MATEMATISK KODNINGSTEORI

Et moderne digitalt kommunikationssystem udnytter avanceret matematik på mange forskellige måder. Ved kildekodning (datakompression) forsøger man at repræsentere data så effektivt som muligt og ved at benytte fejlkorrigerende koder ønsker man at opnå hurtig sikker og pålidelig kommunikation. Når data lagres eller transmitteres kan man ikke være sikker på at de data man aflæser er de samme som de, der blev lagret eller afsendt. Hvis A ønsker at sende information til B, repræsenteres denne først så effektivt som muligt ved brug af kildekodning, og derefter danner A et kodeord ved at tilføje ekstra symboler. Denne proces kaldes *indkodning*. Det ord B modtager er ændret på grund af støj under transmissionen, men ved at benytte de tilføjede symboler er det ofte muligt at genskabe det sendte kodeord- i det mindste med stor sandsynlighed. Denne proces kaldes *afkodning*. Ved konstruktion af koder er der modstridende ønsker: (1) Koderne skal have en struktur således at ind-og afkodningsalgoritmerne har lav kompleksitet og (2) Koden skal kunne rette flest mulige fejl med færrest mulige ekstra symboler. De matematiske problemer der opstår i forbindelse med konstruktion og brug af koder kan behandles med algebraiske, geometriske, sandsynlighedsteoretiske og spilteoretiske metoder. Selvom de spørgsmål man ønsker at besvare har et konkret teknisk udgangspunkt leder det til en lang række vigtige og interessante matematiske problemer.
Fejlrettende koder anvendes i dag i en lang række sammenhænge, i satellitkommunikation, i CD og DVD afspillere, i mobilkommunikation, i modems og i adskillige lagermedier.
Hovedformålet med dette projekt er en videreførelse af gruppens arbejder med konstruktion og analyse af optimale koder og de tilhørende algoritmer.

En klassisk kode

Vi har 16 forskellige meddelelser som vi vil sende (eller lagre). Vi vælger at beskrive dem som ord af længde 4 skrevet med symbolerne 0 og 1, d.vs. at de 16 meddelelser altså er $0000, 1000, 0100, \ldots, 1111$. I stedet for at sende ordene direkte vil vi tlføje ekstra symboler på en systematisk (og smart) måde som sætter os i stand til at rette 1 fejl. For at forklare det indfører vi addition $+$ af symbolerne ved: $0+0=0, 1+0=0+1=1, 1+1=0$ og til ordet (x_1, x_2, x_3, x_4) tilføjer vi så $x_5 = x_1+x_2+x_4, x_6 = x_1+x_3+x_4, x_7 = x_2+x_3+x_4$. På denne måde bliver der til de 16 meddelelser knyttet 16 *kodeord* som det fremgår af nedenstående.

meddelelse	kodeord
0000	0000000
1000	1000110
0100	0100101
100	1100011
0010	0010011
1010	1010101
0110	0110110
1110	1110000
0001	0001111
1001	1001001
0101	0101010
1101	1101100
0011	0011100
1011	1011010
0111	0111001
1111	1111111

Koder på grafer

Der er stor interesse for grafteoretiske beskrivelser af fejlkorrigerende koder som en mulig vej til koder

med lavere dekodningskompleksitet. De fleste resultater er dog asymptotiske og ikke overbevisende for anvendelser. Vi søger i dette projekt specifikke konstruktioner, især konstruktioner som udnytter tidligere resultater om sammensatte koder og koder baseret paa endelige geometrier.

Dekodning af Reed-Solomon koder og sammensatte koder

Nye versioner af dekodningsmetoder for Reed-Solomon koder har åbnet muligheder for at rette væsentlig flere fejl. Disse koder er af stor praktisk betydning. Der synes fortsat at være mulighed for at opnå bedre resultater. I forbindelse med analysen af begrænsninger for dekodningsmetoderne har det også interesse at få en dybere forståelse af kodernes afstandsegenskaber.

Sammensatte koder på støjfyldte kommunikationskanaler

Fejlrettende sammensatte koder anvendes ofte for at opnå effektiv kommunikation over støjfyldte kommunikationskanaler. I tidligere projekter har vi set på sammensatte (konkatenerede) koder, hvor de ydre koder er Reed-Solomon koder eller interleavede Reed Solomon koder, [men også koder afledt af lineære koder over Galois ringe kan analyseres med de metoder, som anvendes på konkatenerede koder].
I projektet undersøges sammensatte koders effektivitet, hvor nye Sudan inspirerede metoder anvendes på dekodningen.

Algebraisk definerede koder og deres dekodning

I nærværende projekt studeres forskellige algebraisk definerede koder og deres dekodning. Der arbejdes især med dekodning af koder defineret ved hjælp af Gröbner basis teoretiske metoder, og det skal specielt søges undersøgt om en klassse af tidligere studerede koder kan listedekodes.
Der studeres koder hørende til algebraiske stukturer af vilkårlig høj transcendensgrad.

Ikke-kommutativ algebraisk geometri, kodningsteori og kryptografi

Ikke-kommutativ algebraisk geometri er grundlagt af A.Connes i 1980'erne og har anvendelser i mange retninger. En lang række ideer fra matematisk fysik, såsom kvante- og strengteori, har haft en stærk indflydelse på matematik og har skabt en række matematiske temaer, der under et kaldes ikke-kommutativ geometri.
Ikke-kommutativ geometri rummer ganske nye temaer i algebraisk geometri med stærke relationer til blandt andet algebraisk talteori.
Disse temaer søges undersøgt for så vidt angår deres anvendelighed i kodningsteori og kryptografi. Udforskningen heraf er inspireret af, at (kommutativ) algebraisk geometri og algebraisk talteori siden 1980 har spillet en hel central rolle i kodningsteori og kryptografi.

Shannon teori og anvendelser

Projektet vedrøer en gren af informationsteorien, Shannon-teori, der beskæftiger sig med mere fundamentale aspekter vedrørende kildekodning. Der bygges på resultater opnået i tiden efter 1998, hvor en spilteoretisk betragtningsmåde har vist sig frugtbar. Dette har åbnet rige muligheder for anvendelser i sandsynlighedsteori, statistik, kvanteinformationsteori, ikke-ekstensiv statistisk fysik, beregningsmæssig lingvistik, visse grene inden for biologien, kalibreringsproblemer i finansieringsteori m.v. Inden for rammerne af projektet vil deltagerne især koncentrere sig om de nedenfor nævnte områder.

Deltagere

Tom Høholdt, Docent, Institut for Matematik, DTU
Jørn Justesen, Professor, COM, DTU
Flemming Topsøe, Docent, Institut for Matematiske Fag. KU
Peter Harremoes, Post.doc, Institut for Matematiske Fag. KU
Johan P. Hansen, Lektor, Afdelingen for Matematiske Fag, Århus Universitet
Olav Geil, Lektor, Afdelingen for Matematik, Ålborg Universitet
Christian Thommesen,Lektor, Afdelingen for Matematik, Ålborg Universitet