Matilde 12 foreligger ikke som samlet PDF-fil. Dette dokument er en samling af de HTML- og PDF-filer der var at finde i Matilde arkivet vedr. Matilde 12.

MATH-AU
2015-11-18

Fejlrettende koder

T. Høholdt

Institut for Matematik
Danmarks Tekniske Universitet Bg. 303
DK-2800 Kgs.Lyngby

February 15, 2002

1 Indledning

I to banebrydende artikler fra 1948 [1] introducerede Claude Shannon , der døde sidste år, begrebet kommunikationskanaler samt de fejlrettende koder der benyttes ved kommunikation over sådanne kanaler. Siden da er teorien blevet videreudviklet både af matematikere og ingeniører og i dag indgår koderne i en lang række anvendelser blandt andet i tekstTV, i CD- og DVD-afspillere og satellit kommunikation [2]. Vi giver en kort indføring i teorien og berører de seneste års anvendelse af algebraisk geometri indenfor området.

2 Kodningsteori

For en matematiker er en (n, k) kode C over $\mathbb{F}_q$ et k-dimensionalt underrum af vektorrummet $V = ({\mathbb{F}_q}^n, +, \mathbb{F}_q)$ hvor $\mathbb{F}_q$ er et endeligt legeme med q elementer. Elementerne i C kaldes *kodeord*. Vektorrummet V forsynes med den såkaldte Hamming metrik hvor afstanden mellem to vektorer er antallet

af positioner hvor de to vektorer har forskellige elementer. Kodens *minimum afstand*, som vi vil kalde d er så den mindste afstand mellem forskellige kodeord og koden kan rette t fejl netop hvis $t < \frac{d}{2}$.

Der gælder altid $d \leq n-k+1$, thi hvis man fjerner $d-1$ bestemte positioner fra alle de q^k kodeord må de afkortede ord være forskellige og derfor er $q^k \leq q^{n-(d-1)}$.

Koden benyttes på den måde at man egentlig har q^k forskellige meddelelser man vil sende og vælger så en bijektiv afbildning fra disse ind i C og sender kodeordene, der altså har længde n i stedet for. Fidusen ved de $n-k$ redundante symboler er at de kan udnyttes til at rette eventuelle fejl der opstår under kommunikationen. Hvordan dette gøres effektivt er et emne for den aktuelle forskning, her vil vi koncentrere os om at beskrive et par konstruktioner af gode koder hvorved vi forstår koder med stor minimum afstand.

Vi beskriver først de såkaldte Reed-Solomon koder (efter opdagerne).

Definition 1
Lad $P = \{P_1, \ldots, P_n\} \subseteqq \mathbb{F}_q$ *med* $|P| = n$. *For* $k \leq n$ *kaldes mængden*

$$RS(P,k) = \{f(P) | f \in \mathbb{F}_q[x],\ grad(f(x)) < k\},$$

hvor $f(P) = (f(P_1), \ldots, f(P_n))$
en Reed-Solomon *kode*.

Ideen er her at man *indkoder* k informationssymboler $i_0, i_1, \ldots, i_{k-1}$ i kodeordet $(i(P_1), \ldots, i(P_n))$ hvor $i(x) = i_0 + i_1 x + \ldots + i_{k-1}x^{k-1}$.

Det er selvfølgelig klart at man hermed får en (n,k) kode. Da et polynomium af grad højst $k-1$ højst har $k-1$ nulpunkter er der altså mindst $n-k+1$ ikke nul symboler i ethvert kodeord ($\neq 0$), så afstanden mellem 0-ordet, der jo også er et kodeord og ethvert andet kodeord er altså mindst $n-k+1$. Men da koden er et underrum betyder det at minimum afstanden også er mindst dette tal og som vi så ovenfor kan den heller ikke være større. Vi har altså $d = n-k+1$ for Reed-Solomon koderne.

Reed-Solomon koder anvendes i CD- og DVD afspillere med $q = 2^8$. Det fremgår af konstruktionen at man højst kan opnå at $n = q$ så på denne måde kan man ikke konstruere gode binære ($q = 2$) koder. Alligevel kan man få en ide til at gå videre , den fik V.D.Goppa i 1979 [3]. Man kan opfatte

elementerne i $\mathbb{F}_q$ som punkter på den affine linie og Reed-Solomon koderne fås så ved at evaluere polynomier i disse punkter. Goppa's ide er nu at tage punkter fra en algebraisk kurve (i et rum af mange dimensioner) og evaluere rationale funktioner fra et vektorrum knyttet til kurven i disse punkter. Med denne teknik er det faktisk lykkedes at konstruere (asymptotisk) gode koder. Det kan man læse mere om i [4].

References

[1] C.E.Shannon: " A mathematical theory of communication", Bell System Tech.J. vol.27 pp.379-423, 623-656 1948.

[2] (V.S.Pless og W.C.Huffman eds.):"Handbook of Coding Theory" Elsevier 1998.

[3] V.D. Goppa : " Codes on Algebraic Curves" Dokl.Akad.Nauk SSSR 259 pp.1289-1290 1981.

[4] T.Høholdt, J.H.van Lint og R. Pellikaan:" Algebraic Geometry Codes" Chapter 10 i Handbook of Coding Theory pp.871-961

Af Marc Skov Madsen PhD-studerende Aarhus Universitet email: marc@imf.au.dk

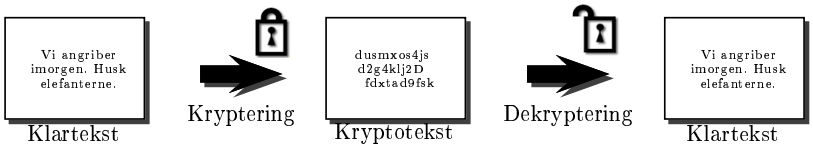
1 Besøgstjenesten

Jeg vil gerne brug lidt spalteplads til at reklamere for besøgstjenesten ved Institut for Matematiske Fag i Aarhus. Vi er to PhD.-studerende som er ansat til at tage ud og formidle matematik. Det kan være sig i form af eksempelvis foredrag. Jeg har også været med til at opbygge en matematikstand som kan byde på verdens hurtigste rutchebane (cykloiden). Den kommer jeg også gerne ud og stiller op.

Nedenstående artikel om kryptografi er bygget over et foredrag, som jeg har holdt, for gymnasieelever. Foredraget kan bestilles ved at skrive til marc@imf.au.dk.

2 Kryptografi

Kryptografi er læren om, hvordan en "tekst" skrevet i et sædvanligt sprog, kan forvandles så teksten bliver uforståelig for uvedkommende, men så den godt kan læses af indviede. Selve processen kan skitseres som følger.



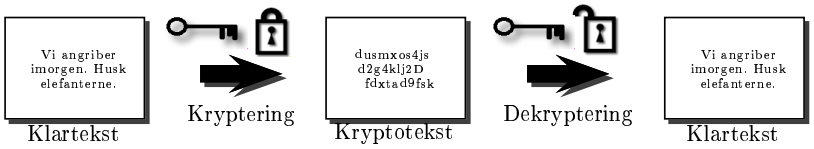
Læg mærke til at "kryptering" svarer til at låse teksten, mens "dekryptering" svarer til at låse den op igen.

3 Alice, Bob og Eva

Vi forestiller os den situation, at Alice er en person som gerne vil sende en hemmelig besked til Bob, eksempelvis over internettet, og Eva er en "spion", der ønsker at aflytte og forstå den hemmelige besked.

3.1 Konventionelt kryptosystem

I gamle dage (*konventionelt kryptosystem*) ville Alice og Bob have mødtes for at få et kryptosystem baseret på en fælles nøgle ( ) op at stå. Det kunne være de eksempelvis aftalte at forskyde bogstaverne i alfabetet 3 pladser, så eksempelvis beskeden "hej" ville blive til "khm". Det skal bemærkes at kryptering ved ombytning af enkeltbogstaver let kan brydes ved frekvensanalyse. Et konventionelt kryptosystem kan illustreres som følger



Konventionel kryptering har det problem, at det kan være både for dyrt og besværligt for Alice og Bob at få aftalt en fælles nøgle. Prøv eksempelvis at forestille dig, at Alice bor i Ansager og Bob i Bilbao!

3.2 Public Key kryptering

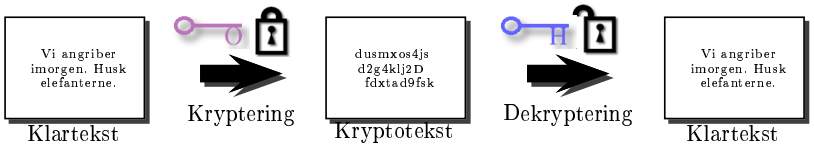
I et Public Key kryptosystem behøves Alice og Bob ikke at mødes før de kan kommunikere hemmeligt over nettet. Der sker nemlig det, at Bob laver

- en *offentlig nøgle* (O)
- og en *hemmelig nøgle* (H).

Den offentlige lægger Bob ud på nettet så alle kan finde den. Den hemmelige nøgle gemmer han eksempelvis på sin harddisk.

Når Alice vil skrive til Bob skal hun blot gå ud på nettet, slå hans offentlige nøgle op og bruge den til at låse/ kryptere med.

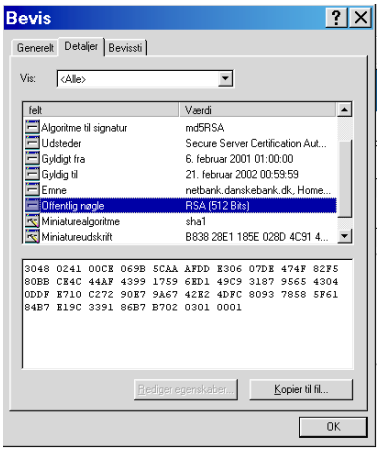
Når Bob vil dekryptere en besked, så bruger han sin hemmelige nøgle.



Det viser sig at man vha. matematiske emner som talteori, gruppeteori og algebraisk geometri kan lave en del forskellige praktiske Public Key kryptosystemer. Vi vil nu se nærmere på det mest anvendte eksempel.

4 RSA

RSA systemet blev udviklet af Rivest, Shamir og Adleman i 1977, og det bruges idag i bl.a. Internet Explorer og Netscape Navigator. Dermed bruges det også, når man bruger homebanking. Vi kan f.eks. tage et kig på Danske Netbanks offentlige nøgle.



5 Matematikken bag RSA

For at kunne få indblik i RSA kryptering skal man ihvertfald kende lidt til *restregning* og *primtal*.

5.1 Division med rest

Matematikere ynder at skrive ting op som sætninger. Her er sætningen om *division med rest*.

Sætning 5.1 (Division med rest). *For alle positive, hele tal m og d findes præcis et helt tal q og et helt tal r så*

$$m = qd + r, \quad 0 \leq r < d$$

Et eksempel er at $17 = 3 \times 5 + 2$. Vi siger at der er 2 til rest.

Vi vil skrive $m \mod d$ for resten ved division af m med d. Så eksempelvis $35 \mod 6 = 5$. Hele pointen er nu at vi kan regne med rester! Det siger følgende sætning nemlig.

Sætning: Antag m, n og d er hele, positive tal. Lad $m' = m \mod d$ og $n' = n \mod d$. Da gælder

$$m \times n \mod d = m' \times n' \mod d$$

Vi kan tage et eksempel, hvor vi bruger sætningen: $98 * 99 \mod 95 = 3 * 4 \mod 95 = 12$.

5.2 Primtal

Et *primtal* p er et tal > 1 som kun har 1 og p som divisorer. Eksempler er $2, 3, 5, 7, 11, 13$ og 3243542347. Grunden til, at primtallene er så vigtige, er, at de er byggestenene for de hele tal.

Sætning 5.2 (Entydig faktorisering). *Ethvert helt, positivt tal større end* 1 *kan på entydig vis faktoriseres i primtal.*

Vi kan tage et eksempel.

$$60 = 2 \times 2 \times 3 \times 5$$

Det er vigtigt at få fastslået, at der er grænser for hvor store tal, man idag kan faktorisere inden for en overskuelig tid. Eksempelvis er der endnu ingen som har faktoriseret nedenstående tal på 174 cifre på trods af, at der på hjemmesiden www.rsasecurity.com er udlovet en præmie på 10.000$ for at faktorisere tallet.

188198812920607963838697239461650439807163563379 41/

738270076335642298885971523466548531906060650474 30/

453173880113033967161996923212057340318795506569 96/

2213051687593076502570 59

6 RSA - hvordan gør man?

6.1 Konstruktion af nøglepar

- Vælg to (store) primtal p og q.
- Beregn $n = pq$.
- Beregn $M = (p-1)(q-1)$
- Find et helt tal $0 < e < M$ så e og M er uden fælles divisorer.
- Find et helt tal $0 < d < M$ så $ed \mod M = 1$.

Offentlig nøgle: (e, n)
Hemmelig nøgle: d

Hele RSA-kryptosystemet som vi skal se i næste afsnit virker nu pga. følgende sætning

Sætning 6.1. *Hvis* (e, n) *og* d *er konstrueret som før, så gælder*

$$m^{ed} \mod n = m \quad \textit{for alle } 0 \leq m < n$$

6.2 Krypteringsprotokol

Klarteksten m er her et tal så $0 \leq m < n$.

- **Kryptering:**

$$m \longrightarrow m^e \mod n = c$$

- **Dekryptering:**

$$c \longrightarrow c^d \mod n$$

6.3 RSA eksempel

Vi kan tage et eksempel baseret på nogle små primtal. Vi vælger p=13 og q=17. Så er n=221 og M=192, Vi kan vælge e=5 og finder at d=77 virker. Den offentlige nøgle er $(5, 221)$ og den hemmelige nøgle er 77.

Vi kan vælge at kryptere bogstavet f.

- klartekst: $m = 6$ (f er det sjette bogstav i alfabetet)
- kryptotekst: $c = 41$ $(= 6^5 \mod 221)$
- klartekst: $m = 6$ $(= 41^{77} \mod 221)$

6.4 Kan RSA brydes?

Ja hvis man ikke er omhyggelig nok så kan det. Hvis Eva kan finde de to primtal p og q som Bob brugte i starten så er det faktisk nemt for hende at finde den hemmelige nøgle d. Dermed vil hun have brudt systemet.

Lad os lave det tankeeksperiment at Eva gik ud på nettet og aflæste Bobs n til at være 35. Så kunne hun faktorisere $35 = 5 \times 7$. Dvs at $p = 5$ og $q = 7$ og hun ville have brudt systemet.

Moralen er at p og q skal vælges så store at n ikke kan faktoriseres indenfor rimelig tid. I øjeblikket anbefaler man at p og q skal være på ca. 500 cifre hver.

7 Digital signatur

En ting som Public Key kryptering åbner op for er *digital signatur*. En digital signatur er en underskrift i elektronisk form. Den kan bruges af Alice til at signere eksempelvis en mail, så Bob kan være sikker på at den kommer fra Alice.

Når Alice vil sende en (ukrypteret) mail til Bob så bruger hun bare sin hemmelige nøgle til at låse mailen med. Bob kan da tjekke om mailen kommer fra Alice ved at finde hendes offentlige nøgle ude på nettet og låse op med

den. Sikkerheden bygger på at ingen andre end Alice kan konstruere den hemmelige nøgle som passer til Alice's offentlige nøgle.

Den digitale signatur og kryptering kan selvfølgelig kombineres.

8 Hvis du vil vide mere

Som introduktion til emnet kan jeg anbefale følgende bøger: Simon Sing: *Kodebogen.* og Peter Landrock og Knud Nissen: *Kryptologi - Fra viden til videnskab.*

ALGEBRAISK GEOMETRI
DISKRETE LOGARITME PROBLEMER
KRYPTOGRAFI

JOHAN P. HANSEN

Hvad er moderne kryptografi

Kryptografi er kunsten åbent at kunne sende information uden at uvedkommende medlyttere kan forstå indholdet og fastslå autenticiteten, altså identiteten af afsenderen (*digital signatur*) og integriteten af informationen.

Formelt består et kryptosystem af tre endelige mængder $\mathcal{M}$ (*kildeteksterne*), $\mathcal{C}$ (*kryptoteksterne*) og $\mathcal{K}$ (*nøglerne*) og *krypteringsfunktioner* $f_k : \mathcal{M} \to \mathcal{C}$, en for hvert k i $\mathcal{K}$.

I 1976 foreslog Diffie og Hellman *offentlig nøgle kryptosystemer* - en tilgang, der har revolutioneret moderne kryptografi. Funktionerne f_k, der er offentligt kendte, skal være lette at beregne, hvorimod f_k^{-1} skal være uberegnbare med mindre man besidder hemmelig viden - den såkaldte hemmelige nøgle.

Udover hemmeligholdelse åbner opsætningen op for begrebet *digital signatur*. En person har offentlige nøgle f_k. Denne person kan *underskrive* en besked m ved at beregne og sende $(m, f_k^{-1}(m))$ under anvendelse af hendes hemmelige nøgle. En modtager kan verificere underskriften ved at bruge den offentlig nøgle og sammenligne m og $f_k(f_k^{-1}(m))$.

ELGamal kryptosystemet fra 1985 er et offentligt nøgle system, der bygger på en cykliske gruppe G frembragt af elementet g. $\mathcal{M} = G, \mathcal{C} = G \times G, \mathcal{K} = \mathbb{Z}$ En person Hansen vælger tallet l som hemmelig nøgle og offentliggør g^l som offentlig nøgle. Jensen, der skal sende beskeden m til Hansen, vælger som hemmelig nøgle et tal k, beregner $g^{lk} = (g^l)^k$ og sender (g^k, mg^{lk}). Modtageren Hansen beregner $g^{kl} = (g^k)^l$ udfra det modtagne og hendes hemmelige nøgle l og er i stand til at rekonstruere m.

Omend systemet skal udbygges lidt for at give mulighed for digital signatur, illustrer det en central problemstilling, nemlig det *diskrete logaritmeproblem*. Systemets sikkerhed beror på om det i den cykliske gruppe $G =< g >$ er vanskeligt (tidskrævende) udfra g^l at bestemme eksponenten l.

Det diskrete logaritme problem

Det diskrete logaritme problem: I den cykliske gruppe $G =< g >$ bestem udfra g^l eksponenten l.

Der er som bekendt kun en abstrakt cyklisk gruppe af en given orden, men vanskeligheden af at løse det diskret logaritmeproblem afhænger i høj grad af den konkrete og præsentation af gruppen, som illustreret af de to følgende eksempler.

Date: Feb. 2002.

Eksempel 1. Lad $G = (\mathbb{Z}/p\mathbb{Z}, +)$. Bestemmelsen af den diskrete logaritme af b med hensyn til a indebærer bestemmelsen af l, så $b \equiv la \mod p$, altså bestemmelse af l (og m) så $b = la + mp$. *Euklids algoritme* til bestemmelse af største fælles divisor gør dette meget effektivt i $O(\log(p))$ heltals operationer. Det kan ikke udgøre grundlaget for et sikkert diskret logaritme system.

Eksempel 2. Lad atter $G = (\mathbb{Z}/p\mathbb{Z}, +)$. Vælg et primtal q, så p går op i $q^f - 1$. Indlejr G i $\mathbb{F}^*_{q^f}$, den multiplikative gruppe i det endelige legeme med q^f elementer. Gruppen $\mathbb{F}^*_{q^f} =< \xi >$ er cyklisk og vi får derved en præsentation af G som potenserne ξ^i, der er p-te enhedsrødder.

Bestemmelsen af den diskrete logaritme indebærer altså at bestemme en eksponent l, så $\eta_1 = \eta_2^l$, hvor η_1, η_2 er p-te enhedsrødder. De bedst kendte metoder er subeksponentielle i q (se senere).

Generiske algoritmer til bestemmelse af den diskrete logaritme er algoritmer, der overhovedet ikke udnytter den konkrete præsentation. Eksempler på sådanne er Shanks algoritme, Pollards ρ-metode og Pohlig-Hellman metoden.

For konkrete præsentationer af den cykliske gruppe, kan der ofte anvises mere effektive algoritmer, der udnytter den viden som præsentationen rummer. I eksempel 1 kunne Euklids algoritme, der er meget effektiv, bruges og i eksempel 2, hvor gruppen er den multiplikative gruppe i et endeligt legeme, viser den såkaldte *indeks kalkule metoden* sig nyttig.

Beregningskompleksitet. Lad os først indføre lidt sprogbrug. Hvis der findes en konstant c og et $\alpha \in [0, 1[$, så den forventede afviklingstiden for en algoritme med inputstørrelse $\log n$ er

$$O\left(\exp(c + o(1))(\log n)^{\alpha}(\log\log n)^{(1-\alpha)}\right),$$

så kaldes algoritmen *subeksponentil*. Bemærk at hvis $\alpha = 0$, så er algoritmen polynomiel, hvis derimod $\alpha = 1$, så er den fuldt eksponentiel.

De generiske algoritmer omtalt ovenfor kræver alle mindst $O(\sqrt{p}\ \log p)$ beregningstrin for en cyklisk gruppe af orden p. Dermed er de altså ikke væsentlig bedre end fuldt eksponentielle algoritmer. De tre nævnte generiske metoder er faktisk alle fuldt eksponentielle.

Indeks kalkule metoden for den multiplikative gruppe i det endeligt legeme $\mathbb{F}_q$ er derimod subeksponentiel, og dermed i klasse bedre. I lyset heraf anses kryptosystemmer, der bygger på den multiplikative gruppe i et endeligt legeme først at være sikre, når legemet er stort (2048 bits).

Algebraisk geomtri som kilde til grupper med gode præsentationer

I og med at det diskrete logaritme problem for den multiplikative gruppe i et endeligt legeme er subeksponentielt, søges andre konkrete grupper, hvor enten det diskrete logaritme problem beviseligt ikke er subeksponentielt eller endnu ikke er bevist at være det. Her kommer algebraisk geometri på banen.

To væsentlige opgaver er at bestemme størrelsen af gruppen og vurdere kompleksiteten af det diskrete logaritme problem.

Elliptiske kurver. Allerede elliptiske kurver over endelige legemer producerer grupper, hvor ingen subeksponentiel algoritme for det diskrete logaritme problem er kendt, pånær for specielle kurver. Der er faktisk argumenteret for, at en indeks kalkule metoden er usandsynlig for elliptiske kurver.

FIGUR 1. Korde-sekant gruppestrukturen på en elliptiske kurve, $P_1 \oplus P_2 = P_3$

FIGUR 2. Gruppestrukturen på Jacobianten af en hyperelliptisk kurve, $(P_1 + P_2) \oplus (Q_1 + Q_2) = R_1 + R_2$

gruppe G	$\sharp G$ kompleksitet	diskret log. kompleksitet
$\mathbb{F}_q^*$	$q-1$	subeksponentiel: $\alpha = \frac{1}{2}, \frac{1}{3}$
Jacobianter		
$g = 1$	polynomiel	$\sqrt{\sharp G}$
$g = 2, 3, 4$	polynomiel?	$\sqrt{\sharp G}$
g stor	polynomiel?	subeksponentiel: $\alpha = \frac{1}{2}$

TABEL 1. Oversigt over kompleksiteten af ordens beregninger af grupper og tilhørende diskrete logaritme problemer

En elliptisk kurve E er en glat kurve, hvis punkter (x, y) er løsning til en ligning af formen

$$y^2 = f(x), \quad \deg(f) = 3.$$

Tilføjes et ekstra punkt ∞ gives punkterne på $E \cup \infty$ en gruppestruktur ved at kræve dels at 3 punkter på linie skal have sum 0 dels at ∞ skal være neutral element, jvf. figur 1. I de seneste år er der gjort store fremskridt i udviklingen af særdeles effektive algoritmer til bestemmelsen af ordenen af gruppen, jvf. Berit Skjernås artikel i Matilde nr. ??.

Kurver og deres Jacobianter. Gruppestrukturen på en elliptisk kurve er blot et specialtilfælde af en mere generel konstruktion. Til enhver kurve C er der knyttet en gruppe $Jac(C)$. Elementerne heri er såkaldte divisorer, som er formelle summer af punkter på kurven, modulo en bestemt ækvivalensrelation. På figur 2 er gruppestrukturen illustreret for en hyperelliptisk kurve.

Har kurven C genus g vides, at $Jac(C)$ er g-dimensional og om gruppens størrelse over legemet $\mathbb{F}_q$ med q elementer gælder, at

$$(\sqrt{q} - 1)^{2g} \leq \sharp Jac(G) \leq (\sqrt{q} + 1)^{2g}.$$

Det giver er væld af store grupper af kardinalitet $\approx q^g$. Der findes imidlertid ikke effektive algoritmer til bestemmelse af gruppeordenen i almindelighed.

Det diskrete logaritmeproblem er for visse (familier) af kurver med store genera imidlertid subeksponentielt med $\alpha = \frac{1}{2}$.

Konklusion må være at anvende kurver med lav genus.

Som afslutning kan bemærkes, at man med udgangspunkt i højere dimensionale varieter X på tilsvarende vis kan knytte en Jacobiant $Jac(X)$, der er en abelsk varietet. Jacobianter synliggør dermed abelske varieteters rolle i moderne kryptografi.

MATEMATISK INSTITUT, ÅRHUS UNIVERSITET
E-mail address: matjph@imf.au.dk

Kvantekryptografi

Ivan Damgård

February 15, 2002

1 Indledning

Kryptografi har lige siden tidernes morgen haft som mål at skabe sikker kommunikation over usikre kommunikationskanaler. I denne artikel vil vi koncentrere os om hemmeligholdelse, altså to parter - lad os kalde dem Alice og Bob - ønsker at udveksle en meddelelse således at deres værste fjende Eve ikke vil have nogen som helst anelse om hvad der er blevet sendt.

I praksis findes en række udmærkede og anvendelige løsninger på dette problem, som imidlertid alle har en ting til fælles: hvis Eve har tilstrækkelig mange resourcer til rådighed (hvilket i praksis vil sige regnekraft), så kan alle disse systemer brydes, dvs. Eve kan alligevel finde ud af hvad der blev sendt. Det er ikke noget tilfælde, at det er sådan: i 40-erne skabte Shannon informationsteorien, og fandt bl.a. præcise betingelser for, hvornår absolut sikkerhed mod Eve kan lade sig gøre, dvs. hvad skal der til for at Eve intet får at vide, uanset hvor mange resourcer hun har til rådighed. Det viser sig at være nødvendigt at Alice og Bob på forhånd er enige om en hemmelig nøgle K, dvs. K er en streng af bits $k_1, ..., k_n$ som er tilfældigt valgt, og som Eve ingen information har om. Man kan nu sende en meddelelse bestående af n bits $M = m_1, ..., m_n$ krypteret v.hj.af K ved at sende $C = m_1 \oplus k_1, ..., m_n \oplus k_n$, dvs. hver bit i meddelelsen adderes modulo 2 med en bit i nøglen. Det er let at se, at hvis Eve ingen information har om K, så er - selv givet C - enhver værdi for M lige sandsynlig, m.a.o. Eve har intet fået at vide. Dette kaldes *perfekt sikkerhed*.

Men Shannons resultat sagde så, at perfekt sikkerhed kræver at nøglen indeholder mindst lige så meget information som meddelelsen, dvs. hvis der n bits i meddelelsen, så skal antal bits i nøglen være mindst n, ligegyldigt hvordan krypteringen foregår. Ydermere kan hver nøgle kun bruges een gang, ellers mistes den perfekte sikkerhed. Denne form for kryptering kaldes derfor *One-Time* Pad.

Et system baseret udelukkende på one-time pads er af naturlige årsager helt uanvendeligt i praksis på grund af de indlysende problemer med at få nøglen på plads på sikker vis inden kommunikationen foregår. Derfor bruger

krypteringssystemer i praksis andre metoder hvor man genbruger den samme korte nøgle til adskillige meddelelser. Men - som forudsagt af Shannon - ethvert sådant system kan i princippet brydes hvis man bruger tid nok på det. Det ville naturligvis være OK, hvis vi med sikkerhed vidste at "tid nok" betyder adskillige millioner år, f.eks. Men desværre er det ikke lykkedes for nogen at konstruere et praktisk anvendeligt system, hvor vi med sikkerhed hvor meget tid der faktisk skal til for at bryde det. Derfor er kryptering i praksis i dag funderet på velunderbyggede formodninger, snarere end beviser. Og selvom vi havde sådanne beviser, så siger Shannon jo at vi aldrig vil kunne fjerne muligheden for at vore systemer kan brydes hvis de også skal være praktisk anvendelige.

Det ser jo alt sammen temmelig utilfredsstillende ud. Imidlertid har det i de senere år vist sig, at Shannon's pessimistiske resultater i virkeligheden bygger på nogle antagelser om hvad Eve i stand til at gøre, nemlig flg.:

- Eftersom vi ikke har fysisk kontrol over hele kommunikationskanalen, er Eve altid i stand til at se på kommunikationen og vil så få at vide præcis hvilke bits der er sendt mellem Alice og Bob (selvom hun måske ikke umiddelbart kan forstå meddelelsen).

- Efter at have set på kommunikationen, kan Eve vælge at lade den gå videre uændret til modtageren, som aldrig vil kunne opdage at andre har set på den.

Det kan umiddelbart virke selvindlysende, at disse antagelser må være rigtige, uanset hvordan kommunikationen foregår. Og så længe vi taler om almindelig digital kommunikation, så er antagelserne helt i orden. Faktisk mente forskere på området i næsten 50 år ikke engang at der var grund til at overveje om dette er en præcis model af verden.

2 Kvanteinformation

Det kan derfor synes overraskende, at billedet skifter fuldstændigt, hvis vi bruger *kvantekommunikation*. Her sendes information kodet i tilstanden af meget små fysiske systemer, såsom elementarpartikler. Man bruger typisk de mindst mulige enheder af lys, nemlig fotoner. Når så små fysiske systemer er i spil, er vi nødt til at bruge kvantefysikken til at beskrive deres opførsel, hvilket har en del uventede konsekvenser.

F.eks. er det et grundlæggende princip i kvantefysik at når man måler på et fysisk system, som inden målingen er i en ukendt tilstand, så er det umuligt altid at bestemme systemets tilstand fuldstændigt; yderligere vil enhver måling med en vis sandsynlighed påvirke systemets tilstand. Det er meget vigtigt at forstå, at disse udsagn er absolutte, og intet har med teknologi at gøre: det er ligemeget hvor store summer vi investerer i at

lave en nøjagtig og skånsom måling af en elementarpartikels tilstand, det vil alligevel ikke være muligt at undgå at målingen påvirker partiklen: selve det faktum at jeg har fået en vis delvis information om dens tilstand medfører i sig selv at den blevet påvirket.

Ser vi nu igen på de to antagelser ovenfor om hvad Eve "naturligvis" kan gøre, så ses det klart, at de grundlæggende principper i kvantefysik vi har set på, præcis siger, at antagelserne er forkerte når vi bruger kvantekommunikation. Det betyder ikke i sig selv at ubetinget sikkerhed kan lade sig gøre i praksis med kvantekommunikation, men muligheden er i det mindste til stede. Vi skal nu se nærmere på hvordan kvantekommunikation opfører sig, og hvordan ubetinget sikkerhed faktisk kan opnås.

3 Qbits

I kvanteinformatik erstatter vi bits med kvantebits, også kaldet *qbits*. Hvor en klassisk bit enten er 0 eller 1, beskrives tilstanden af en kvantebit som en vektor af længde 1 i et komplekst vektorrum. Hvis vi følger den traditionelle notation og kalder de to basisvektorer for $|0\rangle$ og $|1\rangle$, så er tilstanden af en qbit generelt $\alpha|0\rangle + \beta|1\rangle$, hvor α, β er komplekse tal, så $|\alpha|^2 + |\beta|^2 = 1$. I det følgende vil holde os til tilfældet hvor koordinaterne er reelle, da det vil være tilstrækkeligt til at beskrive det vi har brug for. Man kan tænke på de to kanoniske basisvektorer som de to klassiske tilstande, en almindelig bit er begrænset til at have, dvs. en qbit er et "klassisk nul", hhv. et "klassisk 1-tal", hvis den er i tilstand $1 \cdot |0\rangle + 0 \cdot |1\rangle$, hhv. $0 \cdot |0\rangle + 1 \cdot |1\rangle$.

En mulig fysisk implementation af en qbit fås ved at betragte polarisationstilstanden af en foton. Polariseret lys er karakteriseret ved at alle fotoner i lysstrålen er enige om at "svinge" i en bestemt retning, f.eks. vandret eller lodret. Hver enkelt foton har derfor en polarisationstilstand, som kan beskrives ved en vinkel der fortæller hvor mange grader svingningsplanet er fra vandret. Så 0^0 er vandret polarisation, mens 90^O er lodret. I kvantefysikkens formalisme beskrives dette i et vektorrum som før, idet vi udnævner basisvektoren $|0\rangle$ til at være vandret og $|1\rangle$ til at være lodret. Et foton der er polariseret lodret vil så være i tilstanden $0 \cdot |0\rangle + 1 \cdot |1\rangle$, mere generelt, hvis man er polariseret i en vinkel på v^O, så er tilstanden $\cos(v)|0\rangle + \sin(v)|1\rangle$.

Det er nu muligt at sige noget mere præcist om, hvordan en måling foregår. Iflg. kvantefysikken er enhver måling på en qbit begrænset til at specificere to *ortogonale* tilstande (vektorer) V_0, V_1 og spørge qbitten om den er i tilstand V_0 eller V_1. Det kan f.eks. lade sig gøre at spørge en foton om den er i tilstand $V_0 = |0\rangle$ eller $V_1 = |1\rangle$. Resultatet af målingen er bestemt som flg., når fotonen er i tilstand $\alpha|0\rangle + \beta|1\rangle$ inden målingen:

- Målingen vil give resultat $|0\rangle$ med sandsynlighed $|\alpha|^2$, og resultat $|1\rangle$ med sandsynlighed $|\beta|^2$ (det er derfor tilstande er defineret som vektorer

af længde 1, da dette sikrer at summen af sandsynlighederne er 1).

- Efter målingen er qbitten *i den tilstand man har målt den til at være i*, og har glemt alt om den gamle tilstand.

Det skulle være klart hvordan de to principper i kvantefysik vi nævnte overfor materialiserer sig her i målinger på en qbit: generelt kan man ikke få noget præcist at vide om α og β ved en enkelt måling, og man får kun et enkelt forsøg: efter målingen er den gamle tilstand forsvundet. Man kunne tro, at det ville være muligt at lave en mere nøjagtig måling ved at fremstille nogle kopier af qbitten, og måle på alle kopierne, men desværre: en anden fundamental sætning i kvantefysik siger, at det er *umuligt* at lave en perfekt kopi af en ukendt tilstand (den såkaldte no-cloning sætning).

En generel måling, hvor V_0, V_1 ikke nødvendigvis er $|0\rangle$, $|1\rangle$ kan beskrives på lignende måde: givet starttilstanden $\alpha|0\rangle + \beta|1\rangle$ udregner man denne vektors koordinater i basen V_0, V_1, og sandsynlighederne er nu givet ved disse koordinater på samme vis som overfor. Vi siger derfor at måler *i basen givet ved* (V_0, V_1).

Selvom målinger ikke generelt giver fuldstændig information, er der dog visse specielle tilfælde, hvor en måling med sikkerhed fortæller hvad tilstanden var: hvis jeg på forhånd ved, at tilstanden er $|0\rangle$ eller $|1\rangle$, så kan jeg lave en måling der netop spørger om tilstanden er $|0\rangle$ eller $|1\rangle$, altså en måling i basen $(|0\rangle, |1\rangle)$, hvilket ifølge reglerne ovenfor altid vil give det rigtige svar. Men det er netop kun fordi målingen er indrettet efter den givne forhåndsviden. Antag, at vi istedet havde målt i basen der er drejet 45^O, dvs. $(V_0, V_1) = (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, -\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)$. Det er ligetil at regne ud, at denne måling vil give resultat V_0 med sandsynlighed $1/2$ og V_1 med sandsynlighed $1/2$, ligegyldigt om vi måler på tilstanden $|0\rangle$ eller $|1\rangle$. Så i dette tilfælde giver målingen overhovedet ingen information om starttilstanden. Måske en bekræftelse af det gamle ord om, at et dumt spøgrsmål fører til et dumt svar..

I det følgende vil $+$ stå for den kanoniske basis $(|0\rangle, |1\rangle)$, mens $\times$ vil stå for den "diagonale " basis $(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, -\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)$. Endvidere vil vi nruge notationen $|0\rangle_\times = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ og $|1\rangle_\times = -\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. For at gøre notationen mere konsistent, vil vi også bruge $|0\rangle_+ = |0\rangle$, $|1\rangle_+ = |1\rangle$. Vi har så følgende mere generelle resultat, som følger umiddelbart af reglerne for målingers opførsel:

Sætning

Antag der måles på en qbit i tilstand $|0\rangle_+$ eller $|1\rangle_+$. En måling i $+$-basen vil fortælle med sandsynlighed 1 hvilken tilstand der er tale om. En måling i $\times$-basen giver et tilfældigt resultat, som ingen information indeholder om den målte tilstand. Antag dernæst at der måles på en qbit i tilstand $|0\rangle_\times$

eller $|1\rangle_\times$. En måling i $\times$-basen vil fortælle med sandsynlighed 1 hvilken tilstand der er tale om. En måling i $+$-basen giver et tilfældigt resultat, som ingen information indeholder om den målte tilstand.

4 Nøgleudveksling

Vi vil nu på, hvordan den opførsel qbits udviser, kan udnyttes til at skabe ubetinget sikkerhed. Bemærk først, at det er tilstrækkeligt at gøre det muligt for Alice og Bob at udveksle en tilfældig nøgle, som Eve ikke har information om, herefter kan one-time pad teknikken bruges til at sende selve meddelelsen krypteret.

Vi antager, at Alice er i stand til at sende qbits til Bob, men Eve kan undervejs gøre hvad som helst ved de qbits der bliver sendt - måle på dem, erstatte dem med andre qbits, etc. Vi antager også, at Alice kan kommunikere konventionelt med Bob, f.eks. over telefonen. Her er antagelsen at Eve har mulighed for at lytte med, men hun kan ikke ændre på det der bliver sagt. Der er altså ingen hemmeligholdelse givet "gratis" i modellen.

Vi udfører nu flg. protokol:

1. Alice vælger en række tilfældige bits $B = b_1, b_2, ..., b_n$, og en række tilfældige baser $\theta = \theta_1, ..., \theta_n$, hvor altså hver θ_i er enten $+$ eller $\times$. Hun sender qbits $|b_1\rangle_{\theta_1}, ..., |b_n\rangle_{\theta_n}$ til Bob.

2. Bob vælger en tilfældig sekvens af baser $\hat{\theta} = \hat{\theta_1}, ..., \hat{\theta_n}$, og måler qbit nr. i i basen $\hat{\theta_i}$. Hvert resultat kan på naturlig vis tolkes som en bit, lad de målte resultater være $\hat{b_1}, ..., \hat{b_n}$.

På dette tidspunkt har Bob delvis information om den bitsekvens B Alice har sendt, i alt fald hvis Eve ikke har forstyrret kommunikationen: i ca. halvdelen af tilfældene vil $\theta_i = \hat{\theta_i}$, og det medfører iflg. sætningen ovenfor at $b_i = \hat{b_i}$. Problemet er blot at Bob ikke ved hvilke bit-positioner der er gode. Det løses ved flg. skridt:

1. Alice sender sekvensen af baser θ til Bob v.hj.af konventionel kommunikation.

2. Bob fortæller Alice hvilke i-værdier, der opfylder at $\theta_i = \hat{\theta_i}$. Alice og Bob kasserer bits på positioner hvor dette ikke er opfyldt, og beholder resten.

Vi har nu en situation, hvor Alice har en bitsekvens B' og Bob har $\hat{B'}$, begge af længde ca. $n/2$. Hvis Eve ikke har grebet ind i kommunikationen, så er det klart, at $B' = \hat{B'}$. På den anden side, betragt Eve's situation når Alice sender sine qbits: hvis hun vil vide noget som helst om B er hun

nødt til at måle (nogle af) qbittene. Men på dette tidspunkt har hun ingen information om θ, så hun ved ikke hvad den rigtige måling vil være for hver enkelt foton, og hun er altså nødt til at vælge sine målinger efter en eller anden strategi. Som et eksempel, lad os antage at hun vælger tilfældigt mellem en måling i $+$ eller i $\times$-basis. Hvis hun gætter rigtigt for den i'te qbit, dvs. hun bruger θ_i til målingen, så vil hun få b_i som resultat. Hun kan så lave en ny qbit i præcis samme tilstand og sende den videre til Bob. Det vil ikke være være muligt at se, at denne qbit har været angrebet. Men i halvdelen af tilfældene vil gættet være forkert, og Eve vil få en tilfældig bit $\tilde{b_i}$, som kun med sandsynlighed $1/2$ er lig med b_i. Eve ved jo imidlertid ikke på dette tidspunkt om hun har valgt den rigtige måling, så hun er henvist til at sende en qbit til Bob i den tilstand hun har målt. Da Bob's valg af baser når han måler er uafhængige af Eve's, vil denne strategi for Eve derfor betyde at ca. 25% af bittene i $\hat{B'}$ er forskellige fra dem i B'. Til gengæld kender hun med sikkerhed ca. halvdelen af bittene i B', eftersom Alice jo offentliggør θ, hvorefter Eve kender de positioner hvor hun gættede rigtigt.

Denne strategi for Eve er ikke den eneste mulige, f.eks. er Eve jo ikke begrænset til at måle i kun de to baser Alice og Bob bruger. Imidlertid kan man vise at det generelle princip vi illustrerede her er gyldigt generelt: jo flere målinger Eve foretager, jo mere får hun at vide, men samtidig vil det nødvendigvis føre til flere uoverenstemmelser mellem B' og $\hat{B'}$. Dette betyder omvendt, at hvis der faktisk er meget få uoverenstemmelser, så er Eve's information om B' meget begrænset. Derfor vil Alice og Bob nu vurdere hvor mange fejl der faktisk er:

1. Alice vælger en tilfældig indexmængde $I \subset \{1, 2, .., n\}$ af størrelse k og sender den til Bob.

2. Bob sender $\{\hat{b_i} |\ i \in I\}$ til Alice.

3. Alice sender til Bob det antal bits t i I hvor $b_i = \hat{b_i}$. Hvis $t/k \geq \epsilon$ (for et ϵ fastlagt på forhånd, se nedenfor), opgiver Alice og Bob, ellers fortsættes der.

Ideen her er for det første, at man med klassisk sandsynlighedsregning kan vise at et tilstrækkeligt stort k giver en meget præcis vurdering af den faktiske fejlrate; for det andet at man må forvente et vist antal fejl af naturlige årsager på grund af målefejl o.l., derfor må et $\epsilon > 0$ vælges herudfra.

Hvis Alice og Bob går videre herfra, så ved vi med stor sikkerhed, at fejlraten mellem B' og $\hat{B'}$ er højst ϵ, og for det andet at ligegyldigt hvad Eve stiller op, så er hendes information om B' begrænset. For at blive helt færdige skal vi bruge nogle velkendte og klassiske teknikker, som det vil føre for vidt at komme ind på i detaljer her. For det første skal vi have rettet fejlene, så Alice og Bob er enige om samtlige bit, her kan f.eks. fejlkorrigerende koder

anvendes. For det andet har vi brug for at slippe af med den begrænsede mængde information Eve har. Dette er ikke helt ligetil: selvom vi ved at Eve kun kender få af de relevante bits, ved vi ikke hvilke hun kender. Løsningen er en teknik der kaldes *privacy amplification*: hvis Alice og Bob er enige om en bitsekvens X, og Eve's information om X er begrænset på passende vis, så er det altid muligt for Alice og Bob ved hjælp af *offentlig* kommunikation at beregne en *kortere* bitsekvens Y, hvorom Eve har en vilkårligt lille mængde information. Mere præcist, længden af Y kan vælges så Eve's information er mindre end en vilkårlig ønsket grænse.

Det er langt fra trivielt at vise at alt dette faktisk virker som ønsket, og protokollen har været kendt i lang tid, inden et egentligt bevis blev givet. Et sådant kan findes f.eks. i [1]. En lettilgængelig introduktion til kvantekryptografi kan findes i [2].

5 I virkeligheden

Der findes mange eksperimentelle implementationer af kvantekryptografi. Den mest almindelige teknink er at implementere qbits som fotoner, og bruge lyslederkabler som transportmedium. En fuldt funktionsdygtig prototype er fremstillet på Århus Universitet, mere information herom kan findes i [3]. Dette eksperiment fungerer over ca 20 Km, og det ser ud til at den nuværende teknologi vil kunne realisere afstande på op til 100 Km på sigt. Herefter vil nye ideer være nødvendige, men man ved allerede nu at der ikke er nogen principielle grænser for afstanden mellem Alice og Bob.

References

[1] Nielsen and Chuang: *Quantum Computation and Quantum Information*, Cambrigde University Press 2000.

[2] Gilles Brassard: *Modern Cryptology*, Springer Verlag LNCS 325

[3] http://www.cki.au.dk

Da Alain Connes fik Crafoord prisen.

Af: Gert Kjærgård Pedersen, Københavns Universitet, Email: gkped@math.ku.dk

Den 26. september sidste år overrakte Kong Carl Gustav ved en ceremoni i det Kungliga Vetenskapsakademien årets Crafoord pris til professor Alain Connes fra Collège de France. Da prisen på en halv million dollar indtil videre – altså indtil Abel Prisen bliver til virkelighed – er den numerisk største indenfor matematik, og da Alain Connes er en god ven af Danmark fortjener begivenheden at blive omtalt i Mathilde.

Crafoord prisen blev indstiftet i 1980 ved en donation fra Anna-Greta og Holger Crafoord til et fond bestyret af det svenske videnskabsakademi. Midlerne kommer fra familiens virke indenfor hospitalsindustrien. Prisen uddeles hvert år indenfor ét af emnerne: Matematik, Astronomi, Geovidenskab, Biovidenskab med særlig henblik på Økologi samt Gigtforskning. Den er et klart forsøg på at supplere Nobelprisen ved at pege på nogle af de videnskabsgrene som Alfred Nobel overså. Endvidere har det været et ønske fra fondsstifterne at inddrage hjemlandet Skåne i begivenhederne, således at det symposium der afholdes i forbindelse med prismodtagelsen foregår dels i Lund og dels i Stockholm. Symposiet har et budget på endnu en halv million dollar så der er – ligesom for Nobelprisen - et ganske stort råderum for festivitas.

Tidligere modtagere af prisen i matematik har været Vladimir I. Arnold og Louis Nirenberg i 1982, Pierre Deligne og Alexandre Grothendieck i 1988 (Grothendieck afslog som sædvanligt) samt Simon Donaldson og Shing-Tung Yau i 1994. Den nationale stolthed skylder vi at nævne at Willi Dansgaard fik prisen indenfor geofysik i 1995.

Connes fik prisen ”for sit gennemtrængende arbejde indenfor operator algebra teori og for skabelsen af den ikke-kommutative geometri”, for nu at citere akademiet. Det sidste skal vi vende tilbage til. Kort fortalt startede Connes (født 1947 i Draguignan i Sydfrankrig) sin karriere på École Normale i 1966. Han var oprindelig elev af Laurent Schwartz, men skrev sin disputats under ”vejledning” af Jacques Dixmier, som engang beskrev ham som en komet man bare så halen af. Disputatsen ”Classification de facteurs de type III” fra 1973 var et epokegørende arbejde. John (Janos, Johan) von Neumann havde i 30’erne skabt teorien for ”rings of operators”, i dag kaldet *von Neumann algebraer*, som et muligt aksiomatisk grundlag for kvantemekanikken. Han fandt at ”faktorerne”, altså de von Neumann algebraer som er maksimalt ikke-kommutative, dvs. dem hvis center består blot af skalære multipla af enhedsoperatoren, kan inddeles i tre typer, kaldet I, II og III. (Billedsprog var ikke JvN’s stærke side.) Typen I er nem, det er matrixalgebraer af rang 1,2, osv., samt B(H) for Hilbertrum H af enhver uendelig dimension. Algebraer af type II er dem der ikke har nogen minimale projektioner (dette karakteriserer nemlig type I), men som har mange *endelige* projektioner, dvs. projektioner p som ikke er ækvivalente med nogen delprojektion. Hvis altså p=uu* for et element u i algebraen, så kan man ikke have u*u<p. Man udleder heraf (men ikke let !) at en sådan algebra har et *spor*, dvs. en lineær funktional f således at f(xy)=f(yx) for alle elementer x og y – altså en funktion der opfører sig ligesom det kendte spor Tr af en matrix. Type III er det der bliver tilovers, altså ingen minimale projektioner, ingen endelige projektioner og ingen spor. Ganske vist måtte man regne med at der var uendelig mange elementer indenfor hver type, men Frank Murray og von Neumann viste, at hvis faktoren yderligere var ”hyper-endelig”, dvs. var en induktiv limes (i en meget svag topologi) af matrixalgebraer, så var der kun én hyper-endelig faktor af type II der havde en *endeligt* spor. De formodede, men kunne ikke vise, at der også kun var én hyper-endelig faktor af type II med et *uendeligt* (altså ubegrænset) spor. Da de hyper-endelige faktorer er dem, der naturligt fremkommer i modeller for kvantemekanik, er det deres klassifikation der er vigtig. Nu viste Connes – ved at benytte Tomita og Takesaki’s arbejder

om modulære operatorer og modulære grupper for funktionaler på von Neumann algebraer (så pludselig kommer der avanceret komplex funktionsteori ind i den ellers meget abstrakte von Neumann algebra teori !!) – at Type III har en klassifikation efter en reel parameter λ i intervallet [0, 1]. Endvidere viste han, at for ethvert reelt λ strengt mellem 0 og 1 er der netop én hyper-endelig faktor af type III_λ. For type III_0 er billedet mere speget, men der *er* en klassifikation for de hyper-endelige faktorer. Endvidere viste Connes (under aftjening af sin værnepligt i den tidligere koloni Canada) at også den hyper-endelige faktor af type II_∞ var entydigt bestemt. Senere blev vores egen Uffe Haagerup verdensberømt på at vise, at éntydigheden også gælder i type III for λ=1, men det er en anden historie.

For disse opdagelser fik Alain Connes Fields medaljen i 1983. Hans hjemland har heller ikke været karrig med anerkendelse (matematik rangerer stadig højere i Frankrig end i resten af verden). Han blev professor ved Institut des Hautes Études Scientifiques (IHES) i 1979 og medlem af Collège de France i 1884. Han blev optaget i Acadèmie des Sciences i 1982, og både Canada og USA har kvitteret med medlemsskaber af Canadian Academy of Sciences og National Academy of Sciences. I Danmark gjorde vi ham allerede i 1980 til udenlandsk medlem af Videnskabernes Selskab, og i Norge blev han optaget i Videnskaps-Akademiet i 1993 og kreeret doctor honoris causa fra Oslo Universitet i 2001. Han har fortjent det hele og ligner stadig den venlige, imødekommende og lattermilde person, jeg spillede bordtennis med i 1971.

I de senere år har Connes promoveret den ikke-kommutative geometri. Hans indgangsvinkel var nogle mangfoldigheder, såkaldte foliationer, der optræder som løsninger til visse differentialligninger. Det simpleste eksempel er Kronecker's foliation, der beskriver den reelle akses indlejring på 2-torus med en irrational hældning θ. Vi betragter altså differentialligningen $dy = \theta\, dx$ på torus, og får som løsning den reelle linie R injektivt indlejret i det kompakte rum $T \times T$, hvorfor kvotientrummet er ganske grufuldt. Imidlertid er der en operatoralgebra der beskriver dette fænomen simpelt – hvis man altså er fortrolig med C*-algebra teori. Ved nøjere overvejelse er det nu ikke ganske klart hvad ikke-kommutativ geometri egentlig dækker over. Den har i sin simpleste formulering noget at gøre med at erstatte et topologisk rum, altså et geometrisk objekt X, først med den tilsvarende funktionsalgebra C(X) (eller måske snarere $C^\infty(X)$, eller endnu bedre algebraen af Schwartz funktioner) og dernæst med den ikke-kommutative algebra $C(X, M_n)$ af matrix-funktioner, eller en algebra af tværsnit i et n-dimensionalt vektorbundt over X. Set i dette lys er teorien for vektorbundter, også de uendelig-dimensionale, samt store dele af Lie gruppe teorien part af den ikke-kommutative geometri. Det er nok at tage munden for fuld, men der synes ikke at være grænser for hvad man kan komme ud for når man deltager i en konference om emnet. Connes har selv prøvet at afgrænse emnet i sin bog "Noncommutative Geometry" fra 1994, en oversættelse og kraftig udvidelse af den franske udgave fra 1990. Imidlertid er han selv i mellemtiden blevet opslugt af den klassiske kvantemekanik, som den er givet ved "Standard Modellen" (som matematikere ellers stiller sig noget skeptiske overfor, grundet de mange ad hoc antagelser). Herfra har Connes fortsat mod en mulig løsning af Riemann's hypotese, hvor metoden er, at man prøver at finde en operator på Hilbertrummet, formodentlig hørende til kvantemekanikkens arsenal af Schrödinger operatorer, hvis spektrum netop er nulpunkterne for zeta-funktionen.

Crafoord Symposiet 24-26 September 2001 var en rundgang i Connes' verden. Programmet i Lund den 24. og i Stockholm den 25. var næsten identiske, men nok værd at høre to gange. Sir Michael Atiyah indledte med et foredrag om "The Geometry of an n-point Energy Function" . Dernæst fortalte Connes selv om "Noncommutative Geometry and Physics" og Nigel Higson fortsatte med "Noncommutative Geometry and von Neumann algebras". Efter frokosten talte Jean-Louis Loday om "Algebraic K-Theory and Cyclic Cohomology", Henri Moscovici fortsatte

med ”Cyclic Cohomology and Non-Commutative Index Theory”, og Dirk Kreimer rundede af med ”Feynman Diagrams: on Residues and Numbers”. Til sidst styrede Uffe Haagerup og Erling Størmer en kort ”Problem Session” som bød på spredt fægtning med løst krudt.

Om aftenen den 26. var kongeparret vært for Symposiets indbudte deltagere på Grand Hotel. Alain Connes var blevet bedt om at holde tale, og han fortalte sin version af Faust myten: Djævelen frister en matematiker med at give ham alt i bytte for sin udødelige sjæl. Matematikeren ønsker blot en løsning på Riemann hypotesen, og Satan ler hult ved tanken om det lette offer. Men tre dage senere kommer djævelen tilbage i noget forpjusket tilstand og foreslår et kompromis: Jeg kan ikke løse hypotesen lige nu, men jeg har et lille lemma du kan få. Historien ender uden afslutning, men man kan håbe at Alain både redder sin sjæl og får et lille lemma.

Matematikdidaktikken: Kan vi lære at elske den?

Af: Kjeld Bagger Laursen, Centerleder, CND-KU, Email: laursen@math.ku.dk

I sidste nummer af Matilde har Carl Winsløw giver en beskrivelse af matematikdidaktikken. Hans ærinde har været at gøre opmærksom på feltets eksistens som selvstændigt forskningsområde - det vi til daglig kalder 'fag'. Og ikke bare eksistensen af matematikdidaktikken, men også fagets eksistensberettigelse.

I sin argumentation bruger CW bl.a. analogien med fusionskøkkenet. Og han nævner parallellerne til medicin. Dette billede er vældig godt, synes jeg. Her bliver man jo gjort opmærksom på hvordan der er tale om et område der har mange aspekter i sig, og vel at mærke aspekter der indgår symbiotisk i feltet. Ligesom medicin har matematik (bredt anskuet -) mange aspekter i sig: der er selvfølgelig grundforskningen, og der er faget-i-praksis. Denne praksis kan være mange forskellige ting: det kan være matematik anvendt inden for andre fagområder, eller i 'den virkelige, praktiske verden', og det kan være matematik i en formidlingssammenhæng (også 'formidling' er her bredt anskuet, så det omfatter f.eks. al undervisning).

Det er vanskeligt at forestille sig at der kan foregå noget som helst af værdi i praksis-fasen, hvis det ikke er baseret på overvejelser om mål og midler (Det kan selvfølgelig sagtens være overvejelser, som andre end den direkte bruger har gjort sig). Og der er da også mere og mere, også i universitetsverdenen, der opfordrer til at ofre 'praksis-delen', her primært undervisningen, større opmærksomhed.

Visse af de naturvidenskabelige universitetsuddannelser har vigende tilslutning. Og det har både vi selv og samfundet lagt mærke til.

Hvad samfundets opmærksomhed angår er der en anden faktor der gør sig gældende i uddannelsessektorens nuværende situation: ønsket om at holde igen på skatterne bliver udmøntet i krav om større effektivitet.

Den helt klassiske universitetsmodel, hvor lærde og vise professorer omgav sig med elever der af egen drift higede efter indsigt, og hvor en uddannelse bestod af en slags certificering i form af aflagte og beståede eksaminer, er forsvundet. Den er erstattet – i hvert fald i det omgivende samfund – af forestillinger om at vi som uddannelsesinstitutioner ved optagelsen af studerende har påtaget os et vist medansvar for deres uddannelses gennemførelse. Og dermed er opmærksomheden skærpet: ikke blot om hvad vi underviser, men også hvordan vi gør det.

Didaktik bliver pludselig mere interessant for os, der er ansat på et universitet. For mange sker det ikke fordi de opfatter feltet som i sig selv betydningsfuldt – men i det mindste fordi det ikke kan ignoreres helt, af et system der ønsker at bevare sig selv (og findes der systemer der ikke gør det?) Sådan er det også gået ved det naturvidenskabelige fakultet ved Københavns Universitet (NAT-KU i resten af denne artikel). Derfor har også vi fået et didaktisk center , CND – Center for Naturfagsdidaktik.

Hvad skal det gøre godt for? Her er lidt om hvad det skal, hvad det kan, og hvad det måske kan føre til.

Centret skal virke for bedre undervisning i naturvidenskaberne – og det skal gøre det forskningsbaseret . Det retter sig mod alle fakultetets fag, også mod de matematiske og datalogiske fag. Endvidere skal det beskæftige sig med museumsdidaktik (fordi NAT-KU ejer tre eller fire ganske store museer).

Derudover skal CND forestå uddannelsessociologiske undersøgelser, f.eks. rekrutterings- og studieforløbsundersøgelser, og det skal gøre hvad det kan for at fremme naturfagsdidaktikken inden for hele uddannelsessystemet, herunder fx kompetenceudvikling inden for de naturvidenskabelige fag gennem uddannelsessystemet (det er en del af vores ambition at være med i initiativer, der kan styrke forståelse af behovet for, at der i befolkningen er en bred naturvidenskabelig indsigt – det der kaldes 'Public

Understanding of Science'. På dette punkt har NAT-KU flere andre ting: Ungdomslaboratoriet, f.eks.)

Lige nu har centret bare én egentlig medarbejder, nemlig mig, centerleder på halv tid. Men når dette læses har vi også en lektor, Henrik Busch, og en ung videnskabelig medarbejder, Tom Børsen Hansen. Desuden regner vi med at have en professor og endnu en adjunkt i løbet af efteråret 02. Bemærk de 'almindelige' universitetstitler: der er tale om ansættelser på sædvanlige 'delte' betingelser: forskning og undervisning. Meget af undervisningen vil bestå i deltagelse i de aktiviteter og udviklingsprojekter, jeg fortæller om om lidt.

Der er også to ph.d studerende knyttet til centret, Kathrine Eriksen og Ole Ravn Christensen (begge på DCN-stipendier) og vi har en række specialestuderende: To af de nylige kandidater i matematik har således haft tilknytning til centret. Her skal det også nævnes at CND medvirker til etableringen af en national forskerskole for ph.d-studerende i naturfagenes didaktik.

I efteråret 01 stod CND for et tværfagligt semesterkursus i naturfagsdidaktik for 3. års- og kandidatstuderende. Dette forløb bliver gentaget. Og vi arbejder med på at styrke studenterinstruktorernes pædagogiske muligheder, ved afholdelse af jævnlige introduktions-workshops.

Ganske snart vil CND overtage kørslen af de adjunktpædagogikumforløb, som har været godt i gang i en årrække. Når det sker, er det tanken at udvide kundekredsen for disse aktiviteter til også at omfatte interesserede og/eller trængende fastansatte.

Når man kigger efter, finder man adskillige af disse pædagogisk/didaktiske centre, også på andre fakulteter ved KU. Ofte lægger disse centre særlig vægt på IT-baseret læring og undervisning. På NAT-KU er der blevet oprettet et særskilt center, NIK, hvor IK står for IT-kompetence. CND og NIK samarbejder allerede om didaktiske aktiviteter – og vi vil udbygge samarbejdet, så vi i fællesskab kan bidrage til udviklingen af ny universitets-pædagogik, der i højere grad end nu udnytter IT-muligheder i undervisningen.

Den mest ambitiøse studieforløbsundersøgelse, som CND har givet sig i kast med indtil nu, hedder SUS. Den omfatter alle fakultetets studiestartere e2001 (og vil senere, via registersøgninger, komme til at inddrage de seneste fem optagelsesår). Forhåbentlig vil den kunne give vurderinger af, hvilke faktorer, der er vigtige for en højere gennemførelsesprocent

Sådan ligger landet for CND-KU i startfasen. Vi har nogle år til at retfærdiggøre os i – og til at gøre noget for at ændre perspektivet for universitetsuddannelser og for universitetsansatte. Om disse ting er det nok bedst, hvis jeg formulerer mig i et par personlige bemærkninger, der mest har med matematik at gøre.

Det er ikke nogen tilfældighed at matematikdidaktik er den mest udviklede specialisering af didaktikken. Matematik er jo ofte et ganske tanketungt gebet, og det kræver omhu hos den lærende at komme ordentligt ind på livet af faget. Læreren opdager derfor næsten automatisk - måske undtagen i de mest upersonlige forelæsningssituationer - at budskabet (og dets 'indpakning') skal formes omhyggeligt hvis det skal nå frem. Behovet for overvejelser om virkemidler kommer helt af sig selv.

Det er ikke det samme som at vi kan og bør opfylde disse behov hver især, og fra grunden af. Ikke desto mindre er det ofte grundholdningen. Kan du, kære læser, genkende denne opfattelse af matematikdidaktik 'i praksis'? En side af vores liv med matematik, som vi gerne vil tage alvorligt - og som vi faktisk ofrer en del opmærksomhed, men som vi nok ofte er tilbøjelig til at opfatte som af en vis 'sekundær' karakter.

Der er ingen tvivl om at den enkelte universitetslærer har mange gøremål, og at de konkurrerer om hans/hendes tid og opmærksomhed. Karrierestrukturen hjælper os ganske vist med at foretage prioriteringer, fordi den (strukturen) har væsentlig bedre metoder til måling – og honorering - af den professionelle kvalitet af forskningsindsatsen. Det nyeste regelsæt for stillingsstrukturen gør en del for at give undervisningssiden et 'prestige'løft, men som særlig markante opleves ændringerne ikke.

Det generelle klima er dog ved at skifte – jf. det politiske pres, og de ændrede samfundsbetingelser, jeg hentydede til før. Men der er fortsat plads til lidt from ønsketænkning: Måtte vi universitetsforskere – og altså også matematikere – opfatte vores undervisning som en beskæftigelse der er underlagt de samme høje professionaliseringskrav, som vi føler over for vores forskning.

Bodil Branner og Dansk Matematisk Forening

Af: Hans Jørgen Munkholm (på vegne af DMFs tidligere og nuværende bestyrelse og Matildes redaktion)

Af dagsordenen for generalforsamlingen ser jeg, at selv om Bodil er villig til at fortsætte i bestyrelsen, så træder hun nu tilbage som formand. Jeg synes derfor der er grund til at fremhæve nogle af de mange ting, Bodil har gjort for dansk matematik i sin tid som formand for DMF.

Jeg sad med i bestyrelsen, da Bodil blev valgt som formand d.17. februar 1998 og i de første to år af hendes formandsperiode. Måske gør det mig inhabil; men jeg vælger at betragte den anden side af sagen: Jeg har førstehåndskendskab til en del af formandsperioden, og jeg kan bevidne, at Bodil ikke blot har været formand af navn. Det har i høj grad været hendes ideer, der har ligget bag de mange ændringer, som foreningen har gennemgået i de seneste år.

Formatet for generalforsamlingen i 1998 var i sig selv en nyskabelse. Den foregik samtidig på 6 forskellige universiteter, kædet sammen pr. videolink. Det skal dog indrømmes, at arrangementet ikke blev nogen overbevisende demonstration af video-link-systemets anvendelighed, og i referatet af den nye bestyrelses første møde, som fandt sted ni dage senere, hedder det bl.a. ``Med hensyn til DMF foredrag med video link var der moderat interesse. Det foreslås at afholde ca. et foredrag om året.*)..... Vi synes ikke det er nødvendigt med en videolinkgruppe."

Fra starten lå det Bodil meget på sinde at gøre foreningens dækningsområde bredere, både geografisk og fagligt. Ved det netop omtalte bestyrelsesmøde sørgede hun således for, at der blev udpeget kontaktpersoner ved de tre matematiske institutter i landet, som ikke var repræsenteret i bestyrelsen. Senere tog hun initiativ til en ændring af foreningens statutter, så vi ved dette års generalforsamling kan se forslag om en ordinær bestyrelse, der repræsenterer alle de matematiske miljøer ved danske universiteter, ligesom den demonstrerer foreningens interesse for matematikkens anvendelser.

Det var også Bodil, der gennemførte en hårdt tiltrængt reform af optagelsesproceduren for nye medlemmer. Tidligere kunne man kun optages, hvis man anbefaledes af to eksisterende medlemmer, hvad der i høj grad gav foreningen karakter af en lukket loge, hvor ``udenforstående" ikke havde nogen umiddelbar chance for at afgøre, hvorvidt de og deres faglige interesser passede ind. Som medlem af bestyrelsen også før reformen føler jeg trang til at understrege, at der næppe var nogen i bestyrelsen, som aktivt ønskede logepræget, men vi tog altså - i modsætning til Bodil - ikke de nødvendige skridt til at afskaffe det. Nu blev der lagt et ansøgningsskema ud på internettet, og dette viste sig hurtigt at gøre rekrutteringsbasis bredere. Jeg har ikke adgang til de seneste oplysninger - formandens beretning for 2001 er endnu ikke kommet - men beretningerne fra 2000 og fra 1999 viser hver en medlemsfremgang på ca. 10%.

Bladet Matilde er den sidste af Bodils nyskabelser for DMF, jeg vil nævne her, ikke fordi der ikke er andre ting, som kunne/burde omtales, men fordi netop Matildes eksistens giver læseren mulighed for selv at slå tilbage og kigge efter.

Jeg kan dog ikke slutte min lille epistel uden at bemærke, at Bodil ved siden af formandskabet for DMF også har haft energi til at virke som vicepræsident i EMS, hun har været medlem af det Naturvidenskabelige Forskningsråd, og hun har været aktiv i EWM, både nationalt og

internationalt. I dansk matematik har vi grund til at være imponerede over den arbejdskraft, Bodil har, og taknemmelige for den måde hun bruger den på.

*) Så vidt jeg husker blev endda ikke dette moderate mål nået.

Odense d. 5. februar 2002

Interview med Uffe Haagerup

Af: Jacob v. B. Hjelmborg, Institut for Epidemiologi, Email: Jhjelmborg@health.sdu.dk

Det følgende interview er blevet til ved samtaler med professor i matematik ved Syddansk Universitet, Uffe Haagerup. Professor ved universitetet i Oslo, Erling Størmer og professor ved Collège de France i Paris, Alain Connes, har bidraget med kommentarer. Interviewet foregik i januar 2002.

Begyndelsen

Jacob: Hvornår er du født?

Uffe: Den 19. december 1949 i Kolding.

Jacob: Hvor er du vokset op?

Uffe: I Fåborg på Sydfyn fra jeg var halvandet år gammel.

Jacob: Hvor har du gået i skole og hvornår blev du student?

Uffe: Jeg gik i skole i Fåborg, og siden i gymnasiet i Svendborg, hvor jeg blev student i 1968. Der var ikke noget gymnasium i Fåborg.

Jacob: Jeg vil gerne spørge dig om din studietid. Hvad er din uddannelse?

Uffe: Jeg startede i september 1968 på matematik-fysik studiet ved Københavns Universitet. Min bror Jens, som er fire år ældre end mig, læste også denne retning i København. Det lettede studiestarten for mig, at han havde taget turen først, og at jeg kunne spørge ham til råds. På 2. del af studiet valgte jeg fysik.

Jacob: Hvorfor?

Uffe: Fysik havde på 2. del en meget klar kursusstruktur, og jeg tog hovedkurser i almen relativitetsteori og videregående kvantemekanik, som jeg var meget interesseret i. Matematik studiet havde mindre hierakisk opbygning, og appelerede ikke så meget til mig på det tidspunkt.

Jacob: Du er altså på vej til at blive fysiker. Hvorledes kommer du ind i matematik?

Uffe: Jeg tog et valgfrit kursus i matematik, hvor artikler af I.M. Segal blev gennemgået. Det handlede om matematisk behandling af elementar partikelfysik. Det var organiseret af Christian Berg, Mogens Flensted Jensen og Esben Kehlet. Her blev jeg præsenteret for operator algebra teori, idet Segal har von Neumann algebra teori som basis.

Jacob: Operator algebra teori bliver senere dit hovedområde, og dette var altså indledningen?

Uffe: Ja. En anden væsentlig årsag til netop operator algebra var, at jeg sammen med Søren Kjær, som var nylig kandidatstipendiat, gennemgik "Lecture notes on Tomita teori" af Takesaki, som netop var blevet udgivet.

Jacob: Det må have været omkring 1972?

Uffe: Ja, sommeren 1972. Tomita og Takesaki's arbejder blev et gennembrud på det tidspunkt i

operator algebra, og kom til at præge de næste 10 års forskning.

Jacob: Så var du inde i matematik, specielt operator algebra. Hvornår skrev du speciale?

Uffe: Jeg ville gerne, at mit speciale skulle omhandle Tomita-Takesaki teori, specielt med henblik på at simplificere beviset for deres hovedsætning. Jeg gik til G. K. Pedersen, som synes at dette var fint, for det var efterspurgt, og han blev min vejleder i efteråret 1972.

Jacob: Hvordan gik det?

Uffe: Midtvejs blev jeg mere interesseret i anvendelse af teorien, og fik lavet resultater der senere blev til artiklen; "The standard form of von Neumann algebras". En del af disse resultater blev også uafhængigt fundet af Connes og Araki. Dette blev mit speciale, som var færdigt i foråret 1973.

Jacob: Du blev altså færdig med dit speciale, hvad skete der herefter?

Uffe: Der var flere årsager der gjorde, at jeg udskød min kandidateksamen. Dels var min kæreste, nu kone, Pia ikke færdig med sit speciale, dels kom der en tre ugers konference/sommerskole i operator algebra og matematisk fysik i København i 1973. Jeg fik lavet en anden artikel om normale vægte, som blev præsenteret ved sommerskolen. Sommerskolen gav også anledning til, at jeg fik opbygget et netværk til folk i operator algebra.

Jacob: Du har altså to originale arbejder inden du færdiggør din kandidateksamen i januar 1974.

Uffe: Ja.

Jacob: Hvad gjorde du herefter?

Uffe: Jeg søgte hvad der var af stipendie muligheder, men fik afslag. Det var et vanskeligt tidspunkt, og der kom en ny stillingsstruktur. De daværende kandidat-instruktorater, som var meget favorable idet de havde varighed i op til 6 år og med god mulighed for forskning, blev sløjfet og adjunkt-lektor ordningen kom istedet. Jeg blev så lærerkandidat på Nørre Gymnasium i Husum.

Jacob: Hvor længe var du der?

Uffe: I et halvt år. Jeg søgte gymnasiestillinger på det tidspunkt, samt de to universitetsstillinger der var - en i Odense og en i København. På den gamle adjunkt-lektor ordning kunne man blive adjunkt på sit kandidat-eksamensbevis, hvor der idag kræves en Ph.D.-grad for dette.

Jacob: Overvejede du at søge til udlandet på dette tidspunkt?

Uffe: Egentlig ikke. Takesaki var villig til at anerkende mit speciale som en amerikansk Ph.D.-afhandling og opfordrede mig til at søge en post. doc. stilling ved UCLA.

Jacob: Men du afslog.

Uffe: Ja, jeg var måske ikke helt sikker på mig selv - havde kun lavet forskning i halvandet år. Derudover begyndte det at stramme til med hensyn til gymnasiestillinger, hvilke min kæreste Pia også søgte, og de næste fem år så ikke ud til at blive bedre i den henseende. Jeg så et problem i at tage tre år til USA og så komme hjem igen.

Jacob: Jeg vil vende tilbage senere med spørgsmål om stillinger i udlandet. Hvornår mødte du Pia?

Uffe: På 2. studieår, dvs. i 1970. Vi gik på samme hold.

Forsker

Jacob: Du bliver ansat som adjunkt i Odense i en alder af 24 år. Baggrunden for ansættelsen er altså dine to artikler og din kandidatgrad?

Uffe: Ja.

Jacob: Hvad laver Pia i denne periode?

Uffe: Hun bliver ansat som lærerkandidat på Skt. Knuds Gymnasium i Odense for efteråret 1974, og i foråret 1975 har hun et vikariat på universitetet i Odense med undervisning i statistik. Fra sommeren 1975 er hun fastansat på Skt. Knuds Gymnasium.

Jacob: I får altså begge job i Odense på det tidspunkt, hvor du bliver adjunkt. Hvad får nu indflydelse på din forskning?

Uffe: Jeg havde nogle ideer og var meget alene. Nærmeste kollega var Niels Jørgen Nielsen i Banachrumsteori. Men det var egentlig ikke det store problem at være alene i Odense, for jeg havde etableret et netværk udadtil under førnævnte sommerskole i København i 1973. Det største problem for mig var afgjort tiden, for vi var kun få ansatte, og måtte undervise en hel del - minimum var seks timer om ugen. Men det lykkedes mig at få stipendium, og dermed undervisningsfri, i to år.

Uffe Haagerup

Jacob: Hvornår forløb stipendiet, og hvornår blev du lektor?

Uffe: Jeg fik stipendiet i 1977, og havde det indtil jeg blev lektor i 1979.

Jacob: Du nævnte før, at undervisningsbelastningen var minimum seks timer om ugen. Gælder det samme idag?

Uffe: Ja. Adjunkter har dog idag mulighed for et halvt års orlov, samt maximalt fire undervisningstimer om ugen.

Jacob: Du bliver Danmarks yngste professor i matematik. Hvornår var det, og hvad skete der herefter?

Uffe: Det var i august 1981. I 1982-83 er jeg et halvt år på UCLA og et halvt år i Philadelphia. Den senere Fields medalist, Vaughan Jones, var begge steder samtidig med mig, hvilket ikke var planlagt, men gjorde, at jeg kom ind i delfaktor teori.

I 1988-1989 har jeg orlov igen. Sammen med Erling Størmer, professor i Oslo, arrangerede jeg et operator algebra år ved Mittag-Leffler instituttet i Stokholm.

Yderligere havde jeg orlov i foråret 2001, hvor jeg var ansat af CLAY-fonden ved MSRI i Berkeley. Jeg var medorganisator af operator algebra året 2000-01 her.

Jacob: Havde du god tid til forskning under dit ophold ved MSRI i Berkeley?

Uffe: Ja, det må jeg sige. Det var en meget positiv oplevelse, som jeg ikke har oplevet siden min orlov i 1982-83. Mange af mine nære samarbejdspartnere var på MSRI, og vi fik lavet en del.

Champagne problemet

Jacob: Du nævnte, at du i sidste del af din studietid fik opbygget et netværk til forskningskollegaer. Kan du uddybe?

Uffe: Først og fremmest lærte jeg Alain Connes at kende. Jeg fulgte tæt Connes' arbejde med injektive von Neumann algebra faktorer, som blev færdigt i 1975.

Jacob: Hvori bestod Connes' champagne-problem?

Uffe: I 1978 besøgte jeg Connes i to uger i Paris og på hans forældres landsted i Normandiet. Vi diskuterede det åbne problem - det senere omtalte champagne problem, om der kun var én hyperendelig III_1-faktor?

Jacob: Hvad kom der ud af dette?

Uffe: Først under min orlov i 1982-83 fik jeg for alvor mulighed for at arbejde med dette problem. I første omgang blev det til en væsentlig reduktion i beviset for Connes' klassifikationssætning for injektive von Neumann faktorer, men først i efteråret 1984 fik jeg løst problemet med III_1-faktoren - det vil sige, der er kun én.

Jacob: Det kom i Acta Matematica i 1987?

Uffe: Ja.

Jacob: Er det dit bedste resultat?

Uffe: Ja, det er det.

Jacob: Vaughan Jones foreslog i forbindelse med dette interview, at spørge dig om hvilket resultat der er dit bedste. Det har du så svaret på. Var det hårdt at opnå?

Uffe: Det var mest sjovt. Jeg troede, at jeg var tæt på i sommeren 1983, men kunne ikke få kontinuert arbejdstid til dette, og valgte at udskyde det til sommeren efter. Det viste sig at være heldigt, for min oprindelige tilgang faldt til jorden. Den hårdeste periode var faktisk de to måneder der gik fra at jeg mente, at have løst problemet til at have skrevet det ordentligt op. Normalt er jeg meget åben overfor kollegaer, men det problem havde efterhånden opnået en sådan status, at man

ikke bare kunne sige at have løst det uden at have dokumentationen klar.

Jacob: Jeg spurgte Alain Connes, om han ville stille spørgsmål til dig og/eller karakterisere dig i forbindelse med interviewet. Connes valgte det sidste og skrev følgende:

Uffe is the best analyst I ever had a chance to colaborate with. I remember vividly his first appearance in the field of operator algebras and the striking elegance, clarity and strength of his contributions. From my own perspective an analyst is characterized by the ability of having "direct access to the infinite" and Uffe possesses that quality to perfection. Our roads did cross several times, the most notable being the fight with the hyperfinite III_1 on which we had long and intense discussions in my country house, ending up when both of us got a terrible migraine.

I just want to congratulate Uffe for his great achievements, and say "chapeau bas" to this wonderful analyst!

Alain Connes.

Hovedtaler ved ICM 2002

Jacob: Udover en flaske champagne fra Connes har du modtaget priser - kan du uddybe?

Uffe: Der kom nogle i forlængelse af løsningen af champagne problemet, bla. Friedman prisen [The Samuel Friedman Award, red.], som årligt skulle uddeles til en dansk forsker eller kunstner. Det var i april 1985, og der medfulgte 10000 $.

Jacob: Du har fået Ole Rømer medaljen, som nok er den fornemste danske pris i naturvidenskab. Hvornår var det?

Uffe: Det var i foråret 1989.

Jacob: Jeg vil gerne skrue tiden tilbage igen. Hvem var, udover Connes, i det netværk, som du fik etableret i 1973?

Uffe: Det var Takesaki, Kadison, van Daele, og jeg havde forbindelse til den norske operator algebra gruppe; Størmer, Bratteli, Skau, Alfsen, Landstad og Digernes. Jeg blev medvejleder for flere af van Daeles studerende, heriblandt De Canniére.

Jacob: Kadison er en af pionererne i operator algebra.

Uffe: Ja, han sørgede for, at jeg kom til Philadelphia i 1978, hvor jeg mødte Effros, som kom til at betyde meget for mig senere, samt A. Wassermann, som var Ph.D. studerende på det tidspunkt.

Jacob: I forbindelse med dette interview skrev Erling Størmer følgende:

Uffe og jeg har flere fellesarbeider. De fleste har fremkommet på følgende vis. Jeg har jobbet i lengre tid på et problem. Så har jeg spurt Uffe om hjelp, og så har han, vanligvis på kort tid, vist det teknisk vanskelige resultatet som ga løsningen. Et godt eksempel er fra en konferanse i Romania. Jeg skulle holde foredrag om diameterformelen for det normale tilstandsrommet til faktorer. Men jeg var litt usikker, for det var to kandidater til formelen. Så jeg snakket med Uffe. Jo, sa han; det måtte være den ene. Så om kvelden satte han seg for å regne, og neste morgen kom han med et 6 siders bevis for den formelen han sa måtte være den riktige. Så da kunne jeg holde foredraget mitt med en god følelse.

Erling Størmer.

Jacob: Har du en kommentar til dette?

Uffe: Jeg kan godt huske historien; Det var i Rumænien i 1983. Det blev starten på et langt og frugtbart samarbejde med Erling Størmer, specielt arbejdet med klassifikation af tilstande på von Neumann algebraer, som vi startede på, mens vi delte lejlighed ved MSRI i 1985. Vi blev først færdige i 1987, så det var ikke alle problemer, der kunne klares på nogle få timer.

Jacob: Et opslag på MathSciNet under "Haagerup" viser, at du er forfatter og medforfatter på over 65 publicerede artikler, og titlerne på disse antyder stor diversitet. Har du et yndlingsområde?

Uffe: Nok ikke et bestemt emne, men nok mere det at grave sig ned i et problem, og at kunne bidrage med væsenligt nyt. Diversiteten, du nævner, udtrykker nok mere det, at jeg har været i branchen i snart 30 år. Jeg går ikke efter mode-emner. De problemer jeg går efter, kommer nok mere fra mit eget hoved, end fra hvad andre går og laver på et givet tidspunkt. En undtagelse er dog nok delfaktor teori, som startede med, at jeg skulle finde et problem til en dygtig Ph.D. studerende, John Schou, og valgte delfaktor teori, som var et varmt emne på det tidspunkt. Det endte så med at blive mit eget hovedforskningsområde i 6-7 år.

Jacob: Hvad er dit hovedforskningsområde nu?

Uffe: Det er fri sandsynlighedsteori samt stokastiske matricer, hvor jeg forsøger at anvende denne teori på mere klassiske problemer indenfor operator algebra teori. Der er et resultat med Steen Thorbjørnsen, som har betydning for klassifikation af C*-algebraer. Et andet resultat er med Ken Dykema og omhandler "invariant subspace"problemet relativt til en von Neumann algebra.

Jacob: Professor på UCLA, Ed Effros, udtalte under et foredrag følgende: "Be aware of what Haagerup might keep under his desk". Du har over 65 publicerede artikler - hvor mange resultater er upublicerede?

Uffe: Jeg vil gerne indrømme, at jeg er kendt for at have en del upublicerede resultater, som cirkulerer i foreløbigt håndskrevne udgaver. Det sjoveste i processen har været at få problemet løst, og jeg har ikke altid kunnet tage mig sammen til at pudse resultatet af til publikation.

Jacob: Det får mig pudsigt nok til at spørge dig om din position som hovedredaktør på Acta Mathematica.

Uffe: Kan vi udskyde det til senere i interviewet?

Jacob: Gerne.

Jacob: Kan du nævne andre af dine resultater, som du værdsætter højt?

Uffe: Jeg var den første, der lavede en generalisation af et Lp-rum hørende til en vilkårlig von Neumann algebra. Disse anvendes stadig af folk der arbejder på grænseområdet mellem Banachrumsteori og operator algebra. I 1981 fik jeg løst et andet problem formuleret af Connes, nemlig at nukleære C*-algebraer er det samme som amenable C*-algebraer. Tomita-Takesaki teori gav førnævnte resultat med Størmer om klassifikation af tilstande for von Neumann algebraer.

Jacob: Af nyere resultater?

Uffe: Det er nok konstruktionen af delfaktorer med index større end 4, men tæt på 4. Specielt er der en med index $\frac{5+\sqrt{13}}{2}$.

Jacob: Konstruktionen af sidstnævnte er vist ret utraditionel?

Uffe: Ja, man har søgt større maskiner til at konstruere disse, hvor min konstruktionsmetode har mere karakter af "brute force", og eksemplet er eksotisk, men bliver brugt som test-tilfælde for større maskiner.

Jacob: Anvender du matematisk software i din forskning?

Uffe: Ja. Konkrete problemer for delfaktorer ender som regel med, at man skal løse ret komplekse polynomielle ligningssystemer, hvor man med fordel kan anvende computer algebra pakker, "symbolic computation".

Jacob: Du skal være ``plenary speaker" ved ICM 2002 i Beijing. Det er blandt andet ved den lejlighed, at Fields-medaljen bliver uddelt. Der er 20 "Plenary talks" og en række foredrag fordelt på 19 sessioner. Seneste danske hovedtalere ved ICM er Børge Jessen i Amsterdam i 1954, og Harald Bohr i 1950. Sidstnævnte i forbindelse med overrækkelsen af Fieldsmedaljen til L. Schwartz.

Uffe: Jeg er naturligvis meget glad og beæret over at være inviteret.

Jacob: I 1986 talte du ved en lignende lejlighed om Connes champagne problem, dog ikke som ``plenary speaker". Hvad skyldes invitationen denne gang?

Uffe: Jeg kan ikke pege på et bestemt resultat dennegang. Årsagen til invitationen skyldes nok min generelle indsats indenfor feltet over en længere årrække.

Acta Mathematica

Jacob: Jeg erindrer, at du havde undervisningsorlov i Odense i foråret 2000 uden at du rejste. Var det for at få tid til din forskning?

Uffe: Ja, og det kan jeg godt finde på at gøre igen.

Jacob: Var det for egen regning, dvs. med reduceret løn?

Uffe: Ja, det var det.

Jacob: Hvorledes er matematikere i Danmark stillet idag?

Uffe: Jeg synes, at vi er blevet presset gennem årene til mere undervisning og administration. Politikerne er mindre interesserede i forskning. Godt nok er jeg med i et forskningscenter [MaPhySto, red.], men pengene kan ikke benyttes til frikøb fra undervisning. Det er selvfølgelig positivt, at vi får penge til konferencer og post.doc. Stillinger, men det tager altsammen tid.

Jacob: Er du bekymret for fremtiden?

Uffe: Jeg er mest bekymret for vores unge forskere, og det at vi måske kommer til at ansætte de forkerte, når vi pludselig om ti år mangler folk og skal ansætte et stort antal.

Jacob: Altså situationen fra 1960'erne.

Uffe: Ja. Men jeg er også bekymret for vilkårene for universitetsansatte - at vilkårene skal blive så

dårlige, at vi ikke kan tiltrække og fastholde unge dygtige folk.

Jacob: Hvorledes ser du uddannelsen i matematik generelt?

Uffe: Med hensyn til Ph.D. uddannelsen, så var det gamle system, hvor man kunne få kandidatstipendium i op til seks år, og hvor ingen holdt øje med een, for slapt. Nu er vi måske på vej i den modsatte grøft med et lidt firkantet system. Jeg så gerne mere "elastik" med plads til et fjumre-år. Jeg vil ikke gå ind på folkeskole og gymnasie området.

Jacob: Hvordan ser du fremtiden for operator algebra i Odense?

Uffe: Mikael Rørdam har for nyligt sagt ja til at tiltræde som professor i operator algebra 1. juli 2002, så jeg ser ret lyst på fremtiden, både hvad angår forskning, og det at skabe et godt miljø for Ph.D. studerende i operator algebra i Odense.

Jacob: Du blev i år 2000 udnævnt til ansvarshavende redaktør for tidskriftet "Acta Mathematica", som udgives ved Mittag-Leffler instituttet i Stokholm. Kan du beskrive dit arbejde?

Uffe: Jeg har formelt titel af ordførende redaktør. Jeg skal sammen med de fire andre redaktører forsøge at udvælge de bedste af de artikler som indsendes.

Jacob: Det lyder som et stort arbejde. Hvor stor en del af modtagne artikler bliver optaget i Acta?

Uffe: Det er et stort arbejde, og bestemt større end jeg havde forudset, da jeg sagde ja til jobbet. Med hensyn til optagelse af artikler kan man godt sammenligne med et isbjerg; Det man ser i Acta udgør kun 10% af det som indsendes. Det betyder, at vi bruger meget af vores tid og af referee'ernes tid på afvisning, hvilket ikke er opmuntrene.

Jacob: Hvorledes ser du Acta nu, og vil du vove at spå om den fremtidige udvikling?

Uffe: Jeg kunne godt ønske mig tilbage til den tid, hvor tidsskrifternes hovedformål var at gøre forskningsresultater tilgængelige. De fleste tidsskrifter er nok inde i en brydningstid pga. den lette adgang til publikation gennem preprint databaser, og der er måske nok en tendens til at folk bruger tidsskrifter som Annals og Acta til at få et "guldrandet papir", som på hjemmebanen letter adgangen til fondsmidler, jobs og forfremmelse. Det er ikke en udvikling, som jeg er glad for, men håber at Acta og de fleste af de andre gode matematiske tidsskrifter vil få en fornuftig rolle i det fremtidige publikationsspektrum.

Jacob: Kun fire personer før dig har besat hovedredaktørposten på Acta siden stiftelsen i 1882. Måske kommer du til at sidde længe på posten og præge tidskriftet betydeligt?

Uffe: Sidste redaktør, Carleson, var hovedredaktør i 12 år, men meget engageret i Acta i de foregående 30 år. Redaktøren bliver nu udvalgt af bestyrelsen på Mittag-Leffler Instituttet for 3 år ad gangen. Jeg ved ikke hvor længe de vil have mig, eller hvor længe jeg selv har lyst til at fortsætte.

Ungdomsår

Jacob: Hvornår blev du interesseret i matematik?

Uffe: Jeg havde den store fordel, at min storebror, som er fire år ældre end mig, meget gerne ville lære mig det, som han lærte i skolen.

Jacob: Hvad var det typisk?

Uffe: Almindelig regning, men jeg fik fat i en Erlang tabel, da jeg gik i fjerde klasse, så jeg kunne regne med trigonometriske funktioner og logaritmer.

I gymnasiet blev jeg meget optaget af "Feynman Lectures" og noter om kompleks funktionsteori fra min bror, som var på matematik-fysik studiet i København på det tidspunkt. Minimalflader og hyperbolsk geometri interesserede mig også meget. Jeg var nok endt i geometrisk retning, hvis ikke operator algebra.

Jacob: Med hensyn til geometrisk retning, så har du et fællesarbejde med Hans Jørgen Munkholm om hyperbolsk geometri. Det er en artikel i Acta fra 1981. Du er altså ikke blot "skabs-geometriker"?

Uffe: Nej. En del af det fællesarbejde går nok tilbage til min interesse i hyperbolsk geometri i ungdomsårene. Jeg har også senere skrevet artikler om operator algebra, hvor hyperbolske rum spiller en væsentlig rolle.

Jacob: Hvorfra stammer din interesse for landkort og atlas?

Uffe: Som 10 årig startede jeg som medhjælper hos den lokale landinspektør i Fåborg. Jeg fik efterhånden lov til at lave beregningsopgaver på landinspektørkontoret.

Jacob: Dette gav på et tidspunkt anledning til medieomtale.

Uffe: Ja, som 14 årig fik jeg lejlighed til at lave en udstykningsplan for et større sommerhusområde. Det var en lidt pudsig historie, for et københavnsk ingeniørfirma havde først fået opgaven, men havde ikke været grundige nok, så landinspektøren fik opgaven, hvor jeg lavede et løsningsforslag, som istedet blev vedtaget af Horne Kommune. Landinspektøren kunne ikke lade være med at lave grin med, at Horne Kommune ikke kunne få en brugbar løsning fra et ingeniørfirma, men istedet fra en 14 årig. Historien kom først i den lokale avis, og senere i landsdækkende blade i mere eller mindre forvansket form.

Jacob: Du blev immatrikuleret på Københavns Universitet i 1968. Var du med i "ungdomsoprøret" ?

Uffe: Det interesserede mig ikke så meget. Jeg startede i København midt i det hele, og tænkte mest på at overleve det første studieår både socialt og fagligt.

Jacob: Lige en indskydelse. Du er vokset op på Fyn - havde du valgt Odense som studiested, hvis det havde været muligt?

Uffe i barndomshjemmet i Fåborg. Den fjortenårige landmålerassistent viser sit forslag til udstykning af et større sommerhusområde.

Uffe: Jeg var 18 år dengang, og klar til at komme rigtigt hjemmefra. Odense ville nok have været for tæt på.

Jacob: Hvorledes gik filosofikum for dig?

Uffe: Jo, det var nok det eneste "oprør", som jeg har deltaget i. Der var en del ballade med filosofikum; Dårlige forhold og store hold. Bla. blev studenterne tvangsfordelt mellem forelæserne. Der var på det tidspunkt en ung meget populær ekstern underviser fra Norge, Sellin, og jeg valgte at følge hans undervisning med det formål, at få mulighed for at afslutte filosofikum allerede efter et halvt år. Sellin arrangerede, at de som ikke var formelt tilmeldt hans hold kunne gå til eksamen i Norge. Vi var 24 på en fremragende tur til Trondhjem, hvor vi gik til eksamen. Næste år var der 200, som tog til Norge for at gå til eksamen. Det gav en hæftig politisk debat, som resulterede i at filosofikum blev afskaffet året efter.

Far

Jacob: Hvad er "Haagerup Webdesign" og "The Donald Duck Club", som findes på internettet?

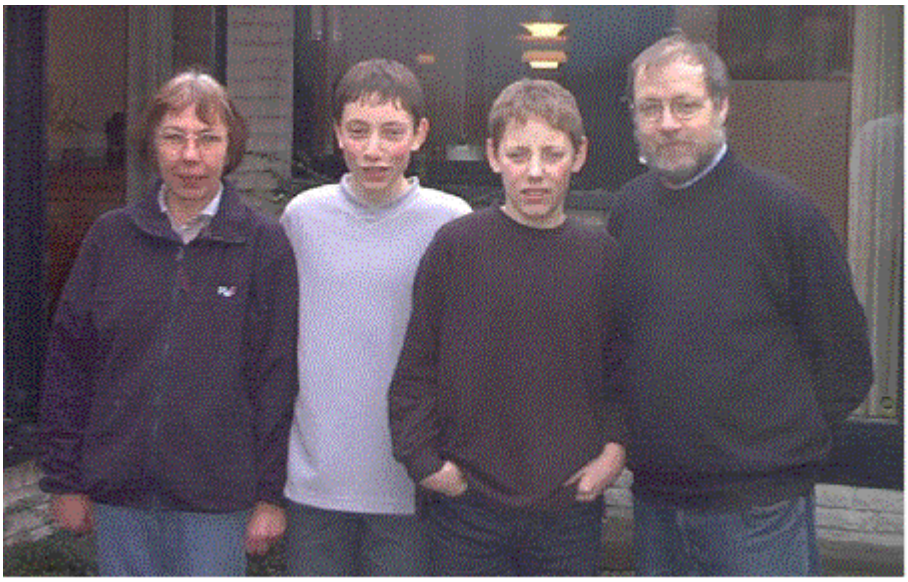
Uffe: Jeg har aldrig rigtig beskæftiget mig med hvad der foregår i computerverdenen, men det gør mine børn, Peter og Søren. De har startet "Haagerup Webdesign" for at supplere deres lommepenge.

Jacob: Hvor gamle er de?

Uffe: 14 og 12 år. Derudover driver de "www.donaldduckclub.com", som er blevet en populær Disney-fan klub på nettet.

Jacob: Det har været en spændende samtale, og jeg vil takke dig herfor. Inden vi slutter vil jeg gerne stille dig et sidste spørgsmål: Har du overvejet job i udlandet?

Uffe: Jeg har aldrig søgt job i udlandet, men har fået enkelte favorable tilbud, som jeg har afslået af hensyn til min kones arbejde, og fordi vi synes, at vores børn skal vokse op i Danmark.



Familien Haagerup. Fra venstre: Pia, Peter, Søren og Uffe.