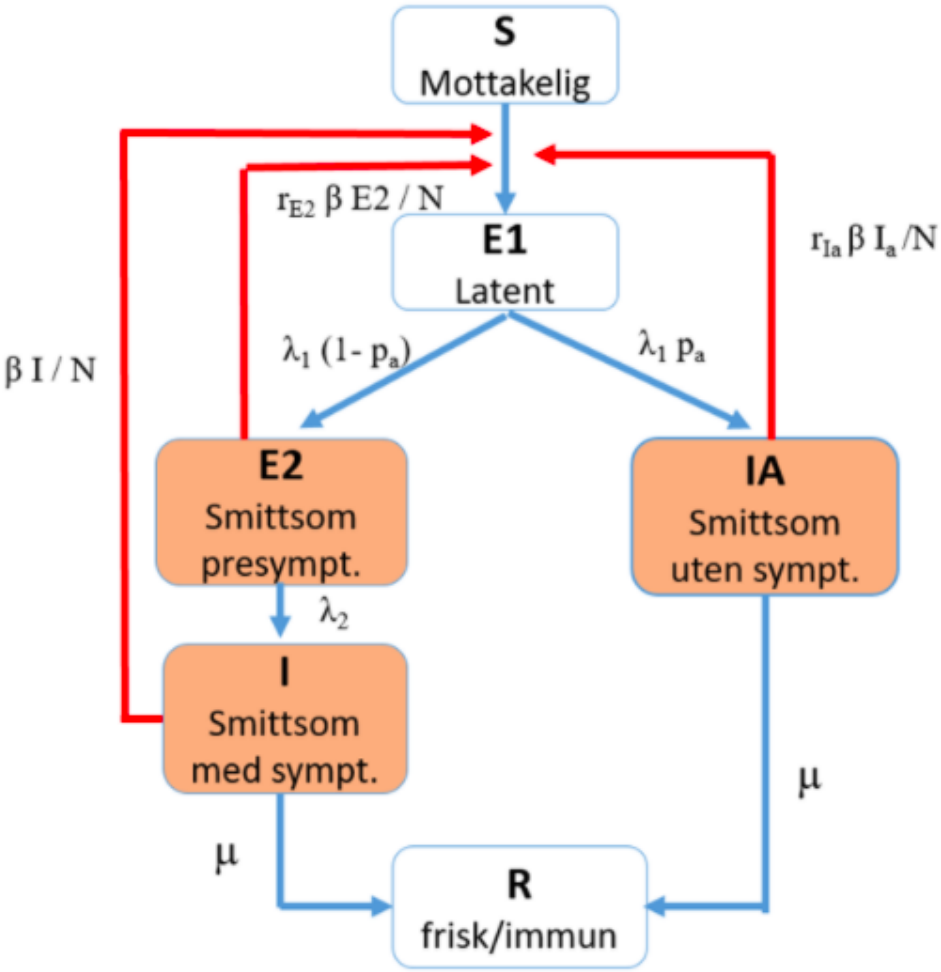
INFOMAT

APRIL 2020



INFOMAT kommer ut med 11 nummer i året og gis ut av Norsk Matematisk Forening. Deadline for neste utgave er alltid den 15. i neste måned. Stoff til INFOMAT sendes til

arnebs at math.uio.no

Foreningen har hjemmeside http://www.matematikkforeningen.no/
Ansvarlig redaktør er Arne B. Sletsjøe, Universitetet i Oslo

Matematisk kalender

På grunn av den pågående situasjonen mht koronaviruset kan flere av arrangementene bli utsatt eller avlyst. Følg med på web-sidene.

Mai:
18.-20. Abelprisutdeling, Oslo [AVLYST, DELES UT NESTE ÅR]

Juni:
2.-6. Sommerskole: ***Mathematics and Data***, Tromsø [UTSATT TIL HØSTEN 2020] <https://mathdat.puremath.no/>
22.-26. Sommerskole:Topics in real algebraic geometry, Nordfjordeid [AVLYST] <https://www.mn.uio.no/math/english/about/collaboration/nordfjordeid/conferences/real-alg-geo-2020/>
25.-30. 10th International Conference on Mathematical Methods for Curves and Surfaces, Oslo [UTSATT TIL SOMMEREN 2021] <www.mn.uio.no/MMCS10>

September:
3.-4. Nasjonalt matematikermøte, Trondheim <https://www.ntnu.no/imf/matematikermote>
28.-29. Mathematics without Borders, IMU 100 år,Strasbourg

November/desember:
30.-4. Vinterskole: ***Geometry and analysis of quantum groups***, Oslo <https://www.mn.uio.no/math/english/research/groups/operator-algebras/events/conferences/ge-anqg-2020/index.html>

NYTT OM ÅRETS ABELPRISUTDELING

På grunn av Koronapandemien er alle arrangementer knyttet til Abelprisuken 2020 avlyst. Abelprisvinnerne Hillel Furstenberg og Gregory Margulis vil bli hedret sammen med neste års Abelprisvinner under neste års prisseremoni som finner sted 25. mai 2021.

NYTT OM NASJONALT MATEMATIKERMøTE 2020

Dear Colleagues,
We hope this message finds you and your families and friends well!
We are monitoring the current health situation. Since the Nasjonalt Matematikermøte i Trondheim is scheduled for early September 2020 we'll take the final decision whether to hold the meeting on Monday, June 15.
Meanwhile, we are happy to announce the speakers:
Plenary speakers:
G. Dahl (UiO)
G. Fløystad (UiB)
M. Rognes (Simula)
K. Seip (NTNU)
Elizabeth Stephansen plenary lecture:
E. Malinnikova (NTNU/Stanford)
Viggo Brun prize plenary lecture: TBA

Session speakers: **K. Rognlien Dahl** (UiO) **F. Godtliebsen**(UiT) **K. Grunert** (NTNU) **B. Krugilov** (UiT) **A. Massing** (NTNU) **H. Munthe-Kaas** (UiB) **T. K. Nilssen** (UiAgd) **C. Riener** (UiT) **S. Selberg** (UiB) **K. Shaw** (UiO) **S. H. Sørbye** (UiT) **V. Vitelli** (UiO)

Kind regards,
Organising committee
K. Ebrahimi-Fard, S. Grepstad, G. Quick

Nye doktorgrader

Yihan Cao ved NTNU forsvarte 3.april 2020 sin avhandling *Statistical methods for estimating fluctuating selection* for graden PhD.
Hovedveileder har vært Professor Jarle Tufto, NTNU, og medveileder Professor Marcel Visser, Wageningen University.

Sammendrag:
Linking the sources of natural selection to the dynamics of evolution has been a major goal of evolutionary biology, however, the lack of a unified framework to quantify the fluctuations in selection

accurately has hampered this progress. Previous empirical findings show that fitness landscapes are not constant over time, and populations are evolving towards a continuously changing fitness optimum. A more statistically robust approach, however, is needed to be applied to a wider range of species, populations, and traits.

This thesis contributes to this end by showing how current methods for estimating fluctuations in selection can be extended using a more flexible statistical framework. In the first chapter, state-space models (SSMs) are used to analyse phenotypic selection and Template Model builder (TMB), an R package for model-fitting. With a long-term great tit (Parus major) dataset, we fit several SSMs for fluctuated directional or autocorrelated stabilizing selection on breeding time of the great tit population. The selected model shows that there is directional selection on the probability of breeding failure, and stabilizing selection on the mean number of fledglings. To explain the observed declining frequency of double brooding in the study population, in the second chapter, a simple quantitative genetic model is formulated for the evolution of double versus single brooding. In the third chapter, the SSMs models in chapter 1 are expanded to include four selective episodes to estimate selection on laying date. Meanwhile, ecological variables are considered to explore ecological drivers of variation in selection. The method can be alternatively implemented in the Bayesian framework by taking prior information into account and using the Bayesian inference tool tmbstan. Therefore, in chapter 4, the simulation and empirical studies, in the context of estimating fluctuating selection, are conducted and by doing this we conclude that turning on Laplace approximation in tmbstan would probably reduce computational efficiency but it is worth trying when there is a good amount of data.

M.Sc. **Herman Galteland** ved NTNU forsvarte 15.april 2020 sin avhandling *Malicous cryptography* for graden PhD.
Hovedveileder har vært Professor Kristian Gjøsteen, NTNU, og medveileder Professor Colin Alexander Boyd, NTNU.

Sammendrag:(Sakset fra Introduksjonen til Galtelands avhandling)
Historically, cryptography has been a tool for the defender. In this thesis we discuss malicious uses of cryptography and countermeasures to such use. That is, we study how attackers could use cryptography to make the defender's work harder, and how such techniques can be countered by the defender. The goal of this thesis is not to develop new attacks, but to understand possible future threats. This is important, because to prepare for future attacks we must know what to defend against. Obviously there is an ethical dilemma here, we have tried to balance this by only considering theoretical studies. We have not developed attack code. We also note that some tools and techniques studied in this thesis are dual-use, technologies that can be used by both a defender and an attacker. The Tor network, and other anonymity networks, is used to avoid surveillance and censorship, but can also be used to hide attackers. Similar for subliminal channels.

Malicious cryptography started with Young and Yung and their submission to the 1996 IEEE Security & Privacy conference, where they proposed malware that encrypts the local files on the infected computer and holds them for ransom. The malicious code generates a symmetric encryption key on the infected computer and uses it to encrypt files. The symmetric key is then encrypted using a public encryption key stored in the code, where the malware author has the secret decryption key. The owner of the infected computer is notified and to recover the symmetric key, and the encrypted files, the owner has to pay the malware author and send the encrypted symmetric key. Using the secret decryption key the malware author decrypts the symmetric key and sends it back, so that the owner can recover their files. This attack was called cryptoviral extortion by Young and Yung. Today such malware is commonly known as ransomware. With the paper Young and Yung showed how malware can use cryptography and by publishing the paper they gave the security community time to prepare. Young and Yung continued this line of work and called it cryptovirology.

This thesis consists of six papers and they appear in logical order, not chronological order. In Section 1 we introduce the two principal actors of this thesis, and discuss the techniques we have

studied that the attacker use. In Section 2 we discuss the countermeasures we have studied that the defender use.

NYTT FRA IMU

Dear ICMI Country Representatives,
I hope this finds you and your families and friends in good health.
Although the ICME14 has been postponed to July 2021, a main item of the General Assembly, which is the election of the new EC must take place this year. This will enable the new EC to take office on January 1, 2021.
Give the current global situation, the only option we have is to hold the election electronically. Fortunately, in our world today this is possible. The EC has thus decided to hold the election in July 2020 as planned. Since all previous elections have taken place during a General Assembly, we will need to make some adjustments this time; however, making sure at the same time, to abide by the Terms of Reference1 within which ICMI operates. Following the procedures carefully will ensure that we will hold a fair, transparent, and secure process. We intend to send out detailed procedures for the election by late April.

Sincerely yours,
Abraham Arcavi
ICMI Secretary General

HOLMBOEPRISEN TIL ANNE SELAND, FLEKKEFJORD VGS.

Norsk matematikkråd har tildelt Holmboeprisen for 2020 til Anne Seland ved Flekkefjord vgs..

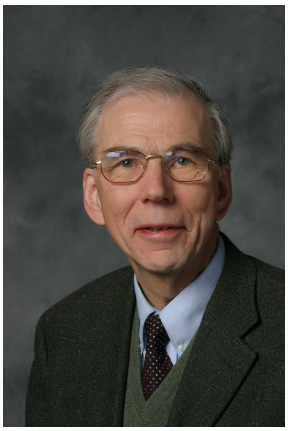
- *Prisvinneren er en svært dyktig, grundig og engasjert lærer, med en uvanlig stor arbeidskapasitet*, skriver priskomiteen. Bent Michael Holmboes minnepris - Holmboeprisen, tildeles årlig en eller
flere lærere som har utmerket seg innen god undervisning i matematikk. Priskomiteen som har jobbet med å finne årets prisvinner understreker spesielt Selands vektlegging av å fremme elevenes matematiske forståelse fremfor pugging av formler.
- *Vi må ikke redusere elevene til å bli avanserte utregningsroboter. Forståelse av de matematiske sammenhengene er avgjørende for å anvende matematikken videre. Norge trenger flere matematikere, naturvitere, statistikere og teknologer. Dette er en forutsetning for omstillingen i samfunnet etter oljen, og for det grønne skiftet. Da må forståelsen være på plass*, sier leder av Norsk Matematikkråd Antonella Zanna Munthe-Kaas, som er svært fornøyd med årets valg av prisvinner.
Priskomiteen har også vektlagt prisvinners jakt etter nye undervisningsmåter som kan gi elevene en dypere forståelse av mønstre, systemer og sammenhenger i matematikkfaget. Dette er noe som i stor grad preger undervisningen til Anne Seland.

Årets hederlige omtale gikk til Ellen Egeland Flø, Mailand videregående skole.
Les hele komiteens omtaler her: https://holmboeprisen.no/
Kort om Holmboeprisen:
- Prisen ble opprettet i 2005 av Norsk matematikkråd.
- Prisbeløpet er på 100 000 kr og deles likt mellom prisvinner og prisvinners skole
- Prisen deles vanligvis ut av Kunnskaps- og integreringsministeren i en høytidelig seremoni på Oslo Katedralskole i mai. (Årets utdeling er utsatt til 2021)

JENS ERIK FENSTAD (1935-2020)

Det var med dyp sorg vi mottok budskapet om at Jens Erik Fenstad, professor i matematisk logikk ved Universitetet i Oslo, døde 14. april, dagen før han ville ha fylt 85 år.
Jens Erik og hans kone Grete ble smittet av koronavirus på ferie i Spania i mars. Grete fikk sykdommen i mild grad, men Jens Erik ble innlagt på Bærum sykehus og døde der.
Jens Erik Fenstad har vært en nøkkelperson i

utviklingen av logikk i Norge, gjennom egne arbeider og ved sin store innsats for å bygge opp et godt og bredt logikkmiljø ved Universitetet i Oslo. Han har også spilt en viktig rolle i norsk og europeisk forskningssamarbeid og forskningsledelse.



Fenstad ble født i Trondheim. Etter artium begynte han i 1954 å studere teknisk fysikk hos Harald Wergeland på NTH. Etter militærtjenesten dro han i 1956 til Oslo for å studere filosofi og matematikk, etter hvert matematikk full tid. Matematisk institutt i Oslo var den gang i en viktig overgangsperiode. Den eldre generasjon, Carl Størmer, Thoralf Skolem, Viggo Brun og Ralph Tambs Lyche, gikk alle av før eller like etter at Fenstad begynte sine studier. Fenstad oppdaget raskt Thoralf Skolems enestående innsikter og hadde gode og viktige samtaler med ham. Også Karl Egil Aubert, 40 år yngre enn disse, fikk stor betydning for Fenstads utvikling som matematiker. Samarbeidet med Ingebrigt Johansson var også viktig. I 1961 startet Johansson, Fenstad og Stål Aanderaa et seminar i logikk, som fikk stor betydning for fremveksten av kompetanse i logikk og tverrfaglige anvendelser av logikken. Gjennom dette seminaret og videregående forelesninger og seminarer ble Fenstad en drivende kraft for logikk og matematikkens filosofi i Norge. Han samarbeidet også med Lindstrøm, Raphael Høegh-Krohn og Sergio Albeverio om boken "Nonstandard Methods in Stochastic Analysis and Mathematical Physic".

Fenstads inngående studium av god begrunnelse førte ham til å legge stadig større vekt på sammenheng. Dette gjenspeiles i titlene på hans mange bøker og artikler opp gjennom årene. Der tar han opp spørsmål fra en rekke ulike fagområder, ikke bare logikk, matematikk og naturvitenskap, men også samfunnsvitenskap og humaniora. Ikke bare filosofien og logikkmiljøet har nytt godt av Fenstads innsats. Et eksempel er et seminar for lingvister, som Fenstad og jeg drev i samarbeid med blant annet psykologen Ragnar Rommetveit, der noen av de mest lovende unge lingvister deltok. Noen har frabedt seg denne inntrengingen av logikere på deres fagområder, og hevder at den er irrelevant og fører til en avsporing av deres fag. Men Fenstads bidrag besto ikke i å avfeie deres studier, men å sette dem inn i en videre sammenheng. Dette gjelder også logikken og matematikken selv. Vektleggingen av argumentasjon og begrunnelse har avdekket sammenhenger som man tidligere ikke var oppmerksom på. Titlene på Fenstads mange bøker og artikler avspeiler dette. Kapitteloverskriftene i hans siste bok "Structures and Algorithms" (2018) gir gode eksempler, som: "Mathematics and the Nature of Knowledge", "Remarks on the Science and Technology of Language", "How Mathematics is Rooted in Life".

I tillegg til dette store og vidtfavnende nybrottsarbeidet har Fenstad brukt mye av sitt liv og sin arbeidsinnsats på å studere og gjøre tilgjengelig Thoralf Skolems betydningsfulle bidrag til matematikken og logikken. Fenstad redigerte hans skrifter og fikk dem utgitt i samlet utgave, og skrev mange inngående analyser av Skolems bidrag. Skolem var meget beskjeden og var lenge lite kjent utenfor logikernes rekker. Et unntak er Oxford University, hvor det utenfor matematisk institutt står en minnesten med navnene på historiens viktigste matematikere inngravert. Der står det to navn fra Norge: Niels Henrik Abel og Thoralf Skolem. Fenstad har også, sammen med en del andre, tatt initiativet til de årlige Skolemforelesninger ved Matematisk Institutt, Universitetet i Oslo.

Fenstad brukte mye av sin tid til organisatorisk arbeid. Han har vært prorektor og fungerende rektor ved Universitetet i Oslo, var en fremragende første formann i Abelstyret, president i International Union of History and Philosophy of Science, og har hatt en rekke lederverv i de europeiske vitenskapelige organisasjoner. I 1998 ble han æresdoktor ved Universitetet i Uppsala og i 2011 Ridder av St. Olavs Orden.

Jens Erik vil bli sterkt savnet.
Våre tanker går til Grete, Anne Marie, Håkon og Erik og barnebarna.

På vegne av kolleger og venner,
Dagfinn Føllesdal
(Sakset fra Klassekampen, 18. april 2020)