



BRÅKET



*Information om seminarier och högre undervisning
i matematiska ämnen i Stockholmsområdet*

NR 37

FREDAGEN DEN 16 NOVEMBER 2007

BRÅKET

Veckobladet från
Institutionen för matematik
vid Kungl Tekniska Högskolan
och Matematiska institutionen
vid Stockholms universitet

Redaktör: Gunnar Karlsson

Telefon: 08-790 84 79

Adress för e-post:
gunnarkn@math.kth.se

Bråket på Internet: <http://www.math.kth.se/braaket.html> eller
<http://www.math.kth.se/braket/>

Postadress:

Red. för Bråket
Institutionen för matematik
KTH
100 44 Stockholm

Sista manustid för nästa nummer:
Torsdagen den 22 november
kl. 13.00.

Disputation i data- och systemvetenskap

Anna-Maria Kessler disputerar vid
SU på avhandlingen *A Systemic
Approach Framework for Opera-
tional Risk: –SAFOR–* fredagen
den 23 november kl. 13.00 i sal C,
Forum, Isafjordsgatan 39, Kista.
Se Bråket nr 36 sidorna 7–8.

Money, jobs: Se sidorna 9–10.

SEMINARIER

Fr 11–16 kl. 15.00. **Small Talk Seminar.** Michelle
Bucher-Karlsson, Matematik, KTH: *Signature
and characteristic classes of surface bundles.* Semi-
narierum 3721, Institutionen för matematik,
KTH, Lindstedtsvägen 25, plan 7. Se Bråket nr 36
sidan 9.

Må 11–19 kl. 13.15–15.00. **Informellt doktorandsemi-
narium i teoretisk datalogi.** Martin Ekerå
och Henrik Ygge: *On recent attacks on hash
functions.* Rum 1537, KTH CSC, Lindstedtsvägen
3, plan 5. Se Bråket nr 36 sidorna 12–13.

Må 11–19 kl. 15.15. **Seminarium i finansiell matematik.**
Alexander Herbertsson, Institutionen för
nationalekonomi med statistik, Handelshögskolan
vid Göteborgs universitet: *Pricing portfolio credit
derivatives using matrix-analytic methods.* Semi-
narierum 3733, Institutionen för matematik,
KTH, Lindstedtsvägen 25, plan 7. Se Bråket nr 36
sidan 5.

Fortsättning på nästa sida.

Workshops vid Institut Mittag-Leffler

Under hösten 2007 anordnas två sådana. Den första av dessa
ägede rum i september. Den andra skall äga rum den 19–23
november. Se Bråket nr 36 sidan 9.

Kurs

Ola Hössjer, Juni Palmgren: *Population Genetics and Gene
Mapping.* Se sidan 8.

Lansering av bok

Boken *Att våga sitt tärningskast. Gösta Mittag-Leffler 1846–
1927* av Arild Stubhaug lanseras vid Institut Mittag-Leffler
onsdagen den 28 november kl. 15.00. Se sidan 5.

Seminarier (fortsättning)

- Ti 11–20 kl. 10.15. Plurikomplexa seminariet.** David Jacquet, SU: *Hartogsområden i \mathbb{C}^2 av klass C^1* . Rum 306, hus 6, Matematiska institutionen, SU, Kräftriket. Se sidan 4.
- Ti 11–20 kl. 13.00. Uppsattsseminarium i statistik. (Observera dagen!)** Rasmus Edlund och Robin Seth: *Hur bör kvalitetsjusteringar utföras vid mätning av tjänsteprisindex?* Sal B705, Statistiska institutionen, SU, Universitetsvägen 10B, plan 7, Frescati.
- Ti 11–20 kl. 13.15. Presentation av examensarbete i matematik.** Maria Svärdh, Civilingenjör & Lärare, KTH: *Webbaserade matematikuppgifter för grundskolans senare del*. Seminarierum 3721, Institutionen för matematik, KTH, Lindstedtsvägen 25, plan 7. Se Bråket nr 36 sidan 10.
- On 11–21 kl. 8.00. Presentation av examensarbete i matematisk statistik.** Tommy Andersson: *Prevalens och förväntad återstående livslängd som funktion av incidens och mortalitet. Utveckling och tillämpning av en modell för demens i en population*. Sal 31, hus 5, Matematiska institutionen, SU, Kräftriket. Se sidan 5.
- On 11–21 kl. 9.00. Presentation av examensarbete i matematisk statistik.** Sandra Lundin: *Ornstein-Uhlenbeck-processens egenskaper vid modellering av finansiella tidsserier*. Sal 31, hus 5, Matematiska institutionen, SU, Kräftriket. Se sidan 5.
- On 11–21 kl. 10.00. Presentation av examensarbete i matematisk statistik.** Stefan Ekwall: *Modell över det förväntade utfallet i en livförsäkringsportfölj*. Sal 31, hus 5, Matematiska institutionen, SU, Kräftriket. Se sidan 6.
- On 11–21 kl. 10.30. Logikseminariet Stockholm-Uppsala.** Nicola Gambino, University of Leicester och Centre de Recerca Matemàtica, Barcelona: *Sheaves of setoids*. Sal Å11167, Ångströmlaboratoriet, Uppsala universitet. Se sidan 4.
- On 11–21 kl. 11.00. Presentation av examensarbete i matematisk statistik.** Jan-Erik Lundin: *An evaluation approach of embedded options and immunization strategies*. Sal 31, hus 5, Matematiska institutionen, SU, Kräftriket. Se sidan 6.
- On 11–21 kl. 11.00. Common SU KoF/KTH Theoretical Physics Seminar.** David Gómez-Ullate, Madrid: *Chaos and multivaluedness: travelling on Riemann surfaces*. Sal FA31, Roslagstullsbacken 21, AlbaNova universitetscentrum.
- On 11–21 kl. 13.15–14.15. Seminarium i analys och dynamiska system.** Joakim Arnlind, KTH: *Title to be announced*. Seminarierum 3721, Institutionen för matematik, KTH, Lindstedtsvägen 25, plan 7.
- On 11–21 kl. 13.15–15.00. Algebra and Geometry Seminar.** Torsten Ekedahl, SU: *Non-triviality examples for $\{BG\}$* . Seminarierum 3733, Institutionen för matematik, KTH, Lindstedtsvägen 25, plan 7. Se sidan 7.
- On 11–21 kl. 14.30–15.30. KCSE (KTH Computational Science and Engineering Centre) Seminar.** Mattias Gärdback, Mekanik, KTH: *Using patches of Finite Elements — instead of just elements*. PDC:s seminarierum, KTH, Teknikringen 14, plan 3.
- On 11–21 kl. 15.00. Distinguished Lecture. Professor Jacques Stern,** École Normale Supérieure, Paris: *Cryptography in financial transactions: Current practice and future directions*. Sal D3, KTH, Lindstedtsvägen 5, b.v. Se sidan 9.
Professor Sterns föreläsning är arrangerad av Wenner-Green Foundations.

Fortsättning på nästa sida.

Seminarier (fortsättning)

- On 11–21 kl. 16.00. KTH/SU Mathematics Colloquium.** John Ockendon, Oxford: *Open problems in dislocation mechanics and cold plasmas*. Seminarierum 3721, Institutionen för matematik, KTH, Lindstedtsvägen 25, plan 7. Kaffe/te serveras kl. 15.30 i pausrummet, Institutionen för matematik, KTH, Lindstedtsvägen 25, plan 4. Se Bråket nr 36 sidan 11.
- To 11–22 kl. 15.15–16.15. AlbaNova and Nordita Colloquium in Physics.** Jan Conrad, Fysikum, SU: *The Gamma-ray Large Area Space Telescope (GLAST)*. Oskar Kleins auditorium, Roslagstullsbacken 21, AlbaNova universitetscentrum. Se sidan 4.
- Fr 11–23 kl. 13.15–14.15. Graduate Student Seminar.** Andreas Strömbergsson, Matematik, KTH: *The Boltzmann-Grad limit of the periodic Lorentz gas*. Seminarierum 3721, Institutionen för matematik, KTH, Lindstedtsvägen 25, plan 7. Se Bråket nr 36 sidan 11.
- Fr 11–23 kl. 15.00. Small Talk Seminar.** Timothy Logvinenko: *NCCR's and Donaldson-Thomas theory on Calabi-Yau threefolds*. Seminarierum 3721, Institutionen för matematik, KTH, Lindstedtsvägen 25, plan 7. Se sidan 7.
- Må 11–26 kl. 13.00. Seminarium i statistik.** (*Observera dagen och lokalen!*) Vice riksbankschef Svante Öberg: *Riksbankens prognosförmåga*. Hörsal 5, plan 3, mellan hus B och hus C, SU, Frescati.
- Må 11–26 kl. 15.15–17.00. Seminarium i finansiell matematik.** Professor Esko Valkeila, Helsinki University of Technology: *Fractional Brownian motion as a model in stochastic finance*. Seminarierum 3733, Institutionen för matematik, KTH, Lindstedtsvägen 25, plan 7. Se sidan 6.
- Ti 11–27 kl. 10.00–11.00. Optimization and Systems Theory Seminar.** (*Observera dagen och tiden!*) Ling Shi: *Title to be announced*. Seminarierum 3721, Institutionen för matematik, KTH, Lindstedtsvägen 25, plan 7.
- On 11–28 kl. 11.00. Common SU KoF/KTH Theoretical Physics Seminar.** Sten Hellman, SU: *Discovering the expected with Atlas*. (The seminar is to be confirmed.) Sal FA31, Roslagstullsbacken 21, AlbaNova universitetscentrum.
- On 11–28 kl. 11.00–12.00. Kombinatorikseminarium.** (*Observera tiden!*) Urban Larsson: *2-pile Nim with a restricted number of move-size imitations*. Seminarierum 3733, Institutionen för matematik, KTH, Lindstedtsvägen 25, plan 7. Se sidan 7.
- On 11–28 kl. 13.15–14.15. Seminarium i analys och dynamiska system.** Paul Malliavin, Paris: *Title to be announced*. Seminarierum 3721, Institutionen för matematik, KTH, Lindstedtsvägen 25, plan 7.
- To 11–29 kl. 15.15–16.15. AlbaNova and Nordita Colloquium in Physics.** Jean-Philippe Bouchaud, Capital Fund Management & Saclay, France: *The subtle nature of financial random walks*. Oskar Kleins auditorium, Roslagstullsbacken 21, AlbaNova universitetscentrum. Se sidan 8.
- Fr 11–30 kl. 13.15–14.15. Graduate Student Seminar.** Brett Wick, University of South Carolina och KTH: *Title to be announced*. Seminarierum 3721, Institutionen för matematik, KTH, Lindstedtsvägen 25, plan 7.
-

PLURIKOMPLEXA SEMINARIET

David Jacquet:

Hartogsområden i \mathbb{C}^2 av klass C^1

Sammanfattning: Vi kommer att betrakta Hartogsområden på formen $H = \{(z, w) : z \in D, |w| < g(z)\}$ där D är en öppen disk. I fallet då den icke-negativa funktionen g är av klass C^2 har Christer Kiselman visat att H är \mathbb{C} -konvex precis om $-\log g^2$ är \mathbb{C} -konvex. Jag kommer att visa ett analogt resultat i C^1 -fallet. Beviset bygger på en annan sats som säger att om g är C^1 så är H \mathbb{C} -konvex precis om H är lineellt konvex. Med hjälp av detta kan vi också konstruera ett motexempel som visar att kontinuerliga \mathbb{C} -konvexa mängder inte låter sig karakteriseras av någon lokal rotationsinvariant egenskap hos avståndsfunktionen till randen.

Tid och plats: Tisdagen den 20 november kl. 10.15 i rum 306, hus 6, Matematiska institutionen, SU, Kräftriket.

LOGIKSEMINARIET STOCKHOLM-UPPSALA

Nicola Gambino: Sheaves of setoids

Abstract: One of the central notions in the development of constructive mathematics in Martin-Löf type theory is that of a setoid.

Setoids are types equipped with an equivalence relation and can be seen as the objects of a category with many good properties. The aim of the seminar is to show how this category supports a construction of sheaves, analogous to the one available for the category of classical sets. This will be done using ideas of Algebraic Set Theory, as introduced by Joyal and Moerdijk, and extending previous work of Moerdijk, Palmgren, and van den Berg.

This is joint work with Steve Awodey, Peter Lumsdaine, and Michael Warren, described in the preprint ArXiv:0711.1529v2.

Tid och plats: Onsdagen den 21 november kl. 10.30 i sal Å11167, Ångströmlaboratoriet, Uppsala universitet.

ALBANOVA AND NORDITA COLLOQUIUM IN PHYSICS

Jan Conrad:

The Gamma-ray Large Area Space Telescope (GLAST)

Abstract: The Gamma-ray Large Area Space Telescope (GLAST) mission is scheduled for launch by NASA in 2008. The main instrument (the Large Area Telescope, LAT) is an imaging, wide field-of-view, high-energy gamma-ray telescope, covering the approximate energy range from 20 MeV to more than 300 GeV, complemented by a secondary instrument (the GLAST Burst Monitor) extending the energy measurement down to 10 keV and providing a fast trigger for Gamma-ray bursts. In this talk I will give a description of the GLAST instruments and their status. Among the numerous physics questions targeted by the mission, I will focus on the search for Dark Matter annihilation signal and briefly discuss GLAST's potential for understanding of the mysterious Gamma-ray bursts.

Tid och plats: Torsdagen den 22 november kl. 15.15–16.15 i Oskar Kleins auditorium, Roslagstullsbacken 21, AlbaNova universitetscentrum.

Lansering av bok

Välkommen till lanseringen av boken *Att våga sitt tärningskast. Gösta Mittag-Leffler 1846–1927* av *Arild Stubhaug*. Boken har översatts till svenska av *Kjell-Ove Widman*. Lanseringen äger rum onsdagen den 28 november kl. 15.00 på Institut Mittag-Leffler, Auravägen 17, Djursholm. Boken kommer därvid att finnas tillgänglig till ett förmånligt pris.

De som vill närvara vid lanseringen skall anmäla sig till Marie-Louise Koskull, telefon 08-622 05 60, e-post koskull@mittag-leffler.se, senast måndagen den 19 november.

PRESENTATIONER AV EXAMENSARBETEN I MATEMATISK STATISTIK

Onsdagen den 21 november kommer fyra examensarbeten i matematisk statistik att presenteras vid Matematiska institutionen, SU. Lokalen för alla presentationerna är sal 31, hus 5, Matematiska institutionen, SU, Kräftriket.

De fyra examensarbetena kommer inom kort att finnas på sidan <http://www.math.su.se/matstat/reports/serieb>.

Tommy Andersson:

**Prevalens och förväntad återstående livslängd
som funktion av incidens och mortalitet.**

Utveckling och tillämpning av en modell för demens i en population

Sammanfattning: Föreliggande rapport ger en redogörelse för hur man kan konstruera en modell som beskriver prevalens (andel sjuka personer vid en viss tidpunkt) som resultat av incidens (andel friska personer som insjuknar under en viss tidsperiod) och mortalitet (andel personer som avlider under en viss tidsperiod). Dessutom beskrivs hur man kan konstruera en modell som skattar återstående livslängd uppdelad på friska och sjuka år. Avslutningsvis görs ett försök att beskriva en modell som, under vissa antaganden, säger något om framtiden.

Tid: Onsdagen den 21 november kl. 8.00.

Sandra Lundin:

**Ornstein-Uhlenbeck-processens egenskaper
vid modellering av finansiella tidsserier**

Sammanfattning: Vid handel med finansiella derivat är det önskvärt att så långt som möjligt kunna förutsäga instrumentets framtida utveckling. Genom att analysera historiska data är det möjligt att anpassa en modell som mer eller mindre beskriver tidsseriens utveckling. I denna uppsats studeras Ornstein-Uhlenbeck-processens egenskaper som modelleringsverktyg för räntor, valuta- och aktieindex. Det är sedan tidigare känt att räntor är s.k. mean-reverting, d.v.s. tenderar att dra sig till ett långsiktigt medelvärde. OU-processen passar därför som väntat relativt bra för att modellera räntor men mindre bra för valutor och aktieindex. En nödvändig del i modellanpassningen är att skatta OU-processens tre parametrar. Detta har gjorts med maximum-likelihood-metoden. Då det konstaterats att en viss tidsserie kan modelleras som en OU-process kan detta utnyttjas för att skapa en regelstyrd positionshantering för den aktuella tillgångsklassen. I detta examensarbete har detta gjorts genom att skapa en regel där två nyttofunktioner, total och riskjusterad avkastning, maximeras.

Tid: Onsdagen den 21 november kl. 9.00.

(Fortsättning på nästa sida.)

Stefan Ekwall:

Modell över det förväntade utfallet i en livförsäkringsportfölj

Sammanfattning: Föreliggande rapport ger en redogörelse för konstruktion och implementation av en sannolikhetsteoretisk modell, vilken beskriver det förväntade ekonomiska utfallet av en befintlig livförsäkringsportfölj. Ett livförsäkringskontrakts ekonomiska utfall beror på flera osäkerhetsfaktorer. Dels beror det på dödlighet och framtida kapitalavkastning, dels kan försäkringstagaren göra olika aktiva val som påverkar kontraktets ekonomiska utfall. Implementation av modellen sker i programmeringsspråket Matlab. Matlab är ett högnivåspråk som har specialiserats för att hantera matematiska funktioner på ett enkelt och effektivt sätt.

Tid: Onsdagen den 21 november kl. 10.00.

Jan-Erik Lundin:

**An evaluation approach of embedded options
and immunization strategies**

Abstract: New Accounting and Solvency regimes are soon standing at the insurance undertakings doorstep and with new rules on how to value the technical provisions. The embedded options such as surrender options and annuity conversion included in insurance policies must be valued and accounted separately as part of the technical reserve. The usage of Black-Scholes option pricing and option valuation will give a survey over the calculation of the extra amount of reserve needed to cover future contractual obligations to the policyholders. As the liabilities in an insurance company are at market value and we constantly have fluctuations in the market interest rates, it is important to be strategic in the hedging management. The most changes in the market interest rate occur during the first ten years, which smooths out to be almost a straight line. The appropriate management of fluctuations in the interest rate and its impact is called immunization and is an instrument to handle the problem of mismatch in present value and duration.

Tid: Onsdagen den 21 november kl. 11.00.

SEMINARIUM I FINANSIELL MATEMATIK

Esko Valkeila:

Fractional Brownian motion as a model in stochastic finance

Abstract: Geometric Brownian motion is a classical model in finance. Fractional Brownian motions are a family of Gaussian processes, and standard Brownian motion belongs to this family. The FBM family allows to model memory with an additional parameter. This is an attractive property concerning the pricing modes in finance, too. But if one replaces geometric Brownian motion by geometric fractional Brownian motion in pricing models, then one has difficulties with the arbitrage pricing axiom. In the talk I will give some new viewpoints concerning these difficulties.

Most of the talk is based on my recent work with C. Bender (Braunschweig), P. V. Gapeev (LSE), and T. Sottinen (Reykjavik).

Tid och plats: Måndagen den 26 november kl. 15.15–17.00 i seminarierum 3733, Institutionen för matematik, KTH, Lindstedtsvägen 25, plan 7.

ALGEBRA AND GEOMETRY SEMINAR

Torsten Ekedahl:

Non-triviality examples for $\{BG\}$

Abstract: This is the third piece in the neverending saga of the class of an algebraic stack. We shall give examples of finite groups such that the class of their classifying stacks (over an algebraically closed field of characteristic zero) is not equal to 1. No knowledge of the discussions in previous pieces will be required.

Tid och plats: Onsdagen den 21 november kl. 13.15–15.00 i seminarierum 3733, Institutionen för matematik, KTH, Lindstedtsvägen 25, plan 7.

SMALL TALK SEMINAR

Timothy Logvinenko:

NCCR's and Donaldson-Thomas theory on Calabi-Yau threefolds

Abstract: We review recent work by Balasz Szendroi which defines an analogue of Donaldson-Thomas invariants on a quiver algebra which is an NCCR (non-commutative crepant resolution) of a threefold conifold singularity $\{x_1x_2 - x_3x_4 = 0\}$. They are then shown to be directly linked to the ordinary Donaldson-Thomas invariants of ordinary, commutative crepant resolutions.

Tid och plats: Fredagen den 23 november kl. 15.00 i seminarierum 3721, Institutionen för matematik, KTH, Lindstedtsvägen 25, plan 7.

KOMBINATORIKSEMINARIUM

Urban Larsson:

2-pile Nim with a restricted number of move-size imitations

Abstract: We study a variation of the combinatorial game of 2-pile Nim. Move as in 2-pile Nim but with the following constraint:

Provided the previous player has just removed, say $x > 0$ tokens from the pile with a less number of tokens, the next player may remove x tokens from the pile with more tokens. But for each move, in “a strict sequence of previous player – next player moves”, such an *imitation* takes place, the value of an *imitation counter* is increased by one unit. As this counter reaches a predetermined natural number, then by the rules of this game, if the previous player once again removes a positive number of tokens from the pile with less tokens, the next player may not remove this same number of tokens from the pile with more tokens.

We show that the winning positions of this game in a sense resembles closely the winning positions of the game of Wythoff Nim — more precisely a version of Wythoff Nim with a Muller twist. In fact, we show a slightly more general result in which we have relaxed the notion of what an imitation is.

As a round off, given that the first player knows the winning strategy for a particular game, we discuss a successful “learning” strategy for the second player.

Tid och plats: Onsdagen den 28 november kl. 11.00–12.00 i seminarierum 3733, Institutionen för matematik, KTH, Lindstedtsvägen 25, plan 7.

ALBANOVA AND NORDITA COLLOQUIUM IN PHYSICS

Jean-Philippe Bouchaud:

The subtle nature of financial random walks

Abstract: It is known since Bachelier 1900 that price changes are nearly uncorrelated, leading to a random-walk like behaviour of prices. However, compared to the simplest Brownian motion, price statistics reveal a large number of anomalies, such as fat tails and long memory in the volatility.

The detailed study of trade by trade and order book data allows one to provide evidence for a subtle compensation mechanism that underlies the ‘random’ nature of price changes. This compensation drives the market close to a critical point, which may explain the sensitivity of financial markets to small perturbations, and their propensity to enter bubbles and crashes.

We argue that the resulting unpredictability of price changes is quite far from the neo-classical view that markets are informationally efficient.

Tid och plats: Torsdagen den 29 november kl. 15.15–16.15 i Oskar Kleins auditorium, Roslagstullsbacken 21, AlbaNova universitetscentrum.

MASTER LEVEL COURSE IN BIOSTATISTICS

Ola Hössjer and Juni Palmgren:

BMC2: Course in Population Genetics and Gene Mapping

The course will be given at Stockholm University, and it is worth 7.5 ECTS points.

Summary: Changes of human DNA over time is a combination of random inheritance (Mendelian laws), recombination of maternal and paternal DNA, mutations and selection principles. This is conveniently described using tools from probability theory and stochastic processes. The population genetic models so obtained are important for understanding variation of DNA between individuals and populations. This in turn has applications for 1) human ancestry and estimating age of populations, 2) locating genes that increase risk for inheritable diseases (gene mapping). The course will focus on mathematical and statistical principles of population genetics and gene mapping. We present concepts of molecular genetics and discuss population genetic models, coalescent theory, familial aggregation, segregation analysis, linkage analysis, testing of candidate gene associations, genome-wide association and linkage disequilibrium mapping.

This course is the second in a Nordplus programme, starting during Fall 2007, where the Universities of Stockholm, Oslo, Helsinki, and Copenhagen jointly organize a set of Master level courses in Biostatistics. The Universities in Newcastle and Gent also take part in this collaboration.

Master- and Ph.D.-students from the collaborating universities as well as from other universities are welcome to take part in the courses.

Deadline for application for the course on Population Genetics and Gene Mapping is Monday, December 3, 2007.

Details about the course are provided at <http://www.math.su.se/matstat/biostat/BMC2>.

Information about the network and the other courses which it offers is given at <http://www.math.su.se/matstat/biostat/BMC-Network>.

Please, feel free to spread this information!

Juni Palmgren

WENNER-GREN FOUNDATIONS DISTINGUISHED LECTURE

Jacques Stern:

Cryptography in financial transactions:

Current practice and future directions

Professor Jacques Stern is Director of the Computer Science Department (LIENS) at École Normale Supérieure in Paris and father of a school of cryptology in France, which is at the forefront of the discipline in Europe. He has published about 150 scientific articles between 1975 and 2006. Since September 2007, Professor Stern is also chairman of the French National Agency for Research (ANR).

Abstract: In this talk I will briefly describe the history of cryptography and explain how it became an area of scientific research, served by a strong community both in academia and in the industry. Next I will cover two case studies. The first is related to banking cards and payment terminals, and the second to Internet banking. In both cases, I will show how cryptographic tools crafted within the research community in the past thirty years entered the picture and how cryptographers were able to provide stronger and stronger levels of security. While applications are now stable in the first area, there is more to come in the second.

Aims and presentation of cryptology or the “Science of secrecy”: For many years, cryptology was used for military and diplomatic issues. It is a young science which developed with the arrival of digital computing and telecommunication after World War II. In 1976 the concept of “public key” was born, and in 1986 cryptology became an academic field of study. Now cryptology is part of our daily life: Internet (login), bank (secret code numbers), mobile telephone (SIM card), satellite TV decoders, medical ID cards, transport documents, cable, etc.

The aims of cryptology are to ensure the integrity of information, its authenticity and the confidentiality of data and transactions.

Cryptology is divided into cryptography and cryptanalysis. *Cryptography* relates to the design of mechanisms intended to guarantee security notions. *Cryptanalysis* involves attempts to penetrate cryptographic systems, especially in order to discover exactly what degree of real security it actually provides.

Tid och plats: Onsdagen den 21 november kl. 15.00 i sal D3, KTH, Lindstedtsvägen 5, b.v.

MONEY, JOBS

Columnist: Johannes Lundqvist, Department of Mathematics, Stockholm University.
E-mail: johannes@math.su.se.

Info = information. This will be given and repeated until obsolete. Rely on other sources as well.

BBKTH = Bulletin Board at the Department of Mathematics, KTH.

BBSU = Bulletin Board at the Department of Mathematics, SU.

The following information, with links, is also available at <http://www.math.su.se/~johannes/mj.html.en>.

Unless stated otherwise, a given date is the last date (e.g. for applications), and the year is 2007. A number without an explanation is a telephone number.

Standard information channels

1. A channel to information from Vetenskapsrådet: <http://www.vr.se/naturteknik/index.asp>.
2. A channel to information from the European Mathematical Society: <http://www.emis.de>.
3. A channel to information from the American Mathematical Society: <http://www.ams.org>.
4. KTH site for information on funds: <http://www.kth.se/aktuellt/stipendier>.

(Continued on the next page.)

5. Stockholm University site for information on funds: <http://www2.su.se/forskning/stipendier/databas.php3>.
6. Umeå site for information on funds: http://www.umu.se/umu/aktuellt/stipendier_fond_anslag.html.
7. Job announcement site: <http://www.maths.lth.se/nordic/Euro-Math-Job.html>. This is run by the European Mathematical Society.
8. Stiftelsen för internationalisering av högre utbildning och forskning (STINT) site for information on funds: <http://www.stint.se>.
9. Nordisk Forskerutdanningsakademi (NorFA) site for information on funds: <http://www.norfa.no>.
10. Svenska institutet (SI) site for information on funds: <http://www.si.se>.

Old information

Money to apply for

11. Institut Mittag-Leffler utlyser postdoktorala stipendier för verksamhetsåret 2008/09. Ämnesområdet för hösten 2008 är: "Geometry, analysis and general relativity". Ämnesområdet för våren 2009 är: "Discrete probability". Sista ansökningsdag är den 31 januari 2008. Web-info: <http://www.mittag-leffler.se/programs/0809/grants.php>.
12. Stiftelsen Längmanska kulturfonden utlyser bidrag för att främja bl.a. naturvetenskaper. Bidrag ges främst till särskilda ändamål, däremot inte till löpande verksamhet, periodiska skrifter och dylikt. Beviljade belopp är i regel i storleksordningen 15 000 – 40 000 kr. Sista ansökningsdag är den 15 januari 2008. Web-info: <http://www.langmanska.se/>.
13. Stiftelsen P. E. Lindahls fond utlyser två stipendier om vardera 150 000 kronor för vetenskapliga studier eller fortsatt praktisk utbildning i naturvetenskapliga ämnen inom eller utom Sverige. Sökande skall ha avlagt doktorsexamen år 2002 eller senare eller vara behörig att antagas till forskarutbildning och får inte inneha tjänst hos stat eller kommun. Tidigare har prioritering givits till nydisputerade forskare samt seniora forskare som är i behov av bidrag till fortsatt utbildning, exempelvis i form av resa/vistelse vid annat universitet. Sista ansökningsdag är den 17 december. Web-info: http://www.kva.se/KVA_Root/swe/awards/scholarships/detail_scholarships.asp?grantsId=15.

Jobs to apply for

14. Lunds universitet söker en biträdande universitetslektor i matematisk statistik med inriktning mot statistiska metoder inom livsvetenskaper. Sista ansökningsdag är den 14 december. Web-info: http://www.naturvetenskap.lu.se/upload/LUPDF/natvet/Utlysningar/071123_3463.pdf.
-