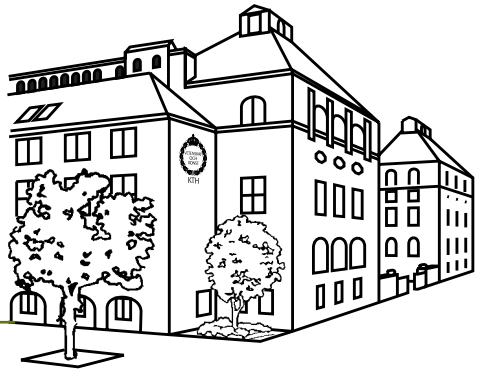
Numero

Veckobladet om forskning, undervisning och administration på Skolan för datavetenskap och kommunikation



Numero nr 11

23 mars 2006 • Årgång 36

Numero är institutionstidningen *på Skolan för datavetenskap och kommunikation vid KTH. Numero utkommer normalt på torsdagsförmiddagar under teminstid.*
Manus måste lämnas in före kl.12 på onsdagar. Manus, tips, förslag och andra bidrag till Numero kan lämnas på något av följande sätt:

- *via en webblankett på adressen www.nada.kth.se/numero/blankett.html*
- *via e-post till numero@nada.kth.se*
- *på papper till Nada, Numero, KTH, 100 44 STOCKHOLM (dvs. facket "Numero" bland postfacken på pl 4)*

Bidrag för artiklar och notiser bör i största möjliga mån vara färdigformulerade och korrekturlästa.
Varje Numeronummer utkommer i två former:

- *På papper för normal postdistribution*
- *Webb: www.nada.kth.se/numero/*

Numeroredaktionen består av Maria Engström. Ansvarig utgivare är Ingrid Melinder. Numeros innehåll uttrycker inte institutionens officiella ståndpunkt annat än då detta anges.

Underhåll av servrar / Server maintenance

Lördagen den 25/3 med start kl 10:00 kommer underhåll att utföras på många av Nadas servrar.

Under det att arbetet pågår kommer många unix-datorer på Nada att råka ut för kraftiga störningar. Tjänster som e-post och WWW kommer också att påverkas.

Maintenance work on many of the servers at Nada will be performed on Saturday Mar 25 starting at 10:00 am.

Most UNIX computers at Nada will be heavily affected during this time. Services like E-mail and WWW, will also be affected.

/Systemgruppen CSC

Passa på att pröva.....

Massagefåtölj

CSC har massagefåtölj på prov 2 veckor från den 20 mars. Den finns på CSC bibliotek, Lindstedtsvägen 3, plan 4. Bokningslista för dessa två veckor finns på dörren in till biblioteket. En instruktion finns uppsatt på väggen vid fåtöljen. Som underlag för beslut om ev. fortsättning är det viktigt med dina synpunkter. Fyll gärna i utvärderings-blanketten som ligger på bordet bredvid fåtöljen. Leverantören rekommenderar 15 minuter 1-3 gånger i veckan.

Eva-Lena

Ny gemensam översikt för forskningsfinansiärerna

En ny version av den för forskningsfinansiärerna gemensamma översikten med korta presentationer av respektive finansiär - på svenska och engelska - finns nu för nedladdning.

Svensk forskning
http://www.stratresearch.se/pdf/Svensk%20forskning%202006.pdf

Swedish Research
http://www.stratresearch.se/pdf/Swedish%20Research%202006.pdf

Disputation

“Large-Scale Information Acquisition for Data and Information Fusion”

Respondent: Ronnie Johansson, Datalogi, KTH

7 april, kl 14.00.
Sal F3, Lindstedtsvägen 26, Stockholm.

Opponent: PHDR David Nicolson, BAE Systems, Advanced Technology Centre, Bristol, Storbritannien
Huvudhandledare: Professor Henrik Christensen

Abstract
The purpose of information acquisition for data and information fusion is to provide relevant and timely information. The acquired information is integrated (or fused) to estimate the state of some environment. The success of information acquisition can be measured in the quality of the environment state estimates generated by the data and information fusion process.

In this thesis, we introduce and set out to characterise the concept of large-scale information acquisition. Our interest in this subject is justified both by the identified lack of research on a holistic view on data and information fusion, and the proliferation of networked sensors which promises to enable handy access to a multitude of information sources. We identify a number of properties that could be considered in the context of large-scale information acquisition. The sensors used could be large in number, heterogeneous, complex, and distributed. Also, algorithms for large-scale information acquisition may have to deal with decentralised control and multiple and varying objectives.

In the literature, a process that realises information acquisition is frequently denoted sensor management. We, however, introduce the term perception management instead, which encourages an agent perspective on information acquisition. Apart from explictly inviting the wealth of agent theory research into the data and information fusion research, it also highlights that the resource usage of perception management is constrained by the overall control of a system that uses data and information fusion.

To address the challenges posed by the concept of large-scale information acquisition, we present a framework which highlights some of its pertinent aspects. We have implemented some important parts of the framework. What becomes evident in our study is the innate complexity of information acquisition for data and information fusion, which suggests approximative solutions.

We, furthermore, study one of the possibly most important properties of large-scale information acquisition, decentralised control, in more detail. We propose a recurrent negotiation protocol for (decentralised) multi-agent coordination. Our approach to the negotiations is from an axiomatic bargaining theory perspective; an economics discipline. We identify shortcomings of the most commonly applied bargaining solution and demonstrate in simulations a problem instance where it is inferior to an alternative solution. However, we can not conclude that one of the solutions dominates the other in general. They are both preferable in different situations. We have also implemented the recurrent negotiation protocol on a group of mobile robots.

We note some subtle difficulties with transferring bargaining solutions from economics to our computational problem. For instance, the characterising axioms of solutions in bargaining theory are useful to qualitatively compare different solutions, but care has to be taken when translating the solution to algorithms in computer science as some properties might be undesirable, unimportant or risk being lost in the translation.

Generic Attacks on Stream Ciphers

John Mattsson

Måndag 27 mars, kl 13.15, rum 1537

Today when so much information is transmitted over open channels like the Internet and wireless channels (GSM, UMTS, Wi-Fi, WiMAX etc.), cryptography is more important than ever. The benefits of stream ciphers compared to block ciphers (like AES) are that they are generally much faster, have low hardware complexity, and no or limited error propagation.

I will first give a short introduction to stream ciphers and how attacks are classified depending on the information avalable to the attacker and the aim of the attack. I will then present the most important generic attacks including distinguishing attacks, time memory tradeoffs, correlation attacks, algebraic attacks, and side channel attacks.

The talk will be given in Swedish or English depending on the participants, and is intended to last for about one hour.

“Usability Engineering Activity in Japan”

Professor Maasaki Kurosu, from the R&D Division of National Institute of Multimedia Education (NIME) of MEXT, the Ministry of Education, Japan

Monday, March 27, at 10.15
at CID-Torget, Lindstedtsvägen 5, floor 6, KTH

Very welcome,
Yngve Sundblad

Just Idag:
23 mars 1900

Utgrävningarna av grekiska Knossos börjar

Short Proofs Are Narrow (Well, Sort of), But Are They Tight?

Jakob Nordström, Teorigruppen, KTH CSC

Måndag 3 april, kl 13.15-15.00, rum 1537,
plan 5, Osquars backe 2 / Lindstedtsvägen 3.

A propositional proof system is an algorithm P(F,pi) that runs in time polynomial in the sizes |F| and |pi| of the inputs and has the property that

• for every valid formula, or tautology, F there is a proof pi such that P(F,pi)=1,
• for every non-tautological formula F it holds that P(F,pi)=0 for all purported proofs pi.

The study of propositional proof complexity is important both from a theoretical and a practical point of view. On the one hand, it is closely related to central questions in computational complexity, in view of the fact that separating NP and co-NP (which would imply P != NP) is equivalent to proving that there is no propositional proof systems where all tautologies F have proofs pi of size at most polynomial in the size of F. On the other hand, designing efficient algorithms for proving tautologies, or equivalently refuting unsatisfiable formulas, is a very important problem in applied research and in industry, e.g. in the context of formal methods.

In this talk, we will focus on resolution, which proves tautologies by showing that their negations, expressed as CNF formulas, are unsatisfiable. It is perhaps the single most studied propositional proof system, and many real-world automated theorem provers are based on it.

In 1999, Ben-Sasson and Wigderson proved a strong (and perhaps somewhat surprising) correlation between the size and the width of proofs, where the width is the size of the largest disjunction in the proof. Another well-studied measure in resolution is space, which intuitively is the maximal number of clauses one needs to keep in memory while verifying the proof. Interestingly, all lower bounds proven so far on space in resolution has turned out to match exactly lower bounds on width. In 2003, Atserias and Dalmau showed the (arguably even more surprising) result that this is true in general.

We will first give an introduction to proof complexity in general and resolution in particular. Then we will provide a fairly detailed overview of the above-mentioned results. Finally, if time permits we will also discuss some open questions (one of which we managed to solve recently and which will be the subject of a separate talk in the TCS seminar series on May 15th).

The talk will be given in Swedish or English depending on the participants.

Seminarierum 1537 ligger på plan 5, Osquars backe 2 / Lindstedtsvägen 3.

Med vänlig hälsning,
Jakob Nordström

TMH, Seminar at Speech, Music and Hearing:

Syntes av disfluenser i tal

Rolf Carlson, Kjell Gustafson och Eva Strangert

15:00 - 17:00, Friday March 31, 2006
The seminar is held in Fantum.

Abstract
The current work deals with the modelling of one type of dis fluency, hesitations. A perceptual experiment using speech synthesis was designed to evaluate two duration features found to be correlates to hesitation, pause duration and final lengthening. A variation of F0 slope before the hesitation was also included. The most important finding is that it is the total duration increase that is the valid cue rather than the contribution by either factor. In addition, our findings lead us to assume an interaction with syntax. The absence of strong effects of the induced F0 variation was unexpected and we consider several possible explanations for this result.

Seminar at CBN

Specification of synaptic connectivity in large scale simulations using SPLIT

Mikael Djurfeldt, CBN

Friday March 24 at 10.15 in room 4329

Välkomna!
/Erik

Exjobb

Exjobbsseminarium i MDI

Nästa exjobbsseminarium i MDI äger rum torsdagen den 23/3 klockan 10:15 i 1625

Moa Söderhielm
Att göra det tråkiga roligt – Innovativ gränssnittsdesign i webbenkäter.
Program: Teknisk fysik
Handledare: Olle Bälter
Examinator: Kerstin Severinson Eklundh
Opponent: Johan Boström

Seminarieledare: Kerstin Severinson Eklundh

Programmet (med sammanfattningar) finns på http://www.nada.kth.se/utbildning/grukth/exjobb/mdi/seminarier2006/aktuellt.html

Fredrik

Exjobb

Redovisning av exjobb i Numerisk Analys

Måndag 27 mars kl 15.30 i D 1625

Carl Troeng, SU SciComp_04: «**Moving Meshes for CFD: Deformation and regeneration**»
Handledare: Jesper Oppelstrup
Lars Gunnilstam, E_01: "Structured products in mean-variance portfolio optimization"
Handledare: Andre Jaun

Välkomna önskar examinator
Axel Ruhe, Professor of Numerical Analysis

Jobs

Professorship in Stockholm

Nordic-Math-Job number: SE-0693
University: Royal Institute of Technology
Department: Department of Mathematics
Position: Professorship in Mathematical Statistics
Deadline: 13 April 2006
Contacts: Anders Lindquist, 08-790 73 11, alq@math.kth.se
Web-info: http://www.kth.se/aktuellt/tjanster/Anst/Prof%20matstat_eng.html

Seminarielänkar

AlbaNova
http://www.albanova.se/aktuellt/

Bråket
http://www.math.kth.se/braaket.html

INSTITUT MITTAG-LEFFLER SEMINARS
www.ml.kva.se

KTH Matematik
http://www.math.kth.se/optsyst seminar/

S3 http://www.s3.kth.se/

SICS
http://www.sics.se/research/seminars.php

TMH, Tal, musik och hörsel
http://www.speech.kth.se/seminars/

Wireless@kth
http://www.wireless.kth.se

Stacken
http://www.stacken.kth.se/kalender/

KTH – Computational Science and Engineering Centre
http://www.kcse.kth.se/seminars.html

Stockholm Bioinformatics Center and Dept Num Analysis and Comp Science
http://www.sbc.su.se/seminars/

Just Idag:
23 mars 1955

Första flygcharterresan till Mallorca.

Just Idag:
23 mars 1925

Balzar von Platen och Carl Munters får medalj för sin uppfinning kylskåpet.

Kalendarium 2006

Mars

23 mars 10:15 Exjobbsseminarium i MDI
Moa Söderhielm. Att göra det tråkiga roligt – Innovativ gränssnittsdesign i webbenkäter. i 1625

23 mars 12.00-13.30 Lunchseminarier på KTH
Internationalisering och språkfrågan. i Salongen KTH Learning Lab, Osquars Backe 31. Ärtsoppa serveras!

23 mars, 13:15 Seminar
Cryptographically Sound Theorem Proving. Christoph Sprenger, Department of Computer Science, ETH Zurich, room 1537

23 mars 15.15 Presentation av exjobb i datalogi
Dahl, Stefan, Anonymous Car Toll Payments using RFID Tags.
Duracz, Adam, Härledning av sannolikhetsfördelningar för riskanalys. i sal E34 Lindstedtsvägen 3, plan 3

24 mars 10.15 Seminar at CBN
Specification of synaptic connectivity in large scale simulations using SPLIT, Mikael Djurfeldt, CBN, in room 4329

27 mars 10.15 Seminar
“Usability Engineering Activity in Japan” Professor Maasaki Kurosu, at CID-Torget, Lindstedtsvägen 5, floor 6, KTH

27 mars, kl 13.15, Seminar
Generic Attacks on Stream Ciphers, John Mattsson, rum 1537

27 mars kl 15.30 Redovisning av exjobb i Numerisk Analys
Carl Troeng, SU SciComp_04: Moving Meshes for CFD: Deformation and regeneration
Lars Gunnilstam, E_01: Structured products in mean-variance portfolio optimization i D 1625

29 mars 12.10-12.50 Lunchkonserter
Lilla Akademiens Stråkorkester, åk 7-9, med Händel och Holst i bagaget. Dirigent: Mark Tatlow

29 mars kl. 13 – 17 Naturvetareförbundets forskningspolitiska seminarium
Den naturvetenskapliga forskningens framtid Aula Magna, Stockholms universitet

31 mars 15:00 - 17:00 TMH, Seminar at Speech, Music and Hearing:
Syntes av disfluenser i tal, Rolf Carlson, Kjell Gustafson och Eva Strangert, The seminar is held in Fantum.

April

3 april, kl 13.15-15.00
Short Proofs Are Narrow (Well, Sort of), But Are They Tight? Jakob Nordström, Teorigruppen, KTH CSC, rum 1537, plan 5, Osquars backe 2 / Lindstedtsvägen 3

5 april 12.10-12.50 Lunchkonserter
“Toner av sucksamt och glatt” Operasångaren Stig Tysklind sjunger, minns och berättar. Vid pianot: Gunnar Julin

7-8 april Symposium
BERÄTTANDE I OLIKA MEDIER på Statens ljud- och bildarkiv, Karlavägen 98

7 april, kl 13.15. Licentiatsemimarium:
A New Finite Element Method for Elliptic Interface Problems. Alexei Loubenets Sal D3, Lindstedtsvägen 5, KTH

7 april, kl 14.00. Disputation
Ronnie Johansson, Datalogi, KTH. Large-Scale Information Acquisition for Data and Information Fusion
Sal F3, Lindstedtsvägen 26, Stockholm

21 april, kl 10.00. Disputation
Maria Enroth, Medieteknik och grafisk produktion, KTH. Developing tools for sustainability in the graphic arts industri. Salongen KTHB, Stockholm