID tags). Self-stabilization of the algorithm was proven (Tammet, Vain, Kuusik).

A semantic-based web service composition framework was proposed that combines an interface engine with databases: a rule server. Using a rule language one can capture semantics in web-based systems (Tammet, Kääramees, Haav, Kadarpik).

A new environment for Priz-style structural synthesis of programs for Java called Cocovila was developed, with particular attention on visual specification and support for "rich" components. It was applied to various engineering domains, in particular to modelling and simulation of hydraulic-mechanical systems, and to web services composition (Tyugu, Saabas, Grigorenko, Ojamaa, Maigre).

Computational methodology was developed for parallel iterative methods for Navier-Stokes equations and application to eigenvalue computation. A parallel solver for PDE systems called DOUG (Domain Decomposition on Unstructured Grids, http://www.dougdevel.org/) was developed, implemented in Fortran 95 and using MPI as communication library. For the highly variable coefficient case, methods for robust aggregation-based coarsening were developed for the additive Schwarz method used in DOUG. Contributions were made towards new methods for solving weakly singular Volterra integral equations using product quasi-interpolation method and their implementation. Development of a new grid infrastructure was initiated for facilitating Instant Messaging to set up a friend-to-friend (F2F) grid computation framework, http://f2f.ulno.net/ (Vainikko, Norbisrath).

Foundations of interactive and location-aware computation were studied, in particular based on multistream interaction machines. The theoretical results were used to build development tools and methods for agent-based software engineering and applications based on those methods. Intelligent dust based cyber-physical systems were studied to enable situation-awareness of computers (Mõtus, Meriste, Preden).

Cryptology and information security

More natural security definitions were proposed for timestamping systems, necessary and sufficient conditions for their existence were clarified (Buldas, Laur, Saarepera et al).

New, efficient protocols were constructed for secure multiparty computation, with particular emphasis towards algorithms used in data mining (Laur, Lipmaa).

Novel data flow analyses and type systems were proposed for checking computational security of information flow in imperative programs (Laud). Computationally sound security analysers were constructed for cryptographic protocols, based on the sequence-of-games approach, or on the application of the universally composable cryptographic library (Laud, Tšahhirov).

The notion of designed verifiability in signature schemes was studied, existing algorithms were broken and a new construction proposed (Lipmaa).

The efficiency and complexity of methods for secure authentic data exchange between different institutions were improved. (Buldas, Willemson, Ansper, Freudenthal, Saarepera).

Several proposed e-voting systems were analyzed for various different security properties (Buldas, Lipmaa).

Existing methods were analysed and new proposed for estimating the optimal level of investment in information security for protection against rational attackers (Buldas, Jürgenson, Willemson).

Efficient methods to cover the path-space and continuously improve the used trajectory of an autonomous robot moving between two different locations in a dynamic environment (Heero, Willemson, Aabloo, Kruusmaa). International tournaments were organized for computer players of various simple combinatorial games (Willemson). Pair-programming, an agile development method for software engineering was tested empirically (Heiberg, Puus, Salumaa, Seeba).

Digital systems design and test

The research of the design and test group was related to the fundamental and practical aspects of mathematical models and methods for diagnostic modeling of digital systems (DSs). We have achieved a pioneering position with introducing Structurally Synthesized Binary Decision Diagrams (SSBDD), and generalizing BDDs for higher level abstractions of DSs. The main difference of SSBDDs compared to traditional BDDs lies in the novelty of representing structural features and faults. We developed efficient methods for fault simulating DS in a very fast way by uniform algorithms at different levels like logic, register-transfer, instruction set or behavioral levels. Promising results were obtained by SSBDDs in delay simulation, design error diagnosis, fault simulation, and in using DDs for hierarchical test pattern generation. The new fault analysis method based on the full Boolean differential equation allowed to parallelize simultaneously both the fault and test handling and create a simulator which is faster than the present commercial tools available. We developed a new approach for defect-oriented test by mapping physical defects to logic or higher levels to overcome the complexity problem. A method and a tool were produced which allow for the first time to prove the redundancy of physical defects and give the possibility to evaluate test quality more adequately compared to existing tools.

Our results were implemented in testing Systems-on-Chip and Networks-on-Chip by targeting delay and crosstalk faults. A novel Boundary Scan Built-In Self-Test (BIST) concept for autonomous at-speed testing and diagnosis of interconnects was developed which brings high universality, scalability, and configuration independence into the at-speed interconnect testing and diagnosis never achieved before. In the field of BIST we developed methods for fast modeling of test processes in complex structures to optimize hybrid BIST solutions and we proposed a new idea to combine pseudorandom, deterministic and functional testing to achieve high BIST quality. New promising ideas were developed to promote the emerging field of embedded diagnosis in DS.

The results in high-level DD (HLDD) based modeling have been extended for using in verification of RTL and system level DSs. In design error diagnosis, a new concept and method was developed, which allows to adopt in a straightforward way the methods and tools of test field, and a new more general approach was developed that does not exploit error models at all.

In the design field the most important new results were achieved in systems modeling and synthesis, in design for testability, and in developing new BIST architectures. A prototype high-level synthesis tool targeting control and memory intensive applications was developed allowing designers to start with design entry from higher abstraction levels. The tool makes efficient use of commercial logic synthesis tools. As a remarkable synergy of interdisciplinary cooperation between design and test researchers of our group, an accelerator for fault simulation based on reconfigurable HW (FPGAs) was developed which allowed to increase the speed of fault simulation in DSs more than 200 times (Ubar, Raik, Jervan, Ellervee et al.)

Internationalization and attraction of young researchers to computer science and engineering

European projects

The institutions of CDC participated in number of European projects:

- 5th Framework Programme:
  - IST accompanying measures project Establishment of the Virtual Center of Excellence for IST RTD in Estonia, eVikings II (Nov 2002-Sept 2005, IoC coordinator)
  - IST thematic network Network of Excellence in Computational Logic, CoLogNet (Jan 2002-June 2005, IoC partner)
  - IST thematic network Applied Semantics II, APPSEM II (Jan 2003-June 2006, IoC partner)
  - IST thematic network European Robotics Research Network, EURON (Dec 2000-Apr 2004, CS/TUT partner)
  - IST accompanying measures project Research and Training Action for System-on-Chip Design, REASON (Jan 2002-June 2005, CE/TUT partner)
  - IST accompanying measures project An Open Source Technology for Data Certification in Value-Added Services, OpenEvidence (Apr 2002-Sept 2003, CybAS partner)
  - IST them network Roadmaps for Europ Research on Smartcard Technologies, RESET (Sept 2002-May 2003, CybAS partner)

- 6th Framework Programme:
  - IST coordination action Types for Proofs and Programs, TYPES (Sept 2004-Apr 2008, IoC partner)
  - IST integrated project Mobility, Ubiquity, Security for Small Devices, MOBIUS (Sept 2005-Aug 2009, IoC partner)
  - IST network of excellence European Robotics Network, EURON II (May 2004-Apr 2008, CS/TUT partner)
  - IST STREP Knowledge Environment for Interacting Robot Swarms, ROBOSWARM (Nov 2006-Apr 2009, CS/TUT coordinator)
  - IST STREP Verification and Validation of Embedded System Design Workbench, VERTIGO (June 2006-Nov 2008, CE/TUT partner)
  - IST integrated project Algorithmic Principles for Building Efficient Overlay Computers, AEOLUS (Sept 2005-Aug 2009, CybAS partner)
  - IST STREP Reinforcing eGovernment services in Baltic States through legal and accountable digital time stamp, BALTICTIME (Jan 2006-Dec 2008, CybAS partner)
- COST:
  - Action 295 Dynamic Communications Networks: Foundations and Algorithms, DYNAMO (Jan 2005-Jan 2009, CC/TUT in MC)
  - Action IC0701 Formal Verification of Object-Oriented Software (Dec 2007-June 2012, IoC in MC)

In addition, they participated on various bilateral projects etc. under different schemes.

International conferences in Estonia

A number of international conferences were organized in Estonia:

- 14th Nordic Wksh on Programming Theory, NWPT ’02, Tallinn, Nov 2002
- 2nd Annual Meeting of APPSEM II, APPSEM ’04, Apr 2004
- 5th Int Summer School on Advanced Functional Programming, AFP ’04, Tartu, Aug 2004
- 9th Biennial Baltic Electronics Conf, BEC ’04, Tallinn, Oct 2004
- 10th European Test Symp, ETS ’05, Tallinn, May 2005
- 20th Int Conf on Automated Deduction, CADE-20, Tallinn, July 2005
- 9th Symp. on Programming Languages and Software Tools, SPLST ’05, Tartu, Aug 2005
- 9th East-European Conf on Advances in Databases and Information Systems, ADBIS 05, Tallinn, Sept 2005
- 6th Int Symp on Trends in Functional Programming, TFP 2005 / 10th ACM SIGPLAN Int Conf on Functional Programming, ICFP 2005 / 4th Int Conf on Generative Programming and Component Engineering, GPCE 2005, Tallinn, Sept/Oct 2005
- IFIP WG 2.8 Meeting #22, Kalvi manor, Oct 2005
- 10th Nordic Wksh on Secure IT Systems, NordSec 2005, Tartu, Oct 2005
- 8th Int Conf on Mathematics of Program Construction, MPC ’06 / 11th Int Conf on Algebraic Methodology and Software Technology, AMAST ’06, Kuressaare, July 2006
- 7th Joint Conf on Knowledge-Based Software Engineering, JCKBSE ’06, Tallinn, Aug 2006
- Joint 19th IFIP Int Conf on Testing Communicating Systems and 7th Int Wksh on Formal Approaches to Testing of Software, TestCom-FATES 2007 / 27th IFIP WG 6.1 Int Conf on Formal Methods for Networked and Distributed Systems, FORTE 2007, Tallinn, June 2007
- TYPES Wksh on Effects and Type Theory, EffTT, Tallinn, Dec 2007

Winter schools, summer schools, theory days

CDC organized various schools and workshops targeted at young researchers.

Estonian Winter Schools in Computer Science IoC continued the organization of EWSCS schools: a series of regional-scope international winter schools in theoretical computer science. The emphasis on these schools is on Theory A (algorithms, complexity) and Theory B (logic and semantics). The programme of an EWSCS school consists of 4..5 courses of 6 hours from renowned scientists and a student session. The typical attendance is 50, whereof 4..5 lecturers and approx students are from abroad. All schools expect for the 1st one in 1996 have taken place at Palmse.

Some lecturers over the years include S Artemov, Arvind, G Barthe, J Bergstra, G Chaitin, P Cousot, I Damgård, O Danvy, W P de Roever, N Halbwachs, J Håstad, A Ingólfsdóttir, A Jung, K G Larsen, H Mannila, J Massey, Yu Matiasevich, K Mehlhorn, P B Miltersen, G Morrisett, M Naor, J N Oliveira, G Păun, J Reynolds, Ph Rogaway, C Schnorr, H Schwichtenberg, H Seidl, M Sudan, R Wilhelm, W Yi, M Yung.

Estonian Summer Schools in Computer and Systems Science The ESSCaSS annual summer schools are a younger sister of EWSCS. These schools have a bias towards systems engineering, software engineering, artificial intelligence. The format is similar to that of EWSCS. The typical attendance is 30..40. Some of the lecturers include D Bjørner, B Fischer, R Dearden, J Hatcliff, J-M Jacquet, R Kurki-Suonio, A Møller, D Peled, A Ravn, M Veanes.

The first school in 2002 was at Kohala, organized by CC/TUT. The next school 2003-2005 (Taagepera, 2 × Pedase) were organized by IoC. The schools of 2006-2007 (Pedase, Lepanina) were organized by CS/UT within the ICT doctoral school project.

Besides CDC, EWSCS and ESSCaSS benefitted from the Tiger University and Tiger University Plus programmes.

Theory Days The Tallinn-Tartu Theory Days targeted primarily at doctoral and master students were born thanks to CDC. The program of these 3-day workshops of consists of tutorials, technical presentations and "interactive seminars" from international guests (1..2), researchers/teachers and students. They are held in different places twice a year from autumn 2002, organized in alternation by IoC and CS/UT.

The theory days are highly popular and their attendance is 35..45.

Guest courses

A number of short courses were taught by international lecturers at IoC, TUT, UT: by T Altenkirch (Nottingham), M Hansen (DTU), R Hartenstein (Kaiserslautern), L Barbosa (Minho), M Fränzle (DTU), T Vierhaus (TU Cottbus), M Bezem (U Bergen), D Borrione & P Amblard (U Grenoble I), E Elkind (U Warwick), M Backes (U Saarlandes), Yu Lifshits (POMI St Petersburg), G Pace (U Malta), D Foty (Gilgamesh), I Kotenko & A Ulanov (SPIIRAS), M Veanes (Microsoft), J van Lent (Bath), G Ganezis (Microsoft).

Many of these were financed by the Tiger University/Tiger University Plus programmes or the doctoral school in ICT.

PhD education

12 PhDs were defended during the centre's existence:

H Tamm (Helsinki UT, 2004), H Nestra (UT, 2006); R Savimaa (TUT, 2005), U Norbisrath (RWTH Aachen, 2007), J Ernits (TUT, 2007); K Heero (UT, 2006); M Brik (TUT, 2002), A Jutman (TUT, 2004), G Jervan (Linköpings Univ., 2 005), J Fomina (TUT, 2005), E Ivask (TUT, 2006), E Orasson (TUT, 2007)

At this moment 38 PhD students are being supervised by the senior staff of CDC.

Sufficient inflow of motivated PhD students and timely graduation are still major concerns and the centre had less opportunities than expected to make an impact on institutional PhD education.

Repatriation / Foreign researchers

Some researchers from Estonia that had studied or worked abroad returned: H Tamm, G Jervan, H Lipmaa. Some researchers of Estonian origin worked here: A Löh, A Eppendahl. We also attracted foreign researchers to work as postdocs: O Shkaravska, U Norbisrath.

Related projects

A number of projects cofinanced the activities of CDC:

- FP5 IST accompanying measures project eVikings II (Nov 2002-Sept 2005): the core workpackages WP2..4 had the same objectives as CDC – strengthening the research in software technologies, information security and digital systems.
- Infrastructure programme for CoEs of Enterprise Estonia: CDC received funds for infrastructure within the CDC-INFRA project,
- Centres of technological competence programme of Enterprise Estonia: CS/TUT, CE/TUT and CybAS participated in the ELIKO centre (electronics and information & communication technologies).
- Doctoral schools of Measure 1.1 of the National Development Plan for the Implementation of EU Structural Funds 2004-06: national doctoral school in ICT (Sept 2005-June 2008).
- Tiger University and Tiger University Plus national programmes to support university education: all winter schools/summer schools of CDC benefitted from this programme.