Conference of PhD Students in Computer Science

Volume of extended abstracts

CS^2

Organized by the Institute of Informatics of the University of Szeged

July 1–4, 2002
Szeged, Hungary

Scientific Committee:

Mátyás Arató (KLTE)
Miklós Bartha (SZTE)
András Benczúr (ELTE)
Tibor Csendes (SZTE)
János Csirik (SZTE)
János Demetrovics (SZTAKI)
Sarolta Dibuz (Ericsson)
József Dombi (SZTE)
Zoltán Ésik (SZTE)
Ferenc Friedler (VE)
Zoltán Fülöp (SZTE)
Ferenc Gécseg (chair, SZTE)
Balázs Imreh (SZTE)
János Kormos (KLTE)
László Kozma (ELTE)
Attila Kuba (SZTE)
Eörs Máté (SZTE)
Gyula Pap (KLTE)
András Recski (BME)
Endre Selényi (BME)
Katalin Tarnay (NOKIA)
György Turán (SZTE)
László Varga (ELTE)

Organizing Committee:

Tibor Csendes, Lajos Schrettner, Mariann Sebő, Péter Gábor Szabó, Boglárka Tóth, Tamás Vinkó

Address of the Organizing Committee

c/o. Tibor Csendes
University of Szeged, Institute of Informatics
H-6701 Szeged, P.O. Box 652, Hungary
Phone: +36 62 544 305, Fax: +36 62 420 292
E-mail: `cscs@inf.u-szeged.hu`
URL: `http://www.inf.u-szeged.hu/~cscs/`

Main sponsor

SIEMENS Sysdata

Sponsors

City Major's Office, Szeged, Novadat Bt., Polygon Publisher, the Szeged Region Committe of the Hungarian Academy of Sciences, TiszaneT Rt, University of Szeged, Institute of Informatics.

Preface

This conference is the third in a series. The organizers have tried to get together those PhD students who work on any fields of computer science and its applications to help them possibly in writing their first abstract and paper, and may be to give their first scientific talk. As far as we know, this is one of the few such conferences. The aims of the scientific meeting were determined on the council meeting of the Hungarian PhD Schools in Informatics: it should

- provide a forum for PhD students in computer science to discuss their ideas and research results,
- give a possibility to have constructive criticism before they present the results in professional conferences,
- promote the publication of their results in the form of fully refereed journal articles, and finally
- promote hopefully fruitful research collaboration between the participants.

The best talks will be awarded with the help of our sponsors. The papers emerging from the presented talks will be forwarded to the journals of Acta Cybernetica (Szeged), and Periodica Polytechnica (Budapest); and the mathematics oriented papers to Publicationes Mathematicae (Debrecen). The deadline for the submission of the papers is the end of August 2002. The manuscripts will be forwarded to the proper journals. To get acquainted with the style of the journals please study earlier issues of them. One sample paper is available at `http://www.inf.u-szeged.hu/~cscs/csallner.tex`.

Although we did not advertise it on the web, a high number of good quality abstracts have been submitted. If you encounter any problems during the meeting, please do not hesitate to contact one of the Organizing Committee members. The organizers hope that the conference will be a valuable contribution to the research of the participants, and wish a pleasant stay in Szeged.

Szeged, June 2002

Tibor Csendes

Contents

Preliminary Program

Overview

Monday, July 1

- 10:00 - 14:00 Registration
- 14:00 - 14:15 Opening
- 14:15 - 15:00 Plenary talk
- 15:00 - 15:15 Break
- 15:15 - 16:45 Talks in 2 streams (3x30 minutes)
- 16:45 - 17:00 Break
- 17:00 - 18:00 Talks in 2 streams (2x30 minutes)
- 18:15 - 19:30 Reception at the Town Hall

Tuesday, July 2

- 08:30 - 10:00 Talks in 2 streams (3x30 minutes)
- 10:00 - 10:15 Break
- 10:15 - 11:00 Plenary talk
- 11:00 - 11:15 Break
- 11:15 - 12:45 Talks in 2 streams (3x30 minutes)
- 12:45 - 14:00 Lunch
- 14:00 - 15:30 Talks in 2 streams (3x30 minutes)
- 15:30 - 15:45 Break
- 15:45 - 17:15 Talks in 2 streams (3x30 minutes)
- 18:00 - 19:30 Supper

Wednesday, July 3

- 08:30 - 09:30 Talks in 2 streams (2x30 minutes)
- 09:30 - 09:45 Break
- 09:45 - 10:30 Plenary talk
- 10:30 - 10:45 Break
- 10:45 - 12:45 Talks in 2 streams (4x30 minutes)
- 12:45 - 14:00 Lunch
- 14:00 - 15:30 Talks in 2 streams (3x30 minutes)
- 15:30 - 15:45 Break
- 15:45 - 17:15 Talks in 2 streams (3x30 minutes)
- 18:00 - 21:00 Excursion and supper

Thursday, July 4

- 08:30 - 10:00 Talks in 2 streams (3x30 minutes)
- 10:00 - 10:15 Break
- 10:15 - 11:00 Plenary talk
- 11:00 - 11:15 Break
- 11:15 - 12:45 Talks in 2 streams (3x30 minutes)
- 12:45 - 14:00 Lunch
- 14:00 - 15:30 Talks in 2 streams (3x30 minutes)
- 15:30 - 15:45 Break
- 15:45 - 17:45 Talks in 2 streams (4x30 minutes)
- 18:00 - 18:30 Closing session, announcing the Best Talk Awards
- 19:00 - 20:30 Supper

Friday, July 5

- 8:30 Departure

Detailed program

Monday, July 1

10:00	Registration	
14:00	Opening session	
14:15	**Plenary talk** Gábor Herman (New York): *Recovery of Label Distributions*	
15:00	Break	
Sections	**Networks**	**Operations Research**
15:15	József Valyon: *Reducing the complexity and controlling the network size of LS-SVM solutions, by solving an overdetermined set of equations*	Péter Kárász: *On a Class of Cyclic-Waiting Queuing Systems with Refusals*
15:45	Alexandrosz Burulitisz, Róbert Maka, Balázs Rózsás, Sándor Szabó, and Sándor Imre: *On the Performance of IP Micro Mobility Protocols*	János Balogh and Tamás Rapcsák: *Test functions and to test functions: a framework for global optimization on Stiefel manifolds*
16:15	Antal Fazakas and Katalin Tarnay: *Inline Expressions in Protocol Test Specification*	Mihály Csaba Markót, José Hernández and Leocadio Casado: *New Interval Methods for Constrained Global Optimization: Solving 'Circle Packing' Problems in a Reliable Way*
16:45	Break	
Sections	**Software engineering**	**Image processing**
17:00	Ákos Kiss, Judit Jász, and Gábor Lehotai: *Static Slicing of Binary Executables*	Gergely Kovásznai and Krisztián Veréb: *Mathematical Morphology in Image Processing by SLD Resolution*
17:30	Gábor Kusper: *Investigation of Binary Representations of SAT especially 2-Literal Representation*	György Koch and József Dombi: *1-dimensional clustering with aggregated functions*
18:15	Reception at the Town Hall	

Tuesday, July 2

Sections	**Databases**	**Artificial intelligence**
08:30	István Szépkúti: *Difference Sequence Compression of Multidimensional Databases*	Tim Fuehner and Gabriella Kókai: *Incorporating Linkage Learning into the GeLog Framework*
09:00	Mohammed Alhaddad: *Utilising Networked Workstations to Accelerate Database Queries*	Zoltán Tóth: *A Graphical User Interface for Evolutionary Algorithms*
09:30	István Katsányi: *On Implementing Relational Databases on DNA strands*	Róbert Ványi: *Structural Description of Binary Images: An Evolutionary Approach*
10:00	Break	
10:15	**Plenary talk** János Pintér (Halifax): *Global / Nonlinear Optimization in Modeling Environments*	
11:00	Break	
Sections	**Optimization**	**Image processing**
11:15	Péter Gábor Szabó: *Optimal substructures in optimal and candidate circle packings*	Attila Tanács, Kálmán Palágyi, and Attila Kuba: *A fully automatic medical image registration algorithm based on mutual information*
11:45	Boglárka Tóth: *Empirical investigation of the convergence of inclusion functions*	Krisztián Veréb: *Complex Pattern Matching Strategies in Image Database: The cut-and-or-not Approach*
12:15	Tamás Vinkó: *Branch and Prune Techniques in Multidimensional Interval Global Optimization Algorithms*	Péter Balázs, Attila Kuba, and Emese Balogh: *A Fast Algorithm for Reconstructing hv-convex 8-connected but not 4-connected Discrete Sets*
12:45	Lunch	

(see next page for the rest of the **Tuesday** program)

Sections	**Networks**	**Artificial intelligence**
14:00	Márta Fidrich, Vilmos Bilicki, Zoltán Sógor, and Gábor Sey: *SIP compression*	Balázs Szörényi: *ID3 is not an Occam algorithm*
14:30	Timót Hidvégi: *Optimized emulated digital CNN-UM (CASTLE) Architectures*	Gábor Gosztolya, András Kocsor, László Tóth, and László Felföldi: *Various Robust Search Methods in a Hungarian Speech Recognition System*
15:00	Endre Horváth: *Bluetooth Modelling, Validation and Test Suite Generation*	Zoltán Nagy: *Fast and Efficient Multi-Layer CNN-UM Emulator Using FPGA*
15:30	Break	
Sections	**Programming**	**Numerical algorithms**
15:45	Raluca Oana Scarlatescu: *Programming by steps*	Tibor Laczó and László Sragner: *Model Order Estimations for Noisy Black-box Identifications*
16:15	Dániel Szegő: *Automatic Wizard Generation*	Gábor Balázs, Béla Drozdik, and András Jókuthy: *New Methods in Tele-cardiology*
16:45	Tamás Kasza, Sarolta Dibuz, Tibor Szabó, and Gyula Csopaki: *Applicability of UML in Protocol and Test Development*	Kristóf Haraszti: *Noise Reduction on ECG-signals with the Help of Syncronized Averaging*
18:00	Supper	

Wednesday, July 3

Sections	**Networks**	**Software engineering**
08:30	János Horváth Cz. and Sándor Imre: *Optimal Platform to Develop Features for Ad Hoc Extension of 4G Mobile Networks*	Róbert Lovas and Péter Kacsuk: *Enhanced Macrostep-based Debugging Methodology for Parallel Programs*
09:00	József Hosszú: *Test Architecture for Distributed Network Management Software*	Tamás Kókai and Tibor Csiszár: *Role oriented software development in practice*
09:30	Break	
09:45	**Plenary talk** Zoltán Fülöp (Szeged): *Tree Transducers*	
10:30	Break	
Sections	**Automata**	**Algorithms**
10:45	Matti Rönkä: *On One-Pass Term Rewriting and Tree Recognizers with Comparisons Between Brothers*	Krisztián Keszthelyi: *The Analysis of the Economy of the Milk Processing Companies in 2000 with Multivariate Methods*
11:15	Lajos Kollár: *Application of Tree Automata in The Validation of XML Documents*	Balázs Polgár and Endre Selényi: *Probabilistic Diagnostics with P-Graphs*
11:45	Miklós Krész and Miklós Bartha: *Soliton graphs and graph-expressions*	Gabriel Raicu: *Distributed Expert System in Port Area*
12:15		Richárd Szabó: *Navigation of simulated mobile robots in the Webots environment*
12:45	Lunch	

(see next page for the rest of the **Wednesday** program)

Sections	**Protocols**	**Programming**
14:00	Sándor Imre, Róbert Schulcz, and Csaba Csegedi: *IPv6 Macromobility Simulation Using OMNeT++ Environment*	Dániel Varró: *A Pattern Based Constraint Language for Metamodels*
14:30	Anna Harmathné Medve: *Relations of Testability and Quality Parameters of SDL Implementation at the Early Stage of Protocol Development Life Cycle*	Dávid Hanák: *Implementing Global Constraints as Structured Networks of Elementary Constraints*
15:00		Tibor Csáki and Krisztián Veréb: *The Jodie Programming Language*
15:30	Break	
Sections	**Artificial intelligence**	**Image processing**
15:45	Tamás Szabó: *CNN Based Early Detection of Acute Ischemic Lesion*	Marianna Dudásné Nagy and Attila Kuba: *Reconstruction of Factor Images of Dynamic SPECT by Discrete Tomography*
16:15	Ákos Zsiros: *Application of Learning Methods in MCDA models: Overview and Experimental Comparison*	Péter Kozma: *Colour Space Transformation, Colour Correction and Exact Colour Reproduction on FALCON Architecture*
16:45	László Felföldi, András Kocsor, and László Tóth: *Classifier Combination in Speech Recognition*	Attila Licsár and Tamás Szirányi: *Hand Gesture-based Film Restoration*
18:00	Excursion and supper	

Thursday, July 4

Sections	**Networks**	**Discrete algorithms**
08:30	Attila Rajmund Nohl and Gergely Molnár: *On the convergence of OSPF*	Csilla Endrődi: *Efficiency Analysis and Comparison of Public Key Algorithms*
09:00	István Pataki and András Gulyás: *End-to-end QoS Management Issues Over DiffServ Networks*	Paula Steinby: *Content Protection: Combining Watermarking with Encryption*
09:30	János Zoltán Szabó: *Performance Testing Architectures for Communication Protocols*	Péter Orvos: *Digital Signatures with Signer's Biometric Authentication*
10:00	Break	
10:15	**Plenary talk** Csaba Fábián (Bukarest): *Evolutionary and Parallel Solving Methods for Cutting Stock Problems*	
11:00	Break	
Sections	**Web solutions**	**Artificial intelligence**
11:15	Andor Abonyi-Tóth, Dénes Eglesz, and Orchidea Edith Kiss: *Examining Private and Professional Websites Regarding Technique and Usability*	Tamás Gergely: *Measures for Decision Tree Building*
11:45	Richárd Jónás: *Building Web Applications via Web*	András Hócza, Gyöngyi Szilágyi, and Tibor Gyimóthy: *LL Frame System of Learning Methods*
12:15	László Zömbik: *Traffic analysis of HTTPS*	András Salamon: *Rewarding Misclassifications in Oblique Decision Tree Learning*
12:45	Lunch	

(see next page for the rest of the **Thursday** program)

Sections	**Networks**	**Artificial intelligence**
14:00	Richárd Jónás, Lajos Kollár, and Krisztián Veréb: *A Communication System Based on Web Service and its Application in Image Processing*	István Juhos, Gyöngyi Szilágyi, János Csirik, György Szarvas, Tamás Szeles, and Attila Kocsis : *Time Series Prediction using Artifical Intelligence Methods*
14:30	Dániel Petri: *Towards Verifyable Design Patterns*	Kornél Kovács and András Kocsor: *Various Hyperplane Classifier Using Kernel Feature Spaces*
15:00		Szilvia Gyapay: *Operation Research Methods in Petri Net Based Analysis of IT Systems*
15:30	Break	
Sections	**Programming**	**Modelling**
15:45	Dávid Hanák and Tamás Szeredi: *FDBG, a CLP(FD) Debugger for SICStus Prolog*	Tibor Csiszár and Tamás Kókai: *The basics of roleoriented modelling*
16:15	Ferenc Havasi and Miklós Kálmán: *XML Semantics*	Nóra Székely: *Simplifying the Model of a Complex Industrial Process Using Input Variable Selection*
16:45	Viktória Zsók, Zoltán Horváth, and Máté Tejfel: *Parallel Functional Programming on Cluster*	Orsolya Dobán: *Software Development Effort Estimation and Process Optimization*
17:15	Dan Laurentiu Jisa: *Comparative Study of Four UML Based CASE Tools*	László Ruskó, Attila Kuba, and Emese Balogh: *VRML Based Visualization of Discrete Tomography Pictures*
18:00	Closing session, announcing the Best Talk Awards	
19:00	Supper	

Examining private and professional websites regarding technique and usability

Andor Abonyi-Tóth, Dénes Eglesz, and Orhidea Edith Kiss

With the growing popularity of the internet, more and more people feel it necessary to publish their own homepage on the World Wide Web. The companies also recognized the importance of their online presence, but they can not always find the best form of their online appearance, so their websites can be criticized in many aspects. One of the reasons can be that there is no general recipe for creating a good website, as these homepages have to suit many – often contradictory – expectations.

In our article we examine homepages of amateur and expert website designers. Andor Abonyi-Tóth examines the self-made homepages of future informatics teachers and programmer-mathematician students at ELTE. In each semester nearly 300 students attend his (distant learning) courses, and create their first own websites. He is compiling a comprehensive listing of typical mistakes and errors on these pages, also indicating the possible solutions for them. (`http://www.html-kezdoknek.ini.hu`)

Dénes Eglesz – editor of online gaming magazine PC Dome (`http://www.pcdome.hu`) – has actively participated in the design and development of several highly visited professional websites. Based on his experience and on other well respected sources, we gathered a list of aspects that will be the reference for examining the amateur and professional websites. This listing will not only be used for this examination, but it will also be made available for the students learning the basics of HTML.

Orhidea Edith Kiss takes part in teaching software ergonomics at her department (Izsó, L., Hercegfi, K.: Website usability. Supplementary resource, BME DEP, 2002). Together with the students she is examining usability issues of navigational solutions and tools offered by different websites.

Based on the sources above, we have created a list of aspects for our examination. Main aspects of usability:

- download speed
- ease of overview
- navigational solutions
- content
- design
- spelling
- regular updates

Besides it we are also examining the sites regarding technical solutions:

- clearness of the HTML code, missing or unnecessary elements
- structure of the page
- usage of tables
- usage, optimization of images and animations, different image types
- support for different browsers
- topological examination, error messages

In our article we will be pointing out the good and bad solutions through concrete examples.

For helping the students examine their work themselves, we are also presenting some free- and shareware programs and online services that can be used for such purposes.

Utilising Networked Workstations to Accelerate Database Queries

Mohammed Alhaddad

The rapid growth in the size of databases and the advances made in Query Languages has resulted in increased SQL query complexity submitted by users, which in turn slows down the speed of information retrieval from the database. The future of high performance database systems lies in parallelism. Commercial vendors´ database systems have introduced solutions but these have proved to be extremely expensive.

The main research in this project considers how network resources such as workstations can be utilised by using Parallel Virtual Machine (PVM) to Optimise Database Query Execution. An investigation and experiments of the scalability of the PVM are conducted. PVM is used to implement parallelism in two separate ways: (i) Remove the work load for deriving and maintaining rules from the data server for Semantic Query Optimisation, therefore clears the way for more widespread use of SQO in databases [1,2]. (ii) Answer users queries by a proposed Parallel Query Algorithm PQA which works over a network of workstations, coupled with a sequential Database Management System DBMS called PostgreSql on the prototype called Expandable Server Architecture ESA [3,4].

Experiments have been conducted to tackle the problems of Parallel and Distributed systems such as task scheduling and load balance.

References

[1] Robinson J, Lowden B, Alhaddad M. "Utilizing Multiple Computers in Database Query Processing and Descriptor Rule Management´´, Dexa´01 September 3-7 2001, LNCS 2113, page 897.

[2] Robinson J, Lowden B, Alhaddad M, "Distributing the Derivation and Maintenance of Subset Descriptor Rules´´,The 5 th World Multi-Conference on Systemics, Cybernetics and Informatics. SCI 2001. July 22-25, 2001. Orlando, Florida USA

[3] Mohammed Al Haddad, Jerome Robinson, "Using A Network of workstations to enhance Database Query Processing Performance´´, Euro PVM/MPI 2001, The 5th World Multi-Conference on Systemics, Cybernetics and Informatics, July 22,2001, LNCS 2131 Page 352.

[4] Alhaddad M Robinson J, "Extending Database Technology by Expanding Data Servers´´,The 6 th World Multi-Conference on Systemics, Cybernetics and Informatics. SCI 2002. July 14-18, 2002. Orlando, Florida USA

New methods in Tele-cardiology[1]

Gábor Balázs, Béla Drozdik, and András Jókuthy

The paper is focusing on new methods aimed to improve the inadequate accessibility of diagnostics-related information (and expertise) for the competent members of the co-operating professional medical community. An intensive application of modern information technology can effectively alleviate this problem. Our goal is to apply proven and new methods of exact and applied natural sciences to this problem, with a special emphasis on the preventive and curative health care of cardiovascular diseases. In our work we would like to present the system overview and the first experiences of a government-funded pilot project of co-operating Hungarian research and industrial institutions. Among others, the project aims to improve preventive cardiac care, design better diagnostic methods for cardiovascular diseases, and support post-treatment remote monitoring. We would like to describe two, loosely coupled subsystems of the overall effort, i.e. the internet-based risk assessment and advisory system (RAS) and the remote monitoring system (**RMS**), both specialized in cardiovascular diseases.

With RAS, our goal is to design an internet based interactive information system, which supports risk assessment, health conservation counselling and can generate weekly menus for a healthy lifestyle. We also plan to integrate decision support into the system with a high level medical background. The system aims to avoid the development of a high-risk medical state at the very basic social level, by minimising the effect of the controllable risk factors. The **RAS** system is designed to provide personalized risk assessment and dietary advice with respect to cardiovascular diseases. The emphasis in this system is on prevention by giving the right and realistic advice. The target users of the system are health-conscious middle-age or younger men and women who want to decrease their cardiovascular risks.

Over the last years there has been an enormous development within the field of internet and telecommunications including mobile applications. Remote monitoring is based on these modern solutions. We can use several technologies to monitor physiological parameters such as ECG parameters. The basic motivation of **RMS** is to cut down healthcare-related costs for both the health institution (hospital) and the patient by supporting some examinations (ECG, blood pressure, etc.) to be performed conveniently at home, and the results to be transmitted to a central medical database. These results automatically evaluated by the system. In case of an emergency situation, information is sent directly for human evaluation to the Monitoring Service, available 24 hours a day. The medical doctor at the Service can contact the patient, the ambulance or the nearest competent hospital by phone. In this way all the costs and troubles (such as travel from remote locations) related to routine medical examinations can be avoided. To achieve intelligent monitoring with alarms based on input parameters there is a need for integrated decision support, the aim of which is to provide a medical decision–making diagnostic support. These auto-diagnoses draw the attention of the doctor to the possible problems.

Remote monitoring and interactive remote counselling provide a cost-effective and comfortable means of medical care. We would like present the first experiences of the two of above systems, both in the field of cardiovascular diseases. The prototype medical instruments, the database design and the user interfaces are elaborated.

[1]The work has been supported by National Research and Development Program NKFP #2/052/2001

A Fast Algorithm for Reconstructing hv-convex 8-connected but not 4-connected Discrete Sets

Péter Balázs, Attila Kuba, and Emese Balogh

One of the most frequently studied area of discrete tomography is the problems of the reconstruction of 2-dimensional (2D) discrete sets from their row and column sum vectors. Reconstruction in certain classes of discrete sets can be NP-hard. Since applications require fast algorithms, it is important to find algorithms in those classes of 2D discrete sets where the reconstruction can be performed in polynomial time.

An important class of discrete sets where the reconstruction problem can be solved in polynomial time is the class of hv-convex 8-connected sets. The worst case complexity of the fastest algorithm known so far for solving the problem describing it by a 2SAT expression is $O(mn \cdot \min\{m^2, n^2\})$. However as it is shown, in the case of 8-connected but not 4-connected sets we can give an algorithm with worst case complexity of $O(mn \cdot \min\{m, n\})$ by identifying the so-called $\mathcal{S}_4$ -components of the discrete set. We also show that our algorithm can be generalized to solve the reconstruction problem in a broader class than the hv-convex 8-connected sets. Experimental results are also presented.

Test functions and to test functions: a framework for global optimization on Stiefel manifolds

János Balogh and Tamás Rapcsák

Some methods of the global optimization are dealt and tested on Stiefel manifolds. The structure of the optimizer points is given theoretically and numerically for the lowest interesting dimensional case, as well as the criterion for the finiteness of the number of optimizer points. Some reduction tricks and numerical results are obtained, and test functions with known optimizer points and their optimal function value. A restriction, discretization of the problem is formulated which is equivalent to the well known assignment problem.

In 1935, Stiefel introduced a differentiable manifold consisting of all the orthonormal vector system $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k \in \mathbb{R}^n$, where $\mathbb{R}^n$ is the n-dimensional Euclidean space and $k \leq n$ [1]. Bolla et al. analyzed the maximization of sums of heterogeneous quadratic functions on Stiefel manifolds based on matrix theory and gave the first-order and second-order necessary optimality conditions and a globally convergent algorithm [2]. Rapcsák introduced a new coordinate representation and reformulated it to a smooth nonlinear optimization problem, then by using the Riemannian geometry and the global Lagrange multiplier rule [3, 4], local and global, first-order and second-order, necessary and sufficient optimality conditions were stated, and a globally convergent class of nonlinear optimization methods was suggested.

In the present work, solution methods and techniques are investigated for optimization on Stiefel manifolds. Consider the following optimization problem:

$$\min \sum_{i=1}^{k} \mathbf{x}_i^T A_i \mathbf{x}_i \tag{1}$$

$$\mathbf{x}_i^T \mathbf{x}_j = \delta_{i,j}, \qquad 1 \leq i, j \leq k, \tag{2}$$

$$\mathbf{x}_i \in \mathbb{R}^n, \quad i = 1, \ldots, k, \qquad n \geq 2,$$

where A_i, $i = 1, \ldots, k$, are given symmetric matrices, and δ_{ij} is the Kronecker delta. Furthermore, let $M_{n,k}$ denote the Stiefel manifold consisting of all the orthonormal systems of k n-vectors.

We characterize the structure of the optimizer points and give a criterion for the finiteness of the number of the optimizer points on $M_{2,2}$ of (1-2). The case of diagonal matrices A, $i = 1, \ldots, k$, is dealt separately where all coordinates of the optimizer points are from the set $\{0, +1, -1\}$ (except the extreme case when all feasible points are optimizer points, as well).

We have studied numerically the same problem to understand the structure of the problem and investigated an example with a diagonal coefficient matrix using a stochastic method [5] and a reliable one [6], [7]. The aim of the last one was to obtain verified solutions. It can be interesting that using the GlobSol program [6], [7], verified solutions are obtained only when making spherical substitutions, while for a similar problem on $M_{3,3}$ it runs a few days without providing verified solution – if no coordinate transformation or reduction of the variables was made. Thus, it seems indispensable to use some reduction tricks to make the numerical tools effective. Some accelerating changes are suggested in the present work.

Since the result can be non-verified as it have been seen, by reversing the process we give a series of test problems with arbitrary size (where n and k are parameters). These belong to an important area of the global optimization (see [8] and [9]), the constrained test problems which are generally related to industrial applications.

Theoretical investigation is given for the discretization of the problem (1-2), which is equivalent to the well-known assignment problem. It can be seen easily that instead of the objective function of (1), we can use another one, for example, the quadratic function

$$\sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{t=1}^{n} \sum_{r=1}^{n} a_{ij} \mathbf{x}_{it} \mathbf{x}_{jr} b_{tr}$$

and the respective restriction to the values give an NP-hard problem, the quadratic assignment problem, see [10] or [11].

Acknowledgment: The support provided by the Hungarian National Research Foundation (project Nos. T 034350 and T029572) and by the APOLL Thematic Network Project within the Fifth European Community Framework Program (FP5, project No. 14084) is gratefully acknowledged.

References

[1] E. Stiefel. Richtungsfelder und Fernparallelismus in n-dimensionalem Mannigfaltigkeiten. Commentarii Math. Helvetici, 8: 305–353, (1935-36).

[2] M. Bolla, G. Michaletzky, G. Tusnády, M. Ziermann. Extrema of sums of heterogeneous quadratic forms. Linear Algebra and its Applications, 269 (1): 331-365, (1998).

[3] T. Rapcsák. On minimization of sums of heterogeneous quadratic functions on stiefel manifolds. In P. Pardalos, A. Migdalas, and P. Varbrand, editors, From local to global optimization. Kluwer, Dordrecht, 277-290, (2001).

[4] T. Rapcsák. On minimization on stiefel manifolds. European Journal of Operational Research, (in print).

[5] T. Csendes. Nonlinear parameter estimation by global optimization – efficiency and reliability. Acta Cybernetica, 8: 361-370, (1988).

[6] G.F. Corliss and R.B. Kearfott. Rigorous global search: Industrial applications. In T. Csendes, editor, Developments in Reliable Computing. Kluwer, Dordrecht, (1999).

[7] R.B. Kearfott. Rigorous Global Search: Continuous Problems. Kluwer, Dordrecht, (1996).

[8] C.A. Floudas and P.M. Pardalos. A Collection of Test Problems for Constrained Global Optimization Algorithms. Lecture Notes in Computer Science 455, Springer-Verlag, Berlin/Hiedelberg/New York, (1990).

[9] C.A. Floudas, P.M. Pardalos, C.S. Adjiman, W.R. Esposito, Z.H. Gumus, S.T. Harding, J.L. Klepeis, C.A. Meyer, C.A. Schweiger. Handbook of Test Problems for Local and Global Optimization. Kluwer Academic Publishers, (1999).

[10] P. Pardalos, F. Rendl, H. Wolkowicz. The quadratic assignment problem: A survey and recent developments. In Proceedings of the DIMACS Workshop on Quadratic Assignment Problems, volume 16 of DIMACS Series in Discrete Mathematics and Theoretical Computer Science, pages 1-41. American Mathematical Society, (1994).

[11] S. Sahni, and T. Gonzalez. P-complete approximation problems, J. Assoc. Comput. Moch. 23: 555-565, (1996).

On the performance of IP micro mobility protocols

Alexandrosz Burulitisz, Róbert Maka, Balázs Rózsás, Sándor Szabó, and Sándor Imre

Due to the growing number of mobile communication systems, there is a demand for IP-based mobile networks [1]. Mobile IP provides mobility support in IP-based networks, but in wireless environment new architecture is needed to support the fast and frequent handovers. The idea of mobile IP is based on the home agent - foreign agent model, where the home agent forwards the packets, addressed to the given mobile computer, to the foreign agent that delivers them to the mobile. Registration at the home agent costs a lot of time, if the mobile is far away from its home network. In mobile networks with small cell sizes, the frequent handovers trigger frequent reregistrations and can lead to frequent disconnection. Micro mobility protocols are the solutions for this problem [2]. These protocols improve the performance of mobile IP by hiding user movement inside a well-defined area. There are several solutions to handle this problem, for example Cellular IP and HAWAII and HMIP [3,4]. At present time there is no standard for micro mobility protocol, that is why the investigation and comparison of the performance of the different proposals is important. We have analyzed and compared the performance of three micro mobility protocols. We gave a theoretical model for performance evaluation of HAWAII, CIP and HMIP protocol based network, and we gave analytical results on the number of the protocol messages and other traffic parameters (e.g. delay time). Besides the mathematical calculation, we analyzed the performance of these protocols - in the function of the number of mobile users, the coverage area of a domain, etc. - using the NS simulator with the Columbia IP Micro-Mobility Suite extension. In this article we present our results on analyzing the IPv4 micro mobility protocols. The monitored parameters of a test network were the mobility related protocol messages, successful handovers and delay. Some analytical results (the number of administrative messages in the function of number of terminals) can be seen in figure 1, and the verification by the NS simulator program is depicted in figure 2.

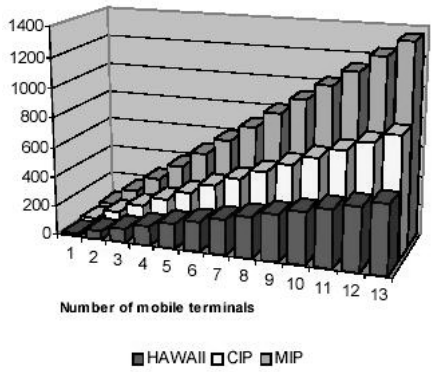

Figure 1. Analytical results

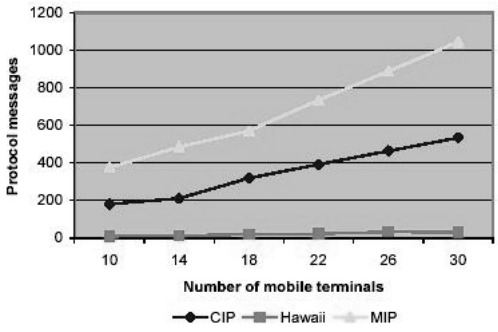

Figure 2. Simulation results

References

[1] Ramachandran Ramjee, Thomas F. La Porta, Luca Salgarelli, Sandra Thuel, and Kannan Varadhan, Bell Labs, Lucent Technologies Li Li, Cornell niversity: IP-Based Access Network Infrastructure for Next-Generation Wireless Data Networks", IEEE Personal Communication, August 2000

[2] Bernd Gloss, Christian Hauser: "The IP Micromobility Approach", 2000

[3] Csaba Keszei, Jukka Manner, Zoltán Turányi, András Valkó: "Mobility Management and Qos in Brain Networks"

[4] R. Ramjee, T. La Porta, S. Thuel, K. Varadhan, S. Wang: "HAWAII: A Domain-based Approach for Supporting Mobility in Wide-area Wireless networks"

The Jodie programming language

Tibor Csáki and Krisztián Veréb

One of the main policies of the Artificial Intelligence (AI) research is the creation of different paradigmatical languages supporting the solutions of AI problems. These developments have resulted the functional LISP and the declarative Prolog programming languages, among others. In spite of its many advantages, the declarative paradigm has the disadvantage of lacking the procedural programming equipment. This programming equipment is essential for large and complex developments. One possible solution to this problem is the creation and use of hybrid languages.

The usual method of creating a multiparadigmatical language is to extend a declarative one. The results of this method are declarative languages with a mixed structure, but they are not as universal as needed. The other possibility is to create an absolutely new language which is expressive enough. However, such a language could be difficult to learn.

To avoid these difficulties, we have decided to have well-known and easy-to-learn languages as the basis of our newly created language, Jodie. The concept of Jodie is to establish a link between a declarative (Prolog) and an imperative (C) programming language. For this establishment it is necessary to introduce new grammatical elements and make compromises. The main goal of Jodie is to separate the elements of different paradigms. We have solved this requirement with the help of new types which work like functions and we can operate on these special functions using 'conventional' C function calls. There are pure Prolog codes in the bodies of these AI functions. The communication has been realised with the help of parameters between the C and the Prolog functions. The parameters transferring information between the called Prolog routine and the calling C syntactical unit have a special type, namely the query type. This type appears only by its literals. Variables with this type are not allowed.

As a result of these steps, it was obvious to integrate programming objects of Automata Theory (e.g., Turing machine, Lindenmayer System, Finite State Automata) like we did it with Prolog before. There are also possibilities of integrating other programming objects, as well. To establish the usage of automata we introduced new AI constant and AI function types to make their description possible.

Since Jodie is easy to learn, contains a whole real Prolog and automata codes can be implemented with its help as well, this language is practical to use in the education of AI and Automata Theory.

Keywords: Artificial Intelligence, Automata Theory, Multi Paradigmatical Languages, Prolog, C

The basics of roleoriented modelling

Tibor Csiszár and Tamás Kókai

Our roleoriented method supports the effective development of frequently changing information systems that handle significant amount of complex data. This article focuses on one, but perhaps the most important part of the development's lifecycle, which is the modelling in our attempt. Through the article we introduce the concepts and definitions used for developing application model.

In the introduction we give a detailed description of the model's approach, and we also take criteria into account that has to be fulfilled by the model.

The modelling method is a procedure for identifying Roles and Relations amongst them. According to this one chapter describes the definition of Role and the possible correlations of Roles. The major part of our article is about Relations. We show the recursive and non-recursive relations used by us, and we also mention the constraints that can be defined by these relations. Our method is not yet finished. The last part lists the tasks to be done in the future.

Comment: We recommend the presentation called "Roleoriented software development in practice" that gives a short review about the application of theories.

References

[1] [Andersen] Andersen, Egil P. Using Roles and Role Models for the Conceptual Modelling of Objects `www.ifi.uio.no/ trygver/documents/index.html`

[2] [Casanave] Casanave, Cory Requirement for Roles Revision 1.0 OMG Object & Reference Model Sub-Committee Green Paper.

[3] [Csiszár 2001] Csiszár, Tibor - Kókai, Tamás An approach of complex information system's modelling Lecture of "Fourth Joint Conference on Mathematics and Computer Science" Baile Felix, Romania 2001.

[4] [Fowler 1997] Fowler, Martin Dealing with Roles Proc.of the 4th Annual Conference on the Pattern Languages of Programs, Monticello, Illinois, USA, Sept. 2-5, 1997(`www.martinfowler.com/apsupp/roles.pdf`)

[5] [Fowler 2000] Fowler, Martin UML Distilled Second Edition, Addison-Wesley, 2000.

[6] [Graham, Simons 1998] Graham, Ian, Simons, Anthony J H 37 Things that Don't Work in Object-Oriented Modelling with UML ECOOP'98 WS pp.209-232.

[7] [Hornyik 2002] Hornyik, Katalin Szereporientált elemzés és tervezés, Diplomamunka ELTE TTK 2002 (only in Hungarian).

[8] [Mili 1998] Mili, F. On the Formalization of Business Rules ECOOP'98 WS pp.122-129.

[9] [Wieringa 1998] Wieringa, Roel A Survey of Structured and Object-Oriented Software Specification Methods and Techniques ACM Computing Surveys, Vol. 30, No.4, pp.459-527.

Software Development Effort Estimation and Process Optimization

Orsolya Dobán

The need for more and more dependable systems has been increased in the last decades. The strategic decisions during the design of these dependable systems require joint control of the technical and economic aspects, i.e. the estimated cost (development time) and the product quality.

Nowadays the bottleneck in software development is the human capacity both in the terms of time and cost. Reacting to this the software industry supports the development process with high level CASE tools, supporting the formal modeling of the system specification. Our aim was to use the

- UML (Unified Modeling Language) to formalise these product models and the
- UML compatible Software Process Engineering Metamodel to model the development process itself

and to integrate into this development environment a cost estimation method to implement automatic cost predictions gradually refined during the design process.

This paper presents the extension of the Software Process Engineering Metamodel to include the input parameters of the well known COCOMO II. cost estimator.

However optimization of the human resource-allocation becomes a crucial productivity and cost factor in project management. In this case the decision space is confined by the restricted human capacity and the candidate architectural solutions. The well known limits are the development capacity, the available cost, the required quality, the dependability etc. The real task is to find the optimal scheduling of the work to keep the given time limits, or to realize the optimal allocation of the human capacity to reduce the cost of the project.

References

[1] Barry W. Boehm : Software Cost Estimation With COCOMO II, Prentice Hall, New Jersey, 2000.

[2] "Object-oriented modelling and optimization of industrial processes" (1999-2001, Foundation for the Hungarian Higher Education and Research)

[3] Proposal for IKTA project, "Project Management Optimization", 2000.

[4] O. Dobán, A. Pataricza: Cost Estimation Driven Software Development Process, EUROMICRO2001 - Proceedings of the 27th EUROMICRO Conference, ISBN 0-7695- 1236-4, pp. 208., Warsaw, Poland, 4-6 September 2001.

Reconstruction of Factor Images of Dynamic SPECT by Discrete Tomography

Marianna Dudásné Nagy and Attila Kuba

In nuclear medicine the metabolism of the human body can be followed by the mapping different γ-ray emitted radioisotopes. The studies are acquired by equipments (e.g. γ-camera) which can detect the distribution of radioisotopes in different organs, tissues. The dynamic SPECT (Single photon emission computer tomography) is a kind of imaging method which gives 4D images from projections acquired by γ-camera. In this case each 4D image represents a time series of 3D images. The series of the projection images from a direction describes the biological process according to that direction. If these projection images are analysed by factor analysis, the factor images can be considered as the projections of the 3D factors. Since the factors are objects with homogenous distribution of radioactivity, they can be reconstructed by a special method of discrete tomography. Discrete tomography reconstructs functions from a few projections. The range of these functions must be a predefined discrete set. During the reconstruction we must take the absorption of the γ-ray into account.

Mathematically the problem is the following. 3D homogenous objects are to be reconstructed from 4 projections. To solve it we applied an iterative method based on simulated annealing. Simulation experiments were applied: projection data of software phantom were generated. The projections contain noise and the effect of absorption and the camera errors. The reconstruction was calculated on each 3D factor slice by slice. The results of our method will be presented on a simulated kidney phantom.

Efficiency Analysis and Comparison of Public Key Algorithms

Csilla Endrődi and Zoltán Hornák

Public key cryptography provides the theoretical background for most data security services (e.g. digital signature, non-reputation, key-agreement algorithms etc.), which became nowadays, as electric administration is spreading widely, quite indispensable. Public key algorithms are based on *mathematical hard problems*. Their essence is a *one-way trapdoor function*, which is very hard to be solved without knowing a specific information, but easy when having this secret. Up to now three hard problems seem to be suitable for this purpose in practice: *Integer Factorisation Problem* (IFP), *Discrete Logarithm Problem* (DLP) and *Elliptic Curve Discrete Logarithm Problem* (ECDLP). The most commonly known and applied public key algorithm, the *RSA* [1] is based on the IFP. Another promising alternative is the *ECC* [2]. It is getting into the lime-light in our days, while there can be found just less efficient method for breaking ECC than other algorithms; that is to say that by ECC the "security-per-key-bit" rate is higher. It flatters nice applicability, but we must not forget that this aspect should not be the only one, when the most appropriate algorithm for a specific application is to be chosen.

For an information system the needed security level must be clearly defined as an assumption. This level depends on the sensitivity of the transferred data (e.g. commercial transaction or a personal digital postcard), the environment the system will work in (e.g. through the Internet or on a separated LAN), etc. The security requirements determine the *data security services* that should be implemented (e.g. authentication, encryption) and the necessary minimal strength of the applied cryptography algorithms (practically the key size). The aim of the security engineer is to create the *most efficient system* satisfying these security requirements, which is usually a great challenge. Each data security service can be implemented by using different cryptography algorithms and the corresponding cryptography protocols. These implementations have different efficiency features and limitations, and these parameters moreover depend on the key size.

The different algorithms are not entirely interchangeable, since they need e.g. different type of environmental variables, different source data for key generation, have different limitations etc. For example, at ECC a sufficient common elliptic curve is needed, which is very critical. To test the goodness of a curve is difficult, that is why when a research group finds a suitable curve, patents it, and others should use these probed curves. Using ECC it is also significant, whether hardware support is used or not. On the other hand RSA works seamlessly without specific hardware, but its critical point is the prime testing, as RSA needs large primes for key-generation. Besides RSA's behaviour mighty depends on the chosen public exponent. Small exponent can radically speed up some operation, but choosing a too small value makes chance for some types of attacks.

Through the various aspects and the diverse behaviours of the algorithms, there does not exist a "clear winner". *The optimal solution for a given system can be determined by both knowing the target application's specialities and the potential cryptography algorithms' behaviour.*

The next difficulty emerges during the comparison of the algorithms. While the efficiency parameters considerably depend on the applied key size, it is important to make clear that besides *which key sizes* the comparison of the measured parameters should be done. With equal key-sizes the algorithms ensure different security level, thus instead the corresponding key sizes, which provide *adequate strength* should be applied. The security of an algorithm is determined by the fastest, generally working breaking method against it. "Fastest" means the *order of its speed* depending on the input data – namely here the key size. For RSA there exists *subexponent-time* breaking method, while against ECC just *exponent-time* method is known. For this reason generally a smaller key size is sufficient for ECC than RSA, and when raising security, the rate of growing the keys by RSA is greater. Now it is generally accepted, that RSA with a 1024 bit-long key is adequate to ECC with a 160 bit-long key.

When comparing efficiency parameters of the algorithms, we should do it besides these adequate key sizes. Another possibility is to compare the security level of the algorithms when they perform the same parameters in the case of a given operation.

To gain experience about the behaviour of the most relevant public key algorithms, RSA and ECC, we made measurements in practice with a chosen implementation (Crypto++ open source crypto library). We gauged the execution time and the *size of generated data* during *key generation, encryption, decryption, data signing* and *signature verification*. The result's dependence was also specially examined on some other parameters, e.g. the *type of the key*, the *size and type of the source data*, in case of ECC the *type of the common curve* and others. For clear observation, when examining the effect of a given parameter, we fixed all other parameters in some relevant combinations successively. The total number of executed measures was approximately 4000 for ECC and more than 2000 for RSA.

After analysing the database of the measurement results, some general conclusion could be unambiguously laid down. These conclusions correspond with the expectations knowing the mathematical background of these algorithms, but some new features were uncovered, as well.

About *speed* it can be claimed that the *key-generation* easy and fast with ECC, but with RSA it takes different and longer times showing an exponential distribution. At *encryption* and *signature checking* RSA with small exponent is the faster, but ECC with pentanomial based curve is not much weaker. However ECC performs higher speed at *decryption* and *data signing*, where RSA is not dependent on the value of the exponent.

About *sizes* the general experience is that in case of ECC the key sizes, the encrypted text and the size of the signature is smaller, therefore the amount of data to be transferred during a communication is less, too. However it must be considered that according to the existing standards [3] the common curve's parameters also must be included into the public key, thus the effective key size becomes bigger. Moreover for better efficiency for ECC a pre-computed table is required, which enlarges the data to be stored, as well.

These above-mentioned statements are representative examples of the collection, which were established about the ECC's and the RSA's behaviour.

References

[1] RFC 2437, PKCS #1: RSA Cryptography Specifications Version 2.0. B. Kaliski, J. Staddon. October 1998.

[2] A. Menezes, "Elliptic Curve Public Key Cryptosystems", Kluwer Academic Publishers, Boston, 1993.

[3] Standards for Efficient Cryptography Group (SECG), SEC1: Elliptic Curve Cryptography, SEC2: Recommended Elliptic Curve Cryptography Domain Parameters

Inline expressions in protocol test specification

Antal Fazakas and Katalin Tarnay

Telecommunication software is a rapidly growing area of software engineering. In the focus of the telecommunication software is the communication protocol. One of the most critical point of the protocol life cycle is the conformance testing and therefore the test specification, too.

The test specification is a set of test cases examining the functionality of a tested system. For these purpose special test languages are developed, standardization organizations and industrial companies support the TTCN. The new version of TTCN contains many new features including special expressions to specify communication and flow control mechanisms.

Some of these new features are represented using Test Sequence Chart (TSC). A TSC represents the flow of test events between test component instances, port instances and environment. The behavioral program statements cover sequential, alternative, interleaved, default behavior and the return statement.

The new behavior operators called inline expressions are used to specify protocol tests. Two test specifications of an up-to-date protocol used in the wireless world will be introduced. One specification is based on the earlier TTCN version, the other on infix expressions. The two methods will be compared and evaluated from the point of view of conformance testing.

One of the most important layer of the WAP protocol is the Wireless Transaction Protocol (WTP) which is defined to provide the services necessary for interactive "browsing" (request/response) applications. This means that the Wireless Transaction Protocol is very representative from point of view of alternative and other operators. For data segmentation, the alternative behavior of the client in situation of packet loss will be presented using both test specifications, the TTCN-1 and TSC infix expressions. The comparison shows the benefits and disadvantages of the inline operators.

Classifier Combination in Speech Recognition

László Felföldi, András Kocsor, and László Tóth

In statistical pattern recognition [1][2] the principal task is to classify abstract data sets. Instead of using robust but computational expensive algorithms it is possible to combine 'weak' classifiers which can be employed solving complex classification tasks. Different classifiers trained on the same data set have different local behavior; each may have its own region in the feature space where it performs better than the others. It is also possible to train the same type of classifiers on various training sets having same characteristics probability distribution or feature spaces. To obtain the best possible separations, a combination of techniques may be used.

A fair number of combination schemes have been proposed in the literature [3], these schemes differing from each other in their architecture, the characteristics of the combiner, and the selection of the individual classifiers. In this comparative study we will examine the effectiveness of the commonly used hybrid schemes - especially for speech recognition problems - concentrating on cases which employ different combination of classifiers. Out of the algorithms available we chose the currently most frequently used classifiers: artificial neural networks, support vector machines [1], decision tree learners and Gaussian mixture models.

References

[1] Vapnik, V. N., Statistical Learning Theory, John Wiley & Sons Inc., 1998.

[2] R. O. Duda, P. E. Hart And D. G. Stork, Pattern Classification, John Wiley & Sons Inc., 2001.

[3] A. K. Jain, Statistical Pattern Recognition: A Review, IEEE Trans. Pattern Analysis And Machine Intelligence, Vol. 22. No. 1, January 2000.

SIP compression

Márta Fidrich, Vilmos Bilicki, Zoltán Sógor, and Gábor Sey

The Session Initiation Protocol (SIP), is a textual protocol engineered for bandwidth rich links. As a result, the SIP messages have not been optimized in terms of size. Typical SIP messages are from a few hundred bytes to as high as 2000. To date, this has not been a significant problem.

With the planned usage of these protocols in wireless handsets as part of 2.5G and 3G cellular networks, the large size of these messages is problematic. With low-rate IP connectivity, store-and- forward delays are significant. Taking into account retransmits, and the multiplicity of messages that are required in some flows, call setup and feature invocation are adversely affected. Therefore, we believe there is merit in reducing these message sizes.

The result is the SigComp. SigComp is typically offered to applications as a "shim" layer between the application and the transport. The service provided is that of the underlying transport plus compression. In the SigComp architecture compression and decompression is performed at two communicating entities. If an entity wants to send a message to the other entity, then the first compresses the message, sends to the another and the other decompresses the message.

The main parts of the SigComp are: the Compressor, the Decompressor (Universal Decompressor Virtual Machine), the Dispatcher and the State Handler.

In our presentation we would like to show our SigComp implementation and present an algorithm for choosing the best compressing method based on transferred data.

Entropy Modeling of Information in Finite State Machines Networks

Elena Fomina

Driven by remarkable theorems of Claude E. Shannon, which motivate entropy as the measure of information content, we have been examining the entropy measures for search of an approximate or indirect method of evaluation information and information dependences in Finite State Machines. Our goal is to originate a quantitative theory of decomposition for FSMs based on the structural decomposition theory by J. Hartmanis and R. E. Stearns. Mathematical foundations of pair algebra supply the algebraic formalism necessary to study problems about information in FSMs when they operate.

We wish to consider information of partition contents in a special sense; it is a measure of the freedom of choice with which a partition is selected from the set of all possible partitions. The greater information in partitions, the lower its information randomness, and hence the smaller its entropy. Assuming notion of partition on finite set as an algebraic equivalent of information, a quantitative measure of information dependence is defined as a channel on this finite set. Shannon's entropy becomes an important measure for evaluating structures and patterns in channels. The lower the entropy (uncertainty) the more structure is already given in the relation.

Entropy criteria for selecting the set of partitions for decomposition of FSMs allow evaluating partitions sets, to build the informational model of the FSM network under design, and to estimate the network implementation complexity. Amount of information that flows through the FSMs network can be also estimated by entropy or statistical technique, which propagates information statistics at the primary input through the network and monitors the distribution of information. In this way, we have possibility to evaluate the informational flows in each terminal and component of FSMs network and thus create an entropy model for it.

The idea of using entropy is based on informational measures can be applied to other phases of logic synthesis. Partitions that are incomparable under the least upper bound and the largest lower bounds in classic lattice usually do have different entropy values, so they become comparable. This property of lattice functions opens perfect new possibilities for decomposition and coding methods. Practically confirmed high correlation proves that partition entropy is a good indicator of implementation complexity. Previously presented implementation-independent approach for low power partitioning synthesis attempts to minimize the average number of signal transitions at the sequential circuit nodes through dynamic power management. A lower power FSM synthesis framework can integrate the proposed techniques because of the fact that decomposition yields attractive power reduction in the final implementations.

As it is stated in many sources, probabilistic behavior of FSMs has been investigated using concepts from the Markov chain theory. The construction of a Markov chain requires two basic ingredients, namely a transition matrix and an initial distribution. We assume that the state lines of the FSM are modeled as Markov chain characterized by the stochastic matrix where elements are conditional probabilities of the FSM transitions. These probabilities, along with the steady state probability vector can be found using standard techniques for probabilistic analysis of FSMs. This paper advocates entropy modeling of information of FSMs networks. We describe a range of aspects of using entropy criteria as measure of information flows. The main objective of the current work is to give a scalable entropy approach to evaluation. By "scalable", we mean that information in all parts of FSMs network can be estimated and analyzed separately and can then be composed, estimated and analyzed completely.

Incorporating Linkage Learning into the GeLog Framework

Tim Fühner and Gabriella Kókai

Various modifications were applied to the *GeLog* framework in order to significantly enhance its abilities[2]. *GeLog* combines two approaches, inductive logic programming and evolutionary computing [1]. Inductive logic programming (ILP) aims at detecting correlations of pieces of data [2]. This is done by inducing over a data set whose objects' relation is already known. Thus, a hypothesis that matches this training data is searched for, assuming that all other data instances are correctly classified by the hypothesis. *GeLog* searches the hypothesis space by means of a genetic algorithm, an optimization technique which utilizes recombination and selection as observed in nature[3]. Also, the data representation resembles representations found in genetics; the objective representation (phenotype) differs from its encoding in the search space (genotype), which most commonly is a string of characters of a discrete alphabet (genes).

Investigations on the dynamics of genetic algorithms have shown that tight linkage, i.e. the clustering of genes which contribute to the quality of the solution, is an important issue [4]. It was long assumed that individuals in genetic algorithms would eventually evolve towards tighter linkage. However, later investigations demonstrated that selection counteracts linkage learning. This made it necessary to tame the forces of selection [5, 6].

After different approaches that incorporate linkage learning were thoroughly reviewed and compared, the modifications necessary to employ linkage learning into the *GeLog* system were implemented. Furthermore, techniques that decelerate selection by maintaining a high level of diversity have been investigated in order to profit from the effects of linkage learning.

Finally, it could be shown that two experiments, which both proved to be hard for the original version of *GeLog*, can be solved using the enhanced version. The excellent results achieved by the modified version of *GeLog* show that the system has improved significantly. These results will have a significant impact on our future investigations on linkage learning and building block processing in genetic algorithms.

References

[1] Gabriella Kókai. GeLog—A System Combining Genetic Algorithm with Inductive Logic Programming. In Proc of the International Conference on Computational Intelligence, 7th Fuzzy Days LNCS, pages 326–345, Dortmund, 2001. Springer Verlag.

[2] Nada Lavrač and Sašo Džeroski. Inductive Logic Programming: Techniques and Applications.

[3] John H. Holland. Adaptation in Natural and Artificial Systems. PhD thesis, University of Michigan, Ann Arbor, 1975. Ellis Horwood, New York, 1994.

[4] Dirk Thierens and David E. Goldberg, Mixing in Genetic Algorithms. In Proceedings of the 5 th International Conference on Genetic Algorithms, pages 38–55, San Mateo, CA, 1993. Morgan Kaufmann.

[5] David E. Goldberg, Bradley Korb, and Kalyanmoy Deb. Messy genetic algorithms: Motivation, analysis, and first results. Complex Systems, 3(5):493–530, 1990.

[6] George Harik. Learning linkage to efficiently solve problems of bounded difficulty using genetic algorithms. PhD thesis, Ann Arbor, Michigan, 1997.

[2]This work is supported by the grants of Bayerischer Habilitationsförderpreis 1999.

Measures for Decision Tree Building

Tamás Gergely

Decision trees are special trees that contain some kind of decisions in the (internal) nodes and some kind of information in the leaves. Often, they are used as a method for knowledge representation in artificial intelligence. The construction of a decision tree (in most cases) can be split into two phases: building and pruning. The building of the decision trees is based on a metric called information gain (entropy-based metric), and it creates a full tree. Although the full tree contains the most precise information it also requires the most resources (the most space in memory). The aim of the pruning is to "balance" the tree between size and information by replacing some subtrees with leaves. There are several metrics used to balance the tree, and. they are obviously dependent on its functionality. In this paper I introduce some metrics we used for pruning our trees. We tried to compress specific data with some coder algorithms using decision tree models. This required new, specific metrics for tree pruning. Our experimental results show whether it is a good idea to use decision trees as models for compression algorithms.

Various Robust Search Methods in a Hungarian Speech Recognition System

Gábor Gosztolya, András Kocsor, László Tóth, and László Felföldi

In any speech recognition application we have to identify spoken words, based on the information provided by various features. In this process a large number of word-combinations must be tried out, and the best fitting ones must be chosen. A reduction of this search space (ie. word-sequences) is quite important for both speed and memory reasons, because most of these hypotheses will, for one reason or another, turn out to be quite unsuitable.

To tackle this problem, a number of standard algorithms are available like Viterbi beam search, stack decoding, forward-backward search and A* [1][2]. We have implemented some of them and focused mainly on an extension of the general purpose stack decoding method. Our OASIS Speech Laboratory package incorporates most of these methods, which we then tested on a set of (Hungarian) speech databases.

In order to find the best fitting word-sequences, language information is obviously quite important. Incorporating this kind of knowledge into a speech recognition system usually means some kind of language model has to be used. Although this paper focuses on the search process, we cannot ignore another related point, that of choosing a good representation for the Hungarian language.

References

[1] Jelinek, F., Statistical Methods for Speech Recognition, The MIT Press, 1997.

[2] Huang, X., Acero, A., Hon, H.-W., Spoken Language Processing, Prentice Hall PTR, 2001.

Operation Research Methods in Petri Net–Based Analysis of IT Systems

Szilvia Gyapay

Petri nets are widely used as an underlying framework for formalizing and verifying IT system models. Based on their easy-to-understand graphical representation, rich mathematical background, and precise semantics, they are appropriate to model IT systems, e.g., production systems with quantitative properties.

The production of desired materials can be formulated as a reachability problem of its Petri net model, which can be analyzed by linear algebraic techniques (solving linear inequality systems). However, traditional reachability analysis techniques can result in a state space explosion, while the much more efficient numerical methods (often with polynomial runtime) for invariant computations give either sufficient or necessary conditions only [1].

Process Network Synthesis (PNS) algorithms are widely used in chemical engineering to estimate optimal resource allocation and scheduling in order to produce desired products from given raw materials. By means of PNS algorithms [2], sufficient **and** necessary conditions for solution structures are determined defining the entirely solution space, and the search of optimal solutions (with respect to functions interpreted over the state space) is provided [3]. Moreover, PNS algorithms that exploit the specific combinatorial features of PNS problems can be applied to Petri nets in order to give more efficient mathematical methods for their analysis.

The current paper presents efficient semi–decision and optimization methods for the reachability problem based on the strong correspondence between Petri nets and Process graphs. PNS algorithms, *Maximal Structure Generation* (MSG), *Solution Structure Generation* (SSG) and *Accelerated Branch and Bound* (ABB) algorithms can be adapted to solve the reachability problem of Petri nets (formulating as a mixed integer linear programming problem). We show that the ABB algorithm can be used to solve scheduling problems efficiently, and can be extended for other Petri net analysis, e.g., to determine T-invariants of a Büchi net [4].

References

[1] A. Pataricza. Semi-decisions in the validation of dependable systems. In Proc. IEEE DSN'01, The IEEE International Conference on Dependable Systems and Networks, pages 114–115, 30.June–4.July 2001.

[2] F. Friedler, J. B. Vajda, and L.T. Fan. Algorithmic approach to the integration of total flowsheet synthesis and waste minimization. In M. M. El-Halwagi and D. P. Petrides, editors, Pollution Prevention via Process and Product Modifications, volume 90 of AIChE Symposium Series, pages 86–87, 1995.

[3] J. B. Vajda, F. Friedler, and L.T. Fan. Parallelization of the accelerated branch and bound algorithm of process synthesis: Application in total flowsheet synthesis. Acta Chimica Slovenica, 42(1):15–20, 1995.

[4] J. Esparza and S. Melzer. Model checking LTL using constraint programming. In Proceedings of Application and Theory of Petri Nets, 1997.

FDBG, a CLP(FD) Debugger for SICStus Prolog

Dávid Hanák and Tamás Szeredi

CLP stands for Constraint Logic Programming. This acronym signifies a group of logic programming (LP) languages which are usually embedded into a host language such as C, Java or Prolog. In these languages the programmer is able to establish correlations between (usually numeric) variables and find the values where these constraints hold. The CLP language family has several branches depending on the variable domains. Thus we can speak of CLP(B), where the variables can have boolean values, CLP(R) and CLP(Q) where the values are real or rational numbers respectively, CLP(FD) where the values are integers, and CHR, a more generic way of handling constraints, where the programmer defines the domain. They have in common a monotonously growing constraint store to keep track of constraints.

In CLP(FD), FD stands for finite domain, because in the constraint store each variable is represented by the finite set of integer values which it can take. These variables are connected by the constraints, which propagate the change of the domain of one variable to the domains of others. A constraint can be thought of like a sleeping "daemon" which wakes up when the domain of at least one of its variables is changed, propagates the change and falls asleep again. This change can be induced by another constraint or by the labelling process, which enumerates the solutions by enumerating all possible values of the variables. There are two major implementation techniques for CLP(FD) constraints: indexicals and global constraints. The former always operate on a fixed number of variables while the latter are more generic and can work with a variable number of variables. These constraints are usually handled very differently for efficiency reasons.

SICStus Prolog includes an implementation of several CLP languages. Prolog as a host language is a very good choice, because the finding of the solutions requires backtracking, which is a fundamental notion in Prolog too. CLP implementations for other (non-logic) host languages on the other hand must explicitly include a backtracker. SICStus also includes a generic and extendible debugger for regular Prolog, but so far a tracing tool for CLP(FD) was missing. And since CLP programs don't run in linear order but behave rather like a set of coroutines, it requires a great effort to trace them with the Prolog debugger.

The main purpose of writing FDBG (which stands for Finite domain DeBuGger) was to enable CLP(FD) programmers to trace the changes of finite domain constraint variables. Our goal was trace the wake-up of constraints and see their effects on variables, as well as labelling events. Because CLP programs run differently than regular Prolog programs do we chose not to implement a traditional step-by-step debugger but to use the wallpaper trace technique instead. This means that every piece of information is printed on the console, to a file, or something similar, and any potential bug may be found by studying this log after the run is complete. Due to the modular and flexible design of FDBG, a graphical front-end may easily be added later, in fact, we already have plans in that respect.

The trace output is a sequence of log entries. Each entry corresponds to a CLP(FD) event, a notion introduced by FDBG. One group of events represent the wake-up and activity of constraints. Such events describe which constraint is active currently and how does it narrow the domains of variables. The other group informs about the proceedings of labelling, containing data on the structure of the search tree, showing its active and failed branches. The appearance of the log entries can be varied freely by the programmer who is given a set of tools to process the events. Filters may also be applied easily to reduce the size of the log. Due to technical reasons only global constraints are handled by FDBG, indexicals are ignored altogether. However, by exploiting a special feature of SICStus CLP(FD), this is already enough to catch every event of a program which doesn't use any self-written indexicals.

It is important to mention that FDBG was written almost entirely in Prolog as user space code, no native routines were used directly. FDBG reached a level of completeness by now where it could be included (with full source) in the official SICStus distribution from version 3.9, which came out in February 2002.

Implementing Global Constraints as Structured Networks of Elementary Constraints

Dávid Hanák

Constraints serve as a basis for Constraint Logic Programming (CLP), a group of logic programming (LP) languages which are usually embedded into a host language such as C, Java or Prolog. A branch of CLP is CLP(FD), a constraint language which operates on variables of integer values. FD here stands for finite domain, because in the constraint store each variable is represented by the finite set of values which it can take. These variables are connected by the constraints, which propagate the change of the domain of one variable to the domains of others. A constraint can be thought of like a sleeping "daemon" which wakes up when the domain of at least one of its variables is changed, propagates the change and falls asleep again. This change can be induced by another constraint or by the labeling process, which enumerates the solutions by gradually substituting all possible values into the variables. There are two major implementation techniques for CLP(FD) constraints: indexicals and global constraints. The former always operate on a fixed number of variables while the latter are more generic and can work with a variable number of variables. These constraints are usually handled very differently for efficiency reasons.

[1] introduces a new aspect of defining and describing global finite domain constraints based on graphs. It gives a description language which enables mathematicians, computer scientists and programmers to share information on global constraints in a way that all of them understands. It also helps to categorize global constraints, and as a most important feature, it makes possible to write programs which, given only this abstract description, can automatically generate parsers, type checkers and pruners (propagators) for specific global constraints.

To define a constraint, an initial graph is generated. The arguments (variables) of the global constraints are assigned to its nodes, while a single elementary constraint is assigned to each of its arcs (elementary constraints are very simple and easy to handle, like A=B). The final graph consists of those arcs of the initial graph for which the elementary constraints hold. The global constraint itself succeeds if a given set of graph properties (i.e. restrictions on the number of arcs, sources, connected components, etc.) holds for this final graph. The description language contains terms to express type and value restrictions on the arguments of the constraint, to determine the graph generator that creates the initial graph, and to specify the elementary constraint and the graph properties that must hold for the final graph.

To put this theory into practice, an interpreter is being written which understands a language very similar to the one defined in [1]. The interpreter is being implemented in SICStus Prolog and its main purpose is to serve as a prototype, therefore the description language was modified slightly in order to suit the syntax of Prolog, thus removing the burden of implementing a parser as well. The interpreter in its current state of development can read the description of a constraint, and given a set of specific values it can check if the values meet the type and value restrictions posed by the constraint and whether the constraint holds for them. Therefore it might be regarded as a complex relation checker. Although it doesn't do any pruning yet, some minor mistakes and inconvenient notations already cropped up by using it.

A design have been created about the extension of the interpreter with pruning capabilities. Here the line of thought is reversed: we assume that the constraint holds, and from the required graph properties we try to deduce conclusions on the domains of its variables. When a constraint wakes up, some of the elementary constraints assigned to the arcs of the graph are sure to hold, some are sure to fail while the state of the rest is yet uncertain. By knowing what graph properties should be achieved and what are the domains of the variables currently, some

of these uncertain constraints can be forced into success or into failure. The global constraint finally becomes entailed when there aren't any uncertain arcs left.

The propagator using the descried algorithm will be implemented and fitted into the CLP(FD) library of SICStus Prolog by utilizing the well defined interface of user defined global constraints. This way it will be possible to thoroughly test both the program and the theory itself in a trusted environment. According to my plans, a working prototype will already be available at the conference and I will be able to present it along with new observations and experiences. Finally, if this case study proves the theory to be worthy of further practical investigation, an emphasis could be put on efficiency matters also when implementing new interpreters and perhaps pruner algorithm generators.

References

[1] Beldiceanu, Nicolas: "Global Constraints as Graph Properties on Structured Network of Elementary Constraints of the Same Type", SICS Technical Report T2000/01, ISSN 1100-3154, January 28, 2000

Noise-reduction and data-compressing of BSPM-signals with the help of synchronized averaging

Kristóf Haraszti

The mechanical working activity of the heart is preceded by electric activity, which can be shunted and measured with the help of electrodes on the surface of the body. This is called an ECG signal.

We can draw conclusions on the working of the heart from the heart's electric activity. A "fore sign" of a probable sudden heart attack may be the presence of the so-called ventricle late potential in the pulses of the ECG record. The reason for this is that the stimulus brunching gets, for some reason, significantly slower in a certain part of the heart muscles, and consequently a necessary electric condition of arrhythmia evolves, which directly endangers life.

The ventricle late potential is to be observed within the heart cycle at the beginning of the so-called ST-period. Since the sign that we are searching for is rather small "falls within the domain of noises" it demands precise sign processing. The aim is to process samples as little torsioned as possible and to work out a process that minimally changes the original sign. It makes the processing even more difficult that the working of the heart is "not periodical".

The process "to prevent the time base torsion" opens a time window above each QRS-complex and on the basis of their formal identity chooses the pulses that would get averaged in order to improve the sign/noise rate. The sign processing overlaps the time windows that represent individual pulses starting out from a preliminary reference point by observing the correlation coefficient, clusters the cycles according to their formal type (with the help of a given correlation threshold value) and runs the averaging with a so-called dominant group.

The process improves the overlapping of the pulses with the help of interpolation. Another possibility for grouping the periods is the so-called SPSA procedure (L. Gerencsér, Gy. Kozmann, Zs. Vágó: *The use of the SPSA method in ECG analysis: improved late potential estimation*), which basically means that the individual time windows each contain n pieces of sampling points, therefore each pulse can be taken as a point of a n dimensional space. The method searches the smallest sphere in the n dimensional space, which covers the point. It is, of course, possible that two different spheres give a better covering, so this can also provide a classification.

The benefit of this method is that it is sensitive to the base line wandering in contrast with the correlation method.

The cycles within one class are "more similar" than the ones belonging to other classes, therefore a better result is to be expected during the averaging. The point of averaging is that the accidental (white) noise "averages itself out", while the constantly present ventricle late potentials that return in each cycle of the ECG signal, arise.

Off course this signal processing method is useful not only in detection of ventricle late potentials, but in getting similar and significant pieces of information from ECG-signals.

The signal processing system was developed under MATLAB 5.3.

Relations of testability and quality parameters of SDL implementation at the early stage of protocol development life cycle

Anna Harmatné Medve

The protocols of distributed and embedded communication systems are getting more and more complex. Testing is the most expensive phase of protocol development life cycle. Testability of the software, as the quality index of development, is also a crucial cost reducing feature.

The idea of DFT – keeping testability in mind even during the defining phase: *Design For Testability* – concentrates on two main phases in software engineering researches: conceptual planning and testing. However, significant testability indexes can be accomplished even during implementation phase depending on its means. The quality index of development can be software-defined on the basis of ISO metrics in the case of wide-spread professional programming languages.

According to my research relations affecting testability can be defined between language units and features of the special domain in the field of domain specific languages. This contingency generally derives from the purposes of creating domain specific languages and the characteristics of language improvement. Applying relations affecting testability in the field of requirement specification, conceptual planning, and in the phase of implementation improves testability indexes. Various factors may have an effect on testing and applied test specification itself during the improvement of special systems.

In my presentation I outline my researches in connection with inserting the testability of communication protocols into the early stage of protocol development life cycle and implementation in SDL language. SDL-2000 offers new possibilities of handling the time problem and testability planning with the potentialities of new types and data definitions.

I demonstrate the development of Bluetooth short distance radio frequency system protocol package for connection establishing process in a case study. I demonstrate the improvement of certain functions of the process and the testability planning divided into life cycle periods. The case study perfectly demonstrates the assertion of Design For Testability idea by means of applying relations which I presented in the lecture with means of algebra.

I introduce new life cycle periods to the phases of development on applying relations between quality parameters of SDL implementation and protocol features affecting testability in the lecture and the case study.

SDL has spread widely in industry and research. Free and commercial versions of its graphical tools provide automatic code generating and test supply generating. It is spreading also in the field of improving real-time systems apart from the telecommunication applications.

Keywords: SDL, EFSM, protocol life-cycle, design for Testability (DFT), conformance test, validation.

XML Semantics

Ferenc Havasi and Miklós Kálmán

These days one of the most popular standards in use for storing structured information is XML. More and more applications are able to export data in an XML format, more databases are stored in XML, and XML processing techniques are becoming more generic. If this trend continues, XML will eventually be present in almost every part of the informatics sphere. Because of this the new research results related to XML should prove important the future.

The main idea behind our paper is based on a connection between XML documents and attribute grammars. The analogy makes it possible to apply techniques of attribute grammar (semantics rules) to the XML environment. The first notion of including semantics to XML was published in , but here we shall introduce a new approach.

We create a format (XML based) which makes it possible for us to define a real XML attribute via semantics rules. The new set of semantics rules then become an organic part of XML documents and do not violate the original XML specification.

This method consists of two major modules, the reduce and the complete module, each having a significant role in the completion and reduction of the designated XML file. The reduce module removes the specific attributes with can be calculated via the semantic rules stored in the SRML file. The complete module recreates the original XML file using the reduced XML and the semantic XML file (SRML). The rules specified will only be applied to the reduction phase when there original attribute values and the calculated values are equal. The SRML file format keeps the original DTD of the XML, since all attributes and nodes are mentioned which need to be IMPLIED.

The method was implemented using the JAVA language thus making it platform independent. It was successfully tested on various CPPML files, each varying in size and complexity. During these tests the number of attributes, thus the size was decreased considerably in case of reduction. The running time of the method is not significant, therefore a file size of 11MB can be reduced in a matter of minutes (approx. 2.30) achieving an average of 64%.

The future of the method includes the dynamic creation of the semantic file using Artificial Intelligence machine learning techniques. This will enable the clarification of the relationship between attributes towards the user, aside from reducing the size of the appointed XML file.

Recovery of Label Distributions

Gabor T. Herman

Our long-term aim is to utilize electron micrographs of biological macromolecules to produce a tessellation of space into small volume elements (voxels), each labeled as containing ice, protein, or RNA. Traditional approaches to achieve this first assign to each voxel a gray value (associated with the density of atoms in the voxel) based on the micrographs and then threshold this gray value image to obtain a label image. A problem with this approach is that at higher resolutions (smaller voxels) the ranges of atom densities corresponding to different labels greatly overlap, and so the label image will need to be of low resolution in order to be reliable. Another difficulty is that, due to the distructive nature of the electron microscope, only a few projections can be taken. We propose to overcome these difficulties by first postulating some low level prior knowledge (based on the general nature of macromolecules) regarding the underlying label images, and then estimating directly a particular label image based on this prior distribution together with the micrographs. We also report on our first experiments aimed at evaluating this approach.

Optimalized emulated digital CNN-UM (CASTLE) Architectures

Timót Hidvégi

The CNN-UM [1],[2] (Cellular Neural Network-Universal Machine) is a stored program analog microprocessor array where the tiny processors are interconnected localy. The CNN-UM architecture can be implemented in analog VLSI [3], in an emulated digital way [4],[5] or by a software simulator. An emulated digital CNN-UM [4] (CASTLE) architecture was publicated few years ago. Some modified, extended CASTLE architectures are shown in this contribution. These new modified architectures are optimalized and analized according to silicon area operating speed and dissipated power.

(i) The CNN can be programmed with different templates. The size of the template (weight matrix) is variable, in most cases the size is 3*3. The original CASTLE can operate only with this templates. There are some problems that cannot be solved with nearest neighborhood templates. New architectures are proposed where we can use templates with 3*3 and 5*5 with these re-configurable arithmetic cores.

(ii) If we use symmetrical templates then the silicon area is decreased significantly. A new emulated digital CNN architecture is shown where we can use arbitrary templates (optimalized to silicon area).

(iii) The original CASTLE arithmetic unit was extended by pipe-lineing technique. The operation speed of the emulated digital CNN-UM is increased significantly with this solution ($\sim$ 10 times) and the silicon area was not changed practically.

References

[1] T.Roska and L.O.Chua, “The CNN Universal Machine: an analogic array computer”, IEEE Transactions on Circuits and Systems-II Vol.40, pp. 163-173, March,1993.

[2] L.O.Chua and L.Yang, "Cellular neural networks: Theory and Applications ", IEEE Trans. on Circuits and Systems, Vol.35, pp. 1257-1290, 1988.

[3] A. Rodrigez-Vazquez, R. Dominguez-Castro, S. Espejo, “Challenges in Mixed-Signal IC Design of CNN Chips in Submicron CMOS”, Proc. of the fifth IEEE Int. Workshop on Cellular Neural Networks and their Applications, London pp: 13, April, 1998.

[4] Péter Keresztes, Ákos Zarándy, Tamás Roska, Péter Szolgay, Tamás Bezák, Timót Hidvégi, Péter Jónás, Attila Katona “An emulated digital CNN implementation” Journal of VLSI Signal Processing Systems Kluwer Academic Publishers,Vol. 23. pp. 291-303, 1999.

[5] K.A.Wen, J.Y.Su and C.Y.Lu, “VLSI design of digital Cellular Neural Networks for image processing”, J. of Visual Communication aand Image Representation, Vol.5, No.2, pp. 1117-126, 19941.

LL Frame System of Learning Methods

András Hócza, Gyöngyi Szilágyi, and Tibor Gyimóthy

Machine learning methods are widely used in many AI applications (e.g. data mining, speech recognition, robot control). To solve a learning problem we have to preprocess the input data, apply an algorithm and then evaluate the output. Generally, it is not enough to use just one algorithm. It is necessary to do experiments by hand, employing various learning algorithms, testing their parameters systematically, this requires a lot of work. It would be nice to develop a general environment which supplies the appropriate methods, automatizes the whole process.

The main result of the LL (Learning and Logic Based Knowledge Management) system is the unified managing of a variety of methods, their inputs and outputs, the development of new learning methods and their integration into the system.

To facilitate the preprocessing of the input data, an editor is used in the handling of various types of examples (ARFF, the C4.5 file format, etc.), and a converter makes it possible to convert to one format to another.

In the LL system we can define a project for a learning problem. A project can include tasks which makes possible to get experience in one go with different algorithms for various parameters. This enables us to find a better solutions for given learning problem. Two main built-in tools help in the postprocessing: One of them stores the result automatically in a dynamic grid for different task-runs and allows the user to view the result. The other is a built-in optimization algorithm that helps one to choose the best solution for the learning problem. The user can define a measure for the accuracy of solution and the search space, including the various parameters of the applied algorithms. The optimization algorithm provides the most suitable parameter settings for the learning problem using a deterministic annealing technique.

The structure of the LL system is modular, so it is easy to insert new learning methods.

In this paper we introduce the LL system and some of its interesting applications.

The previously integrated algorithms and methods are:

- The C4.5 Decision Tree Learner.
- Learning methods for Logic and Constraint Logic Programs: SPECTRE (SAC, DAC, RAC), IMPUT [1], IMPUT-LP-SLICE, IMPUT-CLP-SLICE.
- Slicing methods for (Constraint) Logic programs: SLICER [3].
- Methods including C4.5 from natural language processing: the CHUNKING problem, the POST-TAG problem.

References

[1] Alexin, Z., T. Gyimóthy, Boström, H.: IMPUT: An Interactive Learning Tool based on Program Specialization Intelligent Data Analysis, Vol 1 4 (1997) Elsevier Holland

[2] Horváth, T., Alexin, Z., Gyimóthy, T., Wrobel, S.: Application of Different Learning Methods to Hungarian Part-of-speech Tagging. In Proceedings of Ninth Workshop on Inductive Logic Programming (ILP99) Bled, Slovenia, 24-27 June in the LNAI series Vol 1634 pp. 128-139, Springer Verlag (1999) `http://www.cs.bris.ac.uk/~ilp99/`

[3] Gy. Szilágyi, T. Gyimóthy, J. Maluszynski: Static and Dynamic Slicing of Constraint Logic Programs. Journal of Automated Software Engineering, Kluwer Academic Published Jan 2002, Vol.9 No. 1, pages 45-65

Optimal Platform to Develop Features for Ad Hoc Extension of 4G Mobile Networks

János Horváth Cz. and Sándor Imre

3G mobile telecommunication systems have been presented nowadays. Main attribute of them is the usability of reasonable bandwidth, which is sufficient for multimedia applications. Conception of mobile internet has reached the palpable realization. Evolution of it is unstoppable. On the field of mobile communication the bottle-neck of the relatively constant but not unlimited bandwidth will give stimulation to the application-developers to produce always more efficient applications at least till 2010, when fourth generation mobile systems will be able to ensure extremely big bandwidth. According to the plan of Ericsson [1] by 2011 the mobile connection will be equal to an Internet access of 100 Mbps.

Anatomizing the 4G mobile systems by developing parameters it will be a complete network if set of features are realized like below [2]:

- Majority of people can access to voice- or data-based services what are provided by mobile networks (This requires efficient resource-management, for example usage of ad hoc extension in wireless systems).
- The mobile network is able to attach to Internet fully because of basic concept of it (In this way IP based technologies would be used through mobile network (e.g. VoIP, Voice over IP)).
- Problem of virtual private networks is worked out their security and data-protection is warrantable (Security and authentication technology are improved well).
- The network is able to realign itself (It manage several type backbone and it use the best one, it means adaptation).
- The system is able to keep on QoS parameters (Quality of Service).

There are four technical trends from the current trends what are reckoned among pioneers in this moment but they have well-grounded concepts. They are: managing ad hoc networks, content provision and agents, software radio and virtual private networks.

We deal with topic of ad hoc mobile networks by stressed attention. Ad hoc mobile network is one type of communication systems, where central infrastructures (base stations and central database) are not built up. In this case, the mobile terminals use the each other to reach distant ones by transmitting radio signals. Most important is to develop the suitable routing algorithm. Using this routing algorithm, the mobile nodes of the network can find out their locations and neighborhoods, so they become to be able to hand on data packets by radio channel.

Purpose of our research is developing a scalable ad hoc routing protocol, which works with acceptable performance in different topology situations. This development is done in OmNet++ discrete event simulation environment [3]. We had to develop our ad hoc extension for this simulator program. During the presentation we introduce the simulator, our ad hoc extension and developing phases of our own routing protocols. Finally we show a method for estimating the resource requirements of ad hoc routing algorithms in mobile terminals.

Keywords: Simulator, OMNET++, Resource Estimation, Ad Hoc Networks

References

[1] "Ericsson plans for 4th generation mobile system" , `http://arabia.com/article/0,1690,Business%7C30215,00.html`

[2] János Horváth Cz., Dr. Sándor Imre. "Examination of the Viability of Fourth Generation Mobile Networks", 3GIS, Athen , June 2001

[3] `http://www.hit.bme.hu/phd/vargaa/omnetpp/`

Bluetooth modelling, validation and test suite generation

Endre Horváth

Real-time aspects in protocol modelling, simulation and validation are very important today. Modern systems in the wireless world, like Bluetooth [1], have very hard time constraints, so demands on the specification languages, simulation and validation tools used in protocol technology are high. The main goal of my work was to specify a complete system to simulate and validate the Bluetooth baseband protocol layer and to generate TTCN test suite [2] automatically.

Bluetooth was modelled in SDL [3] for validation and testing purposes [4]. The protocol model is not simple: there are many states and variables used to specify the baseband protocol layer. Therefore the state space to be generated during validation is very large, so it is not easy (or even impossible) to fully validate this SDL model. That is why the Exhaustive state space exploration algorithm was not applicable on this model and so the Bit-state algorithm was used to validate the SDL system. As a result of validation it can be said that serious problem was not found. The validation procedure was helpful to complete the right SDL model because some design failures were detected and only some model specific problems were occurred.

The Telelogic Validator tool (Autolink) [5] were used for TTCN test suite generation combining with SDL Observer processes. The starting point of the generation was the SDL specification and the goal was to get a TTCN test suite in an automated way. The quality of the generated test suite was good but the test cases had to be completed manually since there were no guard timers generated to protect the tester against deadlocks during testing. However it is very positive that naming of constraints could be controlled with configuration of the generator tool and concurrent TTCN was also supported in the Validator.

The plan for the future is to continue this work by modelling more (up to 8) Bluetooth nodes communicating with each other. To describe this system an extra process has to be defined for modelling the radio channel. This solution makes it also possible to simulate the losing of data frames and the channel delay.

References

[1] Specification of the Bluetooth System (Core), Specification Volume 1, 2001

[2] OSI - Open System Interconnection, Conformance testing methodology and framework - Part 3: Tree and Tabular Combined Notation, ISO/IEC 9646-3, 1997

[3] ITU-T Recommendation Z.100 - Specification and Description Language, 1996

[4] R. L. Probert, A. W. Williams: Fast Functional Test Generation Using an SDL Model, Testing of Communicating Systems, Budapest, Hungary, 1999

[5] M. Schmitt, A. Ek, B. Koch, J. Grabowski, D. Hogrefe: Autolink - Putting SDL-based test generation into practice, Testing of Communicating Systems, Tomsk, Russia, 1998

Test Architecture for Distributed Network Management Software

József Hosszú

It is expected that in the near future the appearance of Internet Protocol (IP) based mobile networks and the growing number of users and emerging new applications of wired networks bring new tendencies in the number of routers, reaching even thousands [1]. It is essential to manage, i.e. monitor and control such networks. Network management systems (NMS) are being developed for networks of different technologies, being capable to handle the resulting large amount of management data. Testing functionality and performance of such system requires a test network in which the investigation can be carried out, but any firm – even the largest ones – cannot afford building a real test network due to the horrible hardware costs. Therefore, it is required to introduce a cost-saving and efficient method.

Basic functionality, that covers communication between routers and management system, can be verified in a small test network, however, building a large one (with 10,000 nodes) for testing purposes is rather expensive. Network emulation, i.e. imitating the behavior of a network by sending appropriate responses to the incoming packets, is a suitable concept for testing large-scale networks. It is obvious that one machine cannot compete against the capacity of a distributed system, thus the functionality, provided by the network emulator, have to be limited.

The presentation introduces an approach to software testing applicable for distributed network management systems using network emulation and TTCN-3 (Testing and Test Control Notation)[2]. It discusses the requirements for the testing environment, as well as the applicable types of testing (functional, performance and stress). The test architecture and a sample configuration is also described. The method applied is independent from both the networking technology and the applied NMS, as it only requires the proper specification of their interfaces. Developing test cases requires careful and exhaustive analysis of interfaces and system specifications considering non-deterministic and unhandled events during execution. A generalized test port of the applied Tester application provides a reasonable level of transparency of the lower interface [3] of the NMS, and the upper port is also flexible enough to be easily adopted to the user interface of any management system.

References

[1] Kornél Bigus, “Emulation of Large-scale IP networks”, M.Sc. Thesis, Budapest University of Technology and Economics, 2000.

[2] ETSI, “Methods for Testing and Specification (MTS); The Tree and Tabular Combined Notation version 3; Part 1: TTNC-3 Core Language”, ETSI ES 201 873-1, 2001.

[3] ITU-T, Z.500, “Methods for Validation and Testing - Framework on formal methods in conformance testing”, 1997.

IPv6 macromobility simulation using OMNeT++ environment

Sándor Imre, Róbert Schulcz, and Csaba Csegedi

Nowadays there are two keywords in telecommunications: mobility and Internet. As the capacity and speed of small handheld devices and laptop-sized computers has increased dramatically in the past few years, the demand for mobile Internet access, telephony, videoconference, messaging, etc. while being away from home or moving also became significant. The current technology trends focus on implementing all these applications based on IP (All-IP technology).

The current version of IP – IPv4 – was created for wired networks and the mobility support was added only later. For this reason it can not provide efficient support for mobile devices. The next generation of IP – IPv6 – has built-in mobility support from the beginning with important new features like bigger address space, reduced administrative overhead, support for address renumbering, improved header processing and reasonable security.

We have developed a simulation to prove our concepts of Mobile IPv6 under OMNeT++. OMNeT++ (Objective Modular Network Testbed in C++) is a free, open-source discrete event simulation tool, similar to other tools like PARSEC, NS, or commercial products like OPNET. It allows easy development of complex simulations with its features like message passing, nested submodules, flexible model topologies, parallel execution, etc. Our Mobile IPv6 model can be freely downloaded along with many other models.

Our simulation deals with the IPv6 Mobility Extension, especially with the binding management methods. With our simulator we can easily build different network scenarios by providing a few simple parameters from which the simulator automatically constructs the network.

Every mobile device in IPv6 can always be addressed with its home address. When the mobile device isn´t attached to its home network, it obtains a temporary IP address – a care-of address – from the foreign network it is currently attached to. In order to be able to receive packages in this case the mobile always informs its home agent – a router in its home subnetwork – about its current care-of address. Correspondent nodes can send packages directly to the care-of address if they know it, otherwise they send them to the home address and the home agent forwards them to the mobile. The association between the home address and the care-of address is called binding. In IPv6 networks every node contains a so-called Binding Cache to store binding information about mobile devices.

With the limited capability of mobiles and network overhead caused by triangle routing the optimisation of the binding cache´s size and the binding entries´ lifetimes is very important. Our simulation demonstrates this issue in different network scenarios. We investigate different statistics like end-to-end delay time, rate of packets sent via triangle routing, rate of packet loss, handover frequency, etc.

References

[1] Charles E. Perkins: Mobile IP – Design Principles and Practices, Addison-Wesley, 1998

[2] David B. Johnson: Mobility Support in IPv6, Intenet Draft, draft-ieft-mobileip-ipv6-13.txt, 2000.

[3] Preetha P. Kannadath and Hesham El-Rewino: Simulating Mobile IP Based Network Environments, University of Nebraska at Omaha, 2000.

Comparative study of four UML based CASE tools

Dan Laurentiu Jisa

CASE tools (Computer Aided Software Engineering) represent those applications supporting analysts, designers, programmers, testing teams, to analyze, design, implement (at least partially) modify (expand), build, respectively tests software applications. The problem is how to choose a CASE tools for the development of an information system. To make the objective choice a significant set of criteria to be used for the evaluation (assessment) should be previously established. The instrument evaluation criteria can be divided into criteria depending on the modeling language and criteria independent of the modeling language. This paper analyses the Rational Rose v2001A, Microsoft Visio 2000, OpenTools and MagicDraw 5.0 instruments, taking into consideration the criteria belonging to both categories. The above mentioned tools were selected from the multitude of the existing CASE tools, mainly taking into consideration the support offered to the modeling language (UML), the quality of the graphical interface (also including the support offered for the model navigation), the programming language and the technologies for which is generated code, the platform enabling the instrument operation (except Visio 2000, all the others are available both for UNIX and Windows platforms). The criteria utilized for the tools comparison are the following:

a) Included in the categories depending on language:
   - Support offered for the modeling language;
   - Support for formal text annotations;
   - Maintaining consistency between diagrams;

b) Included in the categories that are independent of the modeling language:
   - Support for model navigation;
   - Forward engineering;
   - Reverse engineering and Round Trip Engineering;
   - Support for data modeling;
   - Support for component modeling;
   - Reusability support;
   - Design pattern support;
   - Project documentation support;
   - Exchange with other instruments;
   - Integration with other development instruments;
   - Support to team work.

A Communication System Based On Web Services and Its Application In Image Processing

Richárd Jónás, Lajos Kollár, and Krisztián Veréb

Due to the exponential growing of Internet, distributed systems have broken not only into the field of object technology and database systems but into the computational-intensive application space, as well. Since there are a huge number of resources with quite different computational capabilities on the Web, distribution of such computational tasks have become more and more important.

One of our goals was to establish such a framework which enables the demonstration of image processing operations via Web. This allows for workstations with limited resources to access and make use of computational-intensive applications. On the other hand, legacy operations—which could be implemented by others—should be used in a 'black-box' manner which can therefore be reused. Our research goes beyond these goals: we have developed a general communication model based on distributed resources which can be used for solving other problems that require a distributed environment, as well.

The system consists of three kinds of software architecture. Users interact the system through thin clients (i.e., Web browsers). Services are placed at Service Controllers and Service Providers. The number of Service Providers is arbitrary. There should be a Web server software running on Service Providers which is used for providing the given services. Service Controllers themselves could also be Service Providers but they have a back-end database for both storing the results of operations—it allows the later reuse of a result of an operation or a sequence of operations—and a repository of the known Service Providers and the services they provide. Services provided by Service Providers and Service Controllers can be thought of like 'functions': starting from input data they produce some output data. It is important, that this process is fully controlled by the user: he starts it—by requesting an operation from a Service Controller—and the results are presented to him, as well, giving the user the possibility of coming to a decision of whether to make these results persistent—by storing it into the database—or not.

Implementation is based on the latest open standards: inputs and outputs of services are given using XML; WSDL and UDDI are used for describing and discovering Web Services; semantics of services are defined with the help of RDF. The generality of the system gives the possibility of extending it to be a general Web-based workflow system.

Building Web Applications via Web

Richárd Jónás

Nowadays growing number of portals are being developed and there are many HTML pages getting their content from databases. One of the special features of development of web applications is the rapidly varying requirements. So the development of web applications contains short-time design and implementation with frequent feedbacks because we have to respond immediately to the new ideas.

In this paper a particular system will be introduced, which web applications and application prototypes can easily be developed with. With this client-server application, HTML or PHP pages can be built in WYSIWYG way, so the new prototypes of application modules can be quickly made and tested. The development process is performed by the help of the Internet, so the mentioned tool can be used anywhere. Therefore this development tool can be used even by thin clients because the application and the database management system run on a server.

The PHP pages—having dynamic content—consist of web components, so a well-organized system of such components builds the mentioned PHP page. Following the MVC principle we can define the model, view and controller of web components which can be done by markup texts. We can define the model part of a component as a SQL query which serves the data to be presented in XML format. The view can be described by an XSL document which transforms the result of the query. The controller part can be described by the navigation and the server-side behaviour of the constructed page.

In the end we examine how our system supports development of such portals which gain information of their pages from databases.

Time Series Prediction using Artificial Intelligence Methods

István Juhos, Gyöngyi Szilágyi, János Csirik, György Szarvas, Tamás Szeles, Attila Kocsis, and Attila Szegedi

Time series prediction [1] is important in a wide range of areas and has numerous applications. Take, for instance, forecasting the traffic of queueing systems, predicting product demand in business, or forecasting share prices in financial markets. Since estimates about future changes and developments are important for taking decisions and actions, there is a constant need for more precise forecasting techniques. A lot of research has been done on time series forecasting regarding queueing systems, but the vast majority of them deal with conventional statistical methods.

When compared to traditional statistical methods, intelligent learning methods have a high degree of flexibility in the types of functions. These can be adaptively approximated during the training process. They are well suited to such approximation tasks. After being trained using the examples from the training set, the theory it has learned can be used to classify (predict) new examples.

The aim of this paper is to describe three different learning methods for solving the problem of forecasting the traffic of queueing systems. The new aspects of this work are: using and developing different AI learning methods to solve such problems, dealing with external factors and applying supervised learning techniques. The applied AI methods are decision trees, support vector machines and artificial neural networks.

Prediction is a difficult problem which confronts most human endeavours. While many specialised time series prediction techniques have been developed, these techniques have certain limitations. Most are restricted to modeling whole series rather than extracting predictive features, and are generally difficult for domain experts to understand. Symbolic machine learning (decision trees [3]) promises to address these limitations.

Support Vector Machines [4] techniques can provide very accurate predictions.

The benefits of using artificial neural networks [2] is that it is possible to encode some predictor variables into the network architecture.

Using a combinations of these methods, we can obtain reasons for the decision as well as an accurate prediction. In the comparision and analysis phase we can see which methods produce better or worse results. Taking the latter into account we can then construct a new hybrid model. An other benefit of this new model is the handling of external factors (trends and special events), which could provide more precise prediction compared to traditional methods.

Keywords: time series prediction, intelligent prediction models, queueing systems, Artificial Intelligent (AI) learning methods.

References

[1] A. S. Weigend and N. A. Gershenfeld: Time Series Prediction: Forecasting the Future and Understanding the Past. Addison Wesley Longman 1993.

[2] Claudia Ulbricht: Multi-recurrent Network for Traffic Forecasting. Proceedings of the AAAI'94 Conference, Seattle, Washington, Volume II, pp. 883-888, 1994

[3] J.Ross Quinlan: C4.5 Programs for machine learning. Morgan Kaufmann

[4] N. Cristianini, J. Shawe-Taylor: An introduction to Support Vector Machines. Cambridge University Press 2000.

On a Class of Cyclic-Waiting Queueing Systems with Refusals

Péter Kárász

Based on a real problem connected with the landing of aeroplanes we investigate a special queueing system, where peculiar conditions prevail. In such systems a request for landing can be serviced upon arrival if the system is free. When other planes are using the runway or waiting to land, the entering plane has to start a circular manoeuvre and can put its further requests when it comes to the starting point of its trajectory. Because of possible fuel shortage it is quite natural to use the *FIFO* rule.

In his works Lakatos has extensively investigated such type of queueing systems, namely where the service of a request can be started upon arrival (in case of a free system) or at times differing from it by multiples of the cycle time T (in case of a busy server). In [1] he considered a system with Poisson-arrivals and uniformly distributed service time. As a generalization, in [2] a special system which serves customers of two different types, was examined. Both types of customers form Poisson processes, and their service time distributions are exponential. In the system only one customer of first type can be present, it can only be accepted for service in the case of a free system, whereas in all other cases the requests of such customers are turned down. There is no such restriction on customers of second type; they are serviced immediately or join a queue in case of a busy server. In this paper we are going to consider the same system but service times are uniformly distributed.

To elaborate the mathematical description of the system we make the following proposals. In the system there might be idle periods, when the service of a request is completed, but the next one has not reached its starting position. We consider these periods part of the service time, making the service process continuous in such way. We also make a restriction on the boundaries of the intervals of the uniform distributions: they are multiples of the cycle-time. This assumption does not violate the generality of the theory, but without it formulae are much more complicated.

For the description of the system we use the *embedded Markov-chain technique*, i. e. we consider the number of customers in the system at moments just before the service of a new customer begins. For this chain we introduce the following transition probabilities:

a_{ji} – the probability of appearance of i customers of second type at the service of a j-th type customer ($j = 1, 2$) if at the beginning there is only one customer in the system;
b_i – the probability of appearance of i customers of second type at the service of a second type customer, if at the beginning of service there are at least two customers in the system;
c_i – the probability of appearance of i customers of second type after free state.

We formulate the results of the paper in the following

Theorem. *Let us consider a queueing system with two types of customers forming Poisson-processes with parameters λ_1 and λ_2, the service times are uniformly distributed in the intervals $[\alpha_1, \beta_1]$ and $[\alpha_2, \beta_2]$, respectively ($\alpha_1, \beta_1, \alpha_2, \beta_2$ are multiples of cycle-time T). There is no restriction on customers of second type; however customers of first type may only join the system when it is free (and only one of them can be present at every instant), all other requests of this type are refused. The service of a customer may start at the moment of its arrival (in case of a free system) or at moments differing from it by multiples of cycle time T; and the* FIFO *rule is obeyed. We define an embedded Markov-chain, whose states correspond to the number of customers in the system at moments just before starting a service.*

The matrix of transition probabilities of this chain has the form:

$$\begin{pmatrix} c_0 & c_1 & c_2 & c_3 & \dots \\ a_{20} & a_{21} & a_{22} & a_{23} & \dots \\ 0 & b_0 & b_1 & b_2 & \dots \\ 0 & 0 & b_0 & b_1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

The condition of existence of ergodic distribution is the fulfilment of inequality:

$$\frac{\lambda_2(\alpha_2 + \beta_2 + T)}{2} < 1$$

The limit distribution while $T \to 0$ is also given.

References

[1] L. Lakatos: On a Cyclic-Waiting Queueing System. Theory of Stochastic Processes Vol. 2 (18) no. 1-2, 1996 pp. 176-180

[2] L. Lakatos: A Special Cyclic-Waiting Queueing System With Refusals. J. Math. Sci. (New York) (to appear)

[3] L. Lakatos: Limit Distributions for Some Cyclic-Waiting Queueing Systems. Theory of Stochastic Processes (to appear)

Applicability of UML in Protocol and Test Development

Tamás Kasza, Sarolta Dibuz, Tibor Szabó, and Gyula Csopaki

In the last few years, UML (Unified Modeling Language) has become the dominant modeling language of the software industry. UML is also in the focus of the telecommunications industry, because – due to its flexible, platform-independent and generalized description features – it is ideal for modeling telecommunications systems. UML regards systems as models from several points of view. The most commons are use case, logical, component and deployment views. The application of the existing standardized description techniques and languages – such as SDL (Specification and Description Language) – is rather time consuming from the business and the technical perspective as well, because those methods are generally very complex for practical use. UML fulfils the needs and requirements of protocol development.

Particularly, UML is a visual modeling language for specifying, constructing, visualizing, and documenting the artifacts of a concurrent, distributed software-intensive system, and it does draw the line as developers move toward code.

In this paper, we investigate three potential ways for utilizing the UML in the field of communication protocol engineering. We discuss the advantages and drawbacks of the standardized mapping from UML to SDL, which is a language primarily used for specifying network protocols and possibly for describing digital logic. On the other hand, we raise the problem of reverse engineering. It is interesting from the aspect of implementation, that is, we investigate the SDL to UML mapping. Finally, we show how to derive conformance test suites from UML models of network protocols.

The standard ITU-T Z.109 introduces the relationship between some elements of SDL specifications and some UML diagrams. It presents the process of the requirement collection, analysis and draft design, which is necessary to formalize the plain text standard. Firstly, this paper discusses the differences and similarities between UML and SDL, investigates UML mapping based on Z.109, and proposes the use UML and SDL together in order to get advantages of both languages.

However, it is interesting to investigate the reverse direction, the use of UML, to create more fine models during the implementation phase. If UML is used in the implementation process as well, the product will have numerous favorable properties. UML provides adaptation to different object-oriented development environments used nowadays. Furthermore, UML meets the requirements of modularity and distributed systems according to the formal specification. This expressing semi-formal technique of modeling makes the process of mapping formal specifications to modern, object-oriented languages considerably easier than the direct mapping. This train of thoughts arises the question whether there is relationship between the UML models used before and after the formal description. Secondly, the article gives an overview on this reverse engineering process as well.

Thirdly, UML can also be used to support the test development for protocol specifications such as conformance test suites. After the identification of independent system components, like the tester(s) and the implementations under tests, test configurations can be developed using component and deployment diagrams. Test case structures and test purposes are defined for several test configurations. We consider the widely-used test description facilities Message Sequence Charts (MSC) and Tree and Tabular Combined Notation (TTCN) to be the target test notation.

Keywords: UML, SDL, MSC, telecommunications protocol specification and testing, TTCN

On Implementing Relational Databases on DNA strands

István Katsányi

In the last decade molecular biology has become the fastest growing discipline in the world. Some of the results are widely known, let us only mention the major breakthroughs in the Human Genome Project and nanotechnology. The progress made possible the birth of a new branch of science, that is called molecular computing (or DNA computing). Leonard M. Adleman published a paper [1] in 1994, which later become the foundation–stone of this new subject. In his article Adleman demonstrates how can a classic NP–complete problem: the problem of searching for a Hamiltonian path in a directed graph can be solved in polynomial time using the techniques of molecular biology and DNA strands. He outlines the great opportunity in the large computing power, and the extremely compact data storage. In a test tube there can be performed as much as 10^{16} operations in a second. That is much more than current supercomputers can execute. In a litre of water the DNA strands can encode 10^8 terabytes, and we can perform associative searches on the data in constant time.

In the past years many papers dealing with the computing power of DNA were published. However, only a few article studied the possibility of data storage and processing (see e.g. [2], [3]). Recently two papers ([4], [5]) described methods that yielded in an operation that closely resembles to the join operation of relational algebra. In spite of this no one has extensively studied the potentialities of the usage of molecular computing in the field of RA.

This work describes the bases of the implementation of relational databases in test tubes, using an abstract model of molecular computing. It specifies the representation of columns, tuples, tables, and databases, and the execution program of the relational operations. We examine the efficiency of each operation and compare them to traditional methods. We investigate the possibilities of practical usage of the proposed model as well as the bounds of it.

Keywords: molecular computing, theory of computing, relational database

References

[1] Leonard M. Adleman. Molecular computation of solutions to combinatorial problems. Science, 266:1021–1024, November 11, 1994.

[2] Eric B. Baum. Building an associative memory vastly larger than the brain. Science, 268:583–585, April 28, 1995.

[3] John H. Reif, T. H. LaBean, M. Pirrug, V. S. Rana, B. Guo, C. Kingsford, and G. S. Wickham. Experimental construction of a very large scale DNA database with associative search capability. In DNA Computing, 7th international Workshop on DNA-Based Computers, DNA 2001, Tampa, U.S.A., 10–13 June 2001, pages 241–250. University of South Florida, 2001.

[4] John H. Reif. Parallel molecular computation: Models and simulations. Algorithmica, 1998. Special issue on Computational Biology.

[5] Masanori Arita, Masami Hagiya, and Akira Suyama. Joining and rotating data with molecules. In IEEE International Conference on Evolutionary Computation, April 13–16, 1997.

The analysis of the economy of the Hungarian milk processing companies in 2000 with multivariate methods

Krisztián Keszthelyi

In the last decade considerable changes passed off in the Hungarian milk sector, which caused that the differences between the individual firms have grown. The purpose of my analysis is to investigate the factors which influence the variation between the milk processing companies. To this analysis I used econometric methods, which methods are rather new at this field.

I based my paper on that database which the Agricultural Research and Informatical Institute gathered from the tax returns of the food processing industry. This database contains only financial data, so only the balance sheet and the profit statements can be defined from it.

At the beginning of the analysis I took the hypothesis that it would have been possible to classify, group and demonstrate the milk processing companies only with using data of the over-mentioned balance sheets and of the profit and loss statements.

From the database after a query it was possible to receive 275 different data or in one word variate. My first aim was to compact these to couple of artificial variates with the help of factor analysis. Receiving these independent factors it was easier to scan the firms.

The analysis of the factors showed which are those dimensions that separate the milk companies. It was possible to scan the main activities and characteristics of the milk industry such as the capacity, the costs, the financial activity or other factors, which mostly determine the economy of these companies.

From my previous research it has turned out that the foreign capital investments greatly affect the economy of companies. That´s why I attached importance to analyse this differentiation with statistical methods.

To this analysis I used discriminant analysis. Previously I classified the two groups according to the determinative foreign subscribed capital and then with the use of the financial data I tried to confirm that this separation is valid.

To the statistical scanning I used the SPSS software package.

Static Slicing of Binary Executables

Ákos Kiss, Judit Jász, and Gábor Lehotai

Program slicing is a technique for determining the set of statements of a program that potentially affect the value of a variable at some point in the program. Static slicing computes slices using static analysis, without making any assumptions regarding the sliced program´s input, while dynamic slicing computes slices for specific test inputs. Both static and dynamic techniques of intra and interprocedural slicing of high-level languages has been greatly studied in the literature.

Analysis of machine code is somehow different from the analysis of high-level languages since central notions as control structures and variables are missing. At machine code level on the architectures of our days the analysis has to work with fully unstructured control flow, registers and memory locations.

In this paper we explain how to apply intraprocedural static analysis to binary executables and we introduce a method to extend the usual analysis of registers to the local stack image of procedures. This way the local variables usually residing on stack can be taken into account during analysis. The extension of the conventional technique enables us to create more precise but still safe slices of binary programs.

The result of the analysis can be useful for reverse engineering tools of binary programs.

Roleoriented software development in practice

Tamás Kókai and Tibor Csiszár

We are developing a frequently changing information system that handles a huge amount of data. At the beginning we tried to complete the task with the Object Oriented (OO) paradigm and Unified Modelling Language (UML), but we often faced problems that we could hardly solved or couldn't solve at all.

Having experienced these problems we started to work out a new software development method in which we attempted to merge the advantages of Relation Database Management (RDBMS) and Object Oriented Programming (OOP).

In the introduction of our article we describe the characteristics of problem domain and the known deficiencies of current methods.

Instead of giving a detailed description of the method our primary goal is to attract attention. According to this we give a brief view of our software development method. We describe the steps from modelling through defining queries until planning views. We mention the operation of the client program and we also introduce an example.

The last part summarizes the advantages and disadvantages of the method and we forecast the future work.

Comment: We recommend the presentation called "The basics of roleoriented modelling" that gives a short review about the theoretical basics of our method.

References

[1] Andersen, Egil P. Using Roles and Role Models for the Conceptual Modelling of Objects `www.ifi.uio.no/~trygver/documents/index.html`

[2] Casanave, Cory Requirement for Roles Revision 1.0 OMG Object & Reference Model Sub-Committee Green Paper

[3] Csiszár, Tibor - Kókai, Tamás An approach of complex information system's modelling Lecture of "Fourth Joint Conference on Mathematics and Computer Science" Baile Felix, Romania 2001.

[4] Fowler, Martin Dealing with Roles Proc.of the 4th Annual Conference on the Pattern Languages of Programs, Monticello, Illinois, USA, Sept. 2-5, 1997 (`www.martinfowler.com/apsupp/roles.pdf`)

[5] Fowler, Martin UML Distilled Second Edition, Addison-Wesley, 2000.

[6] Graham, Ian, Simons, Anthony J H 37 Things that Don't Work in Object-Oriented Modelling with UML ECOOP'98 WS pp.209-232

[7] Hornyik, Katalin Szereporientált elemzés és tervezés, Diplomamunka ELTE TTK 2002 (only in Hungarian)

[8] Mili, F. On the Formalization of Business Rules ECOOP'98 WS pp.122-129

[9] Wieringa, Roel A Survey of Structured and Object-Oriented Software Specification Methods and Techniques ACM Computing Surveys, Vol. 30, No.4, pp.459-527

Application of Tree Automata in The Validation of XML Documents

Lajos Kollár

In recent years, XML has become a communication standard of the Web. Since XML is a meta-language, it needs a schema to define concrete languages for particular applications. Different schema languages have appeared in the past few years, e.g., DTD, XML Schema, RELAX Core, TREX, and so on. In this paper we deal only with RELAX and TREX which are based on tree regular language theory.

All XML documents have a logical structure which forms a tree. Validation of an XML document is the process of checking whether the document corresponds to its schema or not. The validation of a document against its schema written in such a schema description language could simply be done by constructing a tree automaton which is to decide whether the tree representation of this document is generated by the given regular tree grammar or not.

The above mentioned schema languages have quite different characteristics from the viewpoint of Formal Language Theory. RELAX and TREX are appropriate for expressing any regular tree grammar, therefore they are more expressive than the others. Since the class regular tree languages is closed under union, intersection and difference, it has many advantages of using RELAX or TREX to describe the required schema. RELAX Next Generation (RELAX NG) combines the benefits of those two similar languages.

With the progress of time, new requirements could emerge against the application. Hence, schemas evolve to new schemas or new versions of old schemas. There could also be some kind of 'convergence' between applications of the same domain (e.g., on-line book stores): they could share information using the same schema. To achieve this goal, the integration of current schemas should be supported. That is exactly why closure of the communication language is so important.

Beyond these issues, the problem of 'dynamically changing schemas' is examined (which means that the grammar is changing while the application is running): we describe possible kinds of changes that can be applied to the schema. Based on Document Object Model (DOM), a Java implementation of an application which re-validates the document against the changed schema is also given.

Various Hyperplane Classifiers Using Kernel Feature Spaces

Kornél Kovács and András Kocsor

In machine learning the classification approach may be linear or nonlinear, but it seems that by using the so-called kernel idea, linear methods can be readily generalized to the nonlinear ones. The key idea was originally presented in Aizermann's paper [1] and it was successfully renewed in the context of the ubiquitous Support Vector Machines (SVM) [2]. The roots of SV methods can be traced back to the need for the determination of the optimal parameters of a separating hyperplane, which can be formulated both in input space or in kernel induced feature spaces. While the former is a linear method, the latter results in a nonlinear counterpart. Optimality can vary from method to method and SVM is just one of several possible approaches.

In this paper we present a new family of hyperplane classifiers, that make use of various contrast functions for different optimality aspects. However, in contrast to SVM - where a constrained quadratic optimization is used - some of the proposed methods lead to the unconstrained minimization of convex functions while others merely require solving a linear system of equations similar to [3]. Unconstrained convex minimization arises when a convex penalty function is applied to non-separated samples, while the other case occurs for an implicitly defined regression hyperplane. We should add that in our regression-based approach not only the features but the class information is transformed to kernel feature spaces as well.

The main consequence of the paper is that in numerous cases our algorithms proved to be the more beneficial to the classification task out of the methods examined.

References

[1] M. Aizermann, E. Braverman, and L. Rozonoer Theoretical foundations of the potential function method in pattern recognition learning, Automation and Remote Control 25:821-837, 1964.

[2] Vapnik, V. N. Statistical Learning Theory, John Wiley & Sons Inc., 1998.

[3] Lee, Y.-J. and Mangasarian, O. L. SSVM: A Smooth Support Vector Machine for Classification, Philadelphia INFORMS, November 7-10, 1999.

Mathematical morphology in image processing by SLD resolution

Gergely Kovásznai and Krisztián Veréb

The Artificial Intelligence researches are in close ties with image processing (e.g., machine vision, robot controlling etc.). But the most of image processing algorithms need imperative solutions. So a question arises, how can such researches be studied using another paradigm in the Artificial Intelligence. The mathematical morphology is one of the most important parts of the image processing used in the image filtering and skeletonization.

So, the question could be defined in the following way: with given digital sets could its eroded and dilated sets be produced using logic programming (e.g. Prolog)? If it is possible, it allows to examine morphology and digital image processing algorithms in the logic programming.

Mathematical morphology stands as a relatively separate part of image analysis. It is based on the algebra of non-linear operators operating on object shape and in many respects supersedes the linear algebraic system of convolution. Morphological operations are used predominantly for image pre-processing (noise filtering, shape simplification), skeletonizing, thinning (enhancing object structure), segmenting object from the background etc.

The main morphological operators are the erosion and dilation, which are based on Minkowski algebra. To answer our main question we create a suitable first-order logical language and formulate the morphological operators as predicates. We transform the formulated problem into an appropriated set of clauses described by a special point-plus form. Since our transformed clauses have a special form, they can be considered as Horn-clauses. That is the reason why we can use SLD-resolution to examine the morphological operators.

In this lecture we show a possible interpretation of the formulated operators mentioned above and particular Prolog codes as well.

Keywords: SLD Resolution, Prolog, Morphology, Erosion, Dilation

Colour space transformation, colour correction and exact colour reproduction on FALCON architecture

Péter Kozma

Nowadays many problems requiring huge computing power have risen. Although the performance of digital processors doubles yearly, there are certain tasks where the computation cannot be carried out within a reasonable time interval. Such hard problems are the analysis of big dynamical systems or real-time exact colour reproduction. The exact colour visualization of motion pictures is necessary in industrial, medical and scientific research areas. Thus, for example, exact colour reproduction is required for remote medical diagnosis or remote operation. The doctor has to see the same image that appears in reality. Device dependent colour appearance may cause faulty decisions. Nowadays these problems cannot be solved perfectly because many steps of the transformation are not completely known and the huge number of computations cannot be done in real-time even by the fastest PC. In this article is described some methods to produce exact colours in a remote medical diagnostic system.

Recently, the requirements towards remote medical diagnostic systems have changed significantly. The diagnosis based on verbal information is not satisfactory. The communication between the doctor and the patient can be realized in video conferencing system. In some cases it could be a very important point of view of the exact diagnosis that the skin of the patient be displayed on the screen in the same colour as it is in reality. Serious scientific and technological apparatus is required to realize this kind of system. There are two fundamental points of view relating to this type of system. First the main characteristics of the output of the imaging medical systems have to be examined. For example, it is a very important task for the output images of CT (Computer Tomograph) and MRI (Magnetic Resonant Imager) where a minimal deviation is a very important point of view of the diagnosis. On the other hand, the exact colour reproduction in remote medical diagnostic systems has to be assured. Some environmental parameters have to be fixed to realize the exact colour reproduction, for instance the minimal resolution and colour depth of the monitor or the camera or the direction and the luminance of lighting. The real-time processing of motion pictures has a huge claim to computing power. The fastest computer is the ASCI White supercomputer implemented by IBM in 2001 consisting of 8192 processors with 7.226 TFLOPS computing power [1]. In many image processing applications this huge computation power is really needed, the operations are special and do not require the 32 bit floating point accuracy. One alternative is the analogic CNN array computer performing about Tera-equivalent operations per second, on a single chip. The latest analogue CNN chip has a resolution of 128×128 pixels and its equivalent computing power is 4 Tera-equivalent operations per second but its computational precision is about 7 or 8 bits [2]. We need an accuracy of at least 12 bits and higher computing performance than in software simulation, so hardware acceleration is required. The Falcon emulated digital CNN-UM chip is used to speed up our computations. [3] Falcon is a configurable architecture where the neighbourhood value of the templates, the accuracy of the state and template values and the size of the emulated cell array can be changed. The architecture utilizes the flexibility of the FPGAs (Field Programmable Gate Array) that makes it possible to try several configurations on the same hardware and choose the architecture that is the best for our application. In our case the multi-layer extension of the Falcon architecture called Falcon-ML, especially the three-layer case, was extensively used where each colour component had a separate layer. Using the Falcon architecture 20 to 150 fold speedup can be achieved compared to the software simulation; this makes real time colour space transformation, colour correction and exact colour reproduction possible even in the highest resolution.

References

[1] www.top500.org/list/2001/11/, www.llnl.gov/asci/

[2] G. Liñán, R. Domínguez-Castro, S. Espejo, A. Rodríguez- Vázquez, "ACE16k: A Programmable Focal Plane Vision Processor with 128x128 Resolution" in, Proc. of the 15th European Conference on Circuit Theory and Design, Vol. 1, pp. 345-348, 2001.

[3] Zoltán Nagy, "Configurable multi-layer CNN-UM emulator on FPGA", to be published on CNNA 2002, Frankfurt, 2002

Soliton graphs and graph-expressions

Miklós Krész and Miklós Bartha

A graph having at least one vertex with degree one is called an open graph. A soliton graph is an open graph having a perfect internal matching, i.e., a matching that covers all the vertices of the graph with degree at least two. These vertices are called internal, whereas vertices with degree one are classified as external. Soliton graphs are the underlying objects of certain molecular switching devices called soliton automata.

The analysis of soliton automata is a very complex task, and only a few special cases have been successfully dealt with so far. Most of the difficult problems in the general case are still open.

This lecture addresses the issue of generating soliton graphs by context-free grammars over graph expressions. The relevance of describing soliton graphs in this specific way is that it highlights the structure of soliton walks defining the transitions of the corresponding soliton automata.

At first, a decomposition procedure is presented for soliton graphs in terms of their global internal structure. It is shown that the elementary components of soliton graphs can be grouped into pairwise disjoint families based on how they can be reached by alternating paths starting from external vertices. This decomposition is then carried over to soliton automata, using quasi-direct and α_0 products of their component automata.

As a second step, the families of elementary components is characterized. To this aim, the concept of factor-critical graphs is generalized for open graphs, and splitters are introduced as the "open" counterparts of barriers in graphs with perfect matchings. It is shown that all external families are factor-critical open graphs. On the other hand, internal families are characterized as graphs having a maximal splitter in which all vertices are inaccessible from external ones by an alternating path.

Finally, context-free grammars capable of generating graph expressions denoting external/internal families and soliton graphs in general are elaborated on the basis of the structural characterizations above.

Investigation of Binary Representations of SAT especially 2-Literal Representation[3]

Gábor Kusper

The problem of propositional SATisfiability for formulae in conjunctive normal form is the first known NP-complete problem. Many practical NP-hard problems may be transformed efficiently to SAT. Thus, a good SAT solver would likely have considerable utility. Since the complexity of SAT solvers depends also on the representation we shall carefully study this aspect. A formula is conjunction of clauses and a clause is disjunction of literals. There are three kind of literals: positive (+), negative (-) and joker or no occurrence (x) literal. The positive and negative literals are concrete literals. The joker literal means that the corresponding variable does not occur in the clause. There are many possibilities how to represent a formula. For example we may represent a formula as a list of clauses or matrix of literals. We discuss advantages and disadvantages of several SAT representations. First we discuss the natural binary representation, where a literal is represented by 2 bits (`-:01, +:10, x:11`). Than we introduce a new binary representation, called 2-literal representation, which uses 4 bits to represent all the 15 possible basic (basic means cannot be simplified) formulae with 2 variables (`[--]:0001, [-+]:0010, [-x]:0011, [++]:0100, [--,++]:0101, [x+]:0110, [-x,x+]:0111, [+-]:1000, [x-]:1001, [-+,+-]:1010, [-x,x-]:1011, [+x]:1100, [+x,x-]:1101, [+x,x+]:1110, [xx]:1111`). The idea is that every bit corresponds to a 2-clause (a clause with two concrete literals). For example, the least significant bit corresponds to `--`. If a bit is 1 then the corresponding 2-clause is subsumed by the represented formula. The 2-literal representation is better than the natural one because with 4 bits it can represent 2 literals as the natural one and it can represent also any combinations of 2-clauses and many operations are easier with it. We can generalize the 2-literal representation, called n-literal representation, such that it uses 2^n bits to represent all basic formulae with n variable. This representation is rather costly but we give arguments for using 5-literal representation. Finally we give a comparative table with 5 different SAT representations with time complexity information of operations like unit-propagation or formula negation.

[3]Sponsored by Upper Austrian Government (scholarship), FWF SFB F013 (P1302) and Austro-Hungarian Action Foundation

Model Order Estimations for Noisy Black-box Identifications

Tibor Laczó and László Sragner

One of the principal targets of nonlinear system identification is determining the complexity of an unknown system. If the system is dynamic we have to choose the class of the model and determine the order of the model. The order of the model means how many past inputs and outputs are used in the calculation of the current output. There are several information criteria to qualify a model but they need the setting of the model´s parameters what is the most time consuming step in the identification. We will use the Lipschitz method which estimates the order of the model directly form input-output data [1]. The main idea of the method is that a continuous function´s gradient has a definite maximum and this is a characteristic feature of the function. We calculate the following quotient:

$$L^{(n)} = \left(\prod_{k=1}^{p} \sqrt{n} L^{(n)}(k) \right)^{\frac{1}{p}}$$

Where $L^{(n)}(k)$ is the k-th largest gradient of the function calculated from the known points of the function. This quotient has the property that, if n_0 is the optimal order than $L^{(n_0-1)}$ is much larger than $L^{(n_0)}$ and $L^{(n_0+1)}$ is very close to $L^{(n_0)}$, so we have to find the sharpest breakpoint in the graph of $L^{(n)}$ vs. n. The problem with Lipschitz method is that if noise appears on the inputs and outputs the estimation of the order will be improper or the graph has no sharp breakpoint. To avoid this we use the Errors-in-Variables (EIV) cost function what modifies the input data to eliminate or reduce the noise [2]. The main idea of EIV is that we weight the error of the input and the output according to the reciprocal of the noise variance. For each measurement k the sample variances of the inputs $\hat{\sigma}^2_{u,k}$ and outputs $\hat{\sigma}^2_{y,k}$ the sample covariance matrix $\hat{\sigma}^2_{uy,k}$ and the mean values $\hat{u}_k$ and $\hat{y}_k$ can be calculated or can be estimated [2].

$$C_{EIV} = \frac{M}{N} \sum_{k=1}^{N} \left(\frac{(\hat{y}_k - f_{NN}(u_k, \Theta))^2}{\sigma^2_{y,k}} + \frac{(\hat{u}_k - u_k)^2}{\sigma^2_{u,k}} \right)$$

The greater noise causes that the error counts with smaller weight and the training points with less noise cost more. It can be proved that with noisy data it converges to the true model´s parameters. Because of the modification of the input data, the number of free parameters is increased, therefore the EIV training is very prone to overfitting. To avoid overfitting we first train the network with Backpropagation (BP) and Least Squares (LS) cost function. Our main idea is to combine Lipschitz method and EIV cost function to get more characteristic estimations of the model order. First we estimate the order of the unknown model from its input-output data. The Lipschitz method uses the input-output data as a NARX [3] model. Because of the noise this estimation is probably not characteristic enough. Second we create the model with the estimated order and train it with BP and LS. At a defined error level we stop the training and start using the EIV. The training is controlled with early-stopping to avoid overfitting. If training is finished we get the model and we also get a new input sequence modified by the EIV. On the modified input sequence we use the Lipschitz method again and we compare the results. If the curve sharpened at the estimated order than the order could be correct. We test the method on artificial and real-life industrial problems (LD converter in steel production) [4].

References

[1] X. He, H. Asada, "A new method for identifying orders of input-output models for nonlinear dynamic systems" Proceedings of the American Control Conference, San Francisco, California, June 1993, pp. 2520-2523.

[2] G. Vandersteen, “Identification of Linear and Nonlinear Systems in an Errors-In-Variables Least Squares and Total Least Squares Framework”, PhD thesis, Vrije Universiteit Brussel, Belgium, April 1997

[3] K. S. Narendra, K. Pathasarathy, “Identification and Control of Dynamical Systems Using Neural Networks”, IEEE Trans. Neural Networks, Vol.1.pp. 4-27,1990

[4] P. Berényi, G. Horváth, B. Pataki, Gy. Strausz, “Hybrid-Neural Modelling of a Complex Industrial Process”, IEEE Instrumentation and Measurement Technology Conference, Budapest, 2001. vol. III. pp. 1424-1429.

Hand gesture-based film restoration[4]

Attila Licsár and Tamás Szirányi

In the information society the communication between user and computer has become very active research area. As the camera and computer prices are decreasing, the vision-based systems are more available by everyone, the development of computer vision and analysis is becoming an important research area in Human Computer Interaction (HCI).

We have developed a static hand gesture recognition system for the Human Computer Interaction based on shape analysis. This appearance-based recognition uses modified Fourier descriptors for the classification of hand shapes. Usually systems use two phases: training and running phase during the recognition. A new method is shown that under the running phase of the system users can interactively modify and learn hand gestures by the gesture motion, so they could improve the efficiency of the system. With this interactive learning algorithm our system is able to adapt to similar gestures of other users or small changes of hand posture.

In this paper we demonstrate an effective human-computer interface for controlling the steps of the restoration of old films. Film specialists and artists do not like standard computer devices they prefer natural interfaces like in HCI systems. We will show a gesture recognition application applying these methods in the controlling system of old film restoration.

[4]Hand Recognition Demo can be downloaded from `http://www.knt.vein.hu/staff/licsara/`

Enhanced Macrostep-based Debugging Methodology for Parallel Programs

Róbert Lovas and Péter Kacsuk

The macrostep-based debugging concept has been developed originally for message passing parallel programs designed in the frame of P-GRADE graphical programming environment. The macrostep is essentially the set of executed code regions between two consecutive collective breakpoints, which breakpoints are placed on communication operations automatically. The main advantage of the macrostep-based debugging is the handling of non-deterministic behaviour of point-to-point message passing applications that is inherited from wildcard receiving operations. By using the current version of macrostep-based debugger, program developers and testers can replay the entire parallel application and also apply the cyclic debugging technique that was introduced for sequential programs. Moreover, the macrostep debugger tool is able to generate all the possible timing conditions systematically therefore, the parallel application is forced to traverse its entire state-space.

In this paper we present a formal description of macrostep-by-macrostep execution of message passing parallel programs as well as the correctness of macrostep debugging methodology by showing the relation between the state-space of parallel applications without macrosteps and the reduced state-space when we apply macrosteps. Based on the formal description the macrostep-based debugging concept has been enhanced in order to support the different ways of collective communication (multicast, scatter, etc.) and the pre-defined scalable process communication templates, such as pipe, mesh or tree. Hereby, the new prototype of macrostep debugger tool can be used in the P-GRADE graphical programming environment without limitations and its usage is illustrated by a simple example.

Due to the combinatorial explosion the exhaustive traverse of each execution path might be impossible in case of real-size programs but some techniques can help the user traverse the different execution paths of parallel applications efficiently. Finally, we summarise some traditional and some novel methods to reduce further or cut the state-space of parallel applications (that must be traversed during the exhaustive testing), such as run-time temporal logic assertions, low-cost static and dynamic analysis of parallel behaviour based on coloured Petri-nets. The integration and evaluation of these methods are under development but some preliminary results are available and presented in the paper.

New Interval Methods for Constrained Global Optimization: Solving 'Circle Packing' Problems in a Reliable Way

Mihály Csaba Markót, José Fernández Hernández and Leocadio González Casado

The talk gives the theoretical and numerical results of solving inequality constrained global optimization test problems with interval Branch-and-Bound methods using new techniques.

In [1, 3] a new heuristic decision index was discussed for *unconstrained* problems and investigated in detail. This index has the form of $p\hat{f}(\boldsymbol{X}) := (\hat{f} - \underline{\boldsymbol{f}}(\boldsymbol{X}))/w(\boldsymbol{f}(\boldsymbol{X}))$, where $\boldsymbol{X}$ is an interval vector, $\hat{f}$ is an approximation of the global minimum value and $\boldsymbol{f}$ denotes the interval inclusion function of the objective function. The index measures the relative position of the minimum within the inclusion $\boldsymbol{f}(\boldsymbol{X})$ and it is suitable to be applied as a subinterval selection criterion and as a part of the subdivision rule as a decision factor.

J. F. Hernández proposed the idea of extending this index for constrained problems by taking the effect of the constraints into account in a similar way:

$$pu_{\boldsymbol{g}_j}(\boldsymbol{X}) := \min\left\{\frac{-\underline{\boldsymbol{g}_j}(\boldsymbol{X})}{w(\boldsymbol{g}_j(\boldsymbol{X}))}, 1\right\}, \quad pu(\boldsymbol{X}) := \prod_{j=1}^{r} pu_{\boldsymbol{g}_j}(\boldsymbol{X}).$$

(where $\boldsymbol{g}_j$ is the interval inclusion function of the jth constraint). The pu quantity measures the relative position of 0 within the inclusions of the constraint functions, i.e. the feasibility of the box $\boldsymbol{X}$. Finally, the heuristical decision index for constrained problems is formalized by $pup(\hat{f}, \boldsymbol{X}) := pu(\boldsymbol{X}) \cdot p(\hat{f}, \boldsymbol{X})$. We can conclude that if the pup value for a given box is high, then the box should be preferred for an early selection (interval selection step), or it is advisable to split it into a higher number of subboxes (subdivision step).

In the theoretical part of the talk we present convergence properties of the B&B algorithms using the new interval selection criteria. As a conclusion, we can state that a suitable choice of the $\hat{f}$ value is essential to reach the global convergence.

In the numerical tests we introduce the efficiency of the new heuristic rules on three different types of problems: the first is the problem class of the obnoxious facility location model [4]. For such a problem our goal is to place an unpleasing object into a region by considering the disappointment of the inhabitants and the geographical possibilities. The second part of the test problems came basically from unconstrained global optimization; we have selected some harder problems, e.g. Hartman-6, Goldstein-Price, Levy-3, Ratz-4 and EX2 (for the definitions see [2, 9, 10]) and completed them with sets of randomly generated linear and quadratic constraints.

In the third part of the numerical investigation we discuss the 'packing circles into a unit square' problems [5, 6, 8]. For such a problem instance (specified by the number of the circles, n) we want to determine the largest value of r for which the given number of circles having the uniform radius r can be placed into the square without overlapping. We present an improved algorithm giving verified solutions, where the verification can be made in both the local and the global sense.

The main consequence of our investigations is that the new type of interval selection criterion significantly improves the efficiency in terms of both the running time and the memory complexity. In addition, the largest improvements were achieved on the hardest problem instances.

Acknowledgements This work was supported by the Grants FKFP 0449/99, OTKA T 32118 and T 34350.

References

[1] Casado, L. G., Martínez, J. A., and García, I.: Experimenting with a new selection criterion in a fast interval optimization algorithm, J. Global Optimization 19(2001), 247-264.

[2] Csendes T. and Ratz, D.: Subdivision direction selection in interval methods for global optimization, SIAM J. Num. Anal. 34(1997) 922-938.

[3] Csendes T., New subinterval selection criteria for interval global optimization, J. Global Optimization 19(2001), 307-327.

[4] Fernández, J., Fernández, P., and Pelegrín, B.: A continuous location model for siting a non-noxious undesirable facility within a geographical region, European Journal of Operational Research 121(2000), 259–274.

[5] de Groot, C., Monagan, M., Peikert, R. and Würtz, D. (1992), Packing circles in a square: review and new results, *System Modeling and Optimization, Lecture Notes in Control and Information Services*, 180, 45-54.

[6] Markót M. Cs. (2000), An interval method to validate optimal solutions of the "packing circles in a unit square " problems, *CEJOR* 8, 63-78.

[7] Markót M. Cs., Fernández, J., Casado, L.G., and Csendes T.: New interval methods for constrained global optimization. In preparation. Available at `http://www.inf.u-szeged.hu/~markot/`.

[8] Nurmela, K. J. and Östergård, P. R. J. (1999), More optimal packings of equal circles in a square, *Discrete and Computational Geometry* 22, 439-457.

[9] Ratz, D. and Csendes T.: On the Selection of Subdivision Directions in Interval Branch-and-Bound Methods for Global Optimization, J. Global Optimization 7(1995) 183-207.

[10] Törn A. and Žilinkas, A.: Global Optimization, Springer-Verlag, Berlin, 1989.

Fast and efficient multi-layer CNN-UM emulator using FPGA

Zoltán Nagy

A Cellular Neural Network is a non-linear dynamic processor array. Its extended version the CNN Universal Machine (CNN-UM) was invented in 1993. [1] The main application area of this architecture is 2D signal or image processing. The most effective implementation of the CNN-UM architecture seems to be analog VLSI. The latest analogue CNN chip has a 128×128 pixel resolution and its equivalent computing power is 4 tera operation/second but its computational precision is about 7 or 8 bits. [2] In many applications these parameters are not high enough. If the resolution is higher we don't need to slice the images. If the precision is higher, less robust or more sophisticated analogical algorithms can be used.

A multi-layer CNN array can be used to solve the state equation of complex dynamical system. Currently the only method to solve the state equation of multi-layer CNN array is software simulation. If every layer has different time constant very small simulation stepsize must be chosen, thus software simulation is very slow. To achieve affordable runtimes the simulations have to be accelerated. This motivation came from the analysis of a retina model, where the retina is modelled with 3-layer CNN array and every layer has different time constant. [3]

The Falcon emulated digital CNN-UM chip was designed to reach these goals. [4] Especially flexible emulated digital CNN-UM was developed where the accuracy, template size, cell array size and the number of layers can be configured. Simulation runtimes can be hundred times shorter using the Falcon processor array compared to the software simulation. This paper describes the synthesis, implementation and optimization methods used to implement the Falcon processor array on FPGA. The Distributed Arithmetic technique is used to optimize the architecture on FPGAs. [5,6] Using this technique, smaller and faster arithmetic units can be designed than the conventional approach, where multiplier cores and adder trees are used to compute the state equation of the CNN array.

The Falcon architecture was implemented on our prototyping board, using a Virtex-300 FPGA from Xilinx Inc. The performance of the architecture was encouraging, even in a single processor configuration 20 fold speedup can be achieved compared to 1GHz Pentium III Xeon processor. The processor runs only on 80MHz clock frequency because of the limitations of the prototyping board. Using faster memories, higher speed grade FPGA or using the more advanced Virtex-E and Virtex-II FPGAs twenty times higher performance can be easily achieved. The easy scalability of the Falcon architecture makes possible to connect the processor cores in a square grid and achieve even more performance. Using re-configurable devices to implement the Falcon architecture provide us more flexibility compared to the conventional emulated digital architectures e.g. different configurations can be used on the same hardware and extra design effort is not required to implement it.

References

[1] T. Roska and L. O. Chua, "The CNN Universal Machine. An analogic array computer" IEEE Trans. On Circuits and Systems-II, vol. 40, pp. 163-173, 1993.

[2] G. Liñán, R. Domínguez-Castro, S. Espejo, A. Rodríguez-Vázquez "ACE16k: A Programmable Focal Plane Vision Processor with 128x128 Resolution" in Proc. of the 15th European Conference on Circuit Theory and Design, vol. 1, pp. 345- 348, 2001.

[3] D. Bálya, B. Roska, T. Roska and F.S. Werblin, "A CNN Framework for Modeling Parallel Processing in a Mammalian Retina", Int. J. on Circuit Theory and Applications, vol. 29, No. 3, 2002.

[4] Z. Nagy, P. Szolgay, " Configurable multi-layer CNN-UM emulator on FPGA", to be published on CNNA 2002, Frankfurt, 2002.

[5] Peled and B. Liu, “A New Hardware Realization of Digital Filters”, IEEE Trans. on Acoust., Speech, Signal Processing, vol. ASSP-22, pp. 456-462, Dec. 1974.

[6] Mintzer, L. “FIR filters with the Xilinx FPGA” in Proc. of FPGA ’92 ACM/SIGDA Workshop on FPGAs, pp. 129-134, 1992

On the convergence of OSPF

Attila Rajmund Nohl and Gergely Molnár

The Open Shortest Path First (OSPF) [1], [2] routing protocol is the recommended Interior Gateway Protocol (IGP) by the Internet Engineering Task Force (IETF). It is widely deployed in the current Internet and most router vendors support this routing protocol. One of the most important aspects of a routing protocol's performance is its convergence. A routing protocol's convergence is the period during the routers acclimatize themselves to the new network topology after a change in the network. The OSPF routing protocol is a link state routing protocol. It means that every router must have the same view of the network. In case of OSPF, each router must have the same set of Link State Advertisements (LSA) in their LSA databases. When there is a change in the network (e.g. a link goes down), the information about this change is flooded through the Autonomous System so every router can update its LSA database to reflect the new network topology. During this flooding the above stated principle of OSPF is not true (some routers already got the new LSAs, some haven't got them yet) so there can be problems during flooding: rooting loops can arise, networks can become unreachable temporarily. These phenomena could mean degradation of service so it is vital to know how long is this convergence period. In this work the convergence of OSPF was analysed and examined by mathematical tools and by measurements on a test network.

One of the most important aim of this work was to examine the predictability of OSPF convergence from the size of the network. The size here means number of routers and used links. To reach this aim, a model is needed that gives proper measures about the convergence. The first step to get this model is learning how OSPF works and what properties, features and characteristics have effect on convergence. As the convergence depends on the amount of transfered data by the OSPF flooding, the starting point was to see how many data is generated in the relevant flooding situations. Knowing the amount of generated data - i.e. the required bandwith - and the capacity of the network we can predict the convergence. Examining and analysing the frequency of data exchange by OSPF routers, the generated data during flooding leaded to a deterministic model. To validate it, a test network was built and several experiments and measurements were done to see how the model works. The results showed that the deterministic model gives results to be very close to the measured results. To refine the model, a probabilistic component based on measurements was introduced, which led to a better model.

In this paper an OSPF convergence time prediction model is introduced. It is derived from examination and analysis of the generated data by flooding and the behaviour of OSPF. The model was validated and refined by tests and experiments on a test network built for this work. The resulted model can be used to predict the effect and convergence of a change in an OSPF network. This feature is very usable for a preemptive network management.

Keywords: Internet Protocol, Open Shortest Path First (OSPF), convergence

References

[1] J. Moy "OSPF version 2", RFC2328, April 1998. available at `http://www.ietf.org`

[2] F. Baker, R. Coltun "OSPF version 2 management information base", RFC1850, November 1995. available at `http://www.ietf.org`

Digital Signatures with Signer's Biometric Authentication

Péter Orvos

The two aims of digital signatures are to preserve the integrity of the signed document and to ensure the receiving party about the identity of the signing party. The currently used technologies authenticate the signer by proving that the signature was generated using the proper secret key, therefore it identifies the signing person assuming that the secret key can only be possessed by its legal owner.

Unfortunately in real life circumstances this assumption may not stand as the secret key may be stolen from or swindled out of the unqualified user. For this reason several efforts have been taken in order to enforce the relationship between the secret key and its owner: the user of the key is usually identified by a password or a PIN (Personal Identification Number). However, another authentication scheme may be able to strengthen further more this relationship using biometric user authentication techniques.

Biometric User Authentication. In systems using biometric user authentication some physical properties of the user is measured and verified being compared to certain biometric profiles, which were previously created from authentic samples of the appropriate users. This way of user authentication is ideal as it verifies the user himself/herself, however there are also some disadvantages that must be counted with.

Acquiring biometric information requires certain measurements, and because of the nature of measurement techniques the results will contain certain errors that the authentication algorithm must model and eliminate introducing the possibility of false decisions, of which the possibility must be minimized. Another problem originates from the fact that certain biometric information, such as a fingerprint image is handled as classified personal data in several countries, therefore it must be handled accordingly.

Integration of Biometric Authentication and Digital Signatures. Current smart-card based implementations store the secret key and the biometric profile of the owner in the card´s inaccessible memory, and perform biometric authentication each time before creating a signature. Card manufacturers claim that the stored information is inaccessible using current technology, however it might be more secure to store the secret key encoded; that is, it cannot be used even if the memory contents can somehow be retrieved.

The elementary target of my algorithm is to calculate a binary personal identification vector from the retrieved fingerprint image and the biometric profile, what can later be used for encoding or decoding the secret key. In order to result the same vector every time a signature is to be created an error correction method must be applied, of which the correction capability must be carefully adjusted, since correcting too much errors may lead the system to accept fingerprints of unauthorized people.

Two, essentially different algorithms are the subjects of my research, both of which will be introduced in my lecture. One is based on the relative positions of minutiae points [1][2], which are characteristic points of fingerprints situated where ridges end or branch. Another examined approach is based on the calculation of FingerCodes [3] using graphical filters and calculating divergence of certain image regions.

References

[1] Éva Nikodémusz-Székely, Dr. Vladimir Székely, "Image recognition problems of fingerprint identification", Microprocessors and Microsystems, Vol 17, No 4, 1993, page 215-218.

[2] M. Kawagoe, A. Tojo, "Finger pattern Classification", Pattern Recognition, Vol. 17, No 3, 1984, page 295-303.

[3] Anil K. Jain, "FingerCode: A Filterbank for Fingerprint Representation and Matching", MSU-CPS-98-36, 1998.

End-to-end QoS management issues over DiffServ networks

István Pataki and András Gulyás

Recent times the performance of the personal computers increases likewise the number of real-time Internet and multimedia applications. In the case of such applications *best effort* treatment of the Internet traffic is not enough for satisfying the quality demand of end users. However, *best effort* is the only service approach on the Internet today. The network elements try their best to deliver the packets to their destinations without any hard bounds on end-to-end delay, jitter, and latency. These "guarantees" are not sufficient for i.e., a videoconference, because high delay or jitter can cut down or ruin the interactivity and usability.

The goal of the Internet Service Providers (ISPs) is to satisfy the quality demand of customers and to ensure the same sort of QoS and reliability over IP networks as in the circuit switched networks. By applying packet classification they can deliver different kind of services on the same link without downgrading the quality of the important flows. One of the possible solutions is the Differentiated Services architecture.

DiffServ [1] is a model that allows deployment of QoS in a simple fashion using network devices only handling traffic at an aggregate level rather than per flow. DiffServ defines the DS (DiffServ) domain, which is a contiguous set of DiffServ capable nodes. Obviously, without accurate domain management, the concept does not work effectively. A proper domain manager is able to use the resources of the domain more effectively, and makes it possible to satisfy the customer's claims. The domain manager of the DiffServ model is called Bandwidth Broker as introduced in RFC 2638 [2].

The BB is aware of the topology of the domain and has correct information on the currently reserved and free link capacities. The main functions of the BB can be grouped into two groups. The intra-domain functionality covers managing the resources of the own domain. Another group of the BB functions is the inter-domain communication extension, which includes exchange of information on the available services between the Bandwidth Brokers of the adjacent domains, and the negotiation based on the received availability information.

In the last three years several inter-domain protocols has been developed such as BGRP[3], SIBBS[4], RNAP[5] etc. These methods are independent from the routing used in the network and focus mainly on the correct administration of inter-domain reservations. Although there are several solutions for QoS routing, the Internet still uses static routing as well. Since the efficiency of these protocols highly depends on the routing algorithm applied in the network, they may produce low resource utilization among static routing environment.

Our work presents an inter-domain communication protocol, which works in a Bandwidth Broker environment. We use a BB, which support dynamic intra-domain routing. This means that the intra-domain side of the BB is able to change the routing per flow, if the inter-domain part asks it to. We separate two types of routing in this way. The intra-domain routing, which is the part of the intra-domain management, and inter-domain routing as the part of the inter-domain communication. Using our own inter-domain routing method the BB can calculate several alternative routes to the destination domains, and produce higher resource utilization and greater successful reservation ratio.

This protocol defines availability messages for all the available sink domains. An availability message consist of, the name of the sink domain, the available bandwidth, hop number and other parameters. The appropriate propagation of these messages makes it possible to calculate the next hop domain for each sink domain. This propagation works over domains like a distributed QoS routing [6] over routers. We also define a reservation protocol between Bandwidth Brokers, which uses the calculated next hop domains to determine the path of the

reservation. The presentation will give an overview of the simulation of this inter-domain communication method and will introduce the measured results.

References

[1] S. Blake et al., An Architecture for Differentiated Service, RFC 2475, IETF 1998

[2] K. Nichols, V. Jacobson, L. Zhang, A Two-bit Differentiated Services Architecture for the Internet. July 1999.

[3] Ping P. Pan, Ellen L. Hahne, és Henning G. Schulzerinne "BGRP: Sink-Tree-Based Aggregation for Inter-Domain Reservations"

[4] QBone Bandwidth Broker Architekture work in progress
`http://qbone.internet2.edu/bb/bboutline2.html`

[5] Xin Wang, Henning Schulzrinne "RNAP: A Resource Negotiation and Pricing Protocol"

[6] Shigang Chen, Klara Nahrstedt "An Overview of Quality-of-Service Routing for the Next Generation High-Speed Networks: Problems and Solutions"

Towards Verifiable Design Patterns

Dániel Petri

Design pattern [1] is a form for representing proven solutions in a predetermined way. It has three main parts, which describe the problem, the suggested solution and the consequences of applying the solution. Applying these *reusable* solutions to our problems allows us to avoid system development from the scratch and thus shortens the development cycle.

Design patterns are informal: they may contain class diagram fragments, sample source code lines and informal notes partitioned into several subsections. Their formalization can serve purposes like tool support, establishment of the relationships between two design patterns, investigation whether an implementation contains a pattern properly and so on. LePUS[5] [2] is a formal language for describing and reasoning about object oriented software architectures, designs and patterns. It is intended to describe relations between classes and functions. LePUS terms can be expressed both as diagrams and formulas.

The main goal is a tool, which identifies the appropriate design patterns that can be applied to a system under development. The design patterns are described in LePUS and are stored in a database. The system specification is given in UML Class Diagrams. The tool compares the specification with the existing patterns and selects the ones which (partially) fit in the specification. The output is a subset of design patterns with the additional information where each of the patterns fit in the specification.

The first step towards this tool is the transformation of the Class Diagrams into LePUS formalism. As most UML tools support XML export, the most evident way is to base the transformation on XML. This paper first describes the bijective transformation of LePUS diagrams into XML (called LePUS-XML) and the transformation of XML Class diagrams into LePUS-XML. This transformation uses XSLT that specifies rules by which one XML document is transformed into another.

In design patterns properties of the system can also be formulated, e.g. there is no single point of failure (SPoF) in it. If such patterns are implemented properly, statements can be made that the whole system is free of SPoF. The second task of my tool is to analyse whether such patterns are implemented properly.

References

[1] Erich Gamma, Richard Helm, Ralph Johnson, John Vlissides: Design Patterns: Elements of Reusable Object-Oriented Software, Addison-Wesley Professional Computing Series, Addison-Wesley, Reading Mass. 1994.

[2] Amnon H. Eden: Formal Specification of Object Oriented Design, International Conference on Multidisciplinary Design in Engineering, CSME-MDE 2001, November 21-22, Montreal, Canada.

[5] Language for Patterns Uniform Specification

Probabilistic Diagnostics with P-Graphs

Balázs Polgár and Endre Selényi

Diagnostics is one of the major tools for assuring the reliability of complex systems in information technology. System level diagnostics considers the main, replaceable units of the system and does not deal with the exact location of faults within the units. This is the case in multiprocessor systems where only identification of faulty processors is important. According to Preparata et al. [1] in such systems intelligent units test each other and on the basis of the set of test results, called syndrome, the good or faulty state of each unit should be determined. The difficulty comes from the method how a fault in the tester processor invalidates the test result. This is described by test invalidation models.

Deterministic algorithms aim at providing complete and correct diagnosis, i.e., determining the state of each unit without classifying any of the fault free processors as faulty and vice versa. Usually not only a single diagnostic outcome is consistent with the syndrome. To select the correct diagnosis from the set of syndrome-consistent diagnostic outcomes these algorithms need further information on the system. This is the assumption that no more than a predefined number of faults are present. In contrast with this, probabilistic methods generate a diagnostic outcome using solely the information included in the syndrome. These methods try to select the most probable diagnosis but this is not always the correct one, which means the classification can contain misdiagnosed processors. [2][3]

During our work we generalised the traditional test invalidation approach and developed a novel probabilistic syndrome-decoding algorithm. The main idea is based on the reformulation of the error propagation model as a Process Network Synthesis (PNS) model. PNS models are widely used in application fields related to chemical engineering to estimate optimal resource allocation and scheduling. In our approach the same mathematical paradigm is used to model information flow similarly to material flow. As a result, the diagnostic problem has been formulated as an optimisation problem.

The diagnostic accuracy of the solution is discussed on the basis of simulation measurements and a method is introduced how a general framework can be constructed for different aspects of a complex problem with the use of PNS-model.

References

[1] F. P. Preparata, G. Metze, R. T. Chien. On the connection assignment problem of diagnosable systems, IEEE Trans. on Electronic Computers, vol. EC-16, pages 848-854, 1967

[2] T. Bartha, E. Selényi. Probabilistic System-Level Fault Diagnostic Algorithms for Multiprocessors, Parallel Computing, vol. 22, no. 13, pages 1807-1821, Elsevier Science, 1997.

[3] T. Bartha, E. Selényi. Probabilistic Fault Diagnosis in Large, Heterogeneous Computing Systems, Periodica Polytechnica, vol. 43/2, pages 127-149, 1999.

Global / Nonlinear Optimization in Modeling Environments

János D. Pintér

The subject of global optimization (GO) is to find the best solution of complex nonlinear decision models which may have a - typically unknown - number of local optima. GO is an emerging area of research, and it has a broad range of scientific, engineering and economic applications [1-4].

In this talk, we will discuss and demonstrate the use of global and (convex) nonlinear optimization software using several modeling platforms [4-7], to meet a range of needs from the business-focused user to the research scientist.

The presentation is based on recent algorithm and professional software development, and will include illustrative tests, more serious challenges, and real-world application examples.

References

[1] Horst, R. and Pardalos, P.M., Eds. (1995) Handbook of Global Optimization. Vol. 1. Kluwer Academic Publishers, Dordrecht / Boston / London.

[2] Pardalos, P.M. and Romeijn, H.E., Eds. (2002) Handbook of Global Optimization. Vol. 2. Kluwer Academic Publishers, Dordrecht / Boston / London.

[3] Pinter, J.D. (1996) Global Optimization in Action. Kluwer Academic Publishers, Dordrecht / Boston / London.

[4] Pinter, J.D. (2001) Computational Global Optimization in Nonlinear Systems. Lionheart Publishing Inc., Atlanta, GA.

[5] Frontline Systems (2001) Premium Solver Platform - Solver Engines. User Guide. Frontline Systems, Inc. Incline Village, NV.

[6] Schrage, L. (2001) Optimization Modeling with LINGO. LINDO Systems, Inc. Chicago, IL.

[7] Wolfram, S. (1996) The Mathematica Book. (3rd Edn.) Wolfram Media, Champaign, IL, and Cambridge University Press, Cambridge.

Distributed Expert System in Port Area

Gabriel Raicu

A high quality examination is always necessary in naval transports. The paper presented contains a general strategy for Distributed Expert Systems implementation using Jess philosophy and provides an overview of the various expert systems and the role they play in the port. Different elements in naval transports and its combinations possibilities lead to control strategy of the Expert Systems development.

We can easily notice that only a small part of our experience is used to solve a particular problem. We also mention that although we posses a large amount of knowledge acquired from practical activities, the solving of a practical problem uses very few pieces of information. In this way, a high-level control process is generated that is employed to solve the problem. An expert system must be complex enough to solve particular problems too. Hence, even for problems with a low level of complexity, it is necessary, that the expert system be able to permit a high level control as well as a low level control, both controls being based on an 'excitation-response´ type of rule. A correct definition of the two levels is absolutely necessary in order that the expert systems separate them. Thus, the high level control of an expert system (production system) is defined as a set of rules that allow the activation/inhibition of the "excitation-response" type of rules according to the basic principles of the system.

The use of two sets of cooperative expert systems enables the container terminal to expedite the unloading and loading of container vessels and enhance marine services. Such an improvement is necessary in order that the port can compete with neighboring ports that have the advantage of inexpensive labor and large port space. By integrating these systems with each other and with other computer-based information systems, the operation terminal was able to triple volume of business with the same number of employees and reduce the turnaround time of vessels to 25-30% of that in the neighboring ports.

***

The bulk of global trade moving through the world's ports is shipped via containers. A typical port will handle several containers each day, and the goal of the port is to move these containers as quickly and most cost-effectively as possible. Goods delayed at port are invariably tardy upon delivery to customers, thus incurring late charges. It is therefore essential that a port be able to efficiently and rapidly receive, store and dispatch containers. A shipping line may opt to tranship its goods through anyone of several ports on the coast of the Black Sea. Constanta containers terminal, located in the Constanta, section of the Port of Constanta/Agigea, is one of the largest, most modern and best-equipped container terminals in this geographic area. Business applications of expert systems are continuing to increase in number and diversity. International business applications of expert systems, however, are few and far between.

On One-Pass Term Rewriting and Tree Recognizers with Comparisons Between Brothers

Matti Rönkä

In [FJSV] two restricted ways to apply a term rewriting system (TRS) to a tree were considered. When the *one-pass root-started* strategy is followed, rewriting starts from the root and continues step-wise towards the leaves without ever rewriting anything produced by a previous rewrite step. *One-pass leaf-started rewriting* is defined similarly, but rewriting begins from the leaves. In the *sentential form inclusion problem* one asks whether all trees which can be obtained from the trees of some regular tree language T using a given TRS belong to another given regular tree language U, and in the *normal form inclusion problem* the same question is asked about the normal forms of T. These problems are shown to be decidable for both one-pass strategies for a left-linear TRS.

Bogaert and Tison [BoTi] introduce tree automata with equality and disequality constraints on direct subterms ($REC_{\neq}$ automata). They show that the corresponding family of tree languages has good closure properties and, most importantly, that the emptiness problem is decidable for $REC_{\neq}$ automata.

In this paper we define both bottom-up and top-down *generalized tree recognizers with constraints between brothers* (GCBB recognizers), and show that both types are equivalent to $REC_{\neq}$ automata. Using GCBB recognizers we generalize the results in [FJSV] for TRSs in which the left-hand sides of the rules may contain non-linearities in brother positions.

References

[FJSV] Z. Fülöp, E. Jurvanen, M. Steinby and S. Vágvölgyi. On one-pass term rewriting. Acta Cybernetica, 14:83-98, 1999.

[BoTi] B. Bogaert and S. Tison. Equality and disequality constraints on direct subterms in tree automata. STACS 92 In Lecture Notes in Computer Science 577 : 161-171, 1992.

VRML based visualization of discrete tomography pictures

László Ruskó, Attila Kuba and Emese Balogh

Discrete reconstruction tomography deals with reconstruction of cross sections of 2D or 3D discrete objects from their projections. Discreteness means that the picture- or volume elements can take values from a known finite discrete set. In this case the reconstruction of homogenous objects is in focus, when this set is two-valued (i.e. the points of the object and the background). We have proposed an image processing system, which permits of testing and comparison of the most important discrete reconstruction algorithms. One of our purposes was also that the system should be accessible via Internet. The three main parts of the system are generating test data, running reconstruction methods and the visualization of the result.

Visualisation means here the conversion of the results to VRML formatted document to be displayed by Internet browsers. The result of the reconstruction is 2D or 3D binary image, which is saved in an ASCII file with its projections. The system converts these files to VRML document. The user can customize the layout of the displayed object. The style of the object points and the projection points can be specified. One or two object can be displayed at the same time, the number of projections to be displayed is not restricted. If there are more objects in the result of reconstruction, the user can select the object and projection of interest. Further information (grid of discrete space, projection rays, highlighted points of the object etc.) can be also displayed.

Rewarding misclassifications in oblique decision tree learning

András Salamon

Motivation to this work came from a real-world problem, the management of financial risks. Particularly, we had an interest in solving a credit granting (and monitoring) problem: the classification of loan applicants (and debtors).

Although credit granting process covers all the aspects of loan administration, we focus on only the classification process, when the funder institution (usually a bank) classifies the applicants. This classification should not only help to decide whether to give a loan or not, it should also help to determine the price of the loan, and should be included in the credit monitoring subprocess, where the classification is repeated — that time already of the loan debtors — on a regular basis, until the expiration of the loan.

We aimed at applying machine learning techniques for generating decision trees that are consistent with available data and domain knowledge. According to the Hungarian law, every bank should have a credit granting system, which has to be checked by the state authority. Because of the legal regulations, this system cannot be a black-box. Decision-tree algorithms can process the accumulated noisy historical data of the banks while using the predefined indicators of the legal regulations.

This kind of algorithms have been used since the 1960s. From the several variants of decision tree algorithms, we have chosen to use oblique decision trees. Unlike axis-parallel decision trees, oblique decision trees tests a linear combination of the attributes at each internal node. Although oblique decision tree learning requires more resource, we favor this, because it is more general than the axis-parallel variant.

We have enhanced oc1_v3, a well-known oblique decision tree algorithm. Oc1_v3 uses a top-down greedy tree building mechanism, based on the impurity measures of hyperplanes. For a given set of training examples, it cuts by introducing a hyperplane this set into two subsets so that the measure of the so-called impurity of the subsets be minimal. The actual impurity measure has a great impact on the structure and accuracy of the tree learned.

Although credit granting can be a binary classification problem, in our scenario we have five output classes. It is important to distinguish between different types of misclassifications. In our model, a so-called fitness matrix contains all the misclassification rewards: this matrix can be used in the accuracy calculation and in the tree building process.

Two impurity measures have been modified to use the fitness matrix. The new version of Sum Minority and Max Minority impurity measures uses the fitness matrix during hyperplane evaluation. Sum (Max) Minority measure calculates the sum (maximum) of the number of minority elements on both sides of the split. The new version counts the weighted number of minority elements, where the weight is based on the misclassification reward.

We made extensive experiments, working with both of the impurity measures on artificial — though in the credit granting domain realistic — datasets. The noise imposed on the training examples was systematically increased. In most of the cases the new tree learning methods, that rewarded misclassifications during the learning process, clearly dominated the original methods. A detailed confidence test showed that our results were significantly better in case of more noisy data. The test also showed that the enhancement has a greater impact on Max Minority compared to Sum Minority. On the other hand, the new methods were never surpassed significantly by the original tree learning methods.

Programming by steps

Raluca Oana Scarlatescu

The paper introduces a new method of software design and programming. The method is based on the old flow-charts, in order to obtain not only a logical representation of the problem to be solved, but also the real-time working of the software itself. What is a flow-chart? A sequence of steps, that could be classified like iteration, decision, jump, loop, etc. To "make" a step means to perform a certain function. Usually it is the job of the software engineer to put together these functions in a certain order and in this way a program is realised.

This paper presents a different idea to implement a flow-chart. On this is based the method of software design and programming in discussion. The steps of the flow-chart are a finite number of records in a database table, linked with their specific functions associated by name or number identification (id). To "make" a step supposes, like into a normally designed flow-chart, to perform the function and to pass to the next step, and so on, until the steps are finished.

These functions are macro-functions projected and stored in one or more separate programs. The macro-functions are characterised from some input and/or output parameters, that have to be transferred from one step to another, and realise a certain group of activities. The values of the parameters could be fixed or variable, dependent or independent of the execution of the other functions, a priori known or unknown. They could consist in different type of data (character, numerical, date, etc.). The macro-functions have a certain level of abstraction and standardisation, to be used in different situations.

A main software reads the information about each step, gathers the input values of the function associated with and interprets them, runs the function and scatters the output results in its parameters, manages the going over of all steps, and ensures the good execution of the entire system. There is a database management system, that stores the data about the steps and its precedence rules, functions and its parameters, dynamic values of the parameters, errors etc.

In view of all these facts, each program could be designed building the succession of steps with the necessary functions for the respective situations. In other words, the software engineer would fill some fields in the tables with the values necessary to complete the flow-chart and than to run the program. Or, in a future release, with an adapted graphic interface, a non-specialist user could be also the "writer" of the software.

The paper presents in details the principle of the Programming by steps, based on the scenario described above. It explains, also, which were the reasons that originally motivated the development of the method and defines the principal requisites to build an application system, the facility to develop other applications from the same family and the restrictions to be applied. The software package, that was designed and programmed with this method, is still working. It is oriented on the IVR applications, used to manage the phone calls with the computer.

There are enunciated the future aspects of the implementation and the advantages /disadvantages to design, implement and maintain the system.

The paper includes a comparative analysis of the Programming by steps and another two methods of software engineering: the Rapid Prototyping and the Component-based Design and Reuse. A demonstrative application is also enclosed. Integrative comments and conclusive remarks are provided in the conclusions of the paper.

Content protection: combining watermarking with encryption

Paula Steinby

Illegal copying of digital data is a big problem in today's "information society". Unauthorized copying and purchase of such material are claimed to cause a loss of billions of euros for the legal distributors. Content protection systems have been designed to protect media producers and distributors. The existing tools are limited: data encryption, digital watermarking, tamper-resistant and special-purpose devices. The ultimate goal is to make producing illegal copies impossible. While this remains unachievable, we are seeking for methods which make producing, distributing and using illegal copies of some data unattractive: difficult and/or risky.

We consider a scheme where a digital article is distributed over an insecure channel. Due to different interests of the parties involved, we will want to encrypt, watermark and compress the data. Encryption contributes to the privacy of the parties as well as makes the data useless for those without means to decrypt it. Watermarking enables one to distinguish between each copy of the data; this is useful mainly for the purposes of copyright protection. Compression is needed to facilitate the transmission and storage of the data.

In the paper we combine compression, encryption and watermarking to obtain a scheme with the following properties.

- Merchant M has data I for sale. M encrypts (the ready compressed) I into $enc(I)$ with a key K_{enc}. Then $enc(I)$ is set for distribution.
- Buyer B has a Device D to display the data. Each D is assumed to possess a key K_D.
- *Purchase:* B sends an index k for M to compute K_D. M returns B a unique decryption key K_{decB}. Applying K_D to $enc(I)$, D receives a copy of I with a unique watermark W_B.
- *Tracing:* Suppose B illegally redistributes his copy of I. He can be traced on the basis of the watermark W_B, which can be extracted only from the copies originating from his version of I.
- One encryption of I can be distributed to all buyers, but each decryption key is bound to a certain buyer with a certain device. The unique watermarking is forced to be done along the decryption.
- We also sketch a variant of the system for asymmetric fingerprinting with help of a trusted third party.

We assume the data in the scheme to be an image. The compression method is fixed to be a version of JPEG. Therefore, encryption and watermarking are performed on the discrete cosine transformed (DCT) coefficients of I.

Optimal substructures in optimal and candidate circle packings

Péter Gábor Szabó

The densest packing of equal circles in a square problem is a well-known challenge of the discrete and computational geometry. Using a computer-aided method, up to 27 circles could be found the optimal solutions. Based on only mathematical tools, without computer, the best arrangement of 36 circles is also known. For higher number of circles we have only candidate packings up to 200 and for some sporadic values [3]. The candidate packings are the best known arrangements without the proof of optimality.

The greatest difficulty to solve this problem is to find the structures of optimal packings. Some previous articles have already investigated repeated patterns of packings [1, 2] and at the previous $(CS)^2$ conference we have given a classification on structures based on minimal polynomials.

In this talk I would like to show some interesting situations when the optimal and candidate packings contains optimal substructures. These substructures are the locally densest packings inside a packing. The shapes where their density are maximal can be different (e.g. square, triangle or circle).

Sometimes the exact value of the radius of circles in the optimal packing is unknown. In this case, it can be give a minimal polynomial with the first positive root of the correct radius (or the minimal distance between the points). To determine these polynomials in some cases are trivial but sometimes very hard. The calculation usually based on the theory of Groebner bases. In my approach I used generalized minimal polynomials of the substructures to calculation the minimal polynomial for the total structure.

References

[1] P. G. Szabó, Some New Structures for the "Equal Circles Packing in a Square" Problem, Central European Journal of Operations Research 8:79-91, 2000.

[2] P. G. Szabó, T. Csendes, L. G. Casado and I. García, Packing Equal Circles in a Square I., Optimization Theory: Developments from Mátraháza, Kluwer Academic Publishers, pp. 207-224, 2001.

[3] P. G. Szabó and E. Specht, Packing up to 200 Equal Circles in a Square (in preparation).

Navigation of simulated mobile robots in the Webots environment

Richárd Szabó

According to some scientific forecasts robotics can be as important branch of life within reasonable time as it was the automotive industry in the 20th century.

To facilitate the spreading of the discipline engineers research new robot hardwares, while informaticians create new robot controlling softwares. The latter task cannot be imagined without reliable robot simulator environments. These tools may link up powerful algorithms and real-world tasks.

A well-known representant of these programs is Webots, a threedimensional mobile robot simulator. With the use of this tool controller programs using various guidance principles can be developed in C programming language.

This environment was originally implemented for a two-wheel 5 cm diameter mobile robot equipped with 8 infra-red sensors to detect obstacles and light sources, the Khepera. Actual version of Webots are capable of modelling any type of two-wheel differential steering robots using infra-red sensors, color video cameras, and touch sensors.

One of the most important goals of the mobile robot research is the emergence of the ability to efficiently navigate in complex, cluttered, and unknown environments. Various algorithms can be used to support the learning of the environment and the creation of a cognitive map.

The method of navigation strongly depends on the choice of the navigation paradigm. In the last decade two different approaches have been investigated: metrical and topological navigation.

Using metrical navigation the exploring robot creates a metric map of its environment as it would be a "view from above". During topological navigation the robot learns spatial relations of the surrounding objects and models them as a graph.

The author presents the Webots mobile robot simulator and its applicability to handle machine-learning methods in the self-localization and navigation domain. Advantages and disadvantages of metrical and topological navigation paradigms will also be explained.

CNN-Based Early Detection of Acute Ischemic Lesion

Tamás Szabó

CNN-based methods on CT's are introduced in this paper. Medical imaging systems produce volume images featured by characteristics of diagnostical significances which can hardly be appreciated by human vision. Telemedicine is a hot topic of information processing. A decision support means for the early detection of acute ischemic stroke as a part of a telemedical consulting system is outlined in this paper. CNNUM stands for real-time image processing support for a medical expert by the detection of image features which can be misrecognized by a human. Segmentation of CT images is particularly dedicated to a multilayer CNN which provides a huge computing power on 2.5 -D volumes.

Detection of neuroradiological significances primarily based on a grey scale. Mapping pathological syndroms unambiguosly to image features is crucial. Substitution of accumulated medical knowledge by definite formulas is extraordinary relevant. Appearance sort of symptoms strongly depends on age, sex, risk factors, on blood pressure, conditions of main organs, and also on epidemiological antecendents. Building some anatomical knowledge can hardly be avoided. Searching is done by both shape and shade of gray in noisy medium. Falx cerebri, optionally the Putamen, Caudate nucleus, Thalamus, Internal and External capsules, the Insula, Hemispheres, Sulcuses, hyperdensity and homogenity are examined by original parallel local methods implemented by analogic CNN algorithms. Entire grey scale covers hardly a small range of the scale of CT numbers which correspond to the attenuation of different type of tissues. Depending on the tissue of interest a neuroradiologist scales the gray scale window.

Both artifacts and malpractice can be corrected by simple preprocessing techniques. A set of simple template operations may help getting a flawless input image. These adaptive rescaling techniques are shown as prefiltering, a combination of eliminating the irrelevant structures by band-pass filtering and a contrast enhancement.

MRF Image Segmentation is presented demanding a tremendous amount of computing power which can usually be implemented on parallel computing structures, however. Optimal image labeling is performed by minimizing an energy function

$$E(\omega_s, f_s) = \sum_{s \in S} \left(\ln\left(\sqrt{2\pi\sigma_s}\right) + \frac{(f_s - \mu_s)^2}{2\sigma_s^2} \right) + \sum_{C \in \mathbf{C}} \beta_C,$$

where s stands for a site, ω_s is a configuration, f_s is the observed grey level image data, μ and σ stand for mean value and standard deviation, respectively. C is a clique and β_C stands for a parameter that depends on the neighbourhood. One possible way for optimization is a derivation of a PDE that is implemented by the CNN. In the proposed model an anisotropic diffusion model is used

$$F(E(\omega_s, f_s)) = \int_S \left[\Psi(E) + \Phi\left(\|\nabla E\|\right) \right] d\omega_s df_s.$$

Acknowledgements: This research has been supported by National Research and Development Funds of Széchenyi Plan under consortium NKFP OM-2/052/2001 and OTKA #029609. Discussions are kindly acknowledged to Prof. P. Szolgay, P. Barsi, L. Czúni.

References

[1] L.O.Chua and L.Yang, "Cellular neural networks: Theory, Applications", IEEE Trans. on CAS, Vol.35, pp. 1257-1290, 1988.

[2] T.Roska and L.O.Chua, "The CNN Universal Machine: An Analogic Array Computer", IEEE Transactions on CAS-II Vol.40, pp. 147-156, March,1993.

[3] T.Szabó, P.Barsi, P.Szolgay, "Application of Analogic CNN Algorithms in Telemedicine", Proc. of IEEE CNNA'02, Frankfurt, 2002.

Performance Testing Architecture for Communication Protocols

János Zoltán Szabó

In today's telecommunication protocols and applications it is important to check not only the functional correctness of implementations, but their performance characteristics as well. The purpose of performance testing is to verify whether the tested system can work under realistic load conditions and handle overloaded situations. The usual technique for testing the performance of end-to-end services and applications models each service user with a probabilistic timed state machine ([1]). During the test execution a large number of these simple automata are run in parallel by the test environment.

A new test language, the third edition of Tree and Tabular Combined Notation (TTCN-3, [2]), which was recently standardized by ETSI, can be efficiently used to specify such performance test scripts. The built-in TTCN-3 language constructs makes it possible to create dynamically any number of parallel test executor processes, the so called Parallel Test Components (PTCs). Performance testing requires at least as much computational resources for the tester as the tested implementation. Therefore the testing of distributed implementations is feasible only with distributed test environments.

This paper presents our basic ideas for a TTCN-3 based parallel and distributed performance testing prototype environment. The testing system consists of several parallel processes and a control protocol. The behaviour of each PTC is realized in a separate process. Each computer that takes part in test execution runs a special process called Host Controller (HC), which is responsible for the creation of new PTCs on that host. In addition, there is a dedicated process (a so called Main Controller, MC), which provides user interface and performs the tasks that require central coordination, such as load balancing among the computers.

The control protocol between the processes uses reliable transport layer connections (e.g. TCP connections). It covers all parallelism related TTCN-3 operations, such as PTC creation and termination or establishment of internal communication channels between PTCs. The protocol is platform independent, so a group of computers with heterogeneous hardware and operating systems can cooperate and generate load simultaneously.

The key aspects of design were the scalability, the robustness and the execution speed. The test architecture has been successfully implemented as an extension for an existing, compiler based test executor, which translates TTCN-3 test specifications into C++ programs. We have successfully applied the test environment for performance evaluation of two IP mobility protocols.

References

[1] M. Kwiatkowska, G. Norman, R. Segala, J. Sproston: Verifying Quantitative Properties of Continuous Probabilistic Timed Automata, CONCUR'2000, 2000.

[2] Methods for Testing and Specification (MTS); The Tree and Tabular Combined Notation version 3. TTCN-3: Core Language. ETSI ES 201 837-1.

Analysis of QoS Parameters in DiffServ-enabled MPLS Networks

András Szász

The development and spreading of newer applications made the Internet a widely used medium. Hence, the volume of the forwarded traffic through the Internet is increasing, which means that the problem of sharing resources fairly and efficiently is getting more and more difficult. There are newer ways of using the Internet, traffic types are differentiated which require different forwarding methods. However, the transmission based on the Internet Protocol (IP) only can apply the best-effort algorithm currently, which is not enough for forwarding high quality voice and video, and serving businesses with the demanded value-added services.

Therefore various Quality of Service (QoS) parameters have to be provided, different guarantees are required for different types of traffic. In the network layer two architectures have been developed to solve this problem. One of these is the Integrated Services (IntServ) architecture where the routers handle the flows separately. This solution becomes difficult at larger networks because the network components have to manage too many flows, which raises scalability problems. The second solution is the Differentiated Services (DiffServ) [1] architecture where the flows are classified into service classes by their quality requirements (i.e., maximum packet loss, delay, jitter etc.). In this case, the traffic within the DiffServ domain is handled based on the classification rather then per flow. This is a more scalable way of forwarding traffic hence it is more promising in the near future.

Multiprotocol Label Switching (MPLS) [2] is another new technology for building transit domains. It combines the flexibility of the IP network layer with the benefits of a connection-oriented approach to networking. MPLS is a label-switched system that can carry multiple network layer protocols. Similar to Frame Relay, MPLS sends information over the network in frames or packets. Each frame/packet is labeled at an edge router and the network uses the label to decide the destination of the frame, without having to refer to a routing table, thus improving speed and scalability. MPLS adds traffic-engineering functions to IP, allowing service providers to route more efficiently and offer Quality of Service features.

In this paper both of the above techniques are discussed. In our interest there are two DiffServ-enabled domains on the sides and there is a third network between them. In the first scenario the third network operates without using the MPLS technology, while in the other case this is an MPLS network. In both scenarios the two adjacent DiffServ networks must have the ability to reach each other just like if the third domain would be a DiffServ domain. The goal of this paper is to make a comparison between the two scenarios and to check how the QoS parameters are fulfilled.

References

[1] S. Blake et al., "An Architecture for Differentiated Services", IETF – RFC 2475, December 1998

[2] E. Rosen et al., "Multiprotocol Label Switching Architecture", IETF – RFC 3031, January 2001

Automatic wizard generation

Dániel Szegő

Most state of the art software consists of wizards to assists the user in solving some of her common tasks. Traditionally, these wizards are written by software developers and 'hardcoded' directly into the architecture This usually causes that wizards don't reflect exactly the users' need, since they are predicted during software developing before the software has even finished.

This paper investigates both theoretical and practical ways of writing a software in a way that it would be capable of generating wizards automatically, based on the user's behavior. A framework architecture has been developed and will be briefly introduced, which supports automatic wizard generation and can be added to any software.

One of the key problems of automatic wizard generation relates to nature of generic software systems' architecture. To analyze a software system from the user's point of view, four main layers could be considered. Generation of *components* takes place at the lowermost layer. The *user interface* resides at the top level of the architecture. It usually manifests as a set of buttons, textboxes, links or text items. *Services* can be regarded as an abstraction of calls to components' methods. Actually, when the user has access to the program through the user interface, he manipulates the services. There is a fourth layer between service and user interface, called *glue code*, which consists of event handlers and other useful methods.

Services have been chosen to be the basic steps of a dynamically created wizard, so sequence of services manifest as wizards.

The main task of wizard generator is to create a wizard from user's behavior and embed directly into the software so that it could be applied by the user. Wizard generator consists of two major parts, *model engine*, and *validation engine*, which will be introduced in the followings.

Service calls are collected into a universal sample, while the user is using the software. In other words, all service calls are registered as a sequence of service calls. Wizards should be manifested as common subsequences of all service calls. For example, supposing that user calls *open_connection* and *remote_copy* services many times, a candidate for a wizard could be <*open_connection, remote_copy*> two long sequence. The model engine is responsible for computing common sequences, usually called as *schemas*, from all service calls. Its task is realized by a dedicated algorithm. The algorithm collects all service calls into a universal sample, and finds subsequences of the universal sample which occur at least t times and maximal, in a sense that none of its supersequence occur t times, where t is chosen with the help of heuristics. Three algorithms to compute maximal sequences have been developed (Mschema-0, 1, 1-2) with different time and space complexity. Best of them is Mschema-1 algorithm, which computes maximal sequences with $\mathcal{O}(n^3)$ time and $\mathcal{O}(n)$ space complexity.

Model engine generates common sequence of service calls from the user's behavior, however these sequences cannot be considered directly as wizards because the missing of validation. Validation engine gets wizard candidates from the model engine, and checks the validity of these candidates, with the help of a domain specific formal model. This formal model is based on a relational approach; *must preeced* and *must follow* binary homogenous relations are interpreted between the service calls. A wizard candidate is valid if its service calls are in a well-defined order, in a sense that the order satisfies both relations. The valid candidates become real wizards; the non-valid ones are dropped or transformed into valid (repair). Algorithms for validating and repairing wizard candidates, based on the relations, have been developed and successfully implemented, and added to automatic wizard generator architecture.

An automatic wizard generator architecture, consisting of both the model and validation engine, has been developed and implemented in Java. It can be added to a software, so that the software would support automatic wizard generation. The software should be written with the help of a well-defined design pattern, which supports the dynamic appearance of the user interface. If so, wizard generator classes can be automatically added to the software, without further implementation efforts, and the software will be able to generate wizards automatically.

Simplifying the Model of a Complex Industrial Process Using Input Variable Selection

Nóra Székely

This paper deals with some important experiences gained from building a neural model of a Linz-Donawitz (LD) steel converter. Steelmaking with an LD converter is a complex physico-chemical process where many variables have effects on the quality of the resulted steel. During the process a converter is filled with waste iron, melted pig iron and many additives, then it is blasted through with pure oxygen to burn out the unwanted contamination. There are about 30-50 important, known input parameters of the process and two essentially important output parameters: the carbon content of the steel and its temperature at the end of the blasting. The complexity of the whole process and the fact that there are many effects that cannot be taken into consideration make this task difficult. The work we have done is the construction of a neural model and simplifying it using the experiences gained. During this work it turned out that perhaps the most important step of the whole modeling task was the analysis of the large amount of data, the selection of relevant parameters. The paper details the improvement of the neural model using input variable selection methods based on independent component analysis (ICA) and principal component analysis (PCA) techniques. It is believed that these experiments can be utilized in other complex industrial modeling tasks.

Neural networks are one of the possible means to build complex, highly nonlinear mappings between many inputs and some outputs. Experimental data are used to train the neural network, until its operation will be similar or almost identical to that of the real industrial process.

There are many steps of building a model for a complex industrial problem. Among them one of the most important task is to build reliable database that is to select, validate and preprocess the experimental data. These steps are especially important if the experimental data contain noisy, imprecise information, where in some cases there may be false parameter values, and where the problem space is rather large. The use of all measured input parameters makes the neural model very complex, and the learning of the network will be very slow. So the model should be as simple as possible, therefore the irrelevant input parameters are not to be used. For this goal the input parameters must be investigated. Basically three methods were used to select the really relevant parameters:

- Selection of the parameters using the expertise of the steelmaking experts. In this process the irrelevant parameters are simply omitted.
- Selection of the parameters based on principal component analysis (PCA). In this selection process a new parameter set is derived from the original one using a special linear transformation, then the new parameters are again investigated to determine which of them is to be used in the model.
- Selection of the parameters based on independent component analysis (ICA). This process is similar to the PCA based method but a different linear technique is used to produce the derived parameters.

The results of the three methods showed that the model can be significantly simplified when we apply independent component analysis on the original data.

References

[1] Mika, S., B. Schölkopf, A. Smola, K.-R. Müller, M. Scholz, and G. Rätsch (1999). Kernel PCA and de-noising in feature spaces. In M. S. Kearns, S. A. Solla, and D. A. Cohn (Eds.),

Advances in Neural Information Processing Systems 11, Cambridge, MA, pp. 536 – 542. MIT Press.

[2] A. Hyvärinen and E. Oja. Independent Component Analysis: Algorithms and Applications. Neural Networks, 13(4-5):411-430, 2000.

[3] A.D. Back and A. Cichocki: Input variable selection using independent component analysis and higher order statistics, Proc. of the First International Workshop on Independent Component Analysis and Signal Separation - ICA'99 , Aussois, France, Janurary 11-15, 1999, pp. 203-208.

[4] Strausz, Gy., G. Horváth, B. Pataki: Effects of database characteristics on the neural modeling of an industrial process, Proc. of the International ICSC/IFAC Symposium on Neural Computation/NC'98 , Sept. 1998, Vienna pp. 834-840.

Difference sequence compression of multidimensional databases

István Szépkúti

The multidimensional databases often use compression techniques in order to decrease the size of the database. This paper introduces a new method called difference sequence compression. Under some conditions, this new technique is able to create smaller size multidimensional database than other ones like single count header compression [1, 2], logical position compression [3] and base-offset compression [3].

Keywords: compression, multidimensional database, On-line Analytical processing, OLAP.

References

[1] Eggers, S. J. ? Olken, F. ? Shoshani, A., A Compression Techniques for Large Statistical Databases, VLDB, 1981.

[2] Szépkúti, I., Multidimensional or Relational? / How to Organize an On-line Analytical Processing Database, Technical Report, 1999.
`http://www.inf.u-szeged.hu/~szepkuti/ICOMP12.ps`

[3] Szépkúti, I., On the Scalability of Multidimensional Databases, Periodica Polytechnica Electrical Engineering, 44/1, 2000.
`http://www.inf.u-szeged.hu/~szepkuti/CSCS.ps`

ID3 is not an Occam algorithm

Balázs Szörényi

The general task of learning is to predict the outcomes of unseen events by processing some (more-or-less representative) examples. A well-known principle of learning theory is Occam's razor, which suggests, that if one can give a small representation or a short description for the examined activity of some kind of system (for example: customers' habits), then one can be quite sure, that this description can be successfully used for prediction. This principle is incorporated in the definition of the (α, β)-Occam algorithm.

The central question in computational learning theory is, whether a class $\mathcal{C}$ of concepts ($c : X \to \{0, 1\}$ type functions for a given, common base set X) is PAC-learnable - that is: is there an L PAC-learning algorithm for $\mathcal{C}$? It is known that any efficient (α, β)-Occam algorithm is an efficient PAC-learning algorithm, and there is also a certain converse of this result.

The PAC-learnability of decision trees is a major open problem. We study theoretical properties of the best-known learning algorithm in this special area, the ID3 algorithm. The result, we wish to present, is that ID3 is not an Occam-algorithm. This requires the construction of examples where ID3 constructs a much larger than optimal tree.

A fully automatic medical image registration algorithm based on mutual information

Attila Tanács, Kálmán Palágyi, and Attila Kuba

Image registration is a fundamental task in digital image processing used to match two independently acquired images. These images are taken at different times, from different viewpoints or even from different imaging devices. To register images, the geometrical relationship between them is to be determined.

Image registration is an important area of medical image processing. Matching all the geometric data available for a patient provides better diagnostic capability, better understanding of data, and improves surgical and therapy planning and evaluation.

A registration problem is unimodal, if the images are from the same imaging device and multimodal using images taken by different devices.

We developed a fully automatic registration algorithm capable of solving both unimodal and multimodal registration problems. The images can be 2D or 3D. We assume that a rigid-body transformation is to be found which is the case in most applications of brain image registration. We use mutual information as similarity measure which is the most successfully applied measure in multimodal registration.

We validated our algorithm using the image database of Vanderbilt University, Nashville, TN, USA. The results show that our algorithm can be successfully used to register MR-CT and MR-PET images. The description of the Retrospective Registration Evaluation Project can be found at `http://www.vuse.vanderbilt.edu/~image/registration.`

Empirical analysis of the convergence of inclusion functions

Boglárka Tóth

In validated computing many techniques are based on more than one inclusion functions. In interval global optimization e.g. one of the main questions is, which inclusion function should be used to get the minimum efficiently. If we use simple interval-arithmetic it can provide larger overestimation but at a lower cost. More sophisticated inclusion functions may give better inclusion, but at the same time they require more computation.

This paper deals with the empirical convergence speed of inclusion functions. According to our earlier experience the natural inclusion for a given function can be at least as good as a usual second-order inclusion function, and although Taylor models are in general only of second-order, they can perform as one of larger order. These facts indicate that convergence order shouldn't be the only indicator of the efficiency of an inclusion function, we need to know in which situation which inclusion function could be used most efficiently. For this reason we have investigated the usual inclusion functions on some test functions. The results will be reported in the talk.

Keywords: interval arithmetic, global optimization, inclusion function, convergence order.

A Graphical User Interface for Evolutionary Algorithms

Zoltán Tóth

Engineering applications provide a wide range of optimization problems for people working in this area. In most cases, the different tasks require different programming environments to achieve the best results.

The purpose of *Generic Evolutionary Algorithms Programming Library (GEA)* system is to provide researchers with an easy-to-use, widely applicable and extendable programming library which solves these tasks by means of evolutionary algorithms.

Evolutionary algorithms (EAs) are general purpose function optimization methods which search for optima by making potential solutions (individuals) compete for survival in a population. The better an individual is, the better chance it has to survive. The search space is explored by modifying the potential solutions by genetic operators observed in nature: generally mutation and recombination.

Evolutionary algorithms have (among others) the following two advantages over other optimization methods: first, in most cases they converge to global optima, and second, the usage of the black-box principle (which only requires knowledge about a function's input and output to perform optimisation on it) makes them easily applicable to functions whose behavior is too complex to handle with other methods.

The *GEA* system contains algorithms for various evolutionary methods, implemented genetic operators for the most common representation forms for individuals, various selection methods, and examples on how to use and expand the library. An extensive comparison of *GEA* and other evolutionary algorithm implementations shows that *GEA* can be effectively applied on many optimization problems.

The implemented genetic operators, selection methods and evolutionary algorithms make the system easy-to-use even for beginners: If the user wants to solve a problem with *GEA* and the search space consists of, say, bit-strings or real vectors, then he/she only has to define the problem-specific fitness function, set the parameters of the algorithm and start searching for the solution.

GEA is implemented in the `ANSI C++` programming language. The class hierarchy and the applied plug-in technology make the extension of the system with new selection methods, representation forms for individuals or even evolutionary algorithms as easy as possible.

GraphGEA is a graphical user interface to *GEA* written with the GTK API. The numerous parameters of the evolutionary algorithm can be set in appropriate dialog boxes. The program also checks the correctness of the parameters and saving/restoring of parameter sets is also possible. The selected evolutionary algorithm can be executed interactively on the specified optimization problem through the graphical user interface of *GraphGEA*, that is, the execution can be controlled by appropriate buttons and the results and behavior of the EA can be observed on several selected graphs (on-line visualization). The available graphs include several fitness and distribution graphs as well as depictions of the genotypes and phenotypes of individuals.

GraphGEA is capable of off-line visualization, too, i.e. it gathers and saves information during the run of the evolution process and can reconstruct the run from this information later.

It is very important to mention that *GraphGEA* is "only" a graphical user interface to *GEA* and is not necessary for the using of *GEA*. *GEA* runs as a child process of *GraphGEA* and the processes communicate by means of a pipe system and shared memory (UNIX System V IPC).

While the main purpose of *GEA* is solving optimization problems, that of *GraphGEA* is education and analysis. It can be great help for students understanding the characteristics of evolutionary algorithms and researchers of the area can use it to analyze an EA's behavior on particular problems.

Reducing the complexity and controlling the network size of LS–SVM solutions, by solving an overdetermined set of equations

József Valyon

Introduction: In case of noisy learning data, the traditional NN –due to it´s construction – often leads to poor generalization and "over–fitting". The SVM [1],[2] (Support Vector Machine) method, introduced by Vapnik, was designed to overcome these problems. The LS–SVM (Least Squares SVM) [3],[4] provides us with the similar advantages, but in this case training means solving a set of linear equations instead of a long and computationally hard quadratic programming problem involved by the standard SVM. This LS method effectively reduces the algorithmic complexity, but for really large problems, comprising a very large number of training samples, even this least-squares solution can become highly memory and time consuming. The least–squares version incorporates all input vectors in the network to produce the result, while the traditional SVM selects, marks some vectors (called support vectors) as ones that are important in the regression. This behavior can also be reached with LS-SVM by applying a pruning method [4], but in order to achieve it, the entire large problem must be solved at least once. This paper describes a new formulation of the LS–SVM, which provides us with control over the size and structure of the network, and at the same time reduces the complexity –time and memory requirements– of the required calculations. The LS–SVM method is capable of solving both classification and regression problems. Our sample problem concerns regression (LS–SVR), therefore we discuss this in the sequel. With minor changes the given algorithm can also be applied to classification.

The LS-SVR method [3],[4]: A training data set $\{\mathbf{x}_i, d_i\}_{i=1}^{N}$ is obtained, where $\mathbf{x}_i \in \mathbb{R}^p$ represents a p-dimensional input vector and $d_i \in \mathbb{R}$ is the scalar target output. Our goal is to approximate an $y = f(\mathbf{x})$ function, which represents the dependence of the output d from the input $\mathbf{x}$. Let´s define the form of this function as formulated below:

$$y = \sum_{j=0}^{m_1} w_j \varphi_j(\mathbf{x}) = \mathbf{w}^T \boldsymbol{\varphi}(\mathbf{x}), \quad \mathbf{w} = [w_0, w_1, \dots, w_{m_1}]^T, \quad \boldsymbol{\varphi} = \lfloor \varphi_0(\mathbf{x}), \varphi_1(\mathbf{x}), \dots, \varphi_{m_1}(\mathbf{x}) \rfloor.$$

The $\varphi_0(\mathbf{x})$ basis function is assumed to be 1, therefore w_0 represents the bias b. The solution concludes in a constrained optimization, which leads to the following overall solution:

$$\begin{bmatrix} 0 & \vec{\mathbf{1}}^T \\ \vec{1} & \Omega + C^{-1}\mathbf{I} \end{bmatrix} \begin{bmatrix} b \\ \boldsymbol{\alpha} \end{bmatrix} = \begin{bmatrix} 0 \\ \mathbf{y} \end{bmatrix}, \quad \mathbf{y} = [y_0, y_1, \dots, y_N], \quad \vec{\mathbf{1}} = [1, \dots, 1], \quad \boldsymbol{\alpha} = [\alpha_0, \alpha_1, \dots, \alpha_N],$$

$\Omega_{i,j} = K(\mathbf{x}_i, \mathbf{x}_j)$ (C is a chosen constant, $K(\mathbf{x}_i, \mathbf{x}_j)$ is a kernel function) and the estimation is: $y = \sum_{i=1}^{N} \alpha_i K(\mathbf{x}, \mathbf{x}_j) + b$.

The reduced method: If the training set comprises N samples, then our original linear equation set consists of $(N+1)$ equations, $(N+1)$ unknowns and $(N+1)^2$ coefficients. By selecting some (e.g. $M, M < N$) vectors to be "*support vectors*", the number of variables are reduced, resulting in more equations than unknowns. Our problem becomes overdetermined, which can be solved as a *linear least–squares problem*, consisting only $(M+1)^2$ coefficients. Every variable stands for a neuron –representing it´s weight– and each of the M selected training vectors will become a center of a kernel function. Therefore the selected inputs must be chosen accordingly (e.g. equally distanced, less noisy etc.). The above described method solves a much smaller problem, but still takes all known samples into consideration! The result for a simple noisy $sinc(x)$ regression is plotted on figure 1, where (+) –s are the noisy training samples (every second one –*circled*– is selected into set M), (.) represents the result of the reduced LS–SVM method and (o) stands for the result of the normal solution. It can be seen, that the above described method –when the training set is large enough– leads to almost the same results based on a much smaller equation set, as the original solution. The resulting network is smaller, whilst the algorithmic complexity is reduced.

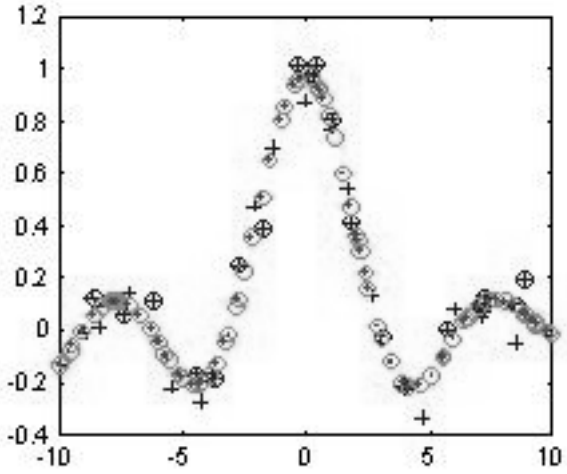

Figure 1: A $sinc(x)$ regression based on the described method ($M = N/2$).

References

[1] S. Haykin: "Neural networks. A comprehensive foundation", Prentice Hall, N. J. 1999

[2] S. Gunn, "Support Vector Machines for Classification and Regression", ISIS Technical Report, 14. May 1998

[3] J. A. K. Suykens and J. Vandewalle, "Least Squares Support Vector Machine Classifiers", Neural Processing Letters, vol. 9, no. 3, Jun. 1999, pp. 293-300.

[4] J. A. K. Suykens, "Nonlinear Modeling and Support Vector Machines", IEEE Instrumentation and Measurement Technology Conference, Budapest, Hungary, May 21–23, 2001.

Structural Description of Binary Images: An Evolutionary Approach

Róbert Ványi

Extraction of some structural information from a binary image may be a very difficult task. In this paper a method using evolutionary algorithms is outlined. The idea is to evolve a structural description that describes the given image as good as possible. However the construction of such an algorithm may also not be trivial.

When one tries to solve a problem with some kind of evolutionary algorithms there are some building blocks of the method which make up the whole algorithm. The evolutionary algorithms use a population, that is a set of possible solutions. From this population some individuals are selected using some kind of goodness measures, called fitness function. Finally from these selected individuals new solutions are produced using evolutionary operators to make up a new population.

First the representation form of these solutions has to be decided. From this usually follow the set of the used evolutionary operators, but there are always some possibilities to choose from. A very important part is the fitness function. This namely influences the convergence speed of the algorithm and it is calculated many times. Finally one have to be careful with the implementation, since the evolutionary algorithms are slow by nature, and therefore each calculation must be as fast as possible. These building blocks are considered in the following sections.

Solution representation: The representation of the solutions depends on the information one would like to extract from the image. Usually this is some kind of picture generating languages, like postscript or turtle graphics. The description can be, however more complex, one can use grammars to produce such descriptions. These higher level descriptions may involve Chomsky or other grammars, like Lindenmayer systems or Collage grammars.

Evolutionary operators: A picture description language usually contains parametrized commands. So a solution is a sequence of parametric symbols. For higher level descriptions the solutions are sets of strings, that is representations of the rewriting rules. It is possible to evolve such structures, but it yields a simpler algorithm and better solutions when the parameters are extracted from the command sequences and evolved separately.

This method yields a *two-level algorithm*. On the upper level the rough structure description is evolved using genetic programming and variable length strings or trees. A goodness measure is however not possible on this level, therefore for each individual the best possible parameter set is approximated using evolution strategies and real vectors on the lower level.

Fitness function: To calculate the fitness of an individual, it has to be interpreted usually yielding a bitmap image. This can then be compared with the given image. One way of this is a pixel by pixel comparison. An easy method is calculating the quadratic error, that is the sum of the squares of pixel value differences for all pixels. There are however better methods involving some distance information. One can also use other types of similarity measurements. For example the Hausdorff distance, which results a very good metric and a very bad calculation time.

Efficient calculation: As the most CPU time is usually consumed by the fitness calculation, to make a fast algorithm this has to be made fast. This can be achieved by the so called *efficient fitness functions*, defined by the author. They can be calculated in linear time with respect to the number of drawn (that is nonzero) pixels. It was shown, that fitness functions that use any information from the given image but only local information from the generated images, can be computed efficiently.

Branch and Prune Techniques in Multidimensional Interval Global Optimization Algorithms [6]

Tamás Vinkó

Interval global optimization algorithms based on branch-and-bound methods provide guaranteed and reliable solutions for the problem

$$\min_{x \in X} f(x),$$

where the objective function $f : D \subseteq \mathbb{R}^n \to \mathbb{R}$ is continuously differentiable and $X \subseteq D$ is the search box representing bound constraints for x.

In these kinds of algorithms there are some classical methods to reject subregions in which the optimum can be guaranteed not to lie. These methods are the cut-off test, the monotonicity test, the range check, the concavity test and so on. Recently many papers ([3, 4, 5]) have studied some new pruning techniques to improve the efficiency of the main algorithm. These methods use the gradient or slope information (i.e first order information) to construct such a technique which can prune the searching interval. All of these works developed the pruning methods for one dimensional case only. However, in [2] there is a suggestion to extend these methods to the multidimensional case with a componentwise approach, where in particular the multidimensional pruning step using slopes have been traced back to the one dimensional case.

In this work we develop the multidimensional extension of the derivative pruning step based on [4], the componentwise extension of the linear boundary value form [1] and its pruning. The multidimensional kite enclosure and its pruning effect will be presented. The test results on 20 standard test functions will be given to compare the performance of these new methods.

References

[1] A. Neumaier (1990): Interval Methods for Systems of Equations, Cambridge University Press, Cambridge.

[2] D. Ratz (1998): Automatic Slope Computation and its Application in Nonsmooth Global Optimization. Shaker-Verlag.

[3] D. Ratz (1999): A Nonsmooth Global Optimization Technique Using Slopes — The One Dimensional Case, Journal of Global Optimization, 14(4):365-393, Kluwer.

[4] D.G. Sotiropoulos, T.N. Grapsa (2001): A Branch-and-Prune Method for Global Optimization, In W. Kraemer and J. W. v. Gudenberg, editors, Scientific Computing, Validated Numerics, Interval Methods, pages 215–226, Kluwer.

[5] T. Vinkó, J.-L. Lagouanelle, T. Csendes (2001): A New Inclusion Function for Optimization: Kite – The One Dimensional Case. Submitted for publication.
Available at: `http://www.inf.u-szeged.hu/~tvinko/kite.ps.gz`

[6] This work has been supported by the grant OTKA T 034350

A Pattern-Based Constraint Language for Metamodels

Dániel Varró

Nowadays, the Unified Modeling Language (UML) [5] has become the de facto standard modeling language of object-oriented system design. A wide range of software applications is being designed using this *unified* and *visual* formalism serving as the common communication platform between customers, system designers, and programmers. However, both academic and industrial applications have revealed several drawbacks of the language concerning, especially, its imprecise semantics, and the lack of flexibility in domain-specific environments.

The scope of **metamodeling** is broader than UML as *metamodeling is the paradigm of defining the syntax and semantics of modeling languages for arbitrary domains* preferably in a visual notation. In dominant metamodeling approaches (such as MML[1], or GME[3]), the *abstract syntax* of a domain is captured by (variants of) visual UML class diagrams, while the *static semantics* of a modeling language is typically formalized by using the textual Object Constraint Language (OCL) [4]. When specifying the dynamic behavior of a modeling language, the use of **graph transformation** [2, 6] is a powerful solution as it provides a mathematically precise underlying formalism without the loss of visual description techniques of UML.

Obviously, there is a huge abstraction gap that has to be bridged when designing a new domain-specific modeling language between the visual specification of abstract syntax (expressed in UML) and dynamic semantics (in graph transformation rules), and the textual description of static semantic constraints (written in OCL). Since visual specifications drastically increase the "legibility" of a model, we focus on the visual definition of static semantics.

In the paper, we propose *a visual constraint language to express first-order structural constraints by graph patterns* in analogy with the pattern matching concepts of graph transformation. We demonstrate how typical structural OCL constraints can be expressed by patterns, and how such visual constraints can be checked automatically using the graph pattern matching engine of the model transformation system VIATRA [6][7].

References

[1] T. Clark, A. Evans, and S. Kent. The Metamodelling Language Calculus: Foundation semantics for UML. In H. Hussmann, editor, Proc. Fundamental Approaches to Software Engineering, FASE 2001 Genova, Italy, volume 2029 of LNCS, pages 17–31. Springer, 2001.

[2] G. Engels, R. Heckel, and J. M. Küster. Rule-based specification of behavioral consistency based on the UML meta-model. In M. Gogolla and C. Kobryn, editors, UML 2001: The Unified Modeling Language. Modeling Languages, Concepts and Tools, volume 2185 of LNCS, pages 272–286. Springer, 2001.

[3] A. Ledeczi., M. Maroti, A. Bakay, G. Karsai, J. Garrett, C. Thomason, G. Nordstrom, J. Sprinkle, and P. Volgyesi. The Generic Modeling Environment. In Proc. Workshop on Intelligent Signal Processing, 2001.

[4] Object Management Group. Object Constraint Language Specification Version 1.3, June 1999. `http://www.rational.com/uml`

[5] J. Rumbaugh, I. Jacobson, and G. Booch. The Unified Modeling Language Reference Manual. Addison-Wesley, 1999.

[6] D. Varró, G. Varró, and A. Pataricza. Designing the automatic transformation of visual languages. Science of Computer Programming. In print.

[7] All papers of the author are available from `http://www.inf.mit.bme.hu/~varro`

Complex Pattern Matching Strategies in Image Databases:the Cut-And-Or-Not Approach

Krisztián Veréb

Matching strategies used for retrieving images from the databases of present time does not really support the usage of complex matchings. In other words, searching for a given image in most image databases — general databases suitable for storing and retrieving images — is executed in a way that a pattern has to be given and the following spoken informal question has to be formed by one of the formation technique of the system: "Select the images from the database, where they are similar to the pattern". The expression 'similar to' is defined by the image pattern matching algorithm of the particular systems. However much more complex questions may occur in practice, which are not at all or just to a certain extent supported by legacy systems. It can be realized that in case of a given matching the different regions of the given images do not have the same importance. Moreover, not all regions have to be matched in particular cases. So one can realize that such a question may also occur as the following: "Select all images from the database where blue is not a dominant colour in its upper part (i.e., the image is possibly not a landscape) and the bottom left quarter is similar to this other image, but if the upper part contains the blue colour dominantly then the bottom right part must be similar to another pattern image." It is supposed to be a rather complex question. To handle such questions, special operations have to be introduced and their examination with logical tools be enabled. In the lecture I present a method (namely the Cut-And-Or-Not method) which is based on fuzzy logics and makes it possible to form and handle such complex questions. In the lecture the formalization needed will be defined, and the whole description of the method, as well. To use the different matchings (shifting invariant, scaling invariant, rotating invariant, etc.) in particular systems the definitions of the most wide-spread invariances and their handling in the Cut-And-Or-Not approach is given. Of course the definition of the fuzzy connectives needed will also be presented using the bases of the Lukasiewicz logics. I introduce the first-order approach of the fuzzy Cut-And-Or-Not method as well, which can be formed and implemented into Database Management Systems much more easily with the help of the relational calculus. Several examples are presented in the lecture about how to form spoken informal questions by the Cut-And-Or-Not method. I also give the steps of realization of the approach in case of a particular Object-Relational database.

Traffic Analysis of HTTPS

László Zömbik

Secure web access became remarkable need for nowadays users. Surfers of the Internet are not only able to reach web pages advertising information, but they even interactively use the services of web server. The essentiality of the interactivity based upon that the user sends information in order to the server can select, create and provide user specific answer. When the users give extra information, this is in most cases not sensitive, (e.g. when a user specifies the date and the destination to query timetables of railway company) but in certain cases user generated traffic must be protected (e.g. when client checks his account using services of an online bank).

Without protecting the sensitive web traffic an eavesdropper may deduce parameters or behavior of the user or even an attacker can identify and impersonate the victim. Therefore several security solutions has evolved, the two most notable security protocol are the SSL [1] and the TLS [2]. The two protocols are very similar, before sending user information the client and the server initially negotiate about the security association, including cryptographic algorithms and keys. After the handshake phase protected traffic is transmitted. If a web server uses SSL or TLS then the HTTP [3] communication is secured. In this case the communication is HTTPS.

It is beneficial to have a model for HTTPS for bandwidth or for cost estimation. This is extremely important for communications that contains expensive links or the link capacity is limited and secure web access is required. Example can be that the subscribers use satellite terminals or GPRS, UMTS equipment for browsing on the web.

In this presentation we introduce a traffic model for HTTPS. This model is verified by traffic measurements. Suggestions for achieving effective HTTPS conversation for web server developers and for users are presented. A correlation between HTTP and HTTPS traffic is shown, and traffic flow confidentiality of HTTPS is evaluated.

References

[1] Frier, Karlton, Kocher, “The SSL 3.0 Protocol”, Netscape Corp., 1996.

[2] Dierks, T. and C. Allen, “The TLS Protocol”, RFC 2246, 1999.

[3] Fielding et Al, “Hypertext Transfer Protocol - HTTP/1.1”, RFC 2616, 1999.

Application of Learning Methods in MCDA models: Overview and Experimental Comparison

Ákos Zsiros

Many real world application lead to a multicriteria decision problem all in the medical, the financial and the engineering area. When there is a set of alternatives described by a set of criteria (attributes) and either sorting, ranking or making a choice is requested by the decision maker while all the criteria have to be taken into consideration, there is a multicriteria decision problem.

In multicriteria decision aid (MCDA) models usually numerical (continuous) inputs are handled, as value functions, orderings on a real interval or preference intensities. One of the simplest – and most commonly used – model we can imagine bases on the aggregation of value of each criteria, for example $\sum_{i=1}^{m} w_i g_i(\mathbf{x})$, where $g_i(\mathbf{x})$ is the value of alternative $\mathbf{x}$ on the i-th criterion and w_i is the importance of the i-th criterion[2].

On the other hand, usually learning or classification methods, from the field of artificial intelligence, can detect relationship among elements of an input dataset described by a set of categorical (discrete) criteria, like hierarchical classifiers, decision trees (ID3). Using a decision tree, the class of an alternative can be easily predicted starting from the root node of the tree and applying the tests specified in the inner nodes of the tree. After the appropriate branches of the nodes had been chosen, finally a leaf node is reached which gives the class of the observed alternative.

In order to apply these methods in decision aid models they had to be extended to work on numerical criteria, both in the model building phase and later, in the application one. In the well-known C4.5[6] method it can be solved only by discretization of values of numerical attributes, while in our Continuous Decision Tree (CDT) building method, introduced in [5], it is not necessary. It builds a decision tree using the numerical domains. In addition, in our method the possible tests – that are applicable in the inner nodes of the tree – are also enlarged, while keeping them still meaningful and interpretable for the decision maker. This is also important to avoid black-box effects.

We examine the applicability of learning methods, like CDT, in decision support systems to build MCDA models and give an extended empirical and numerical comparison of our method to some other ones, for example C4.5[6], CID3[4], SVM[7], CART[3], on some artificial and real life classification tasks[1].

Keywords: Multicriteria Decision Aid (MCDA), Decision tree, Continuous Decision Tree (CDT), ID3, C4.5, Continuous ID3 (CID3), Support Vector Machine (SVM), Classification and Regression trees (CART), Pattern recognition.

References

[1] C.L. Blake and C.J. Merz. UCI repository of machine learning databases, 1998.

[2] D. Bouyssou, Th. Marchant, P. Perny, M. Pirlot, A. Tsoukiàs, and Ph. Vincke. Evaluation and Decision Models: a critical perspective. Kluwer Academic, Dordrecht, 2000.

[3] L. Breiman, J. Friedman, R. Olshen, and C. Stone. Classification and Regression Trees. Wadsworth, Belmont, CA, 1984.

[4] Krysztof J. Cios and Ning Liu. A machine learning method for generation of a neural network architecture: a continuous ID3 algorithm. IEEE Transactions on Neural Networks, 3(2):280–291, March 1992.

[5] J. Dombi and Á. Zsiros. Learning decision trees in continuous space. Acta Cybernetica, 15:213–224, 2001.

[6] J. Quinlan. C4.5: Programs for Machine Learning. Morgan Kaufmann, San Mateo, CA, 1993.

[7] Vladimir N. Vapnik. The Nature of Statistical Learning Theory. Statistics for Engineering and Information Science. Springer-Verlag, New York Inc., second edition, 2000.

Parallel functional programming on cluster [8]

Viktória Zsók, Zoltán Horváth, and Máté Tejfel

Functional programming is very suitable for expressing parallelism. Nowadays is very widespread the use of PC clusters for testing and developing parallel applications. Building such clusters allows for a larger usergroup to experiment the parallel issues of different problems.

Functional programming is very suitable for expressing parallelism. We would like to test and to verify how the functional programming fits into the parallel programming framework offered by a cluster. A special field of the functional programming will be studied, the theme of skeletons, which suits very well to the parallel functional programming.

It is important to see the behaviour of the skeletons on the GRID of the 20 PC computers, because this test helps in enforcing the parallelism in the functional programming style. Less work was done yet for adapting the functional programming to the possibilities offered by clusters, thus this topic provides many opportunities for studying parallelism.

References

[1] Kesseler, M.H.G.: The Implementation of Functional Languages on Parallel Machines with Distributed Memory, PhD Thesis, Catholic University of Nijmegen, 1996.

[2] Serrarens, P.R.: Communication Issues in Distributed Functional Computing, PhD Thesis, Catholic University of Nijmegen, 2001.

[3] Trinder, P.W., Hammond, K., Loidl, H.W., Peyton Jones, S.J.: Algorithm + Strategy = Parallelism. Journal of Functional Programming, Vol. 8, No. 1, pp. 23-60, 1998.

[8] Supported by the Hungarian National Science Research Grant (OTKA), Grant No. T037742 and by the Grid Project No. 01548

Abonyi-Tóth, Andor: Eötvös Lóránd University, Informatics Methodology Group, Budapest, Hungary, E-mail: abonyita@ludens.elte.hu

Alexin, Zoltán: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: alexin@inf.u-szeged.hu

Alhaddad, Mohammad: Department of Computer Science, University of Essex, United Kingdom, E-mail: mjalha@essex.ac.uk

Arató Mátyás: Institute of Mathematics and Informatics, University of Debrecen, H–4010, Debrecen, Hungary, E-mail: arato@math.klte.hu

Balázs, Gábor: University of Veszprém, Department of Information Systems, Veszprém, Hungary, E-mail: balazsg@irt.vein.hu

Balázs, Péter: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: pbalazs@inf.u-szeged.hu

Balogh, Emese: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: bmse@inf.u-szeged.hu

Balogh, János: University of Szeged, JGYTF, Deptartment of Computer Science, H-6725 Szeged, E-mail: balogh@jgytf.u-szeged.hu

Bartha, Miklós: Department of Computer Science, Memorial University of Newfoundland, St. John's, NF, Canada, A1B 3X5, E-mail: bartha@cs.mun.ca

Benczúr, András: Eötvös Lóránd University, Budapest, Hungary, E-mail: abenczur@ludens.elte.hu

Bilicki, Vilmos: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: bilickiv@inf.u-szeged.hu

Bohus, Mihály: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: bohus@inf.u-szeged.hu

Burulitisz, Alexandrosz: Budapest University of Technology and Economics, Budapest, Hungary, E-mail: aleko@elender.hu

Csáki, Tibor: Department of Computer Science, Institute of Mathematics and Informatics University of Debrecen, H–4010, Debrecen, Hungary, E-mail: Tibor.Csaki@prompt92.hu

Csegedi, Csaba: Budapest University of Technology and Economics, Department of Telecommunication, Mobile Communications Laboratory, H-1117 Pázmány P. S. 1/D, Budapest, Hungary

Csendes, Tibor: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: csendes@inf.u-szeged.hu

Csirik, János: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: csirik@inf.u-szeged.hu

Csiszár, Tibor: Eötvös Lóránd University, Budapest, Hungary, E-mail: tibor@draconis.elte.hu

Csopaki, Gyula: Conformance Laboratory, Ericsson Hungary Ltd. Budapest, H-1037, Laborc u. 1, Budapest, Hungary, E-mail: csopaki@ttt-atm.ttt.bme.hu

Demetrovics, János: HAOS SZTAKI, Budapest, Hungary, E-mail: dj@ilab.sztaki.hu

Dibuz, Sarolta: Conformance Laboratory, Ericsson Hungary Ltd. Budapest, H-1037, Laborc u. 1, Budapest, Hungary, E-mail: Sarolta.Dibuz@eth.ericsson.se

Dobán, Orsolya: Budapest University of Technology and Economics, Budapest, Hungary, E-mail: doban@inf.mit.bme.hu

Drozdik, Béla: University of Veszprém, Department of Information Systems, Veszprém, Hungary, E-mail: bela.drozdik@irt.vein.hu

Dudásné Nagy, Marianna: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: marcsi@inf.u-szeged.hu

Eglesz, Dénes: Eötvös Lóránd University, Budapest, Hungary, E-mail: dino@inf.elte.hu

Endrődi, Csilla: BUTE Department of Measurement and Information Systems, Budapest, Hungary, E-mail: csilla@mit.bme.hu

Fábián, Csaba: Academy of Economic Studies, Bucharest, Romania, E-mail: cfabian@starnets.ro

Fazakas, Antal: Nokia Ltd., Budapest, Hungary, E-mail: Antal.Fazakas@nokia.com

Felföldi, László: Research Group on Artificial Intelligence of the Hungarian Academy of Sciences and University of Szeged, H-6720 Szeged, Aradi vértanúk tere 1., Hungary, E-mail: lfelfold@rgai.hu

Fidrich, Márta: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: fidrich@inf.u-szeged.hu

Fomina, Elena: Department of Computer Engineering, Tallinn Technical University, Raja 15, 12617 Tallinn, Estonia, E-mail: elfom@staff.ttu.ee

Friedler, Ferenc: University of Veszprém, Department of Computer Science, Veszprém, Hungary, E-mail: friedler@almos.vein.hu

Fühner, Tim: Department of Computer Science II, University of Erlangen-Nuremberg, Martensstr. 3, D-91058 Erlangen, Germany, E-mail: tim.fuehner@web.de

Gergely, Tamás: Research Group on Artificial Intelligence of the Hungarian Academy of Sciences and University of Szeged, H-6720 Szeged, Aradi vértanúk tere 1., Hungary, E-mail: gertom@rgai.hu

Gosztolya, Gábor: Research Group on Artificial Intelligence of the Hungarian Academy of Sciences and University of Szeged, H-6720 Szeged, Aradi vértanúk tere 1., Hungary, E-mail: ghosty@rgai.inf.u-szeged.hu

Gulyás, András: Budapest University of Technology and Economics, Budapest, Hungary, E-mail: guli@balu.sch.bme.hu

Gyapay, Szilvia: Budapest University of Technology and Economics, Department of Measurement and Information Systems, H-1521 Budapest Magyar tudósok körútja 2., E-mail: gyapay@mit.bme.hu

Gyimóthy, Tibor: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: gyimi@inf.u-szeged.hu

Hanák, Dávid: Budapest University of Technology and Economics, Budapest, Hungary, E-mail: dhanak@inf.bme.hu

Haraszti, Kristóf: University of Veszprém, Ph.D. School of Informatics Sciences, Veszprém, Hungary, E-mail: haraszti@mfa.kfki.hu

Harmathné Medve, Anna: Veszprém University, Department of Information Systems, Veszprém, Hungary, E-mail: medve@almos.vein.hu

Havasi, Ferenc: Research Group on Artificial Intelligence of the Hungarian Academy of Sciences and University of Szeged, H-6720 Szeged, Aradi vértanúk tere 1., Hungary, E-mail: hafy@rgai.hu

Herman, Gábor: Department of Computer Science, Graduate Center, City University of New York E-mail: GHerman@gc.cuny.edu

Hidvégi, Timót: Analog and Neural Computing Systems Laboratory, Computation and Automation Institute, Hungarian Academy of Sciences, P.O.B 63, H-1502, Budapest, Hungary, E-mail: hidvegi@sztaki.hu

Hócza, András: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: hocza@inf.u-szeged.hu

Hornák, Zoltán: BUTE Department of Measurement and Information Systems, Budapest, Hungary

Horváth, Cz., János: Budapest University of Technology and Economics, Department of Telecommunications, BME-HT, Magyar tudósok körútja 2. H-1117 Budapest, Hungary, E-mail: cozi@mlabdial.hit.bme.hu

Horváth, Endre: Department of Telecommunications and Telematics, Budapest University of Technology and Economics, Magyar tudósok körútja 2, H-1117 Budapest, Hungary, E-mail: Endre.Horvath@eth.ericsson.se

Horváth, Zoltán: Department of General Computer Science, Eötvös Loránd University, Budapest, Hungary, E-mail: hz@inf.elte.hu

Hosszú, József: Department of Telecommunications and Telematics, Budapest University of Technology and Economics, Magyar tudósok körútja 2, H-1117 Budapest, Hungary, E-mail: Jozsef.Hosszu@eth.ericsson.se

Imreh, Csanád: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: cimreh@inf.u-szeged.hu

Imre, Sándor: Budapest University of Technology and Economics, Department of Telecommunication, Mobile Communications Laboratory, H-1117 Pázmány P. S. 1/D, Budapest, Hungary, E-mail: imre@hit.bme.hu

Jász, Judit: Research Group on Artificial Intelligence of the Hungarian Academy of Sciences and University of Szeged, H-6720 Szeged, Aradi vértanúk tere 1., Hungary, E-mail: jasy@rgai.hu

Jisa, Dan Laurentiu: E-mail: dan.jisa@ewir.ro

Jókuthy, András: University of Veszprém, Department of Information Systems, Veszprém, Hungary

Jónás, Richárd: Institute of Mathematics and Informatics, University of Debrecen, H–4010, Debrecen, Hungary, E-mail: jonasr@math.klte.hu

Juhos, István: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: juhos@inf.u-szeged.hu

Kacsuk, Péter: MTA SZTAKI, Hungarian Academy of Sciences, H-1518 Budapest, P.O. Box 63, Hungary, E-mail: kacsuk@sztaki.hu

Kálmán, Miklós: Research Group on Artificial Intelligence of the Hungarian Academy of Sciences and University of Szeged, H-6720 Szeged, Aradi vértanúk tere 1., Hungary, E-mail: kalman@rgai.hu

Kárász, Péter: Budapest Polytechnic, John von Neumann Faculty of Informatics, Institute of Applied Informatics, P. O. Box 267, H-1300 Budapest, Hungary, E-mail: karasz@nik.bmf.hu

Kasza, Tamás: Conformance Laboratory, Ericsson Hungary Ltd. Budapest, H-1037, Laborc u. 1, Budapest, Hungary, E-mail: kasza@sch.bme.hu

Katsányi, István: Eötvös Loránd University, Department of General Computer Science, 1117 Budapest, Pázmány Péter sétány 1/D., E-mail: kacsa@ludens.elte.hu

Keszthelyi, Krisztián: Szent István University, Department of Agricultural and Regional Sciences, Budapest, Hungary, E-mail: keszthelyik@freemail.hu

Kiss, Ákos: Research Group on Artificial Intelligence of the Hungarian Academy of Sciences and University of Szeged, H-6720 Szeged, Aradi vértanúk tere 1., Hungary, E-mail: akiss@rgai.inf.u-szeged.hu

Kiss, Orhidea Edith Budapest University of Technology and Economics, Department of Ergonomics and Psychology

Koch, György: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: koch@inf.u-szeged.hu

Kocsis, Attila: E-mail: atkocsis@interware.hu

Kocsor, András: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: kocsor@inf.u-szeged.hu

Kókai, Gabriella: Department of Computer Science II, University of Erlangen-Nuremberg, Martensstr. 3, D-91058 Erlangen, Germany, E-mail: kokai@informatik.uni-erlangen.de

Kókai, Tamás: Eötvös Lóránd University, Budapest, Hungary, E-mail: tomcsi@hali.elte.hu

Kollár, Lajos: Institute of Mathematics and Informatics, University of Debrecen, H–4010, Debrecen, Hungary, E-mail: kollarl@math.klte.hu

Kormos, János: Institute of Mathematics and Informatics, University of Debrecen, H–4010, Debrecen, Hungary, E-mail: kormos@math.klte.hu

Kovács, Kornél: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: kkornel@inf.u-szeged.hu

Kovásznai, Gergely: Institute of Mathematics and Informatics, University of Debrecen, H–4010, Debrecen, Hungary, E-mail: kovasz@zuse.math.klte.hu

Kozma, László: Eötvös Lóránd University, Budapest, Hungary, E-mail: kozma@ludens.elte.hu

Kozma, Péter: Department of Image Processing and Neurocomputing, University of Veszprém, Egyetem u. 10, H-8200 Veszprém, Hungary, E-mail: kozmap@almos.vein.hu

Krész, Miklós: University of Szeged, JGYTF, Deptartment of Computer Science, H-6725 Szeged, E-mail: kresz@jgytf.u-szeged.hu

Kuba, Attila: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: kuba@inf.u-szeged.hu

Kusper, Gábor: Research Institute for Symbolic Computation (RISC-Linz), Johannes Kepler University, Linz, Austria, E-mail: gkusper@risc.uni-linz.ac.at

Laczó, Tibor: Eötvös Lóránd University, DGCS and FÖMI RSC, Budapest, Hungary, E-mail: tibur@sch.bme.hu

Lehotai, Gábor: Research Group on Artificial Intelligence of the Hungarian Academy of Sciences and University of Szeged, H-6720 Szeged, Aradi vértanúk tere 1., Hungary, E-mail: leg@rgai.hu

Licsár, Attila: University of Veszprém, Department of Image Processing and Neurocomputing, H-8200 Veszprém, Egyetem u. 10, Hungary, E-mail: licsara@silicon.terra.vein.hu

Lovas, Róbert: MTA SZTAKI, Hungarian Academy of Sciences,H-1518 Budapest, P.O. Box 63, Hungary, E-mail: rlovas@sztaki.hu

Maka, Róbert Budapest University of Technology and Economics, Department of Telecommunication, Mobile Communications Laboratory, H-1117 Pázmány P. S. 1/D, Budapest, Hungary, E-mail: mr205@hszk.bme.hu

Markót, Mihály Csaba: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: markot@inf.u-szeged.hu

Molnár, Gergely: Ericsson Research, Traffic Analysis and Network Performance Laboratory, Budapest, Hungary E-mail: ethmoge@eth.ericsson.se

Nagy, Zoltán: Department of Image Processing and Neurocomputing, University of Veszprém, Egyetem u. 10, H-8200 Veszprém, Hungary, E-mail: nagyz@almos.vein.hu

Nohl, Attila Rajmund: Eötvös Lóránd University, Budapest, Hungary, E-mail: Attila.Nohl@eth.ericsson.se

Nyúl, László G. Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: nyul@inf.u-szeged.hu

Orvos, Péter: BUTE-DMIS, Budapest, Hungary, E-mail: orvos@mit.bme.hu

Palágyi, Kálmán: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: palagyi@inf.u-szeged.hu

Pap, Gyula: Institute of Mathematics and Informatics, University of Debrecen, H–4010, Debrecen, Hungary, E-mail: papgy@math.klte.hu

Pataki, István Budapest University of Technology and Economics, Budapest, Hungary, E-mail: pi205@hszk.bme.hu

Petri, Dániel: Budapest University of Technology and Economics, Department of Measurement and Information Systems, H-1521 Budapest Magyar tudósok körútja 2., E-mail: dpetri@mit.bme.hu

Pintér, János: Pinter Consulting Services, Inc., 129 Glenforest Drive, Halifax, NS, Canada B3M 1J2, E-mail: jdpinter@hfx.eastlink.ca

Polgár Balázs: E-mail: balazs@mit.bme.hu

Raicu, Gabriel: Constanta Maritime University, Romania, E-mail: graicu@emsolgroup.com

Rapcsák, Tamás: Computer and Automation Institute of the Hungarian Academy of Sciences, Budapest, Hungary, E-mail: rapcsak@sztaki.hu

Recski, András: Budapest University of Technology and Economics, Budapest, Hungary, E-mail: recski@math.bme.hu

Rönkä, Matti: Turku Centre for Computer Science, Lemminkäisenkatu 14 A, FIN-20520 Turku, Finland, E-mail: matti.ronka@utu.fi

Rózsás, Balázs: Budapest University of Technology and Economics, Department of Telecommunication, Mobile Communications Laboratory, H-1117 Pázmány P. S. 1/D, Budapest, Hungary, E-mail: brozsas@mcl.hu

Ruskó, László: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: rusko@inf.u-szeged.hu

Salamon, András: Eötvös Lóránd University, TTK, Budapest, Hungary, E-mail: asalamon@elender.hu

Scarlatescu, Raluca Oana: Academy of Economic Studies, Bucharest, Romania, Faculty of Cybernetics, Statistics and Economic Informatics, E-mail: oana.rs@tiscalinet.it

Schulcz, Róbert: Budapest University of Technology and Economics, Department of Telecommunication, Mobile Communications Laboratory, H-1117 Pázmány P. S. 1/D, Budapest, Hungary, E-mail: schulcz@hit.bme.hu

Sebő, Mariann: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: sebo@inf.u-szeged.hu

Selényi, Endre: BUTE-DMIS, Budapest, Hungary, E-mail: selenyi@mmt.bme.hu

Sey, Gábor: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: Sey.Gabor.Lajos@stud.u-szeged.hu

Sógor, Zoltán Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: weth@nokia5.inf.u-szeged.hu

Sragner, László: Budapest University of Technology and Economics, E-mail: sragner@sch.bme.hu

Steinby, Paula: Turku Centre of Computer Science, Finland, E-mail: paula.steinby@utu.fi

Szabó, János Zoltán: Budapest University of Technology and Economics, Budapest, Hungary, E-mail: szaboj@ttt-atm.ttt.bme.hu

Szabó, Péter Gábor: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: pszabo@inf.u-szeged.hu

Szabó, Richárd: Department of General Computer Science, University Eötvös Loránd, H-1117, Pázmány P. s. 1/D., Budapest, Hungary, E-mail: rics@inf.elte.hu

Szabó, Sándor E-mail: saas@mailbox.hu

Szabó, Tamás: Image Processing and Neurocomputing Department, University of Veszprém, H-8200 Egyetem u. 10, Veszprém, Hungary,, E-mail: tszabo@sztaki.hu

Szabó, Tibor: Conformance Laboratory, Ericsson Hungary Ltd., H-1037 Budapest, Laborc u. 1, Budapest, Hungary, E-mail: szabot@ttt.bme.hu

Szarvas, György

Szász, András: Budapest University of Technology and Economics, Budapest, Hungary, E-mail: szasz@sch.bme.hu

Szegedi, Attila

Szegő, Dániel: E-mail: szegod@mit.bme.hu

Székely, Nóra: Budapest University of Technology and Economics, Department of Measurement and Information Systems, H-1521 Budapest, Magyar Tudósok krt. 2. Hungary, E-mail: sn206@ural2.hszk.bme.hu

Szeles, Tamás

Szépkúti, István: ING Nationale-Nederlanden Hungary Insurance Co. Ltd., H-1061 Budapest, Andrássy út 9, Hungary, E-mail: szepkuti@inf.u-szeged.hu

Szeredi, Tamás

Szilágyi, Gyöngyi: Research Group on Artificial Intelligence of the Hungarian Academy of Sciences and University of Szeged, H-6720 Szeged, Aradi vértanúk tere 1., Hungary, E-mail: szilagyi@rgai.inf.u-szeged.hu

Szirányi, Tamás: Analogical & Neural Computing Laboratory, Computer & Automation Research Institute, Hungarian Academy of Sciences, H-1111 Budapest, Kende u. 13-17, Hungary, E-mail: sziranyi@sztaki.hu

Szörényi, Balázs: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: szorenyi@inf.u-szeged.hu

Tanács, Attila: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: tanacs@inf.u-szeged.hu

Tarnay, Katalin: Nokia Ltd., Budapest, Hungary, E-mail: Katalin.Tarnay@Nokia.com

Tejfel, Máté: Department of General Computer Science, Eötvös Loránd University, Budapest, Hungary, E-mail: matej@inf.elte.hu

Tóth, Boglárka: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: boglarka@inf.u-szeged.hu

Tóth, László: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: tothl@inf.u-szeged.hu

Tóth, Zoltán: Department of Computer Science II, University of Erlangen-Nuremberg, Martensstr. 3, D-91058 Erlangen, Germany, E-mail: Zoltan.Toth@informatik.uni-erlangen.de

Valyon, József: Budapest University of Technology and Economics, Department of Measurement and Information Systems, H-1521 Budapest, Hungary, P. O. Box 91., E-mail: valyon@mit.bme.hu

Ványi, Róbert: Department of Computer Science II, University of Erlangen-Nuremberg, Martensstr. 3, D-91058 Erlangen, Germany, E-mail: Robert.Vanyi@informatik.uni-erlangen.de

Varga, László: Eötvös Lóránd University, Budapest, Hungary, E-mail: varga@inf.elte.hu

Varró, Dániel: Budapest University of Technology and Economics, Department of Measurement and Information Systems, H-1521 Budapest, Magyar tudósok körútja 2., E-mail: varro@mit.bme.hu

Veréb, Krisztián: Institute of Mathematics and Informatics, University of Debrecen, H–4010, Debrecen, Hungary, E-mail: sparrow@math.klte.hu

Vinkó, Tamás: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: tvinko@inf.u-szeged.hu

Zömbik, László: Department of Telecommunications and Telematics, Budapest University of Technology and Economics, Magyar tudósok körútja 2, H-1117 Budapest, Hungary, E-mail: laszlo.zombik@eth.ericsson.se

Zsiros, Ákos: Institute of Informatics, University of Szeged, H-6701 Szeged P.O. Box 652, Hungary, E-mail: zsiros@inf.u-szeged.hu

Zsók, Viktoria: Department of General Computer Science, Eötvös Loránd University, Budapest, Hungary, E-mail: zsv@inf.elte.hu

Notes