Ideel Secret Sharing og Matroider

– Karakterisering af ideelle secret sharing schemes ud fra diskrete kombinatoriske strukturer

af Kåre Janussen

Institut for Matematiske Fag, Aarhus Universitet, juni 2004

Vejleder: Jørgen Brandt

Dedication

To my beloved and my dear friends
with whom I share my secrets.

Indhold

Figurer

Abstract

Ideal secret sharing schemes have been studied for some time but nevertheless, no complete characterization has yet been accomplished. However, it turns out that the properties of an ideal scheme are inherited directly from the access structure of the scheme which henceforth identifies that particular scheme. This thesis summarizes the progress made in various papers on the characterization of ideal access structures in terms of discrete combinatorial structures and particularly matroids.

Some necessary mathematical theory is compiled in chapter 1 and in chapter 2, the basics of secret sharing and its related properties are described along with some examples. In chapter 3, the connection with matroids is established and a necessary condition for matroids to be secret sharing is given. Furthermore, the universally ideal access structures are completely characterized. Chapter 4 covers decomposition of ideal access structures and their associated matroids into uniform components under strong connectivity. Conversely, a decomposition construction is presented, which in combination with the strong connectivity decomposition generates ideal access structures from a number of ideal threshold structures. Chapter 5 summarizes the results and gives suggestions for further investigation into the subject.

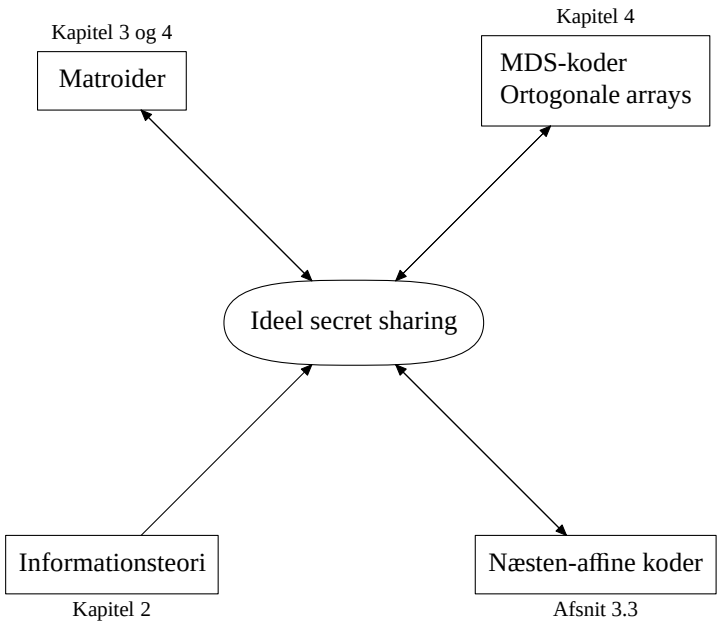
Indledning

Secret sharing er et af de mere utraditionelle emner indenfor moderne kryptologi, men det er samtidig et emne, som kan vise sig at byde på hidtil uudnyttede anvendelsesmuligheder. Den mest interessante type kaldes ideel secret sharing, og dette speciales hovedformål er at afdække, hvor vidt man i forskningen er nået med karakteriseringen af de ideelle secret sharing schemes i en matematisk kontekst. En fuldstændig karakterisering eksisterer dog endnu ikke, dvs. det er endnu ikke helt klarlagt, under hvilke omstændigheder det er muligt at lave ideel secret sharing. Ideen går ud på at karakterisere ideelle secret sharing schemes i termer af andre matematiske objekter, og det er lykkedes for nogle forfattere at kæde ideelle secret sharing sammen med ækvivalente objekter, men desværre har disse så vist sig at være været lige så uudforskede som de ideelle secret sharing schemes selv. I arbejdet med denne karakterisering har de ideelle secret sharing schemes især været tilknyttet matematiske begreber fra kombinatorikken. Navnlig har matroider spillet en stor rolle siden Brickell-Davenports skelsættende artikel [Brickell, Davenport] fra 1991. Siden da har arbejdet vist sig at føre overraskende langt omkring fra klassisk informationsteori over førnævnte matroider til koder, ortogonale arrays og designteori. Det er åbenbart nogle basale og meget generelle egenskaber ved ideel secret sharing, som knytter det sammen med alle disse forskellige kombinatoriske strukturer, og det har ført til, at mange fremskridt i karakteriseringen er blevet beskrevet og repræsenteret fra tilsyneladende vidt forskellige synsvinkler. Dette kan desværre resultere i en vis uoverskuelighed for den, som skal undersøge og kortlægge emnet, og det faktum, at stort set samtlige forfattere har valgt forskellig notation, har ikke gavnet denne situation. Dette er altså motivationen for dette speciale; at sammenfatte de mange forskellige bearbejdninger og resultater samt de seneste fremskridt inden for emnet ideel secret sharing. Jeg skal med andre ord forsøge at give overblik over sammenhængen mellem begreberne vist i figuren på den følgende side.

Hovedvægten i det matematiske grundlag var fra starten lagt på matroidernes betydning, men som før antydet, blev det efterhånden nødvendigt også at inddrage andre kombinatoriske objekter. Matroiderne spiller dog stadig en fremtrædende rolle og må siges at være den enkelte konstruktion, der er blevet vægtet tungest.

Kapitel 1 er en ren teoridel, hvori den største del af den matematiske teori bliver præsenteret. Det drejer sig om matroideteori, grafteori og informationsteori. Som nævnt er der i mange af de artikler, som danner specialets grundlag, anvendt forskellig notation. Min egen notation er derfor ikke fælles med alle disse artikler, men jeg har forsøgt at gøre den konsistent gennem rapporten. Derfor kan det forekomme, at et emne fra specialet bliver

Figur 1. Begreber relaterede til ideel secret sharing.



beskrevet med en væsentlig forskellig notation i forhold til det oprindelige artikelforlæg. Konsistent notation er dog helt nødvendig for at opfylde specialets formål om at skabe overblik.

Kapitel 2 omhandler secret sharing schemes. Begrebet og hele schemets generelle setup bliver defineret, og der gives nogle eksempler på forskellige konkrete konstruktioner og anvendelser. Der gives både eksempler af praktisk samt af mere matematisk karakter. Desuden får læseren her for første gang i rapporten et indblik i, hvordan egenskaber ved ideelle schemes udvisker forskelle i selve konstruktionen, således at de tekniske detaljer omkring konstruktionen af ideelle schemes kan negligeres.

Kapitel 3 kan siges at være specialets "primære" kapitel og handler om samspillet mellem ideelle secret sharing schemes og matroider. Her bliver nogle vigtige resultater vist, som bruges i stor udstrækning gennem resten af specialet. Det antydes endvidere, at matroiderne måske skal suppleres med f.eks. koder i det videre arbejde, idet netop en bestemt type af koder bruges til at rette en fejl i et ellers vigtigt "resultat" af [Brickell, Davenport].

Kapitel 4 gennemgår en alternativ måde at benytte matroiderne fra kapitel 3 på, hvorved nye egenskaber om ideelle secret sharing schemes dukker op. Det viser sig nemlig, at der kan laves en dekomposition af ideelle schemes og deres matroider i et antal mere "primitive" strukturer. Dette viser en vej for videre udvikling indenfor emnet.

Kapitel 5 er selve sammenfatningen. Her opsummeres de vigtige resultater fra de foregående kapitler, og idéer gives til retninger, man kunne gå i det videre arbejde.

Appendiks A og B er appendikser til kapitel 4, idet de indeholder to forskellige udgaver af beviset for et vigtigt resultat, der bruges i kapitel 4. Det er sammenhængen mellem

ideelle threshold schemes og MDS-koder. Appendiks A er det bevis, der henvises til i den oprindelige artikel. Det er dog desværre ikke trivielt, at dette bevis faktisk viser det ønskede, og derfor har jeg selv lavet et appendiks B med en alternativ udledning af resultatet fra kapitel 4.

Kapitel 1

Grundlæggende teori

Dette kapitel er en gennemgang af de redskaber fra den grundlæggende matematik og informationsteori, som jeg vil benytte mig af i resten af denne tekst, og er for så vidt ikke nødvendigvis en del af den teori, der ville være *nødt til* at være gennemgået, hvis det blot antages, at læseren besidder et bredt og stedvist dybt matematisk kendskab. Jeg har dog valgt at lave en kortfattet gennemgang af dette stof dels for fuldstændighedens skyld og dels for at indføre den notation, jeg vil benytte i specialets følgende kapitler. Læseren kan derfor gå hurtigt igennem dette kapitel, hvis denne mener at besidde de kundskaber, der står beskrevet, men jeg vil fraråde at springe kapitlet helt over.

I sektion 1.1 behandles meget kortfattet et vigtigt begreb fra kombinatorikken, nemlig matroiderne. Matroiderne er i denne tekst et matematisk redskab, som kan bruges her, fordi deres egenskaber minder om egenskaberne ved ideelle secret sharing schemes. Det er især matroidernes opbygning på en monoton mængdestruktur, som giver paralleller til secret sharing. Jeg definerer, hvad en matroide er, og så viser jeg nogle af deres grundlæggende egenskaber. Jeg nøjes dog med at medtage de egenskaber ved matroider, som er relevante for deres anvendelse i teksten, idet dette speciale primært handler om sammenhængen mellem matroider og secret sharing schemes og i mindre grad om kombinatorik som sådan. Jeg henviser den matroide-interesserede læser til f.eks. [Welsh] for en mere udførlig gennemgang af matroiderne og deres væsen. Sammenhængen med secret sharing schemes bliver belyst i kapitel 3.

I sektion 1.2 behandles også meget kort et andet matematisk redskab hentet fra kombinatorikken, nemlig graferne. Begrebet bliver defineret, og der bliver redegjort for nogle relevante grundlæggende egenskaber.

Grafer giver faktisk anledning til nogle bestemte typer af matroider, som i forbindelse med secret sharing har meget pæne egenskaber. Jeg bruger grafer til, på en visuelt tiltalende måde, at illustrere nogle konstruktioner på de før omtalte matroider, som graferne giver anledning til. Denne forbindelse mellem grafer og matroider bliver knyttet i afsnit 1.3.

I afsnit 1.4 i slutningen af kapitlet indføres begrebet entropi af en stokastisk variabel, som er et vigtigt redskab fra basal informationsteori. Nogle af de grundlæggende egenskaber ved entropi er opsummeret her.

1.1 Matroide-teori

I dette afsnit defineres en række vigtige begreber omkring matroider til brug i resten af teksten. Først skal det dog opsummeres, hvad en matroide er. En matroide er en abstrakt mængdeteoretisk konstruktion, der defineres som følger:

Definition 1.1.1. En *matroide* $\mathcal{T} = (V, \mathcal{I})$ er en konstruktion bestående af en underliggende punktmængde V samt en familie $\mathcal{I}$ af delmængder af V, som opfylder

1. $\emptyset \in \mathcal{I}$,
2. $X \in \mathcal{I}, Y \subseteq X \Rightarrow Y \in \mathcal{I}$,
3. $X, Y \in \mathcal{I}, |X| = |Y| + 1 \Rightarrow \exists x \in X \setminus Y \colon Y \cup \{x\} \in \mathcal{I}$.

Elementerne i V kaldes *punkter*, og mængderne i $\mathcal{I}$ kaldes *uafhængige mængder*. Konstruktionen bygger altså på et uafhængighedsbegreb imellem elementerne i V. En *afhængig mængde* (mængde af punkter som er indbyrdes afhængige) er en delmængde af V, som ikke ligger i $\mathcal{I}$. Konstruktionen giver en familie af maksimale uafhængige mængder – alle med samme kardinalitet. Dette giver også en familie af minimale afhængige mængder. De minimale afhængige mængder kaldes *cykler*.
Der gøres brug af en speciel type af matroider, som spiller en stor rolle i den teori, der udvikles for secret sharing schemes, nemlig sammenhængende matroider:

Definition 1.1.2. En matroide siges at være *sammenhængende*, hvis ethvert par af punkter er indeholdt i en cykel.

Den næste definition viser lidt af forbindelsen mellem matroider og vektorrum. Der kan nemlig defineres en rangfunktion $\rho : 2^V \to \mathbb{Z}_+$ for delmængder i matroider i stil med den, som kendes fra vektorrum.

Definition 1.1.3. Lad $\mathcal{T} = (V, \mathcal{I})$ være en matroide, og lad $X \subseteq V$. Da defineres *rangen* $\rho(X)$ af X, så

$$\rho(X) = \max\{|A| \colon A \subseteq X,\ A \in \mathcal{I}\}.$$

Rangen af $\mathcal{T}$ defineres til at være $\rho(V)$.

Rangen af en delmængde $X \subseteq V$ af en matroide er dermed kardinaliteten af den største uafhængige delmængde af X. Dette begreb minder meget om dimensionsbegrebet fra vektorrum, hvor en maksimal uafhængig delmængde kaldes en basis for det underrum, som den udspænder, og hvor rangen/dimensionen af underrummet betegner kardinaliteten af basis.

Rang er som antydet et meget grundlæggende begreb ved matroider, og det giver også

anledning til en alternativ definition af matroider ved hjælp af rangfunktionen ρ:

Definition 1.1.4. En funktion ρ på en mængde V siges at være en *rangfunktion* for en matroide, hvis følgende er opfyldt:

1. $\rho(\emptyset) = 0$,
2. Hvis $X \subseteq V$, og $y \in V$, så er $\rho(X) \leq \rho(X \cup \{y\}) \leq \rho(X) + 1$,
3. Hvis $X \subseteq V$, og $y, z \in V$, og $\rho(X) = \rho(X \cup \{y\}) = \rho(X \cup \{z\})$, så er $\rho(X) = \rho(X \cup \{y\} \cup \{z\})$.

Ud fra følgende proposition kan konstrueres *restriktionen* $\mathcal{T}|_A$ af en matroide $\mathcal{T} = (V, \mathcal{I})$ til en delmængde $A \subseteq V$. Det er matroiden på $A \subseteq V$, hvori de uafhængige mængder er de uafhængige mængder fra $\mathcal{T}$, som er indeholdt i A:

Proposition 1.1.5. *Lad $\mathcal{T} = (V, \mathcal{I})$ være en matroide og lad $A \subseteq V$. Da udgør*

$$\mathcal{I}|_A = \{X \in \mathcal{I} \mid X \subseteq A\}$$

mængden af uafhængige delmængder i en matroide $\mathcal{T}|_A = (A, \mathcal{I}|_A)$, som kaldes restriktionen af $\mathcal{T}$ på A.

Beviset er klart og overlades derfor til læseren.

Med disse definitioner på plads kan der vises nogle egenskaber, som skal bruges senere hen.

Proposition 1.1.6. *Lad $C_1 \neq C_2$ være to cykler i en matroide $\mathcal{T}$ med $x \in C_1 \cap C_2$. Da findes en cykel C_3, så $C_3 \subseteq (C_1 \cup C_2)\backslash\{x\}$.*

Bevis. Antag at en sådan cykel C_3 ikke findes. Så er $(C_1 \cup C_2)\backslash\{x\}$ uafhængig i $\mathcal{T}$, så

$$\begin{aligned}\rho((C_1 \cup C_2)\backslash\{x\}) &= \rho((C_1\backslash\{x\}) \cup (C_2\backslash\{x\})) \\ &= |C_1 \cup C_2| - 1.\end{aligned}$$

Da C_1, C_2 er cykler, er $\rho(C_1) = |C_1| - 1$, og $\rho(C_2) = |C_2| - 1$. Det er en velkendt egenskab ved rangfunktionen, at

$$\rho(X \cup Y) + \rho(X \cap Y) \leq \rho(X) + \rho(Y),$$

så det fås, at

$$\begin{aligned}\rho(C_1 \cup C_2) + \rho(C_1 \cap C_2) &\leq \rho(C_1) + \rho(C_2) \\ &= |C_1| + |C_2| - 2 \\ &= |C_1 \cup C_2| + |C_1 \cap C_2| - 2.\end{aligned}$$

Men der gælder $|C_1 \cup C_2| - 1 = \rho((C_1 \cup C_2)\backslash\{x\}) \leq \rho(C_1 \cup C_2)$, og da $C_1 \neq C_2$, gælder det også, at $C_1 \cap C_2$ er uafhængig i $\mathcal{T}$, så $\rho(C_1 \cap C_2) = |C_1 \cap C_2|$. Dette giver en modstrid. □

Lemma 1.1.7. *Lad $C_1 \neq C_2$ være to cykler i en matroide $\mathcal{T}$ med $x \in C_1 \cap C_2$. Så gælder det, at for alle $y \in C_1 \backslash C_2$, at der findes en cykel C, så*

$$y \in C \subseteq (C_1 \cup C_2)\backslash\{x\}.$$

Bevis. Antag at C_1, C_2, x, y er sådan, at lemmaet ikke holder samt, at $|C_1 \cup C_2|$ er minimal med denne egenskab. Ifølge proposition 1.1.6 på foregående side findes en cykel C_3 med $C_3 \subseteq (C_1 \cup C_2)\backslash\{x\}$, og pr. antagelse er $y \notin C_3$.
Nu gælder $C_3 \cap (C_2 \backslash C_1) \neq \emptyset$, thi ellers ville $C_3 \subseteq C_1$, og dermed $C_3 = C_1$, og dette er umuligt, idet $y \in C_1 \backslash C_3$. Lad derfor $z \in C_3 \cap (C_2 \backslash C_1)$. Så er $z \in C_2 \cap C_3$ og $x \in C_2 \backslash C_3$. Da $y \notin C_2$ og $y \notin C_3$, er $y \notin C_2 \cup C_3$, men $y \in C_1 \cup C_2$, så $C_2 \cup C_3 \subsetneq C_1 \cup C_2$. Men på grund af minimaliteten af $C_1 \cup C_2$ må der så eksistere en cykel C_4, så $x \in C_4 \subseteq (C_2 \cup C_3)\backslash\{z\}$.

Nu er $x \in C_1 \cap C_4$ og $y \notin C_2 \cup C_3$, så $y \in C_1 \setminus C_4$. Men $z \notin C_1$ og $z \notin C_4$, så $C_1 \cup C_4 \subsetneq C_1 \cup C_2$, så igen på grund af minimaliteten af $C_1 \cup C_2$ må der eksistere en cykel C_5, så

$$y \in C_5 \subseteq (C_1 \cup C_4)\backslash\{x\}.$$

Men da $C_1 \cup C_4 \subseteq C_1 \cup C_2$, gælder der om C_5, at

$$y \in C_5 \subseteq (C_1 \cup C_2)\backslash\{x\}.$$

Dette er en modstrid. □

Lemma 1.1.8. *Lad $\mathcal{T} = (V, \mathcal{I})$ være en matroide med tre forskellige elementer $x, y, z \in V$. Hvis der findes en cykel C_1 gennem x og y samt en cykel C_2 gennem y og z, så findes også en cykel C_3 gennem x og z.*

Bevis. Beviset er et induktionsbevis i $|V|$. Sætningen gælder for $|V| = 3$. Lad $\{x, y\} \subseteq C_1$ og $\{y, z\} \subseteq C_2$.

Antag først $C_1 \cup C_2 \neq V$, og lad $u \in V \backslash (C_1 \cup C_2)$. Antag at sætningen gælder for $n > 3$, og og lad $W = V\backslash\{u\}$. Så må der være en cykel C_3 i restriktionen $\mathcal{T}|_W$ med $\{x, y\} \subseteq C_3$, og C_3 er automatisk også en cykel i $\mathcal{T}$.

Antag nu $C_1 \cup C_2 = V$. Ifølge lemma 1.1.7 findes der så cykler C_3, C_4, så

$$x \in C_3 \subseteq (C_1 \cup C_2)\backslash\{y\},$$
$$z \in C_4 \subseteq (C_1 \cup C_2)\backslash\{y\}.$$

På grund af minimaliteten af C_1 er $C_3 \cap (C_2 \backslash C_1) \neq \emptyset$. Antag $C_3 \cap C_1 \subsetneq C_1 \backslash C_2$. Så er $x \in C_3$, $z \in C_2$ samt $C_3 \cap C_2 \neq \emptyset$. Der gælder desuden $|C_3 \cup C_2| < |V|$, idet $C_3 \cap C_1 \subsetneq C_1 \backslash C_2$. Pr. induktionsantagelse findes der så en cykel C_5 i restriktionen $\mathcal{T}|_{(C_3 \cup C_2)}$ (og dermed også i $\mathcal{T}$), som indeholder x og z.

Antag derfor nu $C_3 \cap C_1 \supseteq C_1 \setminus C_2$, dvs. $C_3 \supseteq C_1 \setminus C_2$. Ved at lave det samme som ovenfor med C_4 kan det også antages, at $C_4 \supseteq C_2 \backslash C_1$. Da $y \notin C_3$, $y \notin C_4$ og $C_1 \cup C_2 = V$, er $C_3 \cup C_4 \subseteq (C_1 \cup C_2)\backslash\{y\}$. Det gælder, at $C_3 \supseteq C_1 \backslash C_2$ og $C_3 \cap (C_2 \backslash C_1)$ samt $C_4 \supseteq C_2 \backslash C_1$ og $C_4 \cap (C_1 \backslash C_2)$, hvilket giver $C_3 \cap C_4 \neq \emptyset$. Da findes pr. induktionsantagelse en cykel C_6 i $\mathcal{T}|_{(C_3 \cup C_4)}$ og dermed også i $\mathcal{T}$, som indeholder x og z. □

Matroider kan faktisk også karakteriseres ud fra deres cykler. Det er en egenskab, som må regnes for grundlæggende viden om matroider, men det er lidt besværligt at vise. Sætningen findes bl.a. i [Welsh], hvor den også er vist. Sætningen er følgende karakterisering af en matroide:

Sætning 1.1.9 (Cykel-karakterisering). *En familie C af delmængder af V er mængden af cykler i en matroide $\mathcal{T} = (V, C)$, hvis og kun hvis følgende er opfyldt:*

(C1) Hvis $C_1 \neq C_2 \in C$, så er $C_1 \not\subseteq C_2$,

(C2) Hvis $C_1 \neq C_2 \in C$, og $x \in C_1 \cap C_2$, så findes $C_3 \in C$ med $C_3 \subseteq (C_1 \cup C_2)\backslash\{x\}$.

Her er en ret vigtig sætning, som skal bruges i et bevis lige om lidt. Det er egentlig blot en udvidelse af udsagnet i pkt. 3 i definition 1.1.1.

Sætning 1.1.10. *Hvis $X, Y \in \mathcal{I}$ og $|X| < |Y|$, så findes en $Z \subseteq Y \setminus X$, så $|X \cup Z| = |Y|$ og så $X \cup Z \in \mathcal{I}$.*

Bevis. Lad Z_0 være maksimal sådan, at $Z_0 \subseteq Y \setminus X$ og $X \cup Z_0 \in \mathcal{I}$ med $|X \cup Z_0|$ maksimal. Hvis $|X \cup Z_0| < |Y|$, så findes en $Y_0 \subseteq Y$ med $|Y_0| = |X \cup Z_0| + 1$, og da $Y_0 \in \mathcal{I}$, må der findes et $y \in Y_0 \setminus (X \cup Z_0)$, så $(X \cup Z_0 \cup \{y\}) \in \mathcal{I}$. Men dette er i modstid med maksimaliteten af Z_0. □

Endelig kan der også ifølge [Welsh] defineres en matroide ud fra det, der også kaldes basis-aksiomet. I forhold til de andre definitioner af matroiden, er det her vist som en sætning:

Sætning 1.1.11 ("Basis-aksiomet"). *En ikke-tom familie $\mathcal{B}$ af delmængder af V er mængden af baser for en matroide på V, hvis og kun hvis følgende er opfyldt:*

(B1) Hvis $B_1, B_2 \in \mathcal{B}$ og $x \in B_1 \setminus B_2$, så findes et $y \in B_2 \setminus B_1$, så $(B_1 \cup \{y\})\backslash\{x\} \in \mathcal{B}$.

Bevis. Lad $\mathcal{M} = (\mathcal{I}, V)$ være en matroide på V. Da $\emptyset \in \mathcal{I}$, er $\mathcal{B} \neq \emptyset$. Lad $B_1, B_2 \in \mathcal{B}$ og $x \in B_1 \setminus B_2$. Ved brug af sætning 1.1.10 på mængden $B\backslash\{x\}$ fås, at der findes et $y \in B_2$, så $|(B_1\backslash\{x\}) \cup \{y\}| = |B_2|$. Dvs. $y \in B_2 \setminus B_1$ med $(B_1 \cup \{y\})\backslash\{x\}$ et maksimalt element i $\mathcal{I}$, så $(B_1 \cup \{y\})\backslash\{x\} \in \mathcal{B}$.

Lad nu omvendt $\mathcal{B}$ være en ikke-tom familie af delmængder af V, som opfylder (B1) og definér $\mathcal{I}$ til at være familien af delmængder $X \subseteq V$, så X er indeholdt i et element af $\mathcal{B}$. Dvs. $\mathcal{B}$ er familien af maksimale elementer i $\mathcal{I}$. Så opfylder $\mathcal{I}$ helt klart pkt. 1 og 2 fra definition 1.1.1. Det skal nu vises, at pkt. 3 fra definitionen også er opfyldt. Antag derfor at $X, Y \in \mathcal{I}$ og $X \neq Y$ med $X \subseteq B_1$, $Y \subseteq B_2$ og $B_1, B_2 \in \mathcal{B}$. Lad

$$\begin{aligned} X &= \{x_1, \ldots, x_k\}, \\ B_1 &= \{x_1, \ldots, x_k, b_1, \ldots, b_q\}, \\ Y &= \{y_1, \ldots, y_k, y_{k+1}\}, \\ B_2 &= \{y_1, \ldots, y_k, y_{k+1}, c_1, \ldots, c_{q-1}\}. \end{aligned}$$

Betragt nu mængden $B_1 \setminus \{b_q\}$. Ifølge (B1) findes der nu et $z \in B_2 \setminus (B_1 \setminus \{b_q\})$, så

$$(B_1 \setminus \{b_q\}) \cup \{z\} \in \mathcal{B}.$$

Hvis $z \in Y$, er $z \in Y \setminus X$, da $X \cap B_2 \setminus (B_1 \setminus \{b_q\}) = \emptyset$, og så er $X \cup z \in \mathcal{I}$ på en måde, så pkt. 3 er opfyldt. Hvis i stedet $z \notin Y$, så betragt mængden $((B_1 \setminus \{b_q\}) \cup \{z\}) \setminus \{b_{q-1}\}$. Ved at bruge (B1) igen fås, at der eksisterer et $z_1 \in B_2 \setminus ((B_1 \setminus \{b_q\}) \cup \{z\}) \setminus \{b_{q-1}\}$, så

$$\Big(((B_1 \setminus \{b_q\}) \cup \{z\}) \setminus \{b_{q-1}\}\Big) \cup \{z_1\} \in \mathcal{B}.$$

Hvis så $z_1 \in Y$, er beviset igen færdigt. Antag derfor $z_1 \notin Y$ og fjern elementet b_{q-2}.

Da $\big|\{b_1, \ldots, b_q\}\big| > \big|\{c_1, \ldots, c_{q-1}\}\big|$, kan dette argument gentages højst q gange, indtil b_i bliver nødt til at blive erstattet med et $y_j \in Y$. Når det er tilfældet, er det vist, at der kan findes et $y \in Y \setminus X$, så $\mathcal{I}$ opfylder pkt. 3 i definition 1.1.1.

Da $\mathcal{I}$ nu er mængden af uafhængige mængder i en matroide $\mathcal{M} = (\mathcal{I}, V)$, og da $\mathcal{B}$ er familien af maksimale elementer i $\mathcal{I}$, er $\mathcal{B}$ altså basis for matroiden $\mathcal{M}$.

□

To matroider kan siges at være isomorfe, hvis der findes en afhængighedsbevarende bijektion imellem deres punktmængder:

Definition 1.1.12. Lad $\mathcal{T}_1 = (V_1, \mathcal{I}_1)$, $\mathcal{T}_2 = (V_2, \mathcal{I}_2)$ være to matroider. $\mathcal{T}_1$ og $\mathcal{T}_2$ siges at være *isomorfe*, hvis der findes en bijektion $\psi : V_1 \to V_2$, så

$$A \in \mathcal{I}_1 \iff \psi(A) \in \mathcal{I}_2.$$

Denne definition er ækvivalent med, at der imellem $\mathcal{T}_1$ og $\mathcal{T}_2$ vil findes f.eks. en rangbevarende eller en cykelbevarende bijektion.

Der skal defineres et sidste vigtigt matroidebegreb: En matroide siges at være *repræsentérbar* over et legeme $\mathbb{F}$, hvis der findes en afhængighedsbevarende afbildning fra matroidens punkter til mængden af vektorer i et vektorrum over $\mathbb{F}$. Eller mere præcist:

Definition 1.1.13. En matroide $\mathcal{T} = (V, \mathcal{I})$ siges at være repræsentérbar over et legeme $\mathbb{F}$, hvis der findes et $k \in \mathbb{N}$ samt en afbildning $\phi : V \to \mathbb{F}^k$, så

$$A \subseteq V \text{ afhængig i } \mathcal{T} \iff \phi(A) \text{ lineært afhængig i } \mathbb{F}^k.$$

Ikke alle matroider er repræsentérbare, dvs. der findes matroider, som ikke er repræsentérbare over noget legeme. Omvendt findes der dog også matroider, som er repræsentérbare over alle legemer. Ét eksempel på en klasse af matroider, som er repræsentérbare over alle legemer, er de såkaldt grafiske matroider. Disse introduceres i slutningen af dette kapitel.

Følgende proposition viser en stærk egenskab ved matroider.

Proposition 1.1.14. *En matroide $\mathcal{T}$ er repræsentérbar over både* GF(2) *og* GF(3)*, hvis og kun hvis $\mathcal{T}$ er repræsentérbar over ethvert legeme.*

Beviset følger bl.a. af [Tutte], (4.5), p. 169, men det vil føre for vidt at gennemgå dette her. Det kan vises, at en matroide er repræsentérbar over ethvert legeme, hvis og kun hvis matroiden er repræsentérbar over GF(2) samt over et legeme af karakteristik forskellig fra to. Se evt. [Oxley], Theorem 6.6.3.

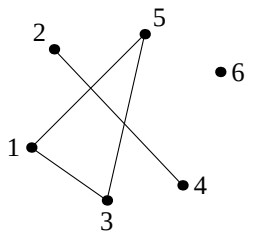
1.2 Graf-teori

For at behandle grafiske matroider, skal nogle begreber vedrørende grafer berøres. Grafer er konstruktioner, som især kendes fra kombinatorikken, og i denne sektion præsenteres nogle grundlæggende definitioner og resultater fra grafteorien.

Definition 1.2.1. En *graf* er en tupel $G = (V, E)$ af en punktmængde V og en kantmængde $E \subseteq V \times V$ med $V \cap E = \emptyset$.

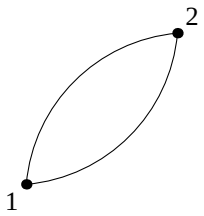
Dette giver ikke så meget intuition af, hvad en graf er, men det er i virkeligheden en ret simpel konstruktion, som måske bedst kan illustreres ved at tegne nogle eksempler på grafer. Som regel tegnes hvert punkt i V som en prik og hvert element (v_1, v_2) fra E som en linie eller kurve imellem to prikker v_1 og v_2. Uformelt kan der defineres følgende begreber for grafer:
En *simpel* graf $G = (V, E)$ består af en endelig mængde V af punkter (eller hjørner) samt en endelig mængde E af kanter imellem uordnede par af forskellige punkter fra V. Se figuren på denne side.

Figur 1.1. Simpel graf

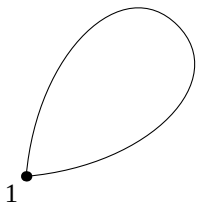


Her er $V = \{1, 2, 3, 4, 5, 6\}$ og
$E = \{(1, 3), (1, 5), (2, 4), (3, 5)\}$.

Figur 1.2. Multibel kant



Figur 1.3. Løkke



Dog er ikke alle grafer simple. Hvis f.eks. en kant optræder mere end én gang, kaldes kanten *multibel*, og grafen kaldes en *multigraf*. Hvis endepunkterne i en kant ikke er forskellige, kaldes kanten en *løkke*, og grafen kaldes en *pseudograf*. Hvis kanterne består af ordnede par, siges grafen at være *orienteret*. En graf siges at være *sammenhængende*, hvis ethvert par af forskellige punkter i V er forbundet med en sti af på hinanden følgende kanter fra E. Enhver graf består af et antal *sammenhængskomponenter*, som hver især er sammenhængende (en sammenhængende graf har kun én sammenhængskomponent). En *cocykel* i en graf er en minimal mængde af kanter med den egenskab, at hvis de fjernes, så

vokser antallet af sammenhængskomponenter i grafen. En sti, der ender i samme punkt, som den begynder uden ellers at krydse sig selv, kaldes en *cykel*. En (del)graf, som ikke indeholder en cykel, kaldes et *træ*. Endelig siges to grafer $G = (V, E)$ og $G' = (V', E')$ at være *isomorfe*, hvis der findes en bijektion $\phi : V \to V'$ med $(x, y) \in E \Leftrightarrow (\phi(x), \phi(y)) \in E'$. Dvs. man kan sige, at to grafer er isomorfe, hvis den ene kan bringes over i den anden ved at flytte punkterne rundt i planen og så lade kanterne følge med deres tilhørende endepunkter. I denne rapport vil der blive benyttet simple, sammenhængende grafer.

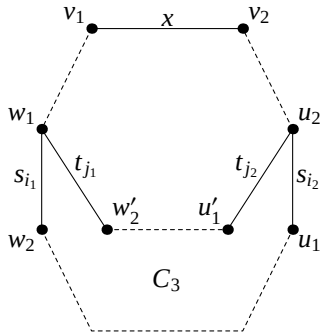
Lemma 1.2.2. *Lad $G = (V, E)$ være en graf og lad $C_1 \neq C_2$ være to cykler fra 2^E med $x \in C_1 \cap C_2$. Da findes en cykel $C_3 \subseteq 2^E$ med*

$$C_3 \subseteq (C_1 \cup C_2) \backslash \{x\}.$$

Bevis. Lad $x \in C_1 \cap C_2$ være sådan, at $x = (v_1, v_2)$. Da C_1 er en cykel med $x \in C_1$, findes en sti $\{s_i\}_{i \in I} \subseteq C_1$ fra v_1 til v_2 med $x \notin \{s_i\}_{i \in I}$. Ligeledes findes en tilsvarende sti $\{t_j\}_{j \in J} \subseteq C_2$ fra v_1 til v_2 med $x \notin \{t_j\}_{j \in J}$. Da $C_1 \neq C_2$, er $\{s_i\}_{i \in I} \neq \{t_j\}_{j \in J}$, så der må findes et $i_1 \in I$ og et $j_1 \in J$ samt et hjørne $w_1 \in V$, så

$$s_{i_1} = (w_1, w_2) \text{ og } t_{j_1} = (w_1, w_2') \text{ med } w_2 \neq w_2'.$$

Figur 1.4. Konstruktion af cyklen C_3



Da begge stierne $\{s_i\}_{i \in I}$ og $\{t_j\}_{j \in J}$ ender i hjørnet v_2, findes et $i_2 \in I$ og et $j_2 \in J$ samt et hjørne $u_2 \in V$, så

$$s_{i_2} = (u_1, u_2) \text{ og } t_{j_2} = (u_1', u_2) \text{ og } u_1 \neq u_1'.$$

Der er således konstrueret en cykel $C_3 \subseteq C_1 \cup C_2 \backslash \{x\}$, som går fra hjørnet w_1 via en sti indeholdt i C_1 til hjørnet u_2 og fra u_2 tilbage til w_1 via en sti indeholdt i C_2. □

Definition 1.2.3. Lad $G = (V, E)$ være en graf. En *cocykel* i G er en mængde af kanter $C^* \subseteq E$, som er minimal med den egenskab, at fjernelse af denne medfører stigning af antallet af sammenhængskomponenter i G.

1.3 Matroider og grafer

Dette afsnit binder de to foregående sammen, idet der her ses på nogle matroider konstrueret på baggrund af grafer. Lad $G = (V, E)$ være en ikke-orienteret graf. Cyklerne i grafen G udgør de minimale afhængige delmængder i en matroide $\mathcal{M}(G)$ på kantmængden E (de minimale afhængige delmængder i en matroide kaldes også for cykler). *Bemærk: Punktmængden i $\mathcal{M}(G)$ er altså kantmængden i G*, og $A \subseteq E$ er en uafhængig mængde i $\mathcal{M}(G)$, hvis og kun hvis A ikke indeholder nogen cykel i G. Dvs. en graf giver anledning til en matroide. Dette kan også formuleres som en proposition, som let lader sig bevise:

Proposition 1.3.1. *Lad $G = (V, E)$ være en ikke-orienteret graf. Cyklerne i grafen G udgør de minimale afhængige delmængder i en matroide $\mathcal{M}(G)$ på kantmængden E.*

Bevis. Det er klart, at ingen grafcykel kan indeholde en anden cykel, og dermed er egenskaben (C1) på side 11 opfyldt. Lemma 1.2.2 giver præcis egenskab (C2), og mængden af cykler i grafen $G = (V, E)$ udgør dermed mængden af cykler i en matroide på E. Denne matroide benævnes $\mathcal{M}(G)$. □

Det er altså slået fast, at enhver graf G giver anledning til en matroide $\mathcal{M}(G)$ knyttet til denne bestemte graf. Begrebet grafisk matroide er en egenskab ved visse matroider, og her er, hvad der menes med dette:

Definition 1.3.2. En matroide $\mathcal{M}$ siges at være en *grafisk matroide*, hvis der findes en graf G, så $\mathcal{M}$ er isomorf med $\mathcal{M}(G)$.

Der kan også knyttes en matroide til en graf på en anden måde. Følgende proposition giver anledning til de såkaldte cografiske matroider[1]:

Proposition 1.3.3. *Lad $G = (V, E)$ være en ikke-orienteret graf. Cocyklerne i grafen G udgør de minimale afhængige delmængder i en matroide $\mathcal{M}^*(G)$ på kantmængden E.*

Dette giver følgende type af matroider:

Definition 1.3.4. En matroide $\mathcal{M}^*$ siges at være *cografisk*, hvis der findes en graf G, så $\mathcal{M}^*$ er isomorf med $\mathcal{M}^*(G)$.

1.4 Informationsteori

Her til slut skal gennemgås lidt klassisk informationsteori (efter Shannon), hvor begrebet entropi indføres, og nogle egenskaber opsummeres.

Det ønskes at opstille et mål for usikkerheden på udfaldene af en stokastisk variabel. Dette mål kaldes *entropi* og er beslægtet med det tilsvarende begreb fra fysikkens

[1] Se f.eks. [Welsh] for nærmere gennemgang.

termodynamik. C. E. Shannon introducerede begrebet entropi i forbindelse med opbygningen af den moderne informationsteori i 1948 (se evt. [Shannon1]) og brugte det i kryptologi-sammenhæng i 1949 i [Shannon2].

Definition 1.4.1. Lad X være en endelig stokastisk variabel med sandsynlighedsfordeling $P(X)$. Da defineres *entropien* af denne stokastiske variabel til at være

$$H(X) = -\sum_{i=1}^{n} P_i \log_2 P_i,$$

hvor $P_i = P(X = x_i)$ for $1 \leq i \leq n$.

Heraf ses det bl.a., at når en stokastisk variabel X er helt fastlagt, så er $H(X) = 0$. Hvis derimod den stokastiske variabel X er fuldstændig uniform, så alle punktsandsynligheder er ens, er $H(X)$ maksimal med $H(X) = \log_2 n$. Se også [Stinson], p. 57. Man kan sige, at entropien betegner "usikkerheden" på den betragtede stokastiske variabel. Hvis udfaldet af den stokastiske variabel kendes, er usikkerheden – og dermed entropien – lille. Hvis overhovedet ingen ikke-triviel information (kaldet *Shannon-information*) kendes om udfaldet, er det bedste, man kan gøre, at gætte tilfældigt over en uniform fordeling. I dette tilfælde har X så maksimal entropi. Spørgsmålet om entropien af en stokastisk variabel afhænger altså af den mængde af ikke-triviel information om udfaldet, som er tilgængelig.

Desuden kan defineres følgende:

Definition 1.4.2. Lad X, Y være stokastiske variable. Da defineres

$$\begin{aligned}
H(XY) &= -\sum_{x \in X} \sum_{y \in Y} P(X = x, Y = y) \log_2 P(X = x, Y = y), \\
H(X \mid Y = y) &= -\sum_{x \in X} P(X = x \mid Y = y) \log_2 P(X = x \mid Y = y), \\
H(X \mid Y) &= \sum_{y \in Y} P(Y = y) \log_2 P(X \mid Y = y).
\end{aligned}$$

Der gælder iflg. [Stinson], lemma 11.6, følgende egenskaber:

Proposition 1.4.3. *Lad X, Y, Z være stokastiske variable. Da gælder*

1. $H(XY) \geq H(X)$,
2. $H(X \mid Y) \geq H(X \mid YZ)$,
3. $H(XY) \leq H(X) + H(Y)$, *hvor "=" gælder, hvis og kun hvis X og Y er uafhængige,*
4. $H(X \mid Y) = H(XY) - H(Y)$.

Af pkt. 4 ovenfor følger, at

$$\begin{aligned} H(XY \mid Z) &= H(XYZ) - H(Z) \\ &= H(Y \mid XZ) + H(XZ) - H(Z) && \text{da } H(Y \mid XZ) = H(XYZ) - H(XZ) \\ &= H(Y \mid XZ) + H(X \mid Z) && \text{da } H(X \mid Z) = H(XZ) - H(Z). \end{aligned}$$

Af pkt. 3 & 4 ovenfor følger, at

$$\begin{aligned} H(X \mid Y) &= H(XY) - H(Y) \\ &\leq H(X) + H(Y) - H(Y) = H(X) \end{aligned}$$

som vel også intuitivt kunne forventes, da viden om Y kunne mindske usikkerheden om X. Det følger også af pkt. 3, at "=" gælder, hvis og kun hvis X og Y er uafhængige.

Kapitel 2

Secret Sharing Schemes

I dette afsnit gennemgås det generelle setup i et secret sharing scheme og de mest grundlæggende begreber og grundantagelser, der benyttes, bliver defineret. Derudover gives et par eksempler på konkrete måder, hvorpå secret sharing schemes kan konstrueres, og dybere egenskaber som perfekthed og idealitet bliver behandlet.

Som eksempel på nogle konkrete konstruktioner vil jeg i afsnit 2.2 gennemgå nogle relativt simple schemes deriblandt det mest velkendte og også mest intuitive – nemlig Shamirs threshold scheme (afsnit 2.2.4). Dette scheme gør brug af velkendte egenskaber ved algebra og specielt aritmetik i restklasseringen $\mathbb{Z}_p$.

I afsnit 2.3 vil jeg behandle begrebet perfekthed samt, som eksempel på et perfekt scheme, gøre rede for Brickells vektorrumskonstruktion, hvilket er en mere kombinatorisk konstruktion end Shamirs threshold scheme. Det ses, at Brickells vektorrumskonstruktion desuden også er mere generel.

Shamirs og Brickells konstruktionerne viser sig i afsnit 2.4 at være eksempler på en vigtig type af secret sharing schemes, som kaldes ideelle secret sharing schemes. Ideelle schemes er en specielt "pæn" type af perfekte schemes pålagt ekstra krav, som giver nogle meget hensigtsmæssige egenskaber. Det er faktisk disse egenskaber, som gør ideelle schemes interessante. Det viser sig bl.a., at de tekniske forskelle i implementeringen af ideelle schemes er underornede. Resten af arbejdet i øvrigt vil hovedsageligt være fokuseret på ideelle schemes.

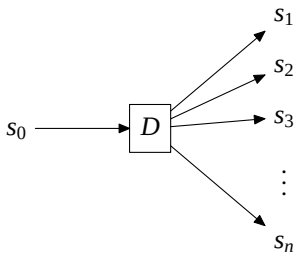
2.1 Grundlæggende konstruktion

I et secret sharing scheme findes en bestemt central *dealer D,* som vælger en *hemmelighed* $s_0 \in \mathcal{K}$ ud af en endelig mængde $\mathcal{K}$ af hemmeligheder. Desuden er der en endelig mængde $\mathcal{P}$ bestående af ialt *n personer* samt en mængde af delmængder af personer $\Gamma \subseteq 2^{\mathcal{P}}$ kaldet *access-strukturen*. Et secret sharing scheme (herefter ofte forkortet SSS) for access-strukturen Γ er da en måde for dealeren D at dele sin hemmelighed, s_0, ud blandt personerne i $\mathcal{P}$ ved at give hver person $p \in \mathcal{P}$ et stykke hemmelig information – en *share* $s_p \in \mathcal{S}$, hvor $|\mathcal{S}| < \infty$, således at *netop* delmængderne i Γ (de autoriserede delmængder)

senere er i stand til i fællesskab at rekonstruere hemmeligheden s_0 entydigt ved hjælp af deres shares.

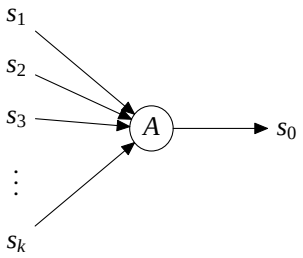
Secret sharing er altså en proces, der kan siges at foregå i to faser, som det er illustreret i figuren nedenfor på denne side.

Figur 2.1. Fordeling



Fase 1: Fordeling af hemmeligheden s_0 gennem dealeren D til personerne $\{p_1, p_2, \ldots, p_n\} = \mathcal{P}$ ved udsendelse af shares $s_1, \ldots, s_n$.

Figur 2.2. Rekonstruktion



Fase 2: Rekonstruktion af hemmeligheden s_0 gennem en autoriseret delmængde $\{p_1, \ldots, p_k\} = A \subseteq \mathcal{P}$ med $A \in \Gamma$ ved samling af shares $s_1, \ldots, s_k$.

Det antages, at dealeren samt alle delmængderne i Γ er ærlige, dvs. ikke lyver om værdien af deres respektive shares under rekonstruktionen[1]. Det er nu klart, at access-strukturen normalt må være en *monoton* mængde af delmængder af $\mathcal{P}$, dvs. hvis $A \subseteq B$, og $A \in \Gamma$, så er $B \in \Gamma$. Enkelte forfattere[2] har dog under noget besvær konstrueret schemes for access-strukturer, som ikke er monotone, men dette har ikke umiddelbart den store interesse i teorien for secret sharing. For det første fordi det er svært at finde på anvendelser, hvor en ikke-monoton access-struktur er nødvendig, og for det andet fordi netop monotoni i access-strukturen giver nogle gode egenskaber, når SSS repræsenteres som matematiske objekter. Netop dette er hovedidéen i dette speciale, og det gøres i afsnit 3.1. Det følgende beskæftiger sig udelukkende med monotone access-strukturer.

Lad Γ^- være familien af minimale mængder i en monoton access-struktur Γ. En sådan familie Γ^- siges da også at være *basis* for Γ. Det antages, at enhver person $p \in \mathcal{P}$ er indeholdt i en af delmængderne fra Γ^-. Dette er det samme som at antage, at der ikke er neglegible personer p', hvor der for alle $A \subseteq \mathcal{P}$ gælder implikationen $p' \in A \in \Gamma \Rightarrow A \backslash \{p'\} \in \Gamma$. Ligeledes kan det for at undgå neglegible personer antages, at intet par af personer i $\mathcal{P}$ altid får samme shares. Personerne adskiller sig jo kun fra hinanden ved værdien af deres respektive shares. Schemes, som opfylder dette krav, kaldes *sammenhængende*.

[1] Schemes, som er resistente overfor uærlighed, er beskrevet i f.eks. [Pieprzyk, Xian-Mo 1] og [Pieprzyk, Xian-Mo 2]

[2] For reference til dette, se [Martin], p. 59.

2.2 Eksempler: (t, w)-threshold schemes

Her beskrives et meget kendt og benyttet eksempel på et SSS, nemlig (t, w)-*threshold schemet* for $t \leq w$, hvor access-strukturen består af samtlige delmængder af personer $A \subseteq \mathcal{P}$ med $|A| \geq t$ og $|\mathcal{P}| = w$. Dvs. alle delmængder af mindst t personer kan beregne hemmeligheden, men ingen delmængde af $t - 1$ personer kan få nogen som helst brugbar information (Shannon-information). Denne konstruktion er formentlig den mest intuitive og nok også umiddelbart den, som er lettest at finde på realistiske anvendelser for.

Herunder gives tre eksempler på threshold schemes. De to første eksempler er et forsøg på at anskueliggøre nogle realistiske anvendelser, idet de udgør to løsninger til det såkaldte *bankboksproblem*. Det tredje eksempel er nok den stærkeste motivation til at beskæftige sig med secret sharing, idet det er en nogenlunde realistisk tænkt situation omhandlende opbevaring af særligt følsomme eller store mængder data i et computernetværk. Dette er et scenarie, som ser ud til at blive stadigt mere aktuelt. Det fjerde eksempel er den rent matematiske konstruktion af Shamirs threshold scheme i det endelige legeme $\mathbb{Z}_p$.

2.2.1 Eksempel: Bankboks (1)

Et ofte brugt eksempel på en anvendelse er problemet med en bankboks, som det ikke er forsvarligt at lade én enkelt ansat have nøglen til. Det vurderes dog at være forsvarligt at lade eksempelvis 3 betroede ansatte om at åbne boksen *sammen*. Derfor konstruerer man en lås med 3 nøglehuller, som man så skal have 3 nøgler for at åbne. Låsen er konstrueret, så alle 3 nøgler skal bruges samtidigt for at åbne låsen, så det kræver, at mindst tre personer med nøgler er tilstede.
Antag, at der er 10 betroede ansatte. En nøgle gives af bankens ledelse til hver betroet ansat. Nu kan enhver delmængde af betroede ansatte af kardinalitet mindst 3 åbne boksen i fællesskab ved at mødes og bruge nøglerne. Dette er et eksempel på et lidt primitivt $(3, 10)$-threshold scheme.

I praksis ville man dog naturligvis være nødt til at sikre sig imod, at nøglerne kan kopieres. Ellers kunne enhver med en nøgle lave kopier til sine venner, som så med kopinøglerne kunne udgive sig for at være betroet medarbejder. Nøglerne kunne derfor eksempelvis være en form for smart-card med indbygget elektronisk chip, som hver indeholder en digital signatur evt. udstedt af bankens ledelse. Låsen skulle så kun kunne åbnes, hvis nøgler med forskellige gyldige signaturer benyttes. Det ville således være umuligt at lave flere nøgler, som kan bruges samtidigt på grund af signaturen, som kun bankens ledelse kan lave. ◇

2.2.2 Eksempel: Bankboks (2)

Man kunne i forlængelse af ovenstående eksempel tænke sig et system, hvor nøglerne var ganske almindelige nøgler til ganske almindelige nøglehuller. Dette ville umiddelbart have den fordel, at man ville kunne undvære førnævnte signatursystem. Problemet er nu, at disse nøgler let kan kopieres. Man må derfor kræve, at alle nøglehullerne tager forskellige

nøgler. Man kan da altid lave et (w, w)-threshold scheme, hvor hver person får en nøgle, som er forskellig fra de andres, men et (t, w)-threshold scheme med $t < w$ er lidt mere besværligt, da det kræver, at hver person har mere end én nøgle.

Jeg vil for ordens skyld her give et eksempel på et $(2, 5)$-threshold scheme med almindelige nøgler. Lad de fem personer være nummereret $p_1, \ldots, p_5$. I dette eksempel benyttes ialt fem forskellige nøgler $s_1, \ldots, s_5$. Hvis hver person får fire nøgler, kan laves et $(2, 5)$-threshold scheme med en nøglefordeling som følger:

Person	Nøgler
p_1	$\{2, 3, 4, 5\}$
p_2	$\{1, 3, 4, 5\}$
p_3	$\{1, 2, 4, 5\}$
p_4	$\{1, 2, 3, 5\}$
p_5	$\{1, 2, 3, 4\}$

Dette kan også skrives på matrixformen nedenfor, hvor hver person p_i modtager nøglen s_j, hvis og kun hvis $M(i, j) = 1$:

$$M = \begin{matrix} \\ p_1 \\ p_2 \\ p_3 \\ p_4 \\ p_5 \end{matrix} \begin{matrix} \begin{matrix} s_1 & s_2 & s_3 & s_4 & s_5 \end{matrix} \\ \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix} \end{matrix}$$

Det er overladt til læseren at checke, at enhver delmængde af personer af kardinalitet mindst 2 nu tilsammen er i besiddelse af alle fem nøgler. Dette er dog klart, idet hver person jo mangler præcis én nøgle, som hver af de andre har.

I dette system er det en oplagt fordel, hvis man kan minimere antallet af nøgler, som hver person skal bære. Et relevant spørgsmål er derfor, hvad det minimale antal nøgler skal være. I [Martin], p. 106, bliver det vist generelt, at for et (t, w)-threshold scheme skal der bruges mindst $\binom{w}{k-1}$ forskellige nøgler, og hver person skal have $\binom{w-1}{k-1}$ nøgler. ◇

2.2.3 Eksempel: Dataopbevaring i netværk

Hvis meget store mængder data skal gemmes – til f.eks. backup eller lignende, kan det være et problem, hvis den *lokale* server i et computernetværk (f.eks. en privat PC eller en mindre virksomheds filserver) ikke selv har lagerplads nok. Det kunne også tænkes, at man ønskede at gemme meget følsom data, som man ikke selv ønskede at opbevare fysisk. Der ønskes derfor en mulighed for at opbevare sin data eksternt f.eks. hos såkaldte lagerudbydere, som faktisk findes på internettet den dag i dag.

I øjeblikket kan det eksempelvis fungere sådan, at man sender sin data (i krypteret form med f.eks. RSA, AES, ...) til udbyderen og så håber på, at denne udbyder ikke ønsker eller er i stand til at bryde krypteringen. Når man så senere ønsker adgang til data,

logger man ind hos lagerudbyderen og downloader den krypterede data, som man så selv dekrypterer. Svagheden i dette system er, at man er nødt til at stole på, at sin lagerudbyder ikke kan bryde krypteringen.

En anden metode kunne i stedet være, at man delte sin data i et SSS og sendte krypterede shares rundt til flere forskellige udbydere, som så hver modtager én share i et (t, t)-threshold scheme. Man antager nu, at ikke alle de valgte udbydere er svindlere. Data er nu sikret, idet hver enkelt udbyder ikke får nogen information om hemmeligheden ved at bryde krypteringen og læse sin share. Selvom alle udbyderne til sammen formelt udgør access-strukturen, kan de heller ikke samle deres shares, medmindre de alle sammen er svindlere. Man rekonstruerer ved at hente sine shares ned, dekryptere dem og så samle det med schemets rekonstruktionsfunktion. Bemærk, at dealeren selvfølgelig er nødt til selv at gemme data indeholdende dekrypteringsnøgle og rekonstruktionsfunktion.

Share-distribution

1. Dealeren vælger sit (t, t)-threshold scheme og konstruerer ud fra hemmeligheden s_0 de t shares $s_1, \ldots, s_t$. Desuden vælges t forskellige lagerudbydere $u_1, \ldots, u_t$.
2. Dealeren vælger en kryptering $e_k : s_i \mapsto y_i$ med nøgle k og krypterer således hver share s_i til cipher-share y_i for $1 \leq i \leq t$.
3. Dealeren giver i hemmelighed hver cipher-share y_i til udbyder u_i for $1 \leq i \leq t$.

Rekonstruktion

1. Dealeren henter hos hver udbyder u_i sin cipher-share y_i og dekrypterer med nøglen k denne: $d_k : y_i \mapsto s_i$ for $1 \leq i \leq t$.
2. Dealeren samler nu alle sine shares $s_1, \ldots, s_t$ og rekonstruerer hemmeligheden s_0 ud fra schemets rekonstruktionsfunktion: $(s_1, \ldots, s_t) \mapsto s_0$.

Grunden til, at de udsendte shares skal være krypterede, er blot den, at man ønsker at beskytte sig imod, at en spion på netværket opsamler alle shares i klartekst. Man kan også øge sikkerheden i krypteringen ved at vælge krypteringsnøgle påny til kryptering af hver share. Alternativt kan man forlade sig på transmission gennem en krypteret kanal som f.eks. SSH, som også er baseret på RSA. Ønsker man desuden at beskytte sig imod tab af shares hos enkelte udbydere, kan man bare lave et (t, w)-threshold scheme med $t < w$. På denne måde kan man rekonstruere, selvom enkelte shares skulle gå tabt.

Jeg har desværre ikke set nogen beskrivelse af denne anvendelse af secret sharing noget sted før, så en grundigere udvikling af denne idé er nok ønskelig, hvis det skal

kunne bruges i praksis. Dette eksempels lødighed står altså helt for min egen regning. Det viser dog en anden måde at bruge secret sharing på, hvor man faktisk ikke ønsker, at "personerne", som modtager shares, skal kunne rekonstruere. Det er altså et scheme, som udelukkende har til opgave at give dealeren en mulighed for at dele sin hemmelighed ud og så *selv* samle den igen.

Ovenfor er ikke beskrevet, hvordan dealeren faktisk laver sit threshold scheme, så her til sidst skal det vises, hvordan den matematiske konstruktion af et (t, w)-threshold scheme i praksis kan laves i legemet $\mathbb{Z}_p$. ◇

2.2.4 Eksempel: (t, w)-threshold scheme i $\mathbb{Z}_p$

I det følgende beskrives en konkret algebraisk konstruktion af et threshold scheme efter Shamir (beskrevet i [Shamir]), nemlig (t, w)-threshold i $\mathbb{Z}_p$. I dette eksempel er hemmelighed og shares elementer i det endelige legeme $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ med p elementer, hvor p er et primtal, og rekonstruktion foregår ved beregning i dette legeme[3].

Lad $t, w \in \mathbb{N}$ med $t \leq w$, og lad p være et primtal med $w \geq p + 1$. Antag, at der gælder $D \notin \mathcal{P}$. Dealeren D ønsker at dele en hemmelighed $s_0 \in \mathcal{K} = \mathbb{Z}_p$. Schemet virker nu som følger:

Initialisation

D vælger w forskellige ikke-nul-elementer $x_i \in \mathbb{Z}_p$, $1 \leq i \leq w$. D giver x_i til person p_i for alle $1 \leq i \leq w$. Værdierne af x_i er offentligt tilgængelige, dvs. ikke hemmelige.

Share-distribution

1. D vælger i hemmelighed $s_0 \in \mathbb{Z}_p$ og dernæst hemmeligt og tilfældigt $t - 1$ elementer $a_1, \ldots, a_{t-1} \in \mathbb{Z}_p$.
2. D udregner $s_i = a(x_i)$ for alle $1 \leq i \leq w$, hvor
$$a(x) = s_0 + \sum_{j=1}^{t-1} a_j x^j \mod p.$$
3. D giver i hemmelighed share s_i til person p_i for alle $1 \leq i \leq w$.

Nu vises, hvordan personerne $p_1, \ldots, p_t$ på en entydig måde kan finde frem til hemmeligheden $s_0 = a(0)$. De kender de t funktionsværdier
$$s_i = a(x_i), \qquad 1 \leq i \leq t$$

[3] At $\mathbb{Z}_p$ er et legeme er et grundlæggende resultat i basal algebra.

for det hemmelige polynomium $a(x) \in \mathbb{Z}_p[x]$. $a(x)$ er af grad højst $t-1$, dvs.

$$a(x) = a_{t-1}x^{t-1} + \cdots + a_1 x + a_0,$$

hvor elementerne $a_0, \ldots, a_{t-1} \in \mathbb{Z}_p$ er ubekendte med $a_0 = s_0$. Ligningerne

$$s_i = a(x_i), \qquad 1 \leq i \leq t$$

udgør derfor t lineære ligninger med t ubekendte med aritmetik i $\mathbb{Z}_p$. Hvis disse ligninger er uafhængige, er der en entydig løsning med a_0 som D's hemmelighed. Det viser sig imidlertid, at dette system af ligninger faktisk har en entydig løsning, som det fremgår af det følgende.

Systemet af de t lineære ligninger i $\mathbb{Z}_p$ er

$$\begin{aligned}
s_1 &= a_{t-1}x_1^{t-1} + \cdots + a_2 x_1^2 + a_1 x_1 + a_0 \\
s_2 &= a_{t-1}x_2^{t-1} + \cdots + a_2 x_2^2 + a_1 x_1 + a_0 \\
&\vdots \\
s_t &= a_{t-1}x_t^{t-1} + \cdots + a_2 x_t^2 + a_1 x_t + a_0,
\end{aligned}$$

hvilket kan skrives

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & x_t^2 & \cdots & x_t^{t-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_t \end{bmatrix}.$$

Koefficientmatricen, kald den A, hedder også en Vandermonde-matrix, og den har som bekendt[4] determinanten

$$\det(A) = \prod_{1 \leq j < k \leq t} (x_k - x_j) \mod p,$$

hvilket altid er forskelligt fra nul i $\mathbb{Z}_p$, da alle faktorer er forskellige fra nul. Ingen af faktorerne $(x_k - x_j)$ kan være nul, da alle x_i'erne er forskellige. Da p er et primtal, er $\mathbb{Z}_p$ et legeme, og så er produktet af ikke-nul-elementer altid forskelligt fra nul. Dvs. $\det(A) \neq 0$. Det gælder derfor, at enhver delmængde af mindst t personer vil finde en entydig værdi for hemmeligheden a_0.

Hvad sker der nu, når en delmængde af $t-1$ personer samler deres shares? Det første, der sker, er, at de får $t-1$ ligninger med t ubekendte. Nu kan de forsøge at gætte på en værdi g_0 for hemmeligheden. Dette vil give en t'te ligning

$$a_0 = a(0) = g_0$$

samt en ny Vandermonde-matrix med entydig løsning. Dvs. for hvert gæt g_0 på værdien af hemmeligheden fremkommer der en entydig løsning, et entydigt polynomium a_{g_0}, med

$$\begin{cases} s_j = a_{g_0}(x_i), & 1 \leq j \leq t \\ g_0 = a_{g_0}(0). \end{cases}$$

[4] Velkendt resultat fra lineær algebra.

Enhver værdi af hemmeligheden er altså mulig. En delmængde af $t-1$ personer har derfor ingen ikke-triviel information om hemmeligheden. Dette er en god egenskab ved et secret sharing scheme, som der skal gøres mere ud af i afsnit 2.3. I praksis ville en autoriseret delmængde beregne s_0 ved hjælp af Lagrange interpolation, hvilket giver

$$s_0 = \sum_{j=1}^{t} b_j s_j,$$

hvor hver koefficient $b_j = \prod_{1 \le k \le t, k \ne j} \frac{x_k}{x_k - x_j}$ kan beregnes fra starten, da x_i'erne jo var offentligt kendte. ◇

2.3 Perfekte Secret Sharing Schemes

Før der kan gås til definitionerne, er en gennemgang af konstruktionen af det generelle SSS nødvendig.

Et generelt SSS kan beskrives som følger. Dealeren har en hemmelighed s_0, som er udvalgt fra mængden $\mathcal{K}$ af mulige hemmeligheder med sandsynligheden $P(s_0)$. Til fordeling blandt de n personer i $\mathcal{P}$ bruger dealeren alfabeterne $\mathcal{S}_1, \ldots, \mathcal{S}_n$, fra hvilke han udvælger de n shares $s_1, \ldots, s_n$. Han giver share s_i til person p_i uden at afsløre noget om værdien af de andre personers shares. Den samlede fordeling har sandsynlighed $P_{s_0}(s_1, \ldots, s_n)$. Her definerer P altså sandsynlighedsfordelingen på produktmængden $\mathcal{S}^{(n)} = \mathcal{K} \times \mathcal{S}_1 \times \cdots \times \mathcal{S}_n$. Nu kaldes parret $\left(P, \mathcal{S}^{(n)}\right)$ for et SSS og hvert punkt $(s_0, s_1, \ldots, s_n)$ benævnes en "fordelingsfunktion". Alle shares s_i kan nu realiseres som værdierne af tilsvarende stokastiske variable S_i med simultan fordeling P med $P(s_0, s_1, \ldots, s_n) = P(s_0)P_{s_0}(s_1, \ldots, s_n)$, da s_0 er uafhængig af hver enkelt s_i, $1 \le i \le n$.

Lad $A \subseteq \mathcal{P}$ være en delmængde af personerne. Lad da $P(s_0 \mid s_p, p \in A)$ betegne sandsynligheden for, at man gætter på s_0 som værdien af hemmeligheden, givet at man kender mængden af distribuerede shares til A, nemlig $\{s_p \mid p \in A\}$. Dvs. hvis personerne i A samler deres shares, så betegner $P(s_0 \mid s_p, p \in A)$ sandsynligheden for, at de i fællesskab når frem til værdien s_0 for hemmeligheden.

Definition 2.3.1. Et secret sharing scheme for access-strukturen Γ siges at være *perfekt*, hvis følgende er opfyldt:

1. $\forall s_0 \in \mathcal{K}\colon P(s_0 \mid s_p, p \in A) \in \{0, 1\}$, hvis $A \in \Gamma$,
2. $\forall s_0 \in \mathcal{K}\colon P(s_0 \mid s_p, p \in A) = P(s_0)$, hvis $A \notin \Gamma$.

Γ siges så at være en *perfekt access-struktur*.

Den første betingelse udtrykker, at for hver værdi s_0 vil en autoriseret mængde $A \in \Gamma$ altid enten finde frem til denne værdi for hemmeligheden eller udelukke denne værdi.

Den næste betingelse kræver, at sandsynligheden for, at en uautoriseret delmængde $A \notin \Gamma$ gætter på s_0 som værdien af hemmeligheden, er den samme som den sandsynlighed, hvormed hemmeligheden blev valgt. Dvs. den uautoriserede delmængde har ingen Shannon-information og kan derfor ikke gøre andet end at gætte tilfældigt på værdien af hemmeligheden. Denne informationsteoretisk inspirerede definition kan naturligvis også udtrykkes ved entropi, så kravene bliver

(E1) $H(s_0 \mid s_p, p \in A) = 0$, hvis $A \in \Gamma$,

(E2) $H(s_0 \mid s_p, p \in A) = H(s_0)$, hvis $A \notin \Gamma$.

2.3.1 Eksempel: Brickells vektorrumskonstruktion

Nu vises et spændende eksempel på secret sharing scheme med Brickells vektorrumskonstruktion. Først og fremmest skal det vises, at dette scheme er perfekt. Det ses dog også, at det faktisk er en generalisering af Shamirs threshold scheme.

Lad Γ være en access-struktur, lad p være et primtal og lad $d \in \mathbb{N}$ med $d \geq 2$. Da er $(\mathbb{Z}_p)^d$ det endelige d-dimensionale vektorrum af d-tupler over legemet $\mathbb{Z}_p$. Det ønskes at konstruere et SSS med $\mathcal{K} = \mathcal{S} = (\mathbb{Z}_p)^d$. Antag at der findes en funktion

$$\phi : \mathcal{P} \to (\mathbb{Z}_p)^d,$$

som opfylder, at

$$(1, 0, \ldots, 0) \in \mathrm{sp}\{\phi(p_i) \mid p_i \in A\} \Leftrightarrow A \in \Gamma.$$

Vektoren $(1, 0, \ldots, 0) \in (\mathbb{Z}_p)^d$ kan altså udtrykkes entydigt ved en linearkombination af vektorer fra billedmængden $\phi(A)$.

Initialisation

D giver vektoren $\phi(p_i) \in (\mathbb{Z}_p)^d$ til personen p_i for alle $1 \leq i \leq |\mathcal{P}|$. Disse vektorer er offentligt kendte.

Share-distribution

1. D ønsker at dele hemmeligheden $K \in \mathbb{Z}_p$. D vælger hemmeligt og tilfældigt $d - 1$ elementer $a_2, \ldots, a_d \in \mathbb{Z}_p$.
2. D udregner for alle $1 \leq i \leq |\mathcal{P}|$ værdien af $s_i = \overline{a} \cdot \phi(p_i)$, hvor
$$\overline{a} = (K, a_2, \ldots, a_d).$$
3. D giver værdien s_i som share til personen p_i for alle $1 \leq i \leq |\mathcal{P}|$.

For enhver vektor $\overline{a} = (a_1, a_2, \ldots, a_d) \in (\mathbb{Z}_p)^d$ defineres altså en distributionsfunktion $f_{\overline{a}} \in \mathcal{F}_{a_1}$ fra rummet $\mathcal{F}_{a_1}$ af alle distributionsfunktioner på hemmeligheden $K = a_1$. Distributionsfunktionen er

$$f_{\overline{a}} : \mathcal{P} \to \mathcal{S}$$

med

$$f_{\overline{a}}(x) = \overline{a} \cdot \phi(x) \quad \forall x \in \mathcal{P},$$

hvor "$\cdot$" betegner det indre produkt modulo p. Hver $\mathcal{F}_K$ indeholder præcis p^{d-1} forskellige distributionsfunktioner. Det, at D vælger de $d-1$ elementer tilfældigt i trin 1 i ovennævnte share-distribution, betyder, at alle sandsynlighedsfordelingerne $p_{\mathcal{F}_K}$ er uniforme, dvs. $p_{\mathcal{F}_K}(f) = \frac{1}{p^{d-1}}$ for alle $f \in \mathcal{F}_K$.

Rekonstruktionen kan foretages af personerne i $A \in \Gamma$ på følgende måde. Da netop $(1, 0, \ldots, 0) \in \mathrm{sp}\{\phi(p_i) \mid p_i \in A\}$, findes en linearkombination, så

$$(1, 0, \ldots, 0) = \sum_{\{i \mid p_i \in A\}} c_i \phi(p_i) \tag{2.1}$$

med $c_i \in \mathbb{Z}_p$. Den i'te share er $s_i = \overline{a} \cdot \phi(p_i)$, hvor $\overline{a} \in (\mathbb{Z}_p)^d$ er D's hemmelige vektor med

$$K = a_1 = \overline{a} \cdot (1, 0, \ldots, 0).$$

Ved brug af ovenstående linearkombination samt lineariteten af skalarproduktet "$\cdot$" fås

$$\begin{aligned} K &= \overline{a} \cdot (1, 0, \ldots, 0) \\ &= \overline{a} \cdot \sum_{\{i \mid p_i \in A\}} c_i \phi(p_i) \\ &= \sum_{\{i \mid p_i \in A\}} c_i \overline{a} \cdot \phi(p_i) \\ &= \sum_{\{i \mid p_i \in A\}} c_i s_i. \end{aligned}$$

Personerne i A skal så beregne koefficienterne c_i ud fra ligning (2.1), idet dette system jo har en løsning.

Nu skal sikkerheden af dette scheme undersøges ved at studere, hvad der sker, hvis en uautoriseret delmængde af personer $B \notin \Gamma$ samler deres shares. Lad

$$e = \dim(\mathrm{sp}\{\phi(p_i) \mid p_i \in B\})$$

Da $(1, 0, \ldots, 0) \notin \mathrm{sp}\{\phi(p_i) \mid p_i \in B\}$, er $\mathrm{sp}\{\phi(p_i) \mid p_i \in B\}$ et ægte underrum af $(\mathbb{Z}_p)^d$ af dimension $e < d$. Betragt ligningssystemet

$$\begin{aligned} \phi(p_i) \cdot \overline{a} &= s_i, \ \forall p_i \in B \\ (1, 0, \ldots, 0) \cdot \overline{a} &= K. \end{aligned}$$

Dette består af lineære ligninger med d de ubekendte $a_1, a_2, \ldots, a_d$. Dette system har rang $e+1$, idet

$$(1, 0, \ldots, 0) \notin \text{sp}\{\phi(p_i) \mid p_i \in B\}.$$

Det skal undersøges, om der er en løsning til dette system. Vektoren $\overline{a}$, valgt af D, er en løsning til de første $|B|$ ligninger, og da $(1, 0, \ldots, 0) \notin \text{sp}\{\phi(p_i) \mid p_i \in B\}$, kan den sidste ligning også løses med løsningen $\overline{a}$, så den sidste ligning er konsistent med de første $|B|$ ligninger. Nu hvor ligningssystemet er konsistent, har løsningsrummet altså dimension $d-(e+1) = d-e-1$. Lad en hemmelighed $K \in \mathcal{K}$ være givet. For hver distribution af shares til mængden B vil der da findes p^{d-e-1} forskellige distributionsfunktioner i $\mathcal{F}_K$.

Det ønskes vist, at personerne i B ikke får nogen information om hemmeligheden, dvs. det skal vises, at

$$H(K \mid B) = H(K)$$

for alle $K \in \mathcal{K}$. Pr. definition af entropien er det imidlertid nok at vise, at

$$p_{\mathcal{K}}(K \mid f|_B) = p_{\mathcal{K}}(K)$$

for alle $K \in \mathcal{K}$ og alle $f|_B \in \mathcal{F}$, hvor $f|_B \in \mathcal{F}_K$ betegner en fordelingsfunktion restringeret til B på hemmeligheden K. Dvs. givet $K \in \mathcal{K}$ så er

$$f|_B(p_i) = s_i \quad \forall p_i \in B.$$

Der gælder

$$p_{\mathcal{K}}(K \mid f|_B) = \frac{p_{S(B)}(f|_B \mid K) p_{\mathcal{K}}(K)}{p_{S(B)}(f|_B)}.$$

Dvs. beviset er færdigt, hvis det bliver vist, at $p_{S(B)}(f|_B \mid K) = p_{S(B)}(f|_B)$. Men da D vælger med en uniform fordeling, er det det samme som at vise, at antallet af fordelingsfunktioner er uafhængigt af den valgte hemmelighed K. Men det er jo netop konstateret, at der til hver distribution af shares til B findes præcis p^{d-e-1} forskellige distributionsfunktioner i $\mathcal{F}_K$.
Dermed er det vist, at Brickells vektorrumskonstruktion udgør et perfekt secret sharing scheme. ◇

Der skal nu vises det interessante, at Shamirs threshold scheme faktisk er et specialtilfælde af Brickells vektorrumskonstruktion. For at vise dette, skal der redegøres for, at hemmeligheder og shares kommer fra de samme mængder respektivt, samt at share-genereringen og hemmeligheds-rekonstruktionen foregår på samme måde i de to schemes. De to konstruktioner sammenlignes nu:

Sæt $d = t$ og lad $x_i \in \mathbb{Z}_p$ være den i'te offentligt kendte værdi fra threshold schemet. Da defineres de offentligt kendte vektorer $\phi(p_i) \in (\mathbb{Z}_p)^d$ for $1 \leq i \leq w$ til at være

$$\phi(p_i) = (1, x_i, x_i^2, \ldots, x_i^{t-1}),$$

som gives til person p_i.

Dealeren vælger i begge schemes $t-1$ hemmelige, tilfældige værdier $a_1, \ldots, a_{t-1} \in \mathbb{Z}_p$ (nummereret $a_2, \ldots, a_d$ i beskrivelsen af Brickells scheme ovenfor) og udregner den i'te share til

$$s_i = a(x_i) = K + \sum_{j=1}^{t-1} a_j x_i^j \mod p$$

i threshold schemet eller ækvivalent

$$s_i = \overline{a} \cdot \phi(p_i) = (K, a_1, \ldots, a_{t-1}) \cdot (1, x_i, x_i^2, \ldots, x_i^{t-1})$$

med indre produkt i $(\mathbb{Z}_p)^d$ som i Brickells scheme. Shares genereres altså fuldstændig ens i de to schemes.

Hemmeligheden K rekonstrueres i begge schemes ved at udregne

$$K = \sum_{i=1}^{t} b_i s_i$$

i $\mathbb{Z}_p$, hvor b_i'erne evt. kan beregnes af D og offentliggøres på forhånd.

2.3.2 Shannons ulighed

Nu skal vises et vigtigt resultat af Shannon vedrørende den nedre grænse for størrelsen af shares i et perfekt SSS. Resultatet afslører, at det generelt ikke er effektivt at lave perfekt secret sharing. Som det vil fremgå nedenfor, skal der for et perfekt SSS gælde, at $|\mathcal{S}| \geq |\mathcal{K}|$. Dvs. størrelsen af hver share (f.eks. målt i bitlængde) er mindst lige så stor som den hemmelighed, man ønsker at dele.

Proposition 2.3.2 (Shannons ulighed). *Antag, at M er et sammenhængende perfekt SSS. Da er*

$$H(s_p) \geq H(s_0).$$

Bevis. Lad $p \in \mathcal{P}$. Da M er sammenhængende, gælder det, at $\exists A \subseteq \mathcal{P}\colon\ p \in A \in \Gamma^-$. Da er $A' = A \backslash \{p\} \notin \Gamma$. Generelt gælder det for entropien af stokastiske variable, at

$$H(XY \mid Z) = H(Y \mid XZ) + H(X \mid Z).$$

Dvs. der gælder

$$\begin{cases} H(s_0, A \mid A') = H(A \mid s_0, A') + H(s_0 \mid A') \\ H(A, s_0 \mid A') = H(s_0 \mid AA') + H(A \mid A') \end{cases}$$

$$\Downarrow$$

$$H(A \mid s_0, A') + \underbrace{H(s_0 \mid A')}_{H(s_0)} = \underbrace{H(s_0 \mid AA')}_{0} + \underbrace{H(A \mid A')}_{H(s_p)}$$

$$\Downarrow$$

$$H(s_p) = H(s_0) + H(A \mid s_0, A')$$

$$\Downarrow$$

$$H(s_p) \geq H(s_0).$$

□

I litteraturen opereres ofte med begrebet information rate for et perfekt SSS. Dette defineres på følgende måde:

Definition 2.3.3. Betragt et perfekt SSS med access-struktur Γ. *Information rate*'en ρ_i for person $p_i \in \mathcal{P}$ er forholdet

$$\rho_i = \frac{\log_2 |\mathcal{K}|}{\log_2 |S(p_i)|}.$$

Hele *schemets information rate* ρ er så defineret som

$$\rho = \min\{\rho_i \mid 1 \leq i \leq |\mathcal{P}|\}.$$

Bemærk: På grund af Shannons ulighed gælder der altid $0 < \rho_i \leq 1$ for perfekte schemes.

Shannons ulighed leder frem til at ønske effektive perfekte SSS med mindst mulige shares, dvs. med $|\mathcal{S}| = |\mathcal{K}|$, eller i informationsteoretisk forstand: $H(s_p) = H(s_0)$ for alle $p \in \mathcal{P}$. Da sådanne schemes er endnu mere ønskværdige end dem, som bare er perfekte, kaldes de for ideelle. Dette giver motivationen for det følgende.

2.4 Ideelle Secret Sharing Schemes

Der er tre betydninger af begrebet ideelt secret sharing scheme, den informationsteoretiske (IT), den matematisk set lidt mere anvendelige kombinatoriske Brickell-Davenport (BD) model samt Brickell-Stinson (BS) modellen. Disse konstruktioner skal nu studeres lidt nærmere, idet der især lægges vægt på BD-modellen.

2.4.1 IT-modellen

Uden restriktioner ligner den informationsteoretiske model umiddelbart den mest generelle model for secret sharing. Dette skyldes, at modellen baserer sig på entropi, hvilket i sig selv er en meget generel beskrivelse af information. Denne beskrivelse er nemlig ikke afhængig af den specifikke konstruktion af schemets distributions- og rekonstruktionsprotokol.

Definition 2.4.1 (IT-Ideelt Secret Sharing Scheme). Et secret sharing scheme siges at være *IT-ideelt*, hvis det er perfekt i henhold til (E1) og (E2), og hvis det for alle $p \in \mathcal{P}$ gælder at $H(s_p) = H(s_0)$.

Fordelen ved denne model, nemlig brugen af det generelle begreb entropi, bliver samtidig også det, som gør den noget uanvendelig i praksis. Den er nemlig så generel i formulering, at det kan blive vanskeligt at bruge den til at vise dybere sammenhænge. Det viser sig dog senere, at der faktisk ikke behøver at tabes generalitet, når ideel secret sharing studeres i de andre modeller.

Bemærk: For et IT-ideelt scheme må der altså gælde om dets information rate, at $\rho = 1$.

2.4.2 Brickell-Davenport modellen

Den kombinatoriske definition af SSS efter [Brickell, Davenport] tager sit udgangspunkt i det tilfælde, hvor alle de stokastiske variable S_i er uniformt fordelte (eller har rationale sandsynligheder for ikke-kanoniske schemes). I det følgende skal et SSS repræsenteres ved en endelig matrix $M(r, p)$, hvor alle rækker er forskellige (kanonisk SSS). Hvis to rækker er ens, betragtes nemlig i stedet det scheme, som har den reducerede matrix. Søjlerne repræsenterer personerne $p_0, p_1, \ldots, p_n$ med p_0 som dealeren. Matricen M kan antages at være offentligt kendt.
For person $p \in \mathcal{P}$ er $S(p) = \{M(r, p) \mid r \text{ række i } M\}$ mængden af elementer i søjle p, dvs. matrixindgangene i søjle p består altså af elementerne i $S(p)$, og søjle p_0 består af elementerne, som udgør $S(p_0) = \mathcal{K}$.

$$M = \begin{array}{c} \left[\begin{array}{c|ccc} & & & \\ \mathcal{K} & S(p_1) & \cdots & S(p_n) \\ & & & \end{array}\right] \\ \begin{array}{cccc} p_0 & p_1 & \cdots & p_n \end{array} \end{array}$$

Hvert element kan altså optræde flere gange i hver søjle.

Share distribution Dealeren ønsker at fordele hemmeligheden $s_0 \in S(p_0) = \mathcal{K}$, så han vælger en række r, som opfylder $s_0 = M(r, p_0)$, dvs. som har s_0 som sit første element. Hver person p_i modtager som share det i'te element fra rækken r, dvs. $M(r, p_i)$.

$$\begin{array}{c} r \\ \left[\begin{array}{c|ccc} \vdots & \vdots & & \vdots \\ \hline s_0 & s_1 & \cdots & s_n \\ \hline \vdots & \vdots & & \vdots \end{array}\right] \\ \begin{array}{cccc} p_0 & p_1 & \cdots & p_n \end{array} \end{array} = M$$

Rekonstruktion Lad $A \subseteq \mathcal{P}$. Hver person $p_a \in A$ modtager en share s_a. Hvis personerne i A nu bruger deres samlede information, vil de finde, at dealeren har valgt en række r, som opfylder, at

$$M(r, p_a) = s_a \quad \forall p_a \in A.$$

Lad access-strukturen være Γ. For $A \subseteq \mathcal{P}$ gælder det, at

$$\begin{array}{l} A \in \Gamma \\ \Downarrow \\ \left(\begin{array}{l} \forall \text{ rækker } r, \hat{r} \text{ med } M(r, p_a) = M(\hat{r}, p_a)\ \forall p_a \in A \text{ gælder, at} \\ M(r, p_0) = M(\hat{r}, p_0). \end{array} \right). \end{array}$$

Dvs. personerne i A finder altid frem til den korrekte hemmelighed $s_0 = M(r, p_0)$.

Denne konstruktion er umiddelbart meget tiltalende, fordi hele schemet bygges op omkring en offentligt kendt matrix. Konstruktionen er derfor nogenlunde håndgribelig så længe $|\mathcal{K}|$ og $|\mathcal{P}|$ er forholdsvis små. Så snart mængden af mulige hemmeligheder vokser, bliver matricen dog hurtigt meget stor, idet antallet af rækker, som det vil fremgå af lemmaerne 3.1.7 og 3.1.8 på side 46, vokser eksponentielt i størrelsen af de autoriserede delmængder og polynomielt i $|\mathcal{K}|$. Men selve schemet som matematisk objekt er stadig ret simpelt at arbejde med.

Nu skal nogle meget vigtige begreber introduceres, nemlig *afhængighed* og *uafhængighed* imellem en person og en mængde personer i $\mathcal{P}$. Jeg vil give to ækvivalente definitioner af hver af disse begreber: Den oprindelige definition som den blev indført af [Brickell, Davenport] og så en lidt mere tiltalende kombinatorisk definition.

Definition 2.4.2 (Uafhængighed). Betragt et secret sharing scheme. En ikke-tom delmængde A af personer siges at være *uafhængig* af en person $p_b \notin A$ (skrives $A \nrightarrow p_b$), hvis der gælder

$$\forall \text{rækker } r \; \forall s_b \in S(p_b) \; \exists \text{ række } r' : \begin{cases} M(r, p_a) = M(r', p_a) & \forall p_a \in A \\ M(r', p_b) = s_b. \end{cases}$$

Dvs. hvis r er en række, så findes der for alle $s_b \in S(p_b)$ en række r', hvis indgange stemmer overens med r på søjlerne i både A og p_b. Da siges A at have *ingen information* om p_b's share. Dvs. personerne i A kan ikke ud fra deres shares få nogen information om p_b's share. Ellers siges A at have *nogen information* om p_b's share, hvilket skrives $A \to p_b$. Dette kan godt præciseres, idet "$A \to p_b$" betyder, at der findes en $s_{p_b} \in S(p_b)$, som kan udelukkes for en distribution af shares til A.

Notation: Med $S(A)$ betegnes mængden af mulige tupler af længde $|A|$ indeholdende A's samlede shares, og s_A er en af disse distributioner af shares til A. Lad $M(r, A)$ være en anden måde at betegne tuplen s_A af shares til mængden A hørende til den bestemte række r i matrixrepræsentationen

$$\begin{array}{c} \\ r \\ \\ \\ \\ p_0 \end{array} \begin{bmatrix} & & \\ \hline s_0 & s_A = M(r, A) & \\ \hline & & \\ & & \\ & & \end{bmatrix} \begin{array}{c} \\ \\ \\ \\ \\ \underbrace{\qquad\qquad}_{A} \end{array}$$

◇

$A \to p_b$ betyder så helt præcist, at der gælder

$$\begin{aligned} \exists s'_A \in S(A)\ \exists s'_b \in S(p_b)\ \forall \text{ rækker } r : M(r,A) = s'_A \\ \Downarrow \\ M(r,p_b) \neq s_b. \end{aligned} \tag{2.2}$$

Definition 2.4.3 (Afhængighed). Betragt et secret sharing scheme. En ikke-tom delmængde A af personer siges at være *afhængig* af en person $p_b \notin A$ (skrives $A \rightrightarrows p_b$), hvis der gælder

$$\forall r, r' \text{ med } M(r,A) = M(r',A) \text{ gælder } M(r,p_b) = M(r',p_b).$$

Dvs. hvis det for alle rækker, som er ens indenfor A's shares, gælder, at de også fastlægger p_b's share entydigt. A siges da at *kende* p_b's share. Så access-strukturen er $\Gamma = \{A \subseteq \mathcal{P} \mid A \rightrightarrows p_0\}$. Bemærk at egenskaben "$\rightrightarrows$" er en forstærkning af "$\to$", idet der specielt gælder "$A \to p_b$", hvis der gælder "$A \rightrightarrows p_b$".

Ovenstående definitioner vil jeg som nævnt også gerne formulere på en anden måde, da det kan hjælpe til at klarlægge, hvad det er, begreberne dækker over. Desuden er de kombinatorisk baserede definitioner lidt mere overskuelige at have med at gøre, når de bruges i beviser.
Den kombinatoriske indgangsvinkel til uafhængighed er denne:

Definition 2.4.4 (Uafhængighed (ækvivalent med 2.4.2)). Betragt et secret sharing scheme. En ikke-tom delmængde A af personer siges at være *uafhængig* af en person $p_b \notin A$ (skrives $A \nrightarrow p_b$), hvis der gælder

$$|S(A \cup \{p_b\})| = |S(A)| \cdot |S(p_b)|.$$

Denne ækvivalens imellem definitionerne må der for en ordens skyld redegøres for, selvom det virker ret oplagt, at det må gælde.

Bevis for ækvivalens mellem definitionerne 2.4.2 og 2.4.4. Ifølge definition 2.4.2 betyder $A \nrightarrow p_b$, at

$$\forall \text{rækker } r\ \forall s_b \in S(p_b)\ \exists \text{ række } r' : \begin{cases} M(r,A) = M(r',A) \\ M(r',p_b) = s_b. \end{cases}$$

Her har schemets matrixrepræsentation maksimalt antal rækker forskellige på $A \cup \{p_b\}$, så der for alle $s_A \in S(A)$ og alle $s_b \in S(p_b)$ findes en række med fordelingen s_A til personerne i A og s_b til personen p_b. Der skal derfor være mindst $|S(A)| \cdot |S(p)|$ forskellige tupler for $A \cup \{p\}$, hvilket betyder, at

$$|S(A \cup \{p\})| \geq |S(A)| \cdot |S(p)|.$$

Det er klart, at der altid må gælde

$$|S(A \cup \{p\})| \leq |S(A)| \cdot |S(p)|, \tag{2.3}$$

for $|S(A)| \cdot |S(p)|$ er ganske simpelt antallet af mulige $(A \cup \{p\})$-tupler. Dvs. der gælder i dette tilfælde "=" i (2.3) ovenfor. Så kravet i definition 2.4.2 medfører kravet i definition 2.4.4.

Definition 2.4.4 af relationen $A \nrightarrow p_b$ betyder omvendt, at

$$|S(A \cup \{p\})| = |S(A)| \cdot |S(p)|,$$

hvilket oplagt medfører, at

$$\forall \text{rækker } r \; \forall s_b \in S(p_b) \; \exists \text{ række } r' : \begin{cases} M(r, A) = M(r', A) \\ M(r', p_b) = s_b. \end{cases}$$

Dvs. kravet i definition 2.4.4 medfører kravet i definition 2.4.2, og så er den ækvivalens bevist. □

Relationen "$\rightarrow$" kan i denne kontekst defineres som negationen af "$\nrightarrow$", så der på grund af ligning (2.3) fås følgende definition:

Definition 2.4.5. Betragt et secret sharing scheme. En ikke-tom delmængde A af personer siges at have *nogen information* om en person $p_b \notin A$ (skrives $A \rightarrow p_b$), hvis der gælder

$$|S(A \cup \{p_b\})| < |S(A)| \cdot |S(p_b)|.$$

Til sidst kan afhængighed redefineres som følger:

Definition 2.4.6 (Afhængighed (ækvivalent med 2.4.3)). Betragt et secret sharing scheme. En ikke-tom delmængde A af personer siges at være *afhængig af* eller have *fuld information om* en person $p_b \notin A$ (skrives $A \rightrightarrows p_b$), hvis der gælder

$$|S(A)| = |S(A \cup \{p_b\})|.$$

Der skal også lige argumenteres for ækvivalensen af denne definition.

Bevis for ækvivalens mellem definitionerne 2.4.3 og 2.4.6. Beviset er et lille modstridsargument. Det er klart, at $|S(A \cup \{p_b\})| \geq |S(A)|$. Antag nu, at $|S(A \cup \{p_b\})| > |S(A)|$. Så findes rækker r_1, r_2, så $M(r_1, a) = M(r_2, a)$ for alle $a \in A$, og $M(r_1, p_b) \neq M(r_2, p_b)$. Men dette er i modstrid med, at $A \rightrightarrows p_b$. Dvs. kravet i definition 2.4.3 medfører kravet i definition 2.4.6.

Antag omvendt, at $|S(A)| = |S(A \cup \{p_b\})|$. Så er der for hver distribution $s_A \in S(A)$ en entydig distribution $s_{A \cup \{p_b\}} \in S(A \cup \{p_b\})$. Dette er præcis kravet i definition 2.4.3, og dermed er også denne ækvivalens bevist. □

Disse tre sidste definitioner er kombinatoriske i den forstand, at de udelukkende baserer sig på antallet af mulige forskellige tupler.

Med relationerne "$\rightarrow$" og "$\rightrightarrows$" kan nu gives definitionen på et perfekt BD-SSS:

Definition 2.4.7. Et secret sharing scheme siges at være *BD-perfekt*, hvis

$$\forall A \subseteq \mathcal{P} \text{ med } A \rightarrow p_0 \text{ gælder } A \rightrightarrows p_0.$$

Så hvis $A \subseteq \mathcal{P}$ har nogen information om hemmeligheden, kan de faktisk bestemme den fuldstændigt. Dvs. A's shares afslører intet om nøglen, med mindre $A \in \Gamma$. Dette kan også formuleres således, at et SSS er BD-perfekt, hvis det opfylder

(BD1) $A \in \Gamma \Rightarrow |S(A \cup \{p_0\})| = |S(A)|$,

(BD2) $A \notin \Gamma \Rightarrow |S(A \cup \{p_0\})| = |S(p_0)| \cdot |S(A)|$.

Definition 2.4.8 (BD-Ideelt Secret Sharing Scheme). Et secret sharing scheme for access-strukturen Γ siges at være *BD-ideelt*, hvis det er BD-perfekt, og

$$|S(p)| = |S(p_0)| = |\mathcal{K}| \quad \forall p \in \mathcal{P}.$$

Γ siges da at være en *ideel access-struktur*.

Denne definition af et ideelt secret sharing scheme er den "kombinatoriske" indgangsvinkel, som er den, der især skal benyttes. Betragt som eksempel nedenstående matrix, der er et eksempel på et ideelt $(3,3)$-threshold scheme i $\mathbb{Z}_2$.

$$M = \left[\begin{array}{c|ccc} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right] \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ p_0 \end{array} \begin{array}{ccc} & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ p_1 & p_2 & p_3 \end{array}$$

Det er en simpel øvelse og derfor overladt til læseren at checke, at ovenstående scheme rent faktisk er ideelt, dvs. at det opfylder

$$\begin{aligned} p_i &\nrightarrow p_k \quad \forall i \neq k \\ \{p_i, p_j\} &\nrightarrow p_k \quad \forall i \neq j \neq k \\ \{p_1, p_2, p_3\} &\rightrightarrows p_0. \end{aligned}$$

Det vil senere i lemma 3.1.5 på side 45 fremgå, at den sidste betingelse faktisk kan forstærkes til at være

$$\{p_i, p_j, p_h\} \rightrightarrows p_k \quad \forall i \neq j \neq h \neq k.$$

2.4.3 Egenskaber ved relationerne "$\rightarrow$" og "$\rightrightarrows$"

I det følgende gøres brug af nogle grundlæggende egenskaber ved relationen "$\rightarrow$" i BD-perfekte schemes. Det lader til, at andre forfattere bevidst eller ubevidst *implicit* har benyttet sig af disse egenskaber til beviser og lignende i diverse artikler, men da ingen imidlertid har gjort sig den umage at formulere eller bevise dem eller endsige nævne, at der eksisterer disse nyttige og nødvendige sammenhænge, har jeg valgt at gøre dette arbejde selv. Det drejer sig om to egenskaber, som jeg vælger at kalde "punktvis monotoni" og "pseudo-transitivitet". Betegnelsen "punktvis monotoni" skal betegne den monotone egenskab ved mængder, som har information om en bestemt person (eller punkt). Ordet "pseudo-transitivitet" kommer af, at hvis $A\backslash\{p\}$ næsten kender hele A, og A kender p_0, så kender $A\backslash\{p\}$ næsten p_0. Disse to egenskaber vil jeg beskrive og bevise herunder. Læg i øvrigt mærke til, at der ikke gøres brug af perfekthed. Egenskaberne er altså forholdsvis generelle. Selvom de senere hen kun skal bruges til perfekte schemes, så vil jeg forsøge at bevise den stærkest mulige sammenhæng. Beviserne kan gøres simplere ved at antage, at det betragtede scheme er perfekt, idet dette betyder, at "$\rightarrow$" bare kan erstattes med "$\rightrightarrows$".

Proposition 2.4.9. *I et ikke nødvendigvis perfekt SSS med $A, B \subseteq \mathcal{P}$, $p \in \mathcal{P}$ og $p_0 \in \mathcal{K}$ har relationen "$\rightarrow$" følgende egenskaber:*

1. *"Punktvis monotoni": Hvis $A \rightarrow p$ og $A \subseteq B$, så er $B \rightarrow p$.*
2. *"Pseudo-transitivitet": Hvis $A\backslash\{p\} \rightarrow p$ og $A \rightrightarrows p_0$, $p_0 \notin A$ og $|\mathcal{S}| = |\mathcal{K}|$, så er $A\backslash\{p\} \rightarrow p_0$.*

Bevis. For at bevise, at $A \rightarrow p$, $A \subseteq B$ medfører $B \rightarrow p$, er det nok at vise, at $A \subseteq B$, $B \nrightarrow p$ medfører $A \nrightarrow p$, idet $A \nrightarrow p$ er negationen af $A \rightarrow p$. Antag derfor at $A \subseteq B$ samt $B \nrightarrow p$. Så gælder det, at

$$\forall \text{ rækker } r, \forall s_p \in S(p)\ \exists \text{ række } r' : \begin{cases} M(r,b) = M(r',b) & \forall b \in B \\ M(r',p) = s_p. \end{cases}$$

Men da $A \subseteq B$, gælder specielt

$$\forall \text{ rækker } r, \forall s_p \in S(p)\ \exists \text{ række } r' : \begin{cases} M(r,a) = M(r',a) & \forall a \in A \\ M(r',p) = s_p. \end{cases}$$

Dvs. $A \nrightarrow p$, og dermed er "punktvis monotoni"-egenskaben bevist.

Til beviset for "pseudo-transitivitet" bruges de alternative definitioner for "$\rightarrow$" og "$\rightrightarrows$". Antag derfor, at

$$|S(A)| = |S((A\backslash\{p\}) \cup \{p\})| < |S(A\backslash\{p\})| \cdot |S(p)|$$
$$|S(A)| = |S(A\backslash\{p_0\})| = |S(A \cup \{p_0\})|.$$

Da antagelsen om $|\mathcal{S}| = |\mathcal{K}|$ giver $|S(p)| = |S(p_0)|$, fås umiddelbart

$$|S(A \cup \{p_0\})| < |S(A \backslash \{p\})| \cdot |S(p_0)|,$$

hvilket giver

$$|S((A \backslash \{p\}) \cup \{p_0\})| \leq |S(A \cup \{p_0\})| < |S(A \backslash \{p\})| \cdot |S(p_0)|.$$

Dette er det samme som $A \backslash \{p\} \rightarrow p_0$.

Den næstsidste ulighed fås, fordi der altid gælder

$$|S(B \backslash \{p\})| \leq |S(B)|$$

for en mængde B med $p \in B$· □

I beviset for "pseudo-transitivitet" var et af kravene, at der i schemet skulle gælde $|\mathcal{S}| = |\mathcal{K}|$. Til gengæld behøvede schemet ikke at være perfekt. Umiddelbart kunne man måske tro, at perfekthed var en egenskab, som var mere grundlæggende og strukturgivende og dermed vigtigere at få med end kravet om antallet af hemmeligheder og shares. Der skal imidlertid nu vises et modeksempel på denne påstand, idet der konstrueres et scheme, som er perfekt med $|\mathcal{S}| \neq |\mathcal{K}|$, men som ikke opfylder pseudo-transitivitet.

Betragt følgende scheme med $\mathcal{S} = \{0, 1, 2\}$ og $\mathcal{K} = \{0, 1\}$:

$$M = \begin{array}{c|cc} 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 2 & 2 \\ 1 & 2 & 0 \\ \hline p_0 & p_1 & p_2 \end{array}$$

Det overlades til læseren at verificere, at schemet er perfekt (altså at $A \rightarrow p_0$ medfører $A \rightrightarrows p_0$ for alle $A \subseteq \mathcal{P}$), samt at der er en access-struktur Γ, som består af følgende delmængde af personer:

$$\{p_1, p_2\}.$$

Der gælder

$$p_1 \rightarrow p_2 \text{ og } p_2 \rightarrow p_1,$$

fordi, hvis f.eks. $s_{p_1} = 0$, så kan det udelukkes, at $s_{p_2} = 0$ og vice versa. Modeksemplet består i, at der her *ikke* gælder hverken $p_1 \rightarrow p_0$ eller $p_2 \rightarrow p_0$, som der jo ellers skulle, hvis der havde gjaldt pseudo-transitivitet for relationen "$\rightarrow$" i dette scheme. Det virker altså som om, at den tilstrækkelige betingelse, $|\mathcal{S}| = |\mathcal{K}|$, også er nødvendig. Et generelt bevis, der fastlægger en betingelse, som både er nødvendig og tilstrækkelig, ville dog for fuldstændighedens skyld være ønskeligt.

Der gælder lignende egenskaber for relationen "$\rightrightarrows$" som dem, der blev vist ovenfor. Blot er det så ikke nødvendigt at lægge krav på størrelsen af $|\mathcal{S}|$ og $|\mathcal{K}|$. Disse egenskaber

er såvidt jeg ved heller ikke eksplicit dokumenterede i andre artikler, så i forlængelse af det foregående vil jeg gøre det her. Her er bare en egenskab kaldet "transitivitet", som betegner, at hvis $A\backslash\{p\}$ kender hele A, og hvis A kender p_0, så gælder det, at $A\backslash\{p\}$ kender p_0, dvs. $A\backslash\{p\} \rightrightarrows A \rightrightarrows p_0$ medfører $A\backslash\{p\} \rightrightarrows p_0$. Udsagnene i denne proposition er egentlig ret klare, når man tænker på hver fordeling som en række og hver share som en indgang i en matrix, men for fuldstændighedens skyld er de alligevel bevist herunder.

Proposition 2.4.10. *I et SSS med $A, B \subseteq \mathcal{P}$, $p \in \mathcal{P}$ og $p_0 \in \mathcal{K}$ har relationen "$\rightrightarrows$" følgende egenskaber:*

1. *"Punktvis monotoni": Hvis $A \rightrightarrows p$ og $A \subseteq B$, så er $B \rightrightarrows p$.*
2. *"Transitivitet": Hvis $A\backslash\{p\} \rightrightarrows p$ og $A \rightrightarrows p_0$, $p_0 \notin A$, så er $A\backslash\{p\} \rightrightarrows p_0$.*

Bevis. For at bevise "punktvis monotoni" for relationen "$\rightrightarrows$" skal man blot betragte schemets matrixrepræsentation samt definition 2.4.6 af "$\rightrightarrows$". Relationen $A \rightrightarrows p$ betyder, at

$$|S(A)| = |S(A \cup \{p\})|.$$

Dvs. for hver distribution i $S(A)$ findes præcis én share i $S(p)$, som passer. $A \subseteq B$ betyder, at der til enhver distribution i $S(B)$ findes præcis én distribution i $S(A)$, som passer, og denne fastlægger jo som sagt værdien af p's share. Dvs. for hver distribution i $S(B)$ findes præcis én distribution i $S(B \cup \{p\})$, så der gælder

$$|S(B)| = |S(B \cup \{p\})|,$$

dvs. $B \rightrightarrows p$.

For at vise "transitivitet" skal man blot som ovenfor observere definitionen af "$\rightrightarrows$". $A\backslash\{p\} \rightrightarrows p$ og $A \rightrightarrows p_0$ betyder, at

$$|S(A\backslash\{p\})| = |S(A)| = |S(A \cup \{p_0\})|. \tag{2.4}$$

Der gælder altid, at $|S(A\backslash\{p\})| \leq |S((A\backslash\{p\}) \cup \{p_0\})| \leq |S(A \cup \{p_0\})|$, hvilket så giver

$$|S(A\backslash\{p\})| = |S(A\backslash\{p\} \cup \{p_0\})|, \tag{2.5}$$

og dermed $A\backslash\{p\} \rightrightarrows p_0$. Så er "transitivitet" bevist. □

Beviserne for propositionerne 2.4.9 og 2.4.10 er egentlig ikke særlig komplicerede, men det ville være ufuldstændigt at bruge egenskaberne, hvis de aldrig er blevet ordentligt formuleret og bevist.

Bemærk iøvrigt, at der i beviset for "transitivitet" ikke blev gjort brug af nogen særlig egenskab ved hemmeligheden s_0 i forhold til en ganske almindelig share s. Ovenstående bevis fra ligning (2.4) til ligning (2.5) kan derfor gennemføres på nøjagtig samme vis, hvis man i stedet for dealeren p_0 indsætter en almindelig person $p' \neq p$. Dette kan formuleres i følgende korollar, som derfor ikke bevises yderligere:

Korollar 2.4.11. *Hvis $A\backslash\{p\} \rightrightarrows p$ og $A \rightrightarrows p'$, $p' \notin A$, så er $A\backslash\{p\} \rightrightarrows p'$.*

Bevis. Substituér p' ind i stedet for p_0 i udregningerne fra ligning (2.4) til ligning (2.5) ovenfor. □

2.4.4 Brickell-Stinson modellen

Der er også et tredje synspunkt, som af og til kaldes Brickell-Stinson modellen (BS). Denne model er ligesom BD-modellen bygget op omkring en matrix, og både share distribution og rekonstruktion er som i BD-modellen. Forskellen er, at BS-modellen beskæftiger sig med *probabilistisk information*.

Lad $A \subseteq \mathcal{P}$ og $p_b \in \mathcal{P} \backslash A$. Da siges A at have *ingen probabilistisk information* om p_b's share (skrives $A \not\rightsquigarrow p_b$), hvis der for alle rækker r findes et $n \in \mathbb{N}$, så det for alle $s_b \in S(b)$ gælder, at der findes præcis n forskellige rækker $r'_1, \ldots, r'_n$, så

$$\begin{aligned} M(r, p_a) &= M(r'_i, p_a) \quad \forall p_a \in A,\ 1 \leq i \leq n, \\ M(r'_i, p_b) &= s_b. \end{aligned}$$

Dvs. for alle rækker r og for alle $s_b \in S(p_b)$ findes der lige mange rækker, som stemmer overens med r på søjlerne i både A og p_b. Ellers siges A at have *probabilistisk information* om p_b, hvilket skrives $A \rightsquigarrow p_b$.

Definition 2.4.12. Et SSS siges at være *BS-perfekt*, hvis det for alle $A \subseteq \mathcal{P}$ gælder, at $A \rightsquigarrow p_0$ medfører $A \rightrightarrows p_0$.

Definitionen af et BS-ideelt scheme er ikke overraskende i tråd med de øvrige definitioner af idealitet, idet det hænger på størrelsen af de indgående alfabeter:

Definition 2.4.13 (BS-Ideelt Secret Sharing Scheme). Et scheme, som er BS-perfekt, kaldes et BS-scheme. Et BS-scheme siges at være *BS-ideelt*, hvis

$$|S(p)| = |S(p_0)| = |\mathcal{K}| \quad \forall p \in \mathcal{P}.$$

2.4.5 Sammenligning af modeller

Det kan nu umiddelbart virke lidt uoverskueligt, hvilken model man skal vælge at studere, men egenskaberne ved de perfekte schemes er heldigvis så stærke, at de tekniske forskelle forsvinder. I [Jackson, Martin] bliver det nemlig vist, at ethvert BS-perfekt SSS specielt også er et IT-perfekt SSS samt, at ethvert IT-perfekt SSS specielt også er BD-perfekt. Dette giver et naturligt hierarki for de forskellige typer af perfekthed, hvor altså BD-perfekthed er den mest generelle.

Hvad ideelle schemes angår, så bliver det endda endnu pænere. Lad BS(Γ) være familien af fordelingsfunktioner på $\{D\} \cup \mathcal{P}$, der opfylder, at $M = (\mathcal{P}, \mathcal{S})$ er et BS-ideelt SSS for Γ. På tilsvarende måde kan IT(Γ) og BD(Γ) defineres. Ifølge [Jackson, Martin] er

$$\mathrm{BS}(\Gamma) = \mathrm{IT}(\Gamma) = \mathrm{BD}(\Gamma),$$

dvs. det er en grundlæggende kombinatorisk struktur, som kendetegner ideelle SSS. Så givet en access-struktur Γ gør det altså ingen forskel, hvilken af definitionerne der bruges til at beskrive et ideelt SSS med.

Dette er selvsagt et meget nyttigt resultat, idet det gør en i stand til at studere et scheme uden at tage hensyn til, på hvilken måde, dets egenskaber defineres. I kapitel 3 kan det derfor arbitrært vælges at benytte BD-schemes, fordi de er enkle i konstruktionen, men teorien for ideelle schemes gælder altså for alle ideelle schemes. Desuden skal der senere gøres brug af de monotone og transitive egenskaber ved relationerne "$\rightarrow$" og "$\rightrightarrows$", som det blev bevist i sektion 2.4.3 i forbindelse med gennemgangen af BD-schemes.

For en alternativ behandling af emnet kan f.eks. henvises til [Ng, Walker], hvor en del af de lemmaer, jeg viser i afsnit 3.1, er formuleret og bevist ved brug af informationsteoretiske argumenter baseret på entropi.

Kapitel 3

Secret Sharing Schemes og Matroider

Det skal i dette kapitel vises, hvordan de ideelle secret sharing schemes korresponderer med matroider, som er objekter kendt fra kombinatorikken (se kapitel 1). Ideen i det følgende er at opfinde et uafhængighedsbegreb for delmængder af deltagerne i et secret sharing scheme for så at bevise sammenhængen mellem den type af uafhængighed og definitionen af uafhængighed i matroideteorien. Denne sammenhæng bliver så vidt muligt bevist i afsnit 3.1 i 1. hovedsætning, sætning 3.1.4 på side 45 og sætning 3.1.12 samt i afsnit 3.3.

Det meste af arbejdet i afsnit 3.1 går ud på at bevise eksistens af korrespondance mellem secret sharing schemes og matroider i sætning 3.1.4 og sætning 3.1.12.

At korrespondancen ydermere er entydig i en vis forstand bliver bevist i afsnit 3.2 i 2. hovedsætning, sætning 3.2.3 på side 52. Den siger, at den korresponderende matroide alene afhænger af access-strukturen.

I afsnit 3.3 ses der på, hvilke matroider, der kan bruges til at repræsentere ideelle secret sharing schemes. Er det alle? Og hvis ikke, hvilke krav må der så stilles? Man lavede desværre en fejl i [Brickell, Davenport], da de troede at have opstillet en betingelse, som var både nødvendig og tilstrækkelig, men det viser sig i [Simonis, Ashikhmin], at den faktisk ikke er helt tilstrækkelig. Jeg gennemgår dette emne i starten af afsnit 3.3 og giver desuden en tilstrækkelig betingelse samt nogle gode eksempler på klasser af matroider, der opfylder denne betingelse.

Afsnit 3.4 handler om en speciel klasse af ideelle access-strukturer, som kaldes universelt ideelle access-strukturer. De universelt ideelle access-strukturer opfylder krav, som er strengere end blot det, at de er ideelle, og det gør, at de kan karakteriseres fuldstændigt. Denne karakterisering udvikles i dette afsnit, idet sætning 3.4.2 bevises.

3.1 Korrespondancen med Matroider

Der skal nu defineres det uafhængighedsbegreb for delmængder af personer $a \subseteq \mathcal{P}$ i et secret sharing scheme, der skal bruges som grundlag for matroidekonstruktionen. Til korrespondancen ønskes nemlig til ethvert SSS at konstruere en matroide. I den følgende definition bruges relationerne "$\rightarrow$" og "$\rightrightarrows$", som blev defineret i forbindelse med BD-modellen i sektion 2.4.2.

Definition 3.1.1. Betragt et secret sharing scheme. En ikke-tom mængde af personer $A \subseteq \{p_0, p_1, \ldots, p_n\}$ siges at være en *uafhængig* mængde mht. dette SSS, hvis

$$\forall p_i \in A\colon A \backslash \{p_i\} \nrightarrow p_i.$$

En mængde af personer $A \subseteq \{p_0, p_1, \ldots, p_n\}$ siges at være en *afhængig* mængde mht. dette SSS, hvis der findes en "afhængighed", dvs. hvis

$$\exists p_i \in A\colon\ (A \backslash \{p_i\}) \rightrightarrows p_i.$$

Bemærk, at afhængighed og uafhængighed mht. til et givet SSS hermed generelt ikke er komplementære begreber. Man kunne nemlig have en mængde A, som havde *nogen* information om en persons share uden dog at kende den helt, dvs.

$$A \backslash \{p_i\} \rightarrow p_i \quad \text{og} \quad A \backslash \{p_i\} \not\rightrightarrows p_i.$$

Da ville mængden A hverken være afhængig eller uafhængig. For ideelle SSS ser det derimod lidt enklere ud, idet enhver mængde A, som ikke er uafhængig, dvs. $A \setminus \{p'\}$ har nogen information om en share $s_{p'}$, faktisk er i stand til at bestemme denne share fuldstændigt. Dermed bliver A automatisk en afhængig mængde. Dette gælder trivielt for alle perfekte SSS, hvis den betragtede share er hemmeligheden s_0, men hvis det er en anden share, er det ikke helt trivielt, at dette gælder. Dette udsagn bliver udtrykt i følgende sætning, som bevises senere:

Sætning 3.1.2. *Lad M være et sammenhængende ideelt SSS. Lad $A \subseteq \mathcal{P}$, og $b \in \mathcal{P}$. Hvis $A \rightarrow b$, så er $A \rightrightarrows b$.*

Beviset for denne sætning vil komme i det følgende som en konsekvens af proposition 3.1.10 på side 49, som i øvrigt bruges til beviset af en hovedsætning. Sætning 3.1.2 siger altså, at afhængighed og uafhængighed er komplementære begreber, hvis blot schemet er ideelt.

Bemærk, ovennævnte definition og sætning tilsammen giver, at hvis $A \in \Gamma^-$ med $p_0 \notin A$, så er A faktisk automatisk uafhængig. Hvis Γ_p^- defineres til at være basen for access-strukturen Γ_p hørende til et sammenhængende ideelt SSS med personen p som dealer, fås følgende:

Proposition 3.1.3. *Lad $A \in \Gamma_p^-$ med $p \in \mathcal{P} \cup \{p_0\}$ og $p \notin A$. Da er A en uafhængig mængde.*

Bevis. Antag at $A \in \Gamma_p^-$ for $p \notin A$ og A ikke uafhængig. Så er

$$A \rightrightarrows p,$$

og der findes en $a \in A$, så

$$A \backslash \{a\} \to a.$$

Ved brug af sætning 3.1.2 ovenfor kan dette forstærkes til

$$A \backslash \{a\} \rightrightarrows a.$$

Men den transitive egenskab (proposition 2.4.10) ved "$\rightrightarrows$" siger så, at $A \backslash \{a\} \rightrightarrows p$, hvilket er i modstrid med minimaliteten af $A \in \Gamma_p^-$. □

3.1.1 Første hovedsætning

I dette afsnit præsenteres den første af dette speciales hovedsætninger, til formålet kaldet hovedsætning 1. Sætningen er dog ikke bevist lige med det samme, for der skal laves en del forarbejde først. Beviset følger her i slutningen af afsnit 3.1.

Jeg starter med at definere en vigtig klasse af delmængder af personer i et SSS:
Lad M være et ideelt scheme. Da defineres

$$D(M) = \{A \subseteq \mathcal{P} \mid \exists y \in A \colon A \backslash \{y\} \rightrightarrows y\},$$

så $D(M)$ består af de delmængder af personer, der er indbyrdes afhængige som beskrevet i definition 3.1.1 på modstående side. Denne type af afhængighed skal kobles sammen med afhængighed i matroide-forstand.

Jeg vil nu give den hovedsætning, som binder de to omtalte typer af afhængighed sammen. Det viser sig, at ethvert sammenhængende ideelt SSS giver anledning til en matroide:

Sætning 3.1.4 (Hovedsætning 1). *Lad M være et sammenhængende ideelt SSS. Da er mængderne i $D(M)$ de afhængige mængder i en sammenhængende matroide.*

Det vides fra hovedsætning 1, at ethvert sammenhængende ideelt SSS giver anledning til en matroide. Denne kaldes også for schemets *associerede matroide*. For at bevise sætning 3.1.4 må man først igennem nogle lemmaer og propositioner omhandlende SSS. Undervejs vises bl.a. også sætning 3.1.2 på modstående side.

Lad i det følgende M være et sammenhængende ideelt SSS og lad $|\mathcal{S}| = q$.

Lemma 3.1.5. *Lad $A \subseteq \mathcal{P}$, og $p \in \mathcal{P}$. Hvis $A \not\rightrightarrows p_0$, og hvis $(A \cup \{p\}) \rightrightarrows p_0$, så er $(A \cup \{p_0\}) \rightrightarrows p$.*

Bevis. Antag $(A \cup \{p\}) \rightrightarrows p_0$, og lad $s_A \in S(A)$ være en bestemt fordeling til A. Relationen $(A \cup \{p\}) \rightrightarrows p_0$ giver nu på baggrund af A's shares en veldefineret surjektiv afbildning

$$\phi_{s_A} : S(p) \twoheadrightarrow S(p_0).$$

Afbildningen ϕ_{s_A} er "rekonstruktionsafbildningen", som $A \cup \{p\}$ bruger til at rekonstruere s_0. I praksis virker ϕ_{s_A} på en værdi $s'_p \in S(p)$ ved at finde en række r' i schemets matrixrepræsentation med $M(r', A) = s_A$ og $M(r', p) = s'_p$. Da kan i matricen aflæses funktionsværdien $\phi_{s_A}(s'_p) = M(r', p_0)$. For hver værdi $s_p \in S(p)$ af p's share findes der nemlig en entydig værdi af p_0's share, idet $(A \cup \{p\}) \rightrightarrows p_0$. Derfor er ϕ_{s_A} veldefineret. Denne afbildning er surjektiv, for hvis der fandtes en værdi $s'_0 \in S(p_0)$ med $s'_0 \notin \mathrm{Im}(\phi_{s_A})$, som derfor ville kunne udelukkes som mulig værdi af hemmeligheden, så ville det betyde, at $A \to s_0$, og dermed $A \rightrightarrows s_0$, idet det ideelle scheme specielt er perfekt. At schemet er ideelt betyder også, at $|S(p)| = |S(p_0)|$, og da disse desuden er endelige, er ϕ_{s_A} også injektiv.

Til hver $s_A \in S(A)$ findes altså en bijektiv afbildning $\phi_{s_A} : S(p) \to S(p_0)$, og der findes dermed en bijektiv afbildning $\phi_{s_A}^{-1} : S(p_0) \to S(p)$, som for hver $p_0 \in S(p_0)$ knytter fordelingen $s_{A\cup\{p_0\}} \in S(A \cup \{p_0\})$ til en entydig værdi af p's share. I praksis virker $\phi_{s_A}^{-1}$ på $s'_0 \in S(p_0)$ ved at finde en række r' i matrixrepræsentationen med $M(r', A) = s_A$ og $M(r', p_0) = s_0$· Funktionsværdien kan da aflæses til $\phi_{s_A}^{-1}(s'_0) = M(r', p)$. Ved hjælp af $\phi_{s_A}^{-1}$ fastlægger $A \cup \{p_0\}$ netop p's share, så $(A \cup \{p_0\}) \rightrightarrows p$. □

Lemma 3.1.6. *Lad $A \subseteq \mathcal{P}$ og $p \in \mathcal{P}$. Hvis $A \not\rightrightarrows p_0$ og $(A \cup \{p\}) \rightrightarrows p_0$, så er*

$$|S(A \cup \{p\})| = q|S(A)|.$$

Bevis. Antag $A \not\rightrightarrows p_0$ og $(A \cup \{p\}) \rightrightarrows p_0$. Det er klart, at

$$|S(A \cup \{p\})| \leq S(p) \cdot |S(A)| = q|S(A)|.$$

Antag $|S(A \cup \{p\})| < S(p) \cdot |S(A)| = q|S(A)|$. Ifølge den alternative definition 2.4.5 af "$\to$" gælder nu $A \to p$, og på grund af pseudo-transitiviteten fra proposition 2.4.9 er så $A \to p_0$, hvilket i et perfekt scheme er det samme som $A \rightrightarrows p_0$. Dette er en modstrid. Der må derfor gælde $|S(A \cup \{p\})| = q|S(A)|$. □

Ovenstående lemma er bevist på en lidt anderledes måde i [Brickell, Davenport], men deres bevis bygger på betragtning af enkelte rækker og shares ud fra definition 2.4.2, og det er lidt mere omstændeligt. Ovenstående bevis er enklere, fordi det udføres ved hjælp af den alternative definition af relationen "$\to$".

Lemma 3.1.7. *Hvis $A \in \Gamma^-$, så er $|S(A)| = q^{|A|}$.*

Bevis. Dette lemma bevises ved modstridsbevis. Antag, at $A \in \Gamma^-$ samt at $|A| = k$. Lad derfor $A = \{a_1, a_2, \ldots, a_k\}$. Antag, at der findes $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathcal{S}$, så der ikke findes nogen række r med $M(r, a_i) = \alpha_i$ for $1 \leq i \leq k$. Lad j være det størst mulige, som opfylder, at der findes en række r' med $M(r', a_i) = \alpha_i$ for $1 \leq i \leq j$. Da schemet er ideelt, er

specielt $|S(a_1)| = q$, dvs. $j \geq 1$. Men så gælder der $\{a_1 \dots a_j\} \to a_{j+1}$, idet der ikke findes nogen række r' med $M(r', a_{j+1}) = \alpha_{j+1}$. Dermed også $\{a_1, \dots, a_j, a_{j+2}, \dots, a_k\} \to p_0$, da $A \in \Gamma^-$ på grund af pseudo-transitiviteten fra proposition 2.4.9. Der gælder jo netop $A \setminus \{a_{j+1}\} \to a_{j+1}$ samt $A \rightrightarrows p_0$, hvilket giver $A \setminus \{a_{j+1}\} \to p_0$. Da M er perfekt, må der derfor endvidere gælde, at $\{a_1, \dots, a_j, a_{j+2}, \dots, a_k\} \rightrightarrows p_0$. Dette er dog en modstrid på grund af minimaliteten, da $A \in \Gamma^-$. □

Lemma 3.1.8. *Lad $A \subseteq \mathcal{P}$ og $A \neq \emptyset$. Hvis $A \not\rightrightarrows p_0$, så er $|S(A)| = q^n$ for et $n \in \mathbb{N}$.*

Bevis. Lad A være en minimal mængde, som opfylder $A \not\rightrightarrows p_0$ samt $|S(A)|$ ikke en potens af q. Lad $B \subseteq \mathcal{P} \setminus A$ være en mængde, som opfylder, at

i. $(A \cup B) \rightrightarrows p_0$,

ii. $B \not\rightrightarrows p_0$,

iii. $(A \cup B \setminus \{b\}) \not\rightrightarrows p_0 \quad \forall b \in B$.

Først må man lige overbevises om, at en sådan mængde B faktisk eksisterer: Lad $a \in A$ og lad $C \in \Gamma^-$ med $a \in C$. Dette findes, da $A \neq \emptyset$, og da M er sammenhængende. Lad da $B \subseteq C \setminus A$ være en minimal mængde, så $(A \cup B) \rightrightarrows p_0$. Nu er (i) og (iii) klart opfyldt, og (ii) er opfyldt, fordi $B \subsetneq C \in \Gamma^-$. En sådan mængde B findes altså.

Det er klart, at $|S(A \cup B)| \leq q^{|A \cup B|}$. Hvis der gælder $|S(A \cup B)| = q^{|A \cup B|}$, så er alle de mulige fordelinger (dvs. rækker) til $A \cup B$ repræsenteret i matricen, og så er specielt også alle de mulige fordelinger til A repræsenteret. Dvs. $|S(A)| = q^{|A|}$, og i dette tilfælde er sætningen dermed vist.

Antag nu $|S(A \cup B)| < q^{|A \cup B|}$, og lad $n \in \mathbb{N}$ være sådan, så $q^n < |S(A)| < q^{n+1}$. Lad $a \in A$. På grund af minimaliteten af A er $|S(A \setminus \{a\})|$ en potens af q, dvs. $|S(A \setminus \{a\})| = q^n$. Lad $A = \{a_1, \dots, a_k\}$ være sådan, at $a_k = a$. Da $|S(A \setminus \{a\})| \leq q^{|A|-1}$, er det er klart, at $n \leq |A| - 1$.

Antag først, at $n < |A|-1$. Lad os bygge A op fra bunden ved at tilføje personerne $a_1, \dots, a_k$ enkeltvis. Da schemet er ideelt, er $S(a_1) = q$, og alle delmængder $A' \subseteq A$ har på grund af minimaliteten af A, at $|S(A')|$ er en potens af q. Ved at tilføje det næste element a_2 til a_1 fås en mængde $\{a_1, a_2\}$ med $|S(\{a_1, a_2\})|$ en potens af q. Dette gentages for hver gang der tilføjes et element a_i, indtil der kommer et element $a_{j+1} \in A$, hvorom det gælder, at

$$|S(\{a_1, \dots, a_j\}| = |S(\{a_1, \dots, a_j, a_{j+1}\})|,$$

hvilket er det samme som

$$\{a_1, \dots, a_j\} \rightrightarrows a_{j+1}. \tag{3.1}$$

Dette element a_{j+1} må eksistere, fordi $S(a_i) = q$ for alle i, og fordi $|S(A')|$ er en potens af q for alle $A' \subseteq A$, mens $|S(A)|$ *ikke* er en potens af q. Antallet af forskellige distributioner til $a_1, a_2, \dots, a_j$ er altså det samme som antallet af forskellige distributioner til $a_1, a_2, \dots, a_j, a_{j+1}$.

Da $\{a_1, \ldots, a_j\} \subseteq A \backslash \{a_{j+1}\}$, gælder det ifølge punktvis monotoni for "$\rightrightarrows$" (prop. 2.4.10), at ligning (3.1) medfører

$$A \backslash \{a_{j+1}\} \rightrightarrows a_{j+1}.$$

Der gælder nu, at

$$|S(A \backslash \{a_{j+1}\})| = |S(A)|,$$

hvilket er i modstrid med minimaliteten af A. Derfor er $n = |A| - 1$, dvs.

$$|S(A \backslash \{a\})| = q^{|A|-1} \quad \forall a \in A.$$

Lad nu $a \in A$ samt $B = \{b_1, \ldots, b_l\}$. Ifølge lemma 3.1.6 på side 46 er

$$|S(A \cup B)| = q|S(A \cup B \backslash \{b\})| = |S(b)| \cdot |S(A \cup B \backslash \{b\})| \quad \forall b \in B,$$

hvilket ifølge den alternative definition 2.4.4 af "$\twoheadrightarrow$" giver

$$A \cup B \twoheadrightarrow b \quad \forall b \in B,$$

og dermed specielt også

$$(A \cup B) \backslash \{a\} \twoheadrightarrow b \quad \forall b \in B.$$

Så for alle j med $1 \leq j \leq l$ gælder det, at

$$\left|S((A \backslash \{a\}) \cup \{b_1, \ldots, b_j\})\right| = q\left|S((A \backslash \{a\}) \cup \{b_1, \ldots, b_{j-1}\})\right|.$$

Så er

$$|S(A \cup B \backslash \{a\})| = q^{|A \cup B|-1} \quad \forall a \in A.$$

Da $|S(A \cup B)| < q^{|A \cup B|}$, viser dette, at det er a's share, som bliver kompromitteret, så det må være $(A \cup B \backslash \{a\}) \rightarrow a$, dvs. $(A \cup B \backslash \{a\}) \rightarrow p_0$ på grund af pseudo-transitiviteten, idet $(A \cup B) \rightrightarrows p_0$. Da schemet er ideelt, gælder faktisk

$$(A \cup B \backslash \{a\}) \rightrightarrows p_0 \quad \forall a \in A.$$

Lad nu $D \in \Gamma^-$ med $B \subset D \subseteq A \cup B$. Bemærk, at $D \cap A \neq \emptyset$, idet $B \notin \Gamma^-$. Lad derfor $a \in D \cap A$. Da $D \in \Gamma^-$, er $D \backslash \{a\} \not\rightrightarrows p_0$, men, som det lige er vist, er $A \cup B \backslash \{a\} \rightrightarrows p_0$. Lad $A \backslash D = \{a_1, \ldots, a_m\}$. Så må der findes et j med $0 \leq j < m$, så

$$\begin{cases} \Big((D \backslash \{a\}) \cup \{a_1, \ldots, a_j\}\Big) \not\rightrightarrows p_0 \\ \Big((D \backslash \{a\}) \cup \{a_1, \ldots, a_j, a_{j+1}\}\Big) \rightrightarrows p_0. \end{cases}$$

Så ifølge lemma 3.1.5 på side 45 er

$$\Big((D \backslash \{a\}) \cup \{a_1, \ldots, a_j\} \cup \{p_0\}\Big) \rightrightarrows a_{j+1}.$$

Da $(A \cup B \backslash \{a_{j+1}\}) \rightrightarrows p_0$, fås

$$\Big(A \cup B \backslash \{a_{j+1}\}\Big) \rightrightarrows \Big((D \backslash \{a\}) \cup \{a_1, \ldots, a_j\} \cup \{p_0\}\Big) \rightrightarrows a_{j+1},$$

og pr. transitivitet af "$\rightrightarrows$" er så $(A \cup B\backslash\{a_{j+1}\}) \rightrightarrows a_{j+1}$, dvs.

$$|S(A \cup B)| = |S(A \cup B\backslash\{a_{j+1}\})| = q^{|A\cup B|-1}.$$

Der gælder nu $q^{|A|-1} < |S(A)|$ samt $|S(A \cup B)| = q^{|A\cup B|-1}$, dvs. der må findes et j med $1 \leq j \leq l-1$, så $|S(A \cup \{b_1, \ldots, b_{j+1}\})| < q|S(A \cup \{b_1, \ldots, b_j\})|$. Men så er $(A \cup \{b_1, \ldots, b_j\}) \to b_{j+1}$, og da $(A \cup B) \rightrightarrows p_0$, fås endelig $(A \cup B\backslash\{b_{j+1}\}) \rightrightarrows p_0$, da M er perfekt. Men dette er i modstrid med (iii) ovenfor.

Det er så vist, at $|S(A \cup B)| = q^{|A\cup B|}$, og dermed $|S(A)| = q^{|A|}$. □

Lemma 3.1.9. *Lad $A \subseteq \mathcal{P}$ og $A \neq \emptyset$. Hvis $A \rightrightarrows p_0$, så er $|S(A)| = q^n$ for et $n \in \mathbb{N}$.*

Bevis. Lad A være en minimal mængde med den egenskab, at $|S(A)|$ ikke er en potens af q. Ifølge lemma 3.1.8 på side 47 må da $A \to p_0$, og dermed, da M er perfekt, $A \rightrightarrows p_0$. Lad $B \subseteq A$ med $B \in \Gamma^-$, og lad $a \in B$. Hvis $A\backslash\{a\} \rightrightarrows p_0$, må der findes en delmængde $C \subseteq A\backslash\{a\}$ med $C \in \Gamma^-$. Idet $C \rightrightarrows p_0$, og $((B\backslash\{a\}) \cup \{p_0\}) \rightrightarrows a$ (lemma 3.1.5 på side 45), er $(C \cup B\backslash\{a\}) \rightrightarrows a$. Ifølge definition 2.4.3 på side 34 gælder da $|S(A)| = |S(A\backslash\{a\})|$. Men dette er en modstrid med minimaliteten af A, idet $|S(A\backslash\{a\})|$ så heller ikke er en potens af q.
Ifølge lemma 3.1.6 på side 46 er nu $|S(A)| = q|S(A\backslash\{a\})|$, og da $|S(A\backslash\{a\})|$ er en potens af q, er også $|S(A)|$ en potens af q. □

Lemmaerne 3.1.8 på side 47 og 3.1.9 viser tilsammen den følgende proposition:

Proposition 3.1.10. *For alle $A \subseteq \mathcal{P}$ gælder det, at $|S(A)| = q^n$ for et $n \in \mathbb{N}$.*

Dette viser samtidigt også sætning 3.1.2 på side 44:

Bevis for sætning 3.1.2 på side 44. Antag $A \to b$. Så er $|S(A \cup \{b\})| < q|S(A)|$. Ifølge proposition 3.1.10 er da $|S(A \cup \{b\})| = |S(A)|$, dvs. $A \rightrightarrows b$. □

Således er forarbejdet gjort, og der kan nu gås til beviset for den første hovedsætning, sætning 3.1.4 på side 45:

Bevis for sætning 3.1.4 (hovedsætning 1) på side 45. Lad en funktion $\rho : 2^{\mathcal{P}} \to \mathbb{Z}_+$ være defineret ved

$$\rho(\emptyset) = 0,$$
$$\rho(A) = \log_q |S(A)| \quad \forall A \subseteq \mathcal{P}.$$

Lad $A \subseteq \mathcal{P}$ og $p \in \mathcal{P}$. Da er det klart, at $\rho(A) \leq \rho(A \cup \{p\}) \leq \rho(A) + 1$. Lad $A \subseteq \mathcal{P}$ og $p_1, p_2 \in \mathcal{P}$ med $|S(A \cup \{p_i\})| = |S(A)|$ for $i = 1, 2$. Så er $A \rightrightarrows p_i$ for $i = 1, 2$, og dermed $|S(A \cup \{p_1, p_2\})| = |S(A)|$. Funktionen ρ er således rangfunktionen for en matroide.

Lad $\mathcal{T}$ være matroiden på $\mathcal{P}$ med rangfunktion ρ. En mængde $A \subseteq \mathcal{P}$ opfylder $A \in D(\mathcal{T})$[1], hvis og kun hvis der findes et $a \in A$, så $(A\backslash\{a\}) \rightrightarrows a$, hvilket sker, hvis og kun hvis

[1] $D(\mathcal{T})$ må her ikke forveksles med den såkaldte cykelmatrix for en binær matroide, som flere andre steder i litteraturen om matroideteori benævnes netop således.

der findes et $a \in A$, så $|S(A\backslash\{a\})| = |S(A)|$. Dette er ækvivalent med $\rho(A\backslash\{a\}) = \rho(A)$ for alle $a \in A$. Dette betyder, at A er en afhængig mængde i $\mathcal{T}$, idet $\rho(A)$ er ordenen af den største uafhængige delmængde af A.

Idet $\mathcal{T}$ er sammenhængende, findes der for ethvert $p \in \mathcal{P}\backslash\{p_0\}$ en cykel, som indeholder p og p_0. Ifølge lemma 1.1.8 på side 10 findes der derfor for alle $p_1, p_2 \in \mathcal{P}$ en cykel, som indeholder dem begge, hvilket betyder, at $\mathcal{T}$ er sammenhængende. □

Til ethvert sammenhængende ideelt SSS kan der altså ifølge hovedsætning 1 (sætning 3.1.4) tilordnes en sammenhængende matroide. Denne kaldes for $\mathcal{T}(M)$.

3.1.2 Ombytningsegenskaben

Denne sektion har til formål at bevise sætning 3.1.12, som udtaler sig om den vigtige egenskab ved sammenhængende ideelle schemes, som jeg vil kalde ombytningsegenskaben.

Først et lemma:

Lemma 3.1.11. *Lad $A \subseteq \mathcal{P} \cup \{p_0\}$ og lad $p \in \mathcal{P} \cup \{p_0\}$. Hvis A er uafhængig og $A \not\rightrightarrows p$, så er $A \cup \{p\}$ uafhængig.*

Bevis. Antag at $A \cup \{p\}$ er afhængig. Så findes et $a \in A \cup \{p\}$, så

$$(A \cup \{p\})\backslash\{a\} \rightrightarrows a. \tag{3.2}$$

Der må gælde $a \neq p$, da der ellers skulle have gjaldt $(A \cup \{p\})\backslash\{p\} \rightrightarrows p$. Men dette ville være i strid med antagelsen om, at A er uafhængig.

Da A er uafhængig, er automatisk også $A\backslash\{a\}$ uafhængig, dvs. $A\backslash\{a\} \not\rightrightarrows a$. Men ifølge ligning (3.2) gælder det, at

$$(A\backslash\{a\}) \cup \{p\} = (A \cup \{p\})\backslash\{a\} \rightrightarrows a.$$

Ved brug af lemma 3.1.5 på side 45 fås nu, at

$$\underbrace{(A\backslash\{a\}) \cup \{a\}}_{A} \rightrightarrows p.$$

Men dette er i modstrid med, at $A \not\rightrightarrows p$. □

Bemærk den interessante egenskab, at lemma 3.1.5 kombineret med sætning 3.1.2 siger, at et sammenhængende ideelt SSS er sammenhængende ideelt med hvilken som helst person optrædende som "dealer". Et sammenhængende ideelt SSS er åbenbart symmetrisk i den forstand, at der ikke er nogen person, som er speciel i forhold til at være dealer, og enhver minimal autoriseret delmængde $\{p_1, p_2, \ldots, p_k\}$ i access-strukturen Γ_{p_0} med personen p_0 som dealer kommer også til at blive minimal autoriseret i access-strukturen Γ_{p_1} med personen p_1 som dealer, når blot p_1 substitueres med p_0:

$$\Gamma^-_{p_0} \ni \{p_1, p_2, \ldots, p_k\} \rightleftarrows \{p_0, p_2, \ldots, p_k\} \in \Gamma^-_{p_1}.$$

Egenskaben kan formuleres i den følgende vigtige sætning:

Sætning 3.1.12 (Ombytningsegenskaben). *Lad $A \in \Gamma^-_{p_0}$, $p_0 \notin A$ med $p_1 \in A$. Da er $(A \cup \{p_0\})\backslash\{p_1\} \in \Gamma^-_{p_1}$.*

Bevis. Ifølge lemma 3.1.5 og sætning 3.1.2 er $((A \cup \{p_0\})\backslash\{p_1\}) \in \Gamma_{p_1}$, dvs. der gælder $(A \cup \{p_0\})\backslash\{p_1\} \rightrightarrows p_1$ og dermed $A \cup p_0 \in D(M)$.

For at vise, at $((A \cup p_0)\backslash\{p_1\}) \in \Gamma^-_{p_1}$, skal det vises, at $(A \cup p_0)$ er minimal i $D(M)$. Men da A er uafhængig med $A \in \Gamma^-_{p_0}$, er $A\backslash\{p_1\}$ også uafhængig, og der gælder $A\backslash\{p_1\} \not\rightrightarrows p_0$. Iflg. lemma 3.1.11 er så også $(A \cup p_0)\backslash\{p_1\}$ uafhængig, og dermed $((A \cup p_0)\backslash\{p_1\}) \notin D(M)$. Dvs. $(A \cup p_0)$ er minimalt element i $D(M)$. □

3.2 Entydighed af den Associerede Matroide

I dette afsnit skal der ses, på hvilken måde den til et secret sharing scheme hørende matroide $\mathcal{T}(M)$ kan siges at være entydigt bestemt. Der viser sig nemlig med hovedsætning 2 (side 52) at gælde den overraskende stærke sammenhæng, at den associerede matroide til et SSS alene afhænger af access-strukturen Γ. Dette er overraskende, fordi det betyder, at det ikke gør nogen forskel, hvilken faktisk konstruktion, M, man vælger at bruge. Hele den kombinatoriske karakteristik ligger i access-strukturen. Denne egenskab gør det lettere at karakterisere de ideelle schemes, da man således kan identificere alle dem med samme access-struktur.

Før jeg giver hovedsætning 2, vil jeg gennemgå lidt mere forarbejde angående matroider og SSS. Jeg starter med et resultat fra matroideteorien om sammenhængende matroider. Disse kan nemlig fastlægges entydigt ud fra deres cykler gennem et enkelt fast punkt.

Lemma 3.2.1. *Lad $\mathcal{M}$ være en sammenhængende matroide på S og lad $e \in S$ være et fast punkt. Mængden af cykler i $\mathcal{M}$ gennem e bestemmer da $\mathcal{M}$ entydigt.*

Bevis. Lad $\mathcal{C}$ være mængden af cykler i $\mathcal{M}$ gennem punktet $e \in S$. Definér for enhver delmængde $X \subseteq S$

$$D(X) = X \setminus \bigcap_{C \in \mathcal{C}} \{C \subseteq X\}.$$

Idet $\mathcal{M}$ er bestemt ved sine cykler, skal man forsøge at bestemme disse. Det skal vises, at de cykler i $\mathcal{M}$, som ikke indeholder e, er præcis de minimale mængder på formen

$$D(C_1 \cup C_2) \quad \text{hvor} \quad C_1, C_2 \in \mathcal{C} \quad \text{og} \quad C_1 \neq C_2. \tag{3.3}$$

Lad $C_1, C_2 \in \mathcal{C}$, $e \in C_1 \cap C_2$ og $C_1 \neq C_2$. Så findes ifølge proposition 1.1.6 på side 9 en cykel $C \subseteq (C_1 \cup C_2)\backslash\{e\}$. Lad nu $y \in C$. Så er $y \in C \cap C_i$ for $i \in \{1, 2\}$, idet $C \subseteq C_1 \cup C_2$. Bemærk, at $C \neq C_i$, idet $e \in C_i$ men $e \notin C$, så igen på grund af proposition 1.1.6 må der eksistere en cykel $C' \subseteq (C \cup C_i)\backslash\{y\}$ for $i \in \{1, 2\}$. For alle $y \in C$ findes der derfor en cykel $C' \in \mathcal{C}$ med

$$C' \subseteq (C \cup C_i)\backslash\{y\} \subseteq (C_1 \cup C_2)\backslash\{y\}.$$

Så gælder det for alle $y \in C$, at

$$y \notin \bigcap_{C'' \in \mathcal{C}} \{C'' \subseteq C_1 \cup C_2\}.$$

Dvs. $C \subseteq D(C_1 \cup C_2)$, og så er $D(C_1 \cup C_2)$ afhængig i $\mathcal{M}$, idet C er afhængig.

Lad nu C være en cykel i $\mathcal{M}$, som ikke indeholder e. Da $\mathcal{M}$ er sammenhængende, findes der en cykel $C_1 \in \mathcal{C}$, så C_1 snitter C. Vælg C_1 således at $C \cup C_1$ er minimal. Så findes en cykel $C_2 \in \mathcal{C}$, så $C_2 \subseteq C \cup C_1$, og $C_2 \neq C_1$. Men for alle $C' \in \mathcal{C}$ med $C' \subseteq C_1 \cup C_2$ gælder det, at C' snitter C, og på grund af minimaliteten af $C \cup C_1$ er $C \cup C'$ ikke en ægte delmængde af $C \cup C_1$. Men $C \cup C' \subseteq C \cup C_1 \cup C_2 = C \cup C_1$, og så er $C \cup C' = C \cup C_1$. Dvs.

$$C \cup C_1 \cup C_2 = C \cup C_1 = C \cup \left(\bigcap_{C' \in \mathcal{C}} \{C' \subseteq C_1 \cup C_2\} \right).$$

Altså $D(C_1 \cup C_2) \subseteq C$, og dermed $D(C_1 \cup C_2) = C$.

Samtlige cykler i $\mathcal{M}$ er så bestemt, idet alle de cykler, som ikke indeholder e er på den bestemte form fra ligning (3.3). Dermed er $\mathcal{M}$ entydigt bestemt. □

Og så et lemma om secret sharing schemes og associerede matroider. Dette lemma skal vise sig at være en vigtig karakterisering af cyklerne i den associerede matroide for et SSS. Der gøres stor brug af denne tankegang i kapitel 4:

Lemma 3.2.2. *Lad M være et ideelt SSS. Cyklerne i den associerede matroide $\mathcal{T}(M)$ gennem et punkt p udgøres netop af mængderne på formen $A \cup \{p\}$, hvor $A \in \Gamma_p^-$.*

Bevis. Hvis $A \in \Gamma_p^-$, er A minimalt autoriseret mht. p som dealer, og iflg. proposition 3.1.3 er A uafhængig, og pr. definition $(A \cup \{p\}) \in D(M)$. Iflg. 1. hovedsætning (3.1.4) er $A \cup \{p\}$ en afhængig mængde i matroiden $\mathcal{T}(M)$. Da $A \in \Gamma_p^-$, gælder det for alle $a \in A$, at $A \backslash \{a\} \not\rightrightarrows p$, og iflg. lemma 3.1.11 er $(A \backslash \{a\}) \cup \{p\} = (A \cup \{p\}) \backslash \{a\}$ uafhængig, dvs. pr. 1. hovedsætning er $((A \cup \{p\}) \backslash \{a\}) \notin D(M)$. Dermed er $A \cup \{p\}$ en minimal afhængig mængde i $\mathcal{T}(M)$, dvs. en cykel.

Hvis omvendt X er en cykel i $\mathcal{T}(M)$ gennem p, så er X iflg. 1. hovedsætning et minimalt element i $D(M)$, og så findes der et element $x \in X$, så $X \backslash \{x\} \rightrightarrows x$, og $X \backslash \{x\}$ er minimal med denne egenskab, dvs. $(X \backslash \{x\}) \in \Gamma_x^-$. Nu kan ombytningsegenskaben (sætning 3.1.12) bruges til at slutte, at $(X \backslash \{p\}) \in \Gamma_p^-$. □

3.2.1 Anden hovedsætning

Det følgende er specialets anden hovedsætning, sætningen om entydighed af den associerede matroide. På baggrund af det foregående kan følgende hovedsætning vises:

Sætning 3.2.3 (Hovedsætning 2). *Lad M være et ideelt SSS for Γ. Så er den associerede matroide $\mathcal{T}(M)$ uafhængig af M og entydigt bestemt ved Γ.*

Bevis. Ifølge lemma 3.2.2 på forrige side udgør mængderne på formen $A \cup \{p_0\}$ med $A \in \Gamma^-$ cyklerne i $\mathcal{T}(M)$ gennem p_0. Da $\mathcal{T}(M)$ desuden er sammenhængende, er $\mathcal{T}(M)$ så ifølge lemma 3.2.1 på side 51 entydigt bestemt ved cyklerne gennem p_0. Dvs. $\mathcal{T}(M)$ er entydigt bestemt ved Γ^-. □

Den associerede matroide til access-strukturen Γ kaldes for $\mathcal{T}(\Gamma)$. Det viser sig altså ifølge hovedsætning 1 og hovedsætning 2, at der er en nøje sammenhæng imellem matroider og ideelle access-strukturer, dvs. access-strukturer for hvilke, der eksisterer et ideelt SSS.

3.3 Secret sharing-matroider

I de foregående afsnit er det vist, hvordan ethvert ideelt secret sharing scheme M giver anledning til en matroide $\mathcal{T}(M)$ (hovedsætning 1). Desuden er entydigheden af denne matroide blevet studeret, idet korrespondancen er forstærket til at vise, at enhver ideel access-struktur Γ associerer en entydig matroide $\mathcal{T}(\Gamma)$ (hovedsætning 2). Spørgsmålet er så nu, hvilke matroider, der giver anledning til et ideelt secret sharing scheme. Matroider med denne egenskab kaldes for *secret sharing-matroider*. En secret sharing-matroide er altså en matroide på formen $\mathcal{T}(\Gamma)$ for en ideel access-struktur Γ. Dette begreb må defineres mere præcist.

Lad $A = \left(a_{i,j}\right)_{i \in I, j \in V}$ være en endelig matrix med indgange i en endelig mængde $\mathcal{S}$. Lad $i \in I$, $p \in V$ og $X \subseteq V \backslash \{p\}$. Da defineres

$$n(i, p, X) = \left\{ a_{j,p} \mid j \in I, a_{j,x} = a_{i,x} \ \forall x \in X \right\}.$$

$n(i, p, X)$ er altså mængden af indgange i søjle p, som sidder i rækker, der stemmer overens på søjlemængden X's shares i række i. Eller set fra X's synspunkt: Betragt indgangene i $a_{i,X} = \{a_{i,x} \mid x \in X\}$. Hvilke værdier $a_{j,p}$ er mulige i søjle p, hvis den tilhørende række skal stemme overens på X med fordelingen $a_{i,X}$? – Det er netop værdierne i $n(i, p, X)$.

Bemærk: Notationen her kommer fra [Seymour], og i min egen beskrivelse af secret sharing schemes efter BD-modellen, brugte jeg en anden betegnelse for $n(i, p, X)$, nemlig s_X, når række i og person p var underforstået. Jeg bruger i dette afsnit notationen fra [Seymour] for at illustrere, at dette handler om at beskrive en bestemt type af matricer og ikke en bestemt type af SSS. Undervejs vil jeg dog pointere noget af analogien med SSS, for at man ikke helt mister forbindelsen dertil.

En secret sharing-matrix defineres som følger:

Definition 3.3.1. En endelig matrix $A = \left(a_{i,j}\right)_{i \in I, j \in V}$ siges at være en *secret sharing-matrix over* $\mathcal{S}$, hvis der for alle $p \in V$ og for alle $X \subseteq V \backslash \{p\}$ gælder enten

$$n(i, p, X) = \mathcal{S} \quad \forall i \in I \qquad \text{eller} \qquad |n(i, p, X)| = 1 \quad \forall i \in I.$$

Matricer af denne type er som nævnt præcis dem, der før er beskrevet som matrixrepræsentationer for ideelle SSS i BD-modellen. Lad nemlig A være en offentligt kendt secret

sharing-matrix efter ovenstående definition og lad D være dealeren i det SSS, der nu skal konstrueres. Lad rækken $i \in I$ være hemmeligt valgt af D. Betragt delmængden af personer $X \subseteq V$. Med denne notation er i forhold til tidligere beskrivelser mængden af personer (inkl. dealeren) $V = \mathcal{P} \cup \{p_0\}$. Lad $p_0 \in V \backslash X$. For at sammenligne egenskaberne ved secret sharing-matricer med de egenskaber, der forventes af et ideelt SSS, skal det undersøges, hvor meget information mængden X har om værdien af a_{i,p_0}. Bemærk, at der allerede nu gælder, at $\mathcal{K} = \mathcal{S}$.

Mængden af mulige værdier er de a_{j,p_0}, $j \in I$, hvor alle $a_{j,x}$ stemmer overens med $a_{i,x}$, $x \in X$. Her svarer $\{a_{i,x} \mid x \in X\}$ til mængden af de shares, som er givet til X. Dvs. mængden af mulige værdier af a_{j,p_0} set fra X's synspunkt er præcis

$$n(i, p_0, X) = \{a_{j,p_0} \mid j \in I, a_{j,x} = a_{i,x}\ \forall x \in X\}.$$

Elementerne i denne mængde kan bestemmes af X ved aflæsning blandt elementerne i søjle p_0 i matricen A, som jo er offentligt kendt.

Da A er en secret sharing-matrix, gælder det, at

$$n(i, p_0, X) = \mathcal{S} \qquad \text{eller} \qquad |n(i, p_0, X)| = 1.$$

Hvis $n(i, p_0, X) = \mathcal{S}$, betyder det, at alle værdier i $\mathcal{S}$ er mulige værdier for hemmeligheden a_{i,p_0}. Så har X altså ingen ikke-triviel information, dvs. $X \notin \Gamma$, og $X \nrightarrow p_0$. Hvis derimod $|n(i, p_0, X)| = 1$, er der kun én mulig værdi for a_{i,p_0}. Da $n(i, p_0, X)$ desuden kan bestemmes af X, kender X hemmeligheden entydigt, dvs. $X \in \Gamma$. Secret sharing-matricer er altså af samme type som dem, der blev defineret under beskrivelsen af BD-modellen i afsnit 2.4.2.

Lad mig nu (gen)definere begrebet secret sharing-matroide. Jeg giver her [Seymour]'s definition. Han definerer afhængighed sådan, at en delmængde $X \subseteq V$ er afhængig, hvis der findes et $p \in X$ sådan, at $|n(i, p, X \backslash \{p\})| = 1$ for alle $i \in I$. Han bruger denne definition af afhængighed til definitionen af secret sharing-matroider. Denne definition er dog ækvivalent med den fra BD-modellen, hvor man definerede en afhængig delmængde til at være en, som opfylder $X \backslash \{p\} \rightrightarrows p$ for et $p \in X$. En secret sharing-matroide efter [Seymour] er altså, hvad der hele tiden blev kaldt den associerede matroide til et ideelt SSS.

Det oplagte spørgsmål at stille først er, om alle matroider er secret sharing-matroider. Dette viser sig imidlertid *ikke* at holde, idet der findes et modeksempel. [Seymour] har vist, at Vamos-matroiden ikke er en secret sharing-matroide. Selve beviset er ikke i sig selv så spændende i denne sammenhæng, men resultatet er selvsagt ret vigtigt.
Vamos-matroiden er matroiden på punktmængden af 8 elementer $V = \{1, 2, \ldots, 8\}$, hvor de uafhængige mængder er alle delmængder af kardinalitet højst 4 undtagen netop følgende fem:

$$\{1, 2, 3, 4\},\ \{1, 2, 5, 6\},\ \{3, 4, 5, 6\},\ \{3, 4, 7, 8\},\ \{5, 6, 7, 8\}.$$

Denne specielle matroide har ikke nødvendigvis nogen egenskab, som ville gøre den ønskelig i secret sharing-sammenhænge, men resultatet betyder, at der faktisk findes matroider, som ikke er associerede til noget ideelt SSS.

3.3.1 En fejl rettes

Hvilke krav skal så stilles til en matroide, for at den bliver en secret sharing-matroide? Dette spørgsmål er desværre ikke så enkelt at besvare helt præcist, idet det stadig er et uløst problem at stille en betingelse, som både er nødvendig og tilstrækkelig. I [Brickell, Davenport] drages den konklusion, at en matroide var en secret sharing-matroide, hvis den var repræsenteret over, hvad de kaldte et "right nearfield" eller blot "nearfield" (et legeme bortset fra at det kun er højre-distributivt). Der viste sig dog imidlertid at være et problem med dette krav, idet der i "beviset" for [Brickell, Davenport], Theorem 2, implicit blev gjort den antagelse, at right nearfield'et faktisk var venstre-distributivt! [Simonis, Ashikhmin] retter denne fejl og giver faktisk et modeksempel, så Brickell-Davenports sætning holder i hvert fald ikke for alle nearfields. For at uddybe dette må man dog ind på emnet "almost affine codes".

Her er den sætning, som Brickell-Davenport troede, de havde vist:

Sætning 3.3.2 (Brickell-Davenports fejlsætning). *Lad $\mathcal{T} = (V, \mathcal{I})$ være en sammenhængende matroide, som er repræsentérbar over et right nearfield R, og lad $v_0 \in V$. Så findes et sammenhængende ideelt secret sharing scheme M, så $R = \mathcal{K}$, $p_0 = v_0$, $\mathcal{P} = V$, og $D(M)$ er de afhængige mængder i $\mathcal{T}$.*

Man kan dog stadig bruge det fejlagtige bevis til at bevise sætningen for legemer. Et legeme er jo blot et nearfield, som er distributivt fra begge sider. Dette gøres lidt senere i beviset for sætning 3.3.11 på side 59. Her bliver det også påpeget præcis, hvor det er, at Brickell-Davenport begår deres fejl.

3.3.2 Næsten-affine koder og ideelle secret sharing schemes

I denne sektion skal der ses lidt nærmere på [Simonis, Ashikhmin]'s konstruktion "almost affine codes", som jeg selv vælger at kalde "næsten-affine koder". Her kommer derfor en kort gennemgang af dette emne – lige nok til at forstå det modeksempel, som gennemgås i næste sektion.

En lineær kode C af længde n og alfabetstørrelse q er et lineært underrum af vektorrummet $\mathbb{F}_q^n$ over legemet $\mathbb{F}_q$. Dvs. $|C| = q^k$ for et $k \in \mathbb{N}$.

Lad $X \subseteq \{1, \ldots, n\}$ og lad $\mathbb{F}^X = \prod_{i \in X} \mathbb{F}_q$. Da er projektionen C_X af C ind i $\mathbb{F}^X$ også en lineær kode, og $|C_X|$ er en potens af q.

Lad $|F| = q \geq 2$ og $S = \{1, \ldots, n\}$. Lad F^S være mængden af afbildninger fra S til F. Lad $X \subseteq S$ og lad

$$\rho_X^S : F^S \to F^X$$

være afbildningen induceret af inklusionen $X \hookrightarrow S$.

En q-adisk kode af længde n er en ikke-tom delmængde af F^S.

Billedet $\rho_X^S(C)$ af en kode $C \subseteq F^S$ benævnes C_X. $C_X = \rho_X^S(C)$ kaldes projektionen af C ind i F^X.

Definition 3.3.3. En kode $C \subseteq F^S$ siges at være *næsten-affin*, hvis

$$r(X) \equiv \log_q |C_X| \in \mathbb{N} \text{ for alle } X \subseteq S.$$

Definition 3.3.4. *Dimensionen* af en næsten-affin kode C er

$$\dim C = r(S) = \log_q |C|.$$

Definition 3.3.5. To næsten-affine koder $C_1, C_2 \subseteq F^S$ siges at være *ækvivalente*, hvis der findes en permutation σ på S samt permutationer π_i for $i \in S$ på F, så bijektionen

$$\begin{aligned} F^S &\longrightarrow F^S \\ (c_i)_{i\in S} &\longmapsto (\pi_i(c_{\sigma(i)}))_{i\in S} \end{aligned}$$

afbilder C_1 på C_2.

Lad $C \subseteq F^S$ være en næsten-affin kode og lad 2^S være potensmængden bestående af samtlige delmængder af S. Da er funktionen

$$\begin{aligned} r : 2^S &\longrightarrow \mathbb{N} \\ X \subseteq S &\longmapsto r(X) = \log_q |C_X| \end{aligned}$$

faktisk rangfunktionen for en matroide $\mathcal{M}(C)$ over S, dvs. den opfylder kravene fra definition 1.1.4 på side 9.

De uafhængige mængder i $\mathcal{M}(C)$ er alle delmængder $X \subseteq S$, så

$$r(X) = |X|, \text{ dvs. så } C_X = F^X.$$

For en cykel C i $\mathcal{M}(C)$ gælder det, at

$$r(C) = |C| - 1 = r(C \setminus \{x\}) \text{ for alle } x \in C.$$

Definition 3.3.6. En matroide $\mathcal{M}$ siges at være *næsten-affint repræsentérbar*, hvis en næsten-affin kode C findes, så $\mathcal{M} = \mathcal{M}(C)$.

Nu skal det præsenteres, hvordan et SSS defineres i forhold til koder. Lad derfor $S = \{1, \ldots, n\}$ være n personer i et SSS. Da kan access-strukturen defineres således:

Definition 3.3.7. En *access-struktur* over S er en monoton delmængde $\Gamma \subseteq 2^S$. Mængden af minimale elementer i Γ kaldes Γ^-.En access-struktur siges at være sammenhængende, hvis

$$\bigcup_{A \in \Gamma^-} A = S.$$

I kode-termer defineres et ideelt SSS da som følger:

Definition 3.3.8. Lad $A' = \{0\} \cup A$ for $A \subseteq S$. Et ideelt SSS for access-strukturen Γ med dealeren 0 er en delmængde (kode) $C \subseteq F^{S'}$, så

1. $C_{\{i\}} = F$ for alle $i \in S' = \{0\} \cup S$,
2. $|C_{A'}| = |C_A|$ for alle $A \in \Gamma$,
3. $|C_{A'}| = q|C_A|$ for alle $A \in 2^S \setminus \Gamma$.

Ækvivalensen mellem ovenstående definition og så Brickell-Davenport modellen skal bevises, så det er klart, at de resultater, der opnås ved hjælp af koder stadig omhandler ideel secret sharing, som de normalt defineres. [Simonis, Ashikhmin] springer over dette og definerer uden videre et ideelt SSS som ovenfor, men her nedenfor beviser jeg ækvivalensen for fuldstændighedens skyld. Bemærk her, at $|C_A|$ for en $A \subseteq S$ præcis svarer til størrelsen $|S(A)|$ for $A \subseteq \mathcal{P}$, som kendes fra BD-schemes. Det er jo antallet af forskellige projektioner af matricens rækker ned på koordinaterne fra A.

Bevis for ækvivalens mellem definition 3.3.8 og Brickell-Davenport. Det skal først vises, at et ideelt SSS for Γ opfylder definition 3.3.8. Idet der i et ideelt SSS gælder $\mathcal{S} = \mathcal{K}$, er pkt. 1 klart opfyldt. Kravet udtrykker blot, at alle personer i schemet (eller alle koordinatpositioner i koden) antager værdier fra den samme mængde. For alle $A \in \Gamma$ gælder der iflg. definition 2.4.6 på side 35, at $|S(A)| = |S(A \cup \{0\})| = |S(A')|$, dvs. $|C_A| = \left|C_{A\cup\{0\}}\right| = |C_{A'}|$, og dermed er pkt. 2 vist. Lad nu $A \notin \Gamma$. Iflg. lemma 3.1.6 på side 46 er $|S(A \cup \{0\})| = q|S(A)|$, og dette giver umiddelbart $|C_{A'}| = \left|C_{A\cup\{0\}}\right| = q|C_A|$.

Det skal nu vises, at kode-definitionen 3.3.8 giver et BD-scheme. Da det iflg. pkt. 1 er klart, at $\mathcal{S} = \mathcal{K}$, skal der blot vises perfekthed. Lad derfor $A \subseteq S$ og antag $A \to 0$. Det skal så vises, at $A \rightrightarrows 0$. Antag derfor $A \not\rightrightarrows 0$, dvs. $A \notin \Gamma$. At der gælder $A \to 0$ er pr. definition 2.4.5 på side 35 det samme som, at $|S(A \cup \{0\})| < |S(A)| \cdot |S(0)|$, dvs.

$$|C_{A'}| = \left|C_{A\cup\{0\}}\right| < |C_A| \cdot \left|C_{\{0\}}\right| = |C_A| \cdot q.$$

Men da $A \notin \Gamma$, må der iflg. pkt. 3 gælde $|C_{A'}| = q|C_A|$, hvilket i ligningen ovenfor giver

$$q|C_A| < |C_A| \cdot q.$$

Dette er dog en modstrid, og der må derfor gælde $A \rightrightarrows 0$. □

Pr. definition 3.3.8 er ethvert ideelt SSS en kode, og ved brug af proposition 3.1.10 på side 49 fås det, at der for enhver delmængde $A \subseteq S$ gælder $|S(A)| = |C_A| = q^n$ for et $n \in \mathbb{N}$. Dette giver følgende proposition:

Proposition 3.3.9. *Et ideelt SSS med $|\mathcal{S}| = q$ og $|\mathcal{P} \cup \{p_0\}| = n+1$ for en sammenhængende access-struktur er en næsten-affin kode af længde $n+1$ over en mængde F med $|F| = q$.*

Betragt nu et ideelt SSS over Γ og lad C være den tilsvarende næsten-affine kode og $\mathcal{M}(C)$ være den tilhørende matroide, som er repræsentérbar over C. Nu skal strukturen af access-strukturens basis Γ^- findes. $A \in \Gamma^-$ giver ifølge lemma 3.1.7 på side 46:

$$\begin{aligned} &|C_A| = S(A) = q^{|A|} \\ &\Downarrow \\ &r(A) = \log_q |C_A| = |A|. \end{aligned}$$

Af definition 3.3.8, pkt. 2 følger, at

$$\begin{aligned} &\left|C_{A\cup\{0\}}\right| = |C_{A'}| = |C_A| \\ &\Downarrow \\ &r(A') = r(A) = |A| = |A'| - 1, \end{aligned}$$

og på grund af ombytningsegenskaben er $r(A') = r(A\backslash\{a\})$ for alle $a \in A'$. Pr. definition er A' altså en cykel i $\mathcal{M}(C)$, så Γ^- er

$$\Gamma^- \subseteq \{A \subseteq S \mid A' \text{ cykel i } \mathcal{M}(C)\}.$$

Betragt nu omvendt en næsten-affin kode $C \subseteq F^{S'}$, hvor matroiden $\mathcal{M}(C)$ er uden løkker. Lad $X \in \{A \subseteq S \mid A' \text{ cykel i } \mathcal{M}(C)\}$. Da $X' = X \cup \{0\}$ er en cykel i $\mathcal{M}(C)$, er

$$r(X') = r(X) \quad \text{dvs.} \quad |C_{X'}| = |C_X|,$$

hvilket pr. definition 3.3.8, pkt. 2 betyder, at $X \in \Gamma$. Da X' er minimal i forhold til at være en cykel, er X også et minimalt element i Γ, så $X \in \Gamma^-$. Da er så

$$\Gamma^- \supseteq \{A \subseteq S \mid A' \text{ cykel i } \mathcal{M}(C)\}.$$

Så et ideelt SSS for access-strukturen $\Gamma(C)$ er defineret ved basen

$$\Gamma^-(C) = \{A \subseteq S \mid A' \text{ cykel i } \mathcal{M}(C)\}.$$

Dvs. nu er faktisk udledt følgende sætning, der karakteriserer ideelle SSS som næsten-affine koder:

Sætning 3.3.10. *$\Gamma(C)$ er access-strukturen for et ideelt SSS, hvis og kun hvis $C \subseteq F^{S'}$ er en næsten-affin kode, hvor $\mathcal{M}(C)$ er uden løkker, og*

$$\Gamma^-(C) = \{A \subseteq S \mid A' \textit{ cykel i } \mathcal{M}(C)\}.$$

3.3.3 Modeksemplet

Det skal nu på baggrund af det foregående afsnits introduktion til næsten-affine koder vises, hvordan [Simonis, Ashikhmin] giver et modeksempel til [Brickell, Davenport]'s fejlagtige sætning. Betragt derfor følgende right nearfield, som kaldes $N(9)$. Det har elementerne $N(9) = \{0, 1, 2, a, b, c, d, e, f\}$ og følgende additions- og multiplikationstabel:

+	0	1	2	a	b	c	d	e	f
0	0	1	2	a	b	c	d	e	f
1	1	2	0	b	c	a	e	f	d
2	2	0	1	c	a	b	f	d	e
a	a	b	c	d	e	f	0	1	2
b	b	c	a	e	f	d	1	2	0
c	c	a	b	f	d	e	2	0	1
d	d	e	f	0	1	2	a	b	c
e	e	f	d	1	2	0	b	c	a
f	f	d	e	2	0	1	c	a	b

×	0	1	2	a	b	c	d	e	f
0	0	0	0	0	0	0	0	0	0
1	0	1	2	a	b	c	d	e	f
2	0	2	1	d	f	e	a	c	b
a	0	a	d	2	e	b	1	f	c
b	0	b	f	c	2	d	e	a	1
c	0	c	e	f	a	2	b	1	d
d	0	d	a	1	c	f	2	b	e
e	0	e	c	b	d	1	f	2	a
f	0	f	b	e	1	a	c	d	2

Brickell-Davenport påstår altså, at enhver $k \times n$-matrix M over et right nearfield R giver anledning til en næsten-affin kode $C = \{xM \mid x \in R^k\}$, men matricen

$$M = \begin{bmatrix} 1 & 1 & b \\ 2 & 0 & c \\ 0 & 2 & d \end{bmatrix}$$

over right nearfield'et $N(9)$ giver ifølge [Simonis, Ashikhmin] ved brug af Maple en kode af længde $q^{k-r(X)} = 3^5 = 243$, hvilket ikke er en potens af 9. Denne kode kan derfor ikke være næsten-affin.

3.3.4 En tilstrækkelig betingelse

Hvad der præcis skal kræves af en matroide, er som tidligere nævnt uvist, så jeg vil i stedet i det følgende gøre rede for nogle tilstrækkelige betingelser. Jeg vil minde om, at en access-struktur Γ siges at være m-ideel, hvis der findes et ideelt SSS, som realiserer Γ med $|\mathcal{K}| = |\mathcal{S}| = m$.

Som nævnt er har [Brickell, Davenport] næsten givet en tilstrækkelig betingelse, idet deres bevis holder for matroider, som er repræsentérbare over legemer. En tilstrækkelig betingelse for, at en matroide fastlægger en m-ideel access-struktur er derfor følgende:

Sætning 3.3.11 (Tilstrækkelig betingelse). *En sammenhængende matroide $\mathcal{T}$ er den associerede matroide til et sammenhængende m-ideelt SSS, hvis $\mathcal{T}$ er repræsentérbar over et legeme af orden m.*

Inden jeg går til beviset, skal vi lige se et lille lemma:

Lemma 3.3.12. *Lad R være et endeligt legeme. Hvis $\alpha, \beta, \delta \in R$ og $\alpha \neq \beta$, så findes et entydigt $x \in R$, så $x\alpha - x\beta = \delta$.*

Bevis. Eksistens: Sæt $x = \delta(\alpha - \beta)^{-1}$. Entydighed: Antag nu at der findes et $y \in R$ med $y \neq x$, så $x\alpha - x\beta = y\alpha - y\beta$. Så er $(x-y)\alpha = (x-y)\beta = \gamma$, og α og β kan ikke begge være 0, da $\alpha \neq \beta$. Da $x \neq y$, er $\gamma \neq 0$, og da er $\alpha = \beta$, hvilket er en modstrid. □

Jeg kan nu gå til beviset for sætning 3.3.11 ovenfor. Beviset er som før antydet præcis [Brickell, Davenport]'s bevis blot omhandlende legemer i stedet for nearfields.

Bevis for sætning 3.3.11. Lad $\mathcal{M}$ være en matroide, som er repræsentérbar over det endelige legeme R med $|R| = m$, og lad rangen af $\mathcal{M}$ være k. Lad desuden $\phi : V \to R^k$ være en afhængighedsbevarende injektion ind i vektorrummet R^k.

Betragt schemet (matricen) M, hvor $\mathcal{P} \cup \{p_0\} = V$, $p_0 = v_0$, $\mathcal{S} = R$, og hvor mængden af rækker i M er R^k. Indgangene i M konstrueres således: For alle $r \in R^k$ og $v \in V$ defineres ud fra prikproduktet "$\cdot$" i R^k matrixelementet $M(r, v) = r \cdot \phi(v)$.

Perfekthed: Lad $A \subseteq V$ med $A \not\twoheadrightarrow p_0$. Så findes to rækker $r_1, r_2 \in R^k$, så

$$M(r_1, A) = M(r_2, A)$$
$$M(r_1, p_0) \neq M(r_2, p_0)$$

eller sagt på en anden måde:

$$r_1 \cdot \phi(a) = r_2 \cdot \phi(a)\ \forall a \in A$$
$$r_1 \cdot \phi(v_0) \neq r_2 \cdot \phi(v_0).$$

Lad $r \in R^k$, $a \in A$ og $x \in R$. Da $r_1 \cdot \phi(a) = r_2 \cdot \phi(a)$, er

$$r \cdot \phi(a) = r \cdot \phi(a) + x(r_1 \cdot \phi(a) - r_2 \cdot \phi(a)) = (r + xr_1 - xr_2) \cdot \phi(a). \tag{3.4}$$

Bemærk: Her i ligning (3.4) blev faktisk brugt venstre-distributet, fordi det bl.a. antages, at

$$(xr_2) \cdot \phi(a) = x(r_2 \cdot \phi(a)).$$

Lad nu $\beta \in R$. Da findes iflg. lemma 3.3.12 et $x \in R$, så

$$xr_1 \cdot \phi(v_0) - xr_2 \cdot \phi(v_0) = \beta - r \cdot \phi(v_0)$$
$$\Downarrow$$
$$(r + xr_1 - xr_2) \cdot \phi(v_0) = \beta.$$

Så er altså $r' = (r + xr_1 - xr_2)$ en række i M, hvor der gælder

$$M(r', A) = M(r, A)$$
$$M(r', p_0) = \beta,$$

hvilket vil sige $A \twoheadrightarrow p_0$, og så er schemet perfekt.

Idealitet: Lad $v \in V$ og $\phi(v) = (v_1, v_2, \ldots, v_k)$. Da $\mathcal{M}$ er en sammenhængende matroide, er mængden $\{v\}$ uafhængig i $\mathcal{M}$, hvilket betyder, at billedet $\phi(\{v\})$ er uafhængigt i R^k, så $\phi(v) \neq 0 \in R^k$. Dvs. der findes et $v_i \neq 0$ for $1 \leq i \leq k$. Vælg nu et $\alpha \in R$ og definér $r = (\rho_1, \rho_2, \ldots, \rho_i, \ldots, \rho_k)$, hvor $\rho_j = 0$ for alle $j \neq i$, og $\rho_i = \alpha v_i^{-1}$. Så er $M(r, v) = r \cdot \phi(v) = \alpha$, og det er vist, at $|S(v)| = |R|$ for alle $v \in V$.

Det skal nu vises, at $D(M)$ udgør de afhængige delmængder i $\mathcal{M}$. Det gælder pr. definition af $D(M)$, at $A \in D(M)$, hvis og kun hvis der findes et $b \in A$, så $A\backslash\{b\} \rightrightarrows b$, dvs. hvis og kun hvis

$$\exists b \in A\ \forall r_1, r_2 \in R^k : \begin{cases} M(r_1, a) = M(r_2, a) & \forall a \in A\backslash\{b\} \\ \Downarrow & \\ M(r_1, b) = M(r_2, b) & \end{cases}$$

eller ækvivalent hermed:

$$\exists b \in A\ \forall r_1, r_2 \in R^k : \begin{cases} r_1 \cdot \phi(a) = r_2 \cdot \phi(a) & \forall a \in A\backslash\{b\} \\ \Downarrow & \\ r_1 \cdot \phi(b) = r_2 \cdot \phi(b) & \end{cases}$$

$$\Updownarrow$$

$$\exists b \in A\ \forall r_1, r_2 \in R^k : \begin{cases} (r_1 - r_2) \cdot \phi(a) = 0 & \forall a \in A\backslash\{b\} \\ \Downarrow & \\ (r_1 - r_2) \cdot \phi(b) = 0. & \end{cases}$$

Dvs. der gælder nu

$$\exists b \in A\ \forall u \in R^k : \begin{cases} u \cdot \phi(a) = 0 & \forall a \in A\backslash\{b\} \\ \Downarrow & \\ u \cdot \phi(b) = 0. & \end{cases}$$

Dette betyder, at $\phi(A)$ er lineært afhængig i R^k, hvilket iflg. definition 1.1.13 også betyder, at A er afhængig i $\mathcal{M}$.

Nu mangler det blot at vise, at schemet M også er sammenhængende. Lad ϕ være den afhængighedsbevarende afbildning fra før. At matroiden $\mathcal{M}$ er sammenhængende betyder, at ethvert par af punkter i V er indeholdt i en cykel. Dette gælder jo specielt også, når det ene punkt er det specielle punkt v_0. Lad derfor punkterne $v_0, v \in V$ svarende til personerne p_0 hhv. $p \in \mathcal{P}$ være indeholdt i cyklen $C \in C(\mathcal{M})$. Da er C afhængig i $\mathcal{M}$ og minimal med den egenskab, og derfor er p_0 og p indeholdt i en afhængige mængde $A \in D(M)$, som iøvrigt også er minimal med denne egenskab. Der gælder altså, at $p_0 \in A$, og der eksisterer et $b \in A$, så

$$\begin{aligned} & A\backslash\{b\} \rightrightarrows b \\ & \Downarrow \\ & |S(A)| = |S(A\backslash\{b\})|. \end{aligned} \tag{3.5}$$

På grund af minimaliteten af A og perfektheden af schemet er

$$\begin{aligned} & A\backslash(\{p_0\}\cup\{b\}) \twoheadrightarrow b \\ & \Downarrow \\ & |S(A\backslash\{p_0\})| = |S(A\backslash(\{p_0\}\cup\{b\}))|\cdot|S(b)|, \end{aligned} \tag{3.6}$$

og desuden

$$\begin{aligned} & A\backslash(\{p_0\}\cup\{b\}) \twoheadrightarrow p_0 \\ & \Downarrow \\ & |S(A\backslash\{b\})| = |S(A\backslash(\{p_0\}\cup\{b\}))|\cdot|S(p_0)|. \end{aligned} \tag{3.7}$$

Da schemet er ideelt, er $|S(b)| = |S(p_0)|$, og ligningerne (3.6) og (3.7) kan nu kombineres til

$$|S(A\backslash\{b\})| = |S(A\backslash\{p_0\})|,$$

og ligning (3.5) kan derfor skrives som

$$|S(A)| = |S(A\backslash\{p_0\})|.$$

Dette er det samme som $A \rightrightarrows p_0$, og da A er minimal med denne egenskab, er $A \in \Gamma^-$, og p er indeholdt i en mængde fra Γ^-. M er altså sammenhængende. □

Denne sætning giver som sagt kun en tilstrækkelig betingelse, og det vides med sikkerhed, at den desværre ikke også er nødvendig. I [Simonis, Ashikhmin], Example 2 & Example 4, vises det nemlig, at den såkaldte Non-Pappus-matroide er næsten-affint repræsentérbar. Den er nemlig matroiden hørende til den næsten-affine kode af længde 9 defineret som rækkerummet i følgende matrix over GF(3) × GF(3):

$$\begin{bmatrix} 10 & 10 & 00 & 10 & 00 & 10 & 10 & 10 & 00 \\ 01 & 01 & 00 & 01 & 00 & 01 & 01 & 01 & 00 \\ 00 & 00 & 00 & 10 & 10 & 21 & 01 & 10 & 10 \\ 00 & 00 & 00 & 02 & 01 & 20 & 12 & 02 & 01 \\ 00 & 10 & 10 & 01 & 00 & 01 & 00 & 11 & 10 \\ 00 & 01 & 01 & 21 & 00 & 21 & 00 & 10 & 01 \end{bmatrix}.$$

Men ifølge [Welsh] er Non-Pappus-matroiden ikke repræsentérbar over noget legeme. Der findes altså secret sharing-matroider, som ikke er repræsentérbare over noget legeme, og den tilstrækkelige betingelse kan derfor ikke også være nødvendig.

Det er i sætning 3.3.10 på side 58 vist, at secret sharing-matroiderne præcis er de matroider, som er næsten-affint repræsentérbare, så for at bestemme hvilke matroider, der er secret sharing, skal man åbenbart blot finde ud af, hvilke der er næsten-affint repræsentérbare. Desværre er det stadig et åbent problem at fastlægge matroiderne med denne egenskab.

Der kan dog stadig godt gøres noget for at kaste lys over secret sharing-matroiderne. For at finde eksempler på matroider, som er secret sharing-matroider, kan man jo i hvert

fald bruge den tilstrækkelige betingelse og søge blandt dem, som er repræsentérbare over et legeme. Specielle eksempler på matroider, som er repræsentérbare over et legeme er dem, som er repræsentérbare over *alle* legemer.

Der findes som nævnt i kapitel 1 en bestemt "pæn" klasse af matroider blandt dem, som har den egenskab, at de er repræsentérbare over alle legemer. Det er de såkaldt *grafiske* matroider [Welsh]. Disse er "pæne", fordi de fremkommer i forbindelse med grafer, som også kendes fra kombinatorikken, og grafer appellerer til en form for visuel forståelse, som er meget håndgribelig.

3.3.5 Grafisk access-struktur

Man kan konstruere access-strukturen til et secret sharing scheme M med grafisk associeret matroide $\mathcal{T}(M)$ ud fra en graf G (jeg vil derfor også kalde en sådan access-struktur for grafisk[2]). Den associerede matroide bliver da $\mathcal{T}(M) = \mathcal{M}(G)$ knyttet til grafen G. Dette gøres på følgende måde. Lad en graf $G = (V, E)$ være givet, hvor $V = \{0, 1, \ldots n\}$ og $E \subseteq V \times V$. Lad nu kanten $e_0 = (0, 1) \in E$ være den specielle kant, som skal svare til dealeren D. Da kan schemets access-struktur $\Gamma(G)$ konstrueres ved at tage familien af alle supersets af mængderne $C \setminus \{e_0\}$, hvor $C \subseteq E$ er en cykel, som indeholder e_0. Dvs.

$$\Gamma(G) = \mathrm{cl}\{C \setminus \{e_0\} \mid C \subseteq E \text{ en cykel, som indeholder } e_0\}.$$

Man har dermed ud fra grafen G konstrueret en access-struktur med associeret matroide $\mathcal{T}(\Gamma) = \mathcal{M}(G)$.

Det vises nu, hvordan man kan lave et perfekt secret sharing scheme på denne access-struktur ved at betragte eksemplet i den følgende paragraf.

3.3.6 Eksempel: Konstruktion af scheme på grafisk access-struktur

Lad $G = (V, E)$ være en graf. Lad $s \in \mathcal{K}$ være hemmeligheden, dealeren ønsker at dele, og lad $\mathcal{K} = \mathbb{Z}_m$. Lad $r = (r_1, r_2, \ldots, r_{|V|-1})$ være en af dealeren tilfældigt valgt vektor med $r_i \in \mathbb{Z}_m$, og lad $(i, j) \in E$ være en kant med $i < j$. Da udregnes den hemmelige share til kanten (i, j) til at være

$$\sigma(i, j) = \begin{cases} r_i - r_j \mod m, & i \neq 0 \\ r_1 + s - r_j \mod , m & i = 0. \end{cases}$$

Det ses, at dealeren (kanten $(0, 1)$) får hemmeligheden s som share. Access-strukturen i schemet består således af kanterne i alle de delgrafer af G, som indeholder en sti fra 0 til 1. En autoriseret delmængde $\{(0, v_1), (v_1, v_2), (v_2, v_3), \ldots, (v_{k-1}, v_k), (1, v_k)\}$ vil kunne rekonstruere hemmeligheden ved at trække deres shares fra hinanden (aritmetik i $\mathbb{Z}_m$), som det fremgår i det følgende.

Her er hvilke shares, der gives til hvilke personer/kanter:

[2]Bemærk: I nogen engelsksproget litteratur bruges navnet "graph access structure" om en access-struktur, hvor basis Γ^- består af alle delmængder af kardinalitet 2. Disse begreber må ikke forveksles.

Kant	Share
$(0, v_1)$	$r_1 + s - r_{v_1}$
(v_1, v_2)	$r_{v_1} - r_{v_2}$
(v_2, v_3)	$r_{v_2} - r_{v_3}$
$\vdots$	$\vdots$
(v_{k-1}, v_k)	$r_{v_{k-1}} - r_{v_k}$
$(1, v_k)$	$r_1 - r_{v_k}$

Hvis man således tager $(0, v_1)$'s share og derfra subtraherer de resterende shares, får man præcis hemmeligheden s tilbage:

$$(r_1 + s - r_{v_1}) - (r_{v_1} - r_{v_2}) - (r_{v_2} - r_{v_3}) - \cdots - (r_{v_{k-1}} - r_{v_k}) - (r_1 - r_{v_k}) = s \mod m.$$

Bemærk: I det ovenstående antages det, at $v_i < v_{i+1}$, idet dette altid kan opnås ved en passende om-nummerering af hjørnerne i grafen. Bemærk også, at ovenstående autoriserede delmængde faktisk var en sti fra hjørne 0 til hjørne 1. Hvis man tager et superset af denne delmængde, fås naturligvis også en autoriseret mængde, men man behøver så kun at tage de shares, som hører til stien fra 0 til 1.

Hvis man nu betragter en delmængde, som ikke indeholder nogen sti fra 0 til 1, så er der to muligheder:

1. Ingen kant har hjørne i 0
2. Ingen sti fra 0 ender i 1.

Hvis ingen kant har hjørne i 0, er alle shares på formen $r_i - r_j$, og så er der ingen share, der afhænger af s, da alle r_i'erne er uafhængige af hinanden og af s. Delmængden uden hjørne i 0 har derfor ingen information om s.

Hvis man betragter en sti, som starter i 0, men som ikke ender i 1, kan man aldrig være sikker på at kunne isolere andet end $s + r_j \mod m$, hvor værdien af r_j er ukendt. I dette tilfælde har man heller ingen information om s, idet

$$\psi_{r_j} : s \longmapsto s + r_j$$

er en bijektion på $\mathbb{Z}_m$. Hver værdi af s svarer derfor til præcis én værdi af $s + r_j$ og vice versa. Så hvis sandsynlighedsfordelingerne, hvormed s og r_j er valgt, er uniforme på $\mathbb{Z}_m$, så bliver også uniform på $\mathbb{Z}_m$.

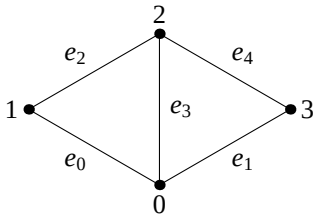
Dette scheme er dermed perfekt, og da $|\mathcal{K}| = |\mathcal{S}| = \{0, 1, \ldots, m\}$, er det ideelt for alle $m \geq 2$.

Betragt nu schemet på en konkret graf. [Beimel, Chor] brugte følgende eksempel, som jeg synes, er meget anvendeligt. Lad os sige, at man vil lave en grafisk access-struktur på grafen G_0 i figur 3.1 på næste side, hvor kanten $e_0 = (0, 1)$ skal svare til dealeren, og de øvrige personer repræsenteres af kanterne e_1, e_2, e_3 og e_4.

Det ses, at cyklerne i G_0 udgøres af følgende mængder af kanter:

$$\{e_0, e_2, e_3\}, \{e_0, e_1, e_2, e_4\}, \{e_1, e_3, e_4\}.$$

Figur 3.1. Graf-eksemplet G_0



Ifølge proposition 1.3.1 på side 15 så udgør disse grafcykler netop cyklerne i den grafiske matroide $\mathcal{M}(G_0)$. De minimale mængder (basen) i den ønskede access-struktur er da kanterne i de simple stier fra 0 til 1, og access-strukturen består dermed af alle supersets af mængderne

$$\{e_3, e_2\}, \{e_1, e_4, e_2\}.$$

3.3.7 Cografisk access-struktur

For fuldstændighedens skyld skal det nævnes, at der i stil med de grafiske access-strukturer også kan defineres de *cografiske access-strukturer*. En cografisk access-struktur Γ er en access-struktur, som har en cografisk associeret matroide $\mathcal{M}(\Gamma)$. En sådan kan konstrueres ud fra en graf i stil med den grafiske access-struktur. Ved at tage supersets af cyklerne i en matroide knyttet til grafen.

Lad $G = (V, E)$ være en graf med $V = \{0, 1, \ldots, n\}$ og $E = V \times V$ og lad kanten $e_0 = (0, 1)$ være den specielle kant, som skal svare til dealeren i schemet. Access-strukturen $\Gamma(G)$ konstrueres da ved at tage familien af supersets af mængderne $C^* \backslash \{e_0\}$, hvor $C^* \subseteq E$ er en cocykel, som indeholder e_0. Dvs.

$$\Gamma(G) = \text{cl}\{C^* \backslash \{e_0\} \mid C^* \subseteq E \text{ en cocykel, som indeholder } e_0\}.$$

Hvis man igen betragter graf-eksemplet G_0 fra figur 3.1, så ses det, at snittene i G_0 udgøres af mængderne

$$\{e_0, e_1, e_3\}, \{e_0, e_2\}, \{e_0, e_3, e_4\}, \{e_1, e_2, e_3\}, \{e_1, e_4\}, \{e_2, e_3, e_4\}.$$

Basen til access-strukturen udgøres dermed af mængderne

$$\{e_1, e_3\}, \{e_2\}, \{e_3, e_4\},$$

og access-strukturen fremkommer ved at tage supersets heraf.

Det er dog ifølge [Beimel, Chor] ikke helt så let at konstruere konkrete ideelle schemes på cografiske access-strukturer, som det er at gøre det på de grafiske, hvorfor jeg ikke vil gå dybere i dette.

3.4 Universelt ideelle access-strukturer

Fra [Benaloh, Leichter] vides det, at enhver monoton access-struktur kan realiseres som et *perfekt* SSS. Der findes dog access-strukturer, som ikke kan realiseres af noget *ideelt* SSS. Problemet i forhold til karakterisering består i, at der findes access-strukturer, som *ikke* er m-ideelle for noget m, men som har associerede matroider.

I stedet kan man prøve at karakterisere nogle access-strukturer, som opfylder krav, der er lidt strengere end blot det, at de skal være ideelle, nemlig de såkaldte *universelt* ideelle access-strukturer, som jeg vil behandle i det følgende. Ved brug af den tilstrækkelige betingelse fra sætning 3.3.11 på side 59 fås f.eks. den pæne egenskab, at hvis en access-struktur associerer til en grafisk matroide, så er denne access-struktur m-ideel for alle $m \geq 2$, fordi de grafiske matroider er repræsentérbare over legemer af vilkårlig orden[3]. De grafiske access-strukturer er altså eksempler på ekstra pæne ideelle access-strukturer, fordi de er m-ideelle for alle $m \geq 2$. Der kan defineres følgende:

Definition 3.4.1. En access-struktur, som er m-ideel for alle $m \geq 2$, siges at være *universelt ideel*.

Som eksempler på universelt ideelle access-strukturer kan ud over de grafiske- også nævnes de cografiske access-strukturer. Disse er også universelt ideelle, fordi deres respektive associerede matroider er repræsentérbare over alle legemer (se [Welsh]).

Grunden til, at jeg nu vil studere denne specielle type af ideelle access-strukturer er, at de universelt ideelle i modsætning til de almindelige ideelle access-strukturer faktisk kan karakteriseres fuldstændigt. Betingelsen er iøvrigt overraskende let at formulere. Der gælder nemlig følgende stærke sætning ifølge [Beimel, Chor], hvis bevis senere skal gennemgås:

Sætning 3.4.2 (Karakterisering af universelt ideelle access-strukturer). *En access-struktur Γ er universelt ideel, hvis og kun hvis Γ er* både *2-ideel* og *3-ideel.*

Fremgangsmåden er først at karakterisere alle 2-ideelle og siden alle 3-ideelle access-strukturer fuldstændigt. Derefter skal dette resultat kombineres til en karakterisering af alle q-ideelle access-strukturer, hvor q er en primtalspotens. Den sidste del af karakteriseringen af de universelt ideelle access-strukturer er en udvidelse af resultatet for de q-ideelle strukturer. Men for at klare beviset, skal der lidt forudsætninger på plads. Sektion 3.4.1 gennemgår lidt nødvendig teori.

3.4.1 Lineære schemes og sensitive funktioner

I resten af afsnit 3.4 vil jeg gennemgå, hvordan [Beimel, Chor] beviser ovenstående sætning. Først skal der dog lige defineres et par ting og vise nogle små lemmaer angående linære schemes og de associerede matroiders repræsentérbarhed. Desuden skal der benyttes egenskaber om såkaldte komponent-sensitive funktioner.

[3] Se f.eks. [Welsh] eller en anden lærebog om matroider.

Definition 3.4.3. Lad M være et q-ideelt SSS, hvor q er en primtalspotens. M siges at være et *lineært secret sharing scheme*, hvis der for alle $A \subseteq \mathcal{P}$ og alle $b \notin A$ med $A \rightrightarrows b$ findes konstanter $\{\alpha_j\}_{j\in A}$ og σ i GF(q), så der for hver hemmelighed $s_0 \in$ GF(q) gælder, at alle mulige shares $s_b(s_0)$ til b er på formen

$$s_b(s_0) = \sigma + \sum_{j\in A} \alpha_j s_j,$$

hvor al aritmetik foregår i legemet GF(q).

Et oplagt eksempel på et lineært secret sharing scheme er Shamirs (t, w)-threshold scheme beskrevet i sektion 2.2.4.

Det vides fra den tilstrækkelige betingelse i sætning 3.3.11, at en matroide, som er repræsentérbar over et legeme af orden m, er den associerede matroide til et m-ideelt SSS, men det følgende lemma giver den modsatte vej for lineære schemes, hvis associerede matroider er repræsentérbare over legemer, som er på formen GF(q), hvor q er en primtalspotens.

Lemma 3.4.4. *Hvis* Γ *er en access-struktur i et lineært* q*-ideelt SSS, så har* Γ *en associeret matroide, som er repræsentérbar over* GF(q)*.*

Bevis. Ifølge hovedsætning 1 på side 45 findes der en associeret matroide $\mathcal{T} = (V, \mathcal{I})$ til Γ. Det skal nu vises, at denne matroide er repræsentérbar, dvs. der skal konstrueres en afhængighedsbevarende afbildning ϕ fra matroidens punktmængde $V = \{0, 1, \ldots, n\}$ ind i et vektorrum over GF(q).

Lad R være den endelige mængde, hvorfra dealeren vælger sit hemmelige, tilfældige input til konstruktionen af shares, således at hver share til person $p \in \mathcal{P}$ er værdien af en funktion $s_p(s_0, r)$ af hemmeligheden $s_0 \in \mathcal{K}$ og $r \in R$. Person p kan da modtage shares fra mængden $S(p) = \{s_p(s_0, r) \mid s_0 \in \mathcal{K}, r \in R\}$. På mængden af personer $p \in \mathcal{P} = V$ kan nu defineres en afbildning ϕ_1 over i vektorrummet GF$(q)^{q|R|}$:

$$\phi_1 : V \to \text{GF}(q)^{q|R|}$$

ved

$$\phi_1(p) = \Big(s_p(0, r_1), \ldots, s_p(0, r_{|R|}), \ldots, s_p(q-1, r_1), \ldots, s_p(q-1, r_{|R|})\Big),$$

dvs. $\phi_1(p)$ er tuplen i GF$(q)^{q|R|}$ bestående af alle de mulige shares til p for alle mulige hemmeligheder, dvs. alle elementerne i $S(p)$.

Lad for alle $\sigma \in$ GF(q) vektoren $\vec{\sigma} \in$ GF$(q)^{q|R|}$ være $\vec{\sigma} = (\sigma, \sigma, \ldots, \sigma)$. Ifølge hovedsætning 1 på side 45 er mængden $B \subseteq \{0, \ldots, n\}$ afhængig i $\mathcal{T}$, hvis og kun hvis $B \in D(M)$, dvs. hvis og kun hvis der eksisterer et $b \in B$, så $B\backslash\{b\} \rightrightarrows b$. Da schemet er lineært, findes der i så fald konstanter $\{\alpha_j\}_{j\in B\backslash\{b\}}, \sigma$ i GF(q), så b's shares for alle mulige hemmeligheder s og inputs r er på formen

$$s_b(s, r) = \sum_{j\in B\backslash\{b\}} \alpha_j s_j(s, r) - \sigma,$$

hvilket svarer til, at

$$\sum_{j\in B\setminus\{b\}} \alpha_j s_j(s,r) - s_b(s,r) = \sum_{j\in B} \alpha_j s_j(s,r) = \sigma \quad \text{hvor } \alpha_b = -1.$$

Dette er igen ækvivalent med

$$\sum_{j\in B} \alpha_j \phi_1(j) = \vec{\sigma} \quad \text{hvor } \alpha_b = -1.$$

Afbildningen ϕ_1 opfylder da, at en mængde $B \subseteq \{0,\ldots,n\}$ er afhængig i $\mathcal{T}$, hvis og kun hvis der findes konstanter $\{\alpha_j\}_{j\in B}, \sigma$ i GF(q), med mindst en α_j forskellig fra 0, så

$$\sum_{j\in B} \alpha_j \phi_1(j) = \vec{\sigma}.$$

Betragt nu det lineære underrum Y af $\mathrm{GF}(q)^{q|R|}$ givet ved

$$Y = \mathrm{sp}\left\{\vec{1}, \phi_1(0), \phi_1(1), \ldots, \phi_1(n)\right\},$$

og lad t være sådan, så $\dim(Y) = t+1$. Lad $\phi_2 : Y \to \mathrm{GF}(q)^t$ være en lineær afbildning med $\ker(\phi_2) = \mathrm{sp}\left\{\vec{1}\right\}$, dvs. $\phi_2(v) = \vec{0}$, hvis og kun hvis $v = \vec{\sigma}$ for et $\sigma \in \mathrm{GF}(q)$. Hvis man vælger en ortogonal basis $\left\{\vec{1}, \vec{v}_1, \ldots, \vec{v}_t\right\}$ for Y, så er afbildningen ϕ_2 faktisk bare projektionen af Y ned på underrummet $\mathrm{sp}\{\vec{v}_1,\ldots,\vec{v}_t\} \subseteq Y$. Denne projektion har så kerne $\mathrm{sp}\left\{\vec{1}\right\}$, fordi $\mathrm{sp}\left\{\vec{1}\right\}$ er det ortogonale komplement $\mathrm{sp}\{\vec{v}_1,\ldots,\vec{v}_t\}^\perp$.

For hver $X \subseteq Y$ er mængden $\phi_2(X) = \{\phi_2(x) \mid x \in X\} \subseteq \mathrm{GF}(q)^t$ lineært afhængig, hvis og kun hvis der findes en ikke-triviel linearkombination af elementer fra X, som ligger i $\mathrm{sp}\left\{\vec{1}\right\}$. Dvs. der findes konstanter $\{\alpha_x\}_{x\in X}$ ikke alle 0, så

$$\sum_{x\in X} \alpha_x x = \vec{\sigma}$$

for et $\sigma \in \mathrm{GF}(q)$.

Afbildningerne ϕ_1 og ϕ_2 har altså den egenskab, at $B \subseteq V$ er afhængig i $\mathcal{T}$, hvis og kun hvis $\phi_2 \circ \phi_1(B)$ er lineært afhængig i $\mathrm{GF}(q)^t$. Dvs. der er konstrueret en afhængighedsbevarende afbildning $\phi = \phi_2 \circ \phi_1 : V \to \mathrm{GF}(q)^t$. □

Definition 3.4.5. En funktion $f : S^t \to S$ siges at være *komponent-sensitiv*, hvis der for alle $1 \le i \le t$ og alle $s_1,\ldots,s_{i-1},s_i,s_i',s_{i+1},\ldots,s_t \in S$ med $s_i' \neq s_i$ gælder

$$f(s_1,\ldots,s_{i-1},s_i,s_{i+1},\ldots,s_t) \neq f(s_1,\ldots,s_{i-1},s_i',s_{i+1},\ldots,s_t).$$

Dvs. en komponent-sensitiv funktion ændrer altid værdi, hvis værdien af en af dens variable ændres.

Lemma 3.4.6. *Lad M være et q-ideelt SSS. Lad $\mathcal{S} = \{0, \ldots, q-1\}$ og $i \in \{0, \ldots, n\}$ og lad $B \subseteq \{0, \ldots, n\}$ være minimal med den egenskab, at $B \rightrightarrows i$ med $i \notin B$. Lad $f : \mathcal{S}^{|B|} \to \mathcal{S}$ være rekonstruktionsfunktionen af den i'te share ud fra B's samlede shares. Så gælder*

1. *Rekonstruktionsfunktionen f er defineret på hele domænet $\mathcal{S}^{|B|}$,*
2. *Rekonstruktionsfunktionen f er komponent-sensitiv.*

Bevis. Antag at $B = \{1, \ldots, t\}$ er minimal med den egenskab, at $B \rightrightarrows i$ med $i \notin B$. Antag desuden, at der findes en vektor af shares $(s_1, \ldots, s_t)$, som f ikke er defineret på. Idet $B \rightrightarrows i$, findes der dog også en vektor af shares, som f *er* defineret på. Der findes derfor et j med $1 \leq j \leq t$, så $f(s_1, \ldots, s_{j-1}, s'_j, s'_{j+1}, \ldots, s'_t)$ er veldefineret – man kan f.eks. altid vælge $j = 1$, hvilket bare giver en af de vektorer, som f i forvejen er defineret på. Lad nu imidlertid j være maksimal med denne egenskab. Lad $P_{s_0}(r)$ være sandsynlighedsfordelingen på hemmelighed s som funktion af input r. Da gælder altså der følgende om sandsynligheden for værdien af j's share:

$$\Pr_{s, P_s(r)}\left(s_j(s,r) = s_j \;\middle|\; \bigwedge_{1 \leq k \leq j-1} s_k(s,r) = s_k \right) = 0,$$

$$\Pr_{s, P_s(r)}\left(s_j(s,r) = s'_j \;\middle|\; \bigwedge_{1 \leq k \leq j-1} s_k(s,r) = s_k \right) > 0,$$

hvor $\wedge$-operatoren er logisk "og".

Der findes altså en værdi $s_j \in S(j)$, som personerne i $B \setminus \{j\}$ givet deres shares kan udelukke for j's share, dvs. $B \setminus \{j\}$ har nogen information om j, hvilket igen betyder, at $B \setminus \{j\} \to j$, som i et ideelt scheme yderligere giver $B \setminus \{j\} \rightrightarrows j$. På grund af transitiviteten af "$\rightrightarrows$" fra proposition 2.4.10 gælder der derfor $B \setminus \{j\} \rightrightarrows i$. Dette er i modstrid med minimaliteten af B. Det er derfor nu vist, at f er defineret over hele $\mathcal{S}^{|B|}$.

Antag nu, at f ikke er komponent-sensitiv, dvs. at der findes et $j \in B$, en share $s_i \in \mathcal{S}$ samt shares $s_1, \ldots, s_{j-1}, s_j, s'_j, s_{j+1}, \ldots, s_t \in S$ med $s'_j \neq s_j$ og

$$f(s_1, \ldots, s_{j-1}, s_j, s_{j+1}, \ldots, s_t) = f(s_1, \ldots, s_{j-1}, s'_j, s_{j+1}, \ldots, s_t) = s_i.$$

Da f er defineret over hele $\mathcal{S}^{|B|}$, findes hemmeligheder $s_0, s'_0 \in \mathcal{S}$ og inputs $r, r' \in R$ med $P_{s_0}(r) > 0$ og $P_{s'_0}(r') > 0$, så

- $s_k(s,r) = s_k(s',r') = s_k$ for alle $k \in B \setminus \{j\}$,
- $s_i(s,r) = s_i(s',r') = s_i$,
- $s_j(s,r) = s_j \neq s'_j = s_j(s',r')$.

De tre ovenstående udsagn siger tilsammen følgende: $B \setminus \{j\}$ fik tildelt share-vektoren $(s_1, \ldots, s_{j-1}, s_{j+1}, \ldots, s_t)$ og kan rekonstruere den samme værdi for i's share, nemlig s_i, men for to forskellige værdier af j's share. Men da der kun er q mulige værdier for j's

share, kan der derfor kun være højst $q-1$ mulige værdier for i's share, dvs. der findes shares $s_i, s_i' \in \mathcal{S}$, så

$$\Pr_{s,P_s(r)}\left(s_i(s,r) = s_i' \;\middle|\; \bigwedge_{k\in B\setminus\{j\}} s_k(s,r) = s_k\right) = 0,$$
$$\Pr_{s,P_s(r)}\left(s_i(s,r) = s_i \;\middle|\; \bigwedge_{k\in B\setminus\{j\}} s_k(s,r) = s_k\right) > 0.$$

Dette er som bekendt det samme som at $B\setminus\{j\}$ udelukker en værdi for i's share, hvilket i et ideelt scheme resulterer i $B\setminus\{j\} \rightrightarrows i$. Dette er igen i modstrid med minimaliteten af B. □

3.4.2 2-ideelle- og 3-ideelle access-strukturer

Inden jeg kan gå til selve beviset for sætning 3.4.2, skal der ses lidt nærmere på de 2-ideelle- og 3-ideelle access-strukturer. Faktisk så skal de her karakteriseres fuldstændigt ved at fastlægge deres associerede matroider.

Lemma 3.4.7. *Lad $f : \mathrm{GF}(2)^t \to \mathrm{GF}(2)$ være en komponent-sensitiv funktion. Så kan f udtrykkes som en lineær funktion med ikke-nul-koefficienter over* GF(2)*:*

$$f(x_1,\ldots,x_t) = \sigma + \sum_{i=1}^{t} x_i. \tag{3.8}$$

Bevis. Da $\mathrm{GF}(2) = \{0,1\}$, kan det WLOG antages, at $f(0,\ldots,0) = 0$. Lad et element $(x_1,\ldots,x_t) \in \mathrm{GF}(2)^t$ være givet med præcis k koordinater forskellige fra 0 (Hamming weight k). Konstruér nu en følge af længde $k+1$ af elementer fra $\mathrm{GF}(2)^t$, som starter i $(0,\ldots,0)$, ender i $(x_1,\ldots,x_t)$, og hvor hvert par af to på hinanden følgende elementer har Hamming distance 1, dvs. har præcis 1 koordinat forskellig. Da f er komponent-sensitiv, antager f hele tiden skiftevis værdierne 0 og 1 eftersom f anvendes på elementerne i følgen. Da desuden f anvendt på det 0'te element $(0,\ldots,0)$ gav værdien 0, gælder der om det l'te ($0 \le l \le k$) element i følgen, at f antager værdien $l \mod 2$. Derfor er specielt værdien af f på det k'te element

$$f(x_1,\ldots,x_t) = k \mod 2,$$

hvilket præcis svarer til opskrivningen i ligning (3.8) med $\sigma = 0$. Husk, vi valgte arbitrært $\sigma = 0$, fordi vi valgte, at $f(0,\ldots,0) = 0$. □

Korollar 3.4.8. *En access-struktur Γ er 2-ideel, hvis og kun hvis den associerede matroide $\mathcal{T}(\Gamma)$ er repræsentérbar over* GF(2).

Bevis. Lad M være et 2-ideelt SSS på access-strukturen Γ. Ifølge lemma 3.4.6 er rekonstruktionsfunktionen for hver afhængig mængde komponent-sensitiv. Ifølge lemma 3.4.7 er alle rekonstruktionsfunktioner derfor lineære over GF(2), og pr. definition 3.4.3 er M et

lineært scheme. Lemma 3.4.4 siger nu, at den associerede matroide $\mathcal{T}(\Gamma)$ er repræsentérbar over GF(2).

Den anden vej følger klart af den tilstrækkelige betingelse i sætning 3.3.11 på side 59. □

Hermed er de 2-ideelle access-strukturer karakteriseret, så nu skal det tilsvarende bare gøres for de 3-ideelle.

Lemma 3.4.9. *Lad $f : \mathrm{GF}(3)^t \to \mathrm{GF}(3)$ være en komponent-sensitiv funktion. Så kan f udtrykkes som en lineær funktion med ikke-nul-koefficienter over* GF(3)*:*

$$f(x_1, \ldots, x_t) = \sigma + \sum_{i=1}^{t} \alpha_i x_i, \quad \text{hvor } \alpha_i \neq 0 \text{ for alle } i. \tag{3.9}$$

Bevis. Bemærk først, at enhver funktion $f : \mathrm{GF}(q)^t \to \mathrm{GF}(q)$ kan udtrykkes som et multivariabelt polynomium over GF(q), hvor hvert monomium har grad højst $q-1$, idet $x^q \equiv x$ for alle $x \in \mathrm{GF}(q)$. Der må nemlig være $(q^t)^q = q^{tq}$ forskellige afbildninger $f : \mathrm{GF}(q)^t \to \mathrm{GF}(q)$, da der er q^t punkter i domænet GF(q) og q mulige værdier af f på hvert punkt. Man kan nu tælle antallet af multivariable polynomier over GF(q). Der er q^t led i hvert polynomium, idet der er t variable, som hver kan have grad fra 0 til $q-1$. Da hver koefficient kan have q mulige værdier, giver dette ialt $(q)^{q^t} = q^{tq}$ mulige polynomier. Der er altså lige så mange polynomier over GF(q), som der er funktioner $f : \mathrm{GF}(q)^t \to \mathrm{GF}(q)$, og hver funktion må derfor være et polynomium.

Da $q = 3$, skal det derfor nu vises, at ingen led i polynomiet f har grad 2. Antag at x_1^2 optræder i et monomium i f. Polynomiet f er derfor på formen.

$$x_1^2 \cdot p_1(x_2, \ldots, x_n) + x_1 \cdot p_2(x_2, \ldots, x_n) + p_3(x_2, \ldots, x_n),$$

hvor polynomiet p_1 ikke er 0-polynomiet, og hvor p_2 samt p_3 er polynomier. Så findes der en vektor $(x_2', \ldots, x_n')$, så $p_1(x_2', \ldots, x_n') \neq 0$. Dvs. givet ovennævnte vektor kan f skrives som en funktion af x_1 på formen $f_{(*,x_2',\ldots,x_n')}(x_1) = ax_1^2 + bx_1 + c$, hvor $a \neq 0$. Bemærk, at nu er funktionen $f_{(*,x_2',\ldots,x_n')}(x_1)$ komponent-sensitiv, idet $f(x_1, \ldots, x_n)$ jo er komponent-sensitiv, og en komponent-sensitiv funktion af én variabel er faktisk en permutation af sit domæne. Ethvert polynomium over GF(3) er altså en permutation, men der er kun $3! = 6$ permutationer af elementerne i GF(3), og der er $2 \cdot 3 \cdot 3 = 18$ forskellige polynomier over GF(3) af grad 2. Alle polynomier over GF(3) af grad 2 kan derfor ikke være permutationer, hvilket er en modstrid. Dvs. f indeholder ikke noget led af grad 2.

Antag nu at f indeholder et monomium med mindst 2 variable og betragt et sådant monomium af minimal længde, som indeholder de to variable x_1, x_2, dvs. WLOG er på formen $ax_1x_2x_3 \cdots x_k$. Sæt nu værdierne til alle andre variable i monomiet end netop x_1, x_2 til 1, dvs. sæt $x_j = 1$ for alle $3 \leq j \leq k$ og værdierne af alle andre variable i polynomiet $x_{k+1}, \ldots, x_n$ til 0. Der fås derved WLOG en funktion

$$f_{(*,*,1,\ldots,1,0,\ldots,0)}(x_1, x_2) = ax_1x_2 + bx_1 + cx_2 + d,$$

hvor $a \neq 0$. Denne funktion er også komponent-sensitiv. Den kan dog omskrives til $x_1(ax_2 + b) + cx_2 + d$ og sætte $x_2 = -b/a$, hvilket giver en funktion af x_2 alene, som derfor ikke afhænger af x_1. Funktionen kan derfor ikke være komponent-sensitiv, hvilket er en modstrid.

Det kan derfor konkluderes, at f ikke indeholder monomier af grad større end 1, samt at disse kun indeholder én variabel. f er derfor på formen $\sigma + \sum_{i=1}^{t} \alpha_i x_i$, og $\alpha_i \neq 0$ for alle i, fordi f for at være komponent-sensitiv specielt skal afhænge af alle variable. □

Korollar 3.4.10. *En access-struktur* Γ *er 3-ideel, hvis og kun hvis den associerede matroide* $\mathcal{T}(\Gamma)$ *er repræsentérbar over* GF(3).

Bevis. Beviset er en kopi af beviset for korollar 3.4.8, hvor man i stedet for 2-lineær skriver 3-lineær og i stedet for GF(2) skriver GF(3). Man bruger bare lemma 3.4.9 til at konkludere, at 3-ideelle schemes er lineære. □

Nu er de 2-ideelle- og de 3-ideelle access-strukturer karakteriseret, og jeg skal derfor se nærmere på access-strukturer, som er *både* 2-ideelle *og* 3-ideelle.

3.4.3 Selve beviset

Inden jeg går til beviset for sætning 3.4.2 på side 66, skal jeg dog lige give et lille korollar samt opfriske et resultat fra talteorien.

Korollar 3.4.11. *Lad* Γ *være en access-struktur, som er* både *2-ideel* og *3-ideel. Da er* Γ *q-ideel for alle primtalspotenser q.*

Bevis. Det er vist i korollar 3.4.8 og 3.4.10, at hvis en access-struktur Γ er 2-ideel, så er den associerede matroide $\mathcal{T}(\Gamma)$ repræsentérbar over GF(2), og hvis Γ tillige er 3-ideel, så er $\mathcal{T}$ også repræsentérbar over GF(3). Husk, at den associerede matroide er entydigt bestemt. Ved brug af proposition 1.1.14 på side 12 ses derfor, at $\mathcal{T}(\Gamma)$ må være repræsentérbar over ethvert endeligt legeme. Dette giver så igen ifølge den tilstrækkelige betingelse omvendt, at Γ er q-ideel for enhver primtalspotens q. □

Lemma 3.4.12 (Kinesisk Restklasse-sætning[4]). *Lad* $m_1, \ldots, m_r$ *være parvis indbyrdes primiske heltal og antag, at* $a_1, \ldots, a_r$ *er heltal. Så har systemet af de r kongruenser*

$$x \equiv a_i \mod m_i \quad 1 \leq i \leq r$$

en entydig løsning modulo $M = m_1 m_2 \cdots m_r$*, der er givet som*

$$x = \sum_{i=1}^{r} a_i M_i y_i \mod M,$$

hvor $M_i = M/m_i$ *og* $y_i = M_i^{-1} \mod m_i$ *for* $1 \leq i \leq r$.

[4]Se enhver lærebog om basal algebra eller talteori for bevis af den Kinesiske Restklasse-sætning.

Og så endelig til det vigtigste i denne sektion, beviset for sætning 3.4.2 på side 66:

Bevis for sætning 3.4.2. Det er klart, at den ene vej gælder: Hvis Γ er universelt ideel, så er den selvfølgelig specielt både 2-ideel og 3-ideel.

Lad nu $\mathcal{S}$ være mængden af hemmeligheder med $|\mathcal{S}| = m$, og antag at m har primtalsfaktoriseringen $m = p_1^{i_1} \cdots p_t^{i_t}$. Lad en hemmelighed $s_0 \in \mathcal{S}$ være givet. Da kan man ifølge korollar 3.4.11 dele hemmeligheden s_0 modulo $p_j^{i_j}$ i et $p_j^{i_j}$-ideelt SSS uafhængigt for alle $1 \leq j \leq t$. Enhver delmængde $B \in \Gamma$ kan nu konstruere $s_0 \mod p_j^{i_j}$ med deres shares i det tilhørende $p_j^{i_j}$-ideelle scheme, og de kan derfor konstruere s_0 ud fra kongruenssystemet $\left(s_0 \mod p_j^{i_j}\right)_{1 \leq j \leq t}$ ved hjælp af den Kinesiske Restklasse-sætning. En delmængde $B' \notin \Gamma$ har ingen information om $s_0 \mod p_j^{i_j}$, da alle de $p_j^{i_j}$-ideelle schemes er konstrueret uafhængigt af hinanden. $B' \notin \Gamma$ har derfor heller ingen information om s_0. Access-strukturen Γ er derfor m-ideel. □

Kapitel 4

Dekomposition af secret sharing-matroider

Det skal i dette kapitel udvikles, hvordan alle sammenhængende matroider dekomponerer i et antal uniforme matroider. Dette svarer til, at threshold access-strukturer dybest set kan siges at være byggesten for ideelle access-strukturer. Denne opbygning har selvfølgelig grund i strukturen og dekompositionen af de tilhørende matroider. Desuden præsenteres en metode, som måske kan bane vejen for en fremtidig forbedring af den tilstrækkelige betingelse fra kapitel 3. En del af dette kapitel vil som antydet indeholde en hel del ren matroide-teori, som også kunne have været beskrevet i kapitel 1. Men disse matroide-relaterede resultater er temmelig nye, og det, de skal bruges til, bygger ovenpå mange af de andre resultater fra tidligere kapitler. Disse ting stammer desuden udelukkende fra to artikler, [Ng, Walker] og [Ng], og jeg finder det derfor mest naturligt, at holde det samlet i et kapitel for sig.

I afsnit 4.1 vises det, hvordan dekompositionen af sammenhængende matroider generelt foregår, idet de faktisk dekomponerer under en ækvivalensrelation formuleret i [Ng, Walker] i et antal uniforme matroider.

Jeg vil i afsnit 4.2 bruge dekompositionen fra afsnit 4.1 til at redegøre for, hvordan enhver sammenhængende ideel access-struktur Γ dekomponerer i et antal threshold-strukturer $\Gamma_1, \ldots, \Gamma_N$. Dette baserer sig altså på det tilsvarende resultat for matroider, men kan også bevises uden dette resultat, som det er gjort af [Ng, Walker].

Afsnit 4.3 er en fortsættelse af behandlingen af dekomposition af matroider fra afsnit 4.1. Her ses på sammenhængende matroider, som dekomponerer i præcis to ækvivalensklasser og ender faktisk med en fuldstændig karakterisering af disse matroiders cykler. Resultaterne overføres i afsnit 4.3.1 til et resultat vedrørende antallet af de ideelle access-strukturer, som dekomponerer i netop to threshold-strukturer. Det viser sig iøvrigt, at alle matroider med præcis to uniforme sammenhængskomponenter faktisk er secret sharing.

I afsnit 4.4 forfølges tankegangen med, at lade ideelle access-strukturer være byggesten for en større access-struktur. Jeg viser, hvordan man kan bruge en allerede kendt konstruktion til at konstruere en ideel access-struktur udfra disjunkte ideelle access-strukturer.

4.1 Dekomposition af matroider

Først defineres en relation på en sammenhængende matroides punktmængde. Denne relation kaldes stærk sammenhæng, og bagefter vises det, at det faktisk er en ækvivalensrelation.

Lad $\mathcal{M} = (V, C)$ være en sammenhængende matroide med punktmængden V og mængden af cykler C. For hvert $a \in V$ defineres nu Γ_a^- til at være mængden af "a-punkterede cykler"[1], dvs.

$$\Gamma_a^- = \{A \setminus \{a\} \subseteq V \mid a \in A \in C\}.$$

Γ_a^- kan altså også siges at være mængden af træer $A' \subseteq V$, hvor $A' \cup \{a\}$ er en cykel.

For $b \in V$ kan man definere delmængderne af Γ_a, som ikke indeholder b:

$$\Gamma_a^-(b) = \{A \in \Gamma_a^- \mid b \notin A\},$$

og endelig defineres begrebet stærk sammenhæng for $a, b \in V$ på følgende måde:

Definition 4.1.1. Lad $\mathcal{M} = (V, C)$ være en sammenhængende matroide. To punkter $a, b \in V$ siges at være *stærkt sammenhængende*, hvis $\Gamma_a^-(b) = \Gamma_b^-(a)$. Dette skrives $a \sim b$.

Der gælder følgende om relationen stærk sammenhæng:

Lemma 4.1.2. *Lad $\mathcal{M} = (V, C)$ være en matroide. Da er stærk sammenhæng en ækvivalensrelation på V.*

Bevis. Det er klart, at $\sim$ er både refleksiv og symmetrisk, og det skal da bare vises, at den også er transitiv. Antag derfor for $a, b, c \in \mathcal{P}$ at der gælder $a \sim b$ og $b \sim c$, dvs.

$$\Gamma_a^-(b) = \Gamma_b^-(a) \text{ samt } \Gamma_b^-(c) = \Gamma_c^-(b).$$

Det skal så vises, at $\Gamma_a^-(c) = \Gamma_c^-(a)$. Først vises $\Gamma_c^-(a) \subseteq \Gamma_a^-(c)$. Antag $X \in \Gamma_c^-(a)$. Da er $X \in \Gamma_c^-$ med $a \notin X$. Da $\Gamma_b^-(c) = \Gamma_c^-(b)$, må der gælde enten $X \in \Gamma_b^-(c)$ eller $b \in X$.

Antag først at $X \in \Gamma_b^-(c)$, og $b \notin X$. Så er $X \in \Gamma_b^-$ og $a \notin X$, dvs. $X \in \Gamma_b^-(a) = \Gamma_a^-(b)$. Desuden er $c \notin X$, så man har $X \in \Gamma_a^-(c)$.

Antag nu i stedet $X \in \Gamma_c^-(a)$ og $b \in X$. Så er $A = (X \cup \{c\}) \setminus \{b\} \in \Gamma_b^-(a)$, og dermed $A \in \Gamma_a^-(b)$. Så er også $A \in \Gamma_a^-$, og $c \in A$, og $(A \cup \{a\}) \setminus \{c\} \in \Gamma_c^-$. Dvs. $(X \cup \{a\}) \setminus \{b\} \in \Gamma_c^-$, og dermed også

$$(X \cup \{a\}) \setminus \{b\} \in \Gamma_c^-(b) = \Gamma_b^-(c). \tag{4.1}$$

Nu kan iflg. ligning (4.1) a og b ombyttes, så man får $\Big(((X \cup \{a\}) \setminus \{b\}) \cup \{b\}\Big) \setminus \{a\} = X \in \Gamma_a^-$, dvs. $X \in \Gamma_a^-(c)$.

For at vise $\Gamma_a^-(c) \subseteq \Gamma_c^-(a)$, kan der laves et argument helt magen til, hvor man antager, at $X \in \Gamma_a^-(c)$ og viser $X \in \Gamma_c^-(a)$. □

[1] En a-punkteret cykel er altså ikke en cykel! Men hvis man tilføjer punktet a, så får man en cykel.

Nu da stærk sammenhæng er en ækvivalensrelation, vil V opdeles i stærke ækvivalensklasser $V_1, \ldots, V_N$. Lad $a \in V_i$. Da kan defineres

$$ {}^{i}\Gamma_a^- = \{A \in \Gamma_a^- \mid A \subseteq V_i\} \tag{4.2} $$

som den delmængde af basen Γ_a^-, der er indeholdt i klassen V_i. Definér foreningen

$$ {}^{i}\Gamma^- = \bigcup_{a \in V_i} {}^{i}\Gamma_a^-, \tag{4.3} $$

${}^{i}\Gamma^-$ betegner hermed alle de mængder $A \subseteq V_i$, hvor der findes et $a \in V_i$, så $A \cup \{a\}$ er en cykel indeholdt i V_i. Definér også

$$ {}^{i}\Gamma_a^-(b) = \left\{A \in {}^{i}\Gamma_a^- \mid b \notin A\right\}. $$

Lemma 4.1.3. *Lad $a \in V_i$ og $X \in {}^{i}\Gamma_a^-$ og lad $c \in X$. For alle $b \in V_i \backslash (X \cup \{a\})$ er mængden*

$$ Y = ((X \cup \{b\}) \backslash \{c\}) \in {}^{i}\Gamma_a^-. $$

Bevis. Lad $b \in V_i \setminus (X \cup \{a\})$. Da begge $a, b \in V_i$, er $a \sim b$, og så er $X \in {}^{i}\Gamma_b^-$. Dvs. mængderne

$$ A = X \cup \{a\} \quad \text{og} \quad B = X \cup \{b\} $$

udgør to forskellige cykler. Nu er $c \in A \cap B$ og $a \in A \backslash B$, og iflg. lemma 1.1.7 på side 10, at der findes en cykel C, så $a \in C \subseteq (A \cup B) \backslash \{c\} = (X \cup \{a, b\}) \backslash \{c\}$. Men da både A og B er cykler, er de minimale afhængige mængder, og C kan derfor ikke være helt indeholdt i hverken A eller B, dvs. C indeholder både a, b samt en delmængde af $X \backslash \{c\}$.

Antag at C indeholder en ægte delmængde af $X \backslash \{c\}$. Da C er en cykel gennem a, er

$$ C \backslash \{a\} \in {}^{i}\Gamma_a^-(c), $$

og da $c \sim a$, er $C \backslash \{a\} \in {}^{i}\Gamma_c^-(a)$. Dvs. $(C \backslash \{a\}) \cup \{c\}$ er en cykel. Men hvis C indeholder en ægte delmængde af $X \backslash \{c\}$, er $(C \backslash \{a\}) \cup \{c\}$ en ægte delmængde af $(X \cup \{b\}) = B$, hvilket er en modstrid, da B er en cykel. Så C må derfor indeholde både a, b samt hele $X \backslash \{c\}$, dvs. $C = (A \cup B) \backslash \{c\}$.

Nu gælder det, at mængden $Y = (X \cup \{b\}) \backslash \{c\} = C \backslash \{a\} \in {}^{i}\Gamma_a^-$. □

Sætning 4.1.4. *Restriktionen $\mathcal{M}|_{V_i}$ er en uniform matroide, og mængden af cykler er*

$$ C_i = \{X \in C \mid X \subseteq V_i\} = \bigcup_{a \in V_i} \left\{A \cup \{a\} \,\middle|\, A \in {}^{i}\Gamma_a^-\right\}. $$

Bevis. Den første halvdel af beviset går ud på at vise, at alle cykler indeholdt i V_i gennem et enkelt bestemt punkt i V_i har samme størrelse. Lad $a \in V_i$ og $X, Y \in {}^{i}\Gamma_a^-$. Så er

$$ X \cup \{a\} \text{ og } Y \cup \{a\} $$

to cykler gennem a, som er helt indeholdt i V_i. X og Y kan opskrives, så

$$X = \{c_1, \ldots, c_j, c_{j+1}, \ldots, c_k\} \quad \text{og} \quad Y = \{c_1, \ldots, c_j, b_{j+1}, \ldots, b_m\},$$

hvor $c_i \neq b_{i'}$ for alle i, i'. Antag WLOG $k \leq m$. Det gælder nu, at $c_{j+1} \in X \in {}^i\Gamma_a^-$, og $b_{j+1} \in V_i \backslash (X \cup \{a\})$, så iflg. lemma 4.1.3 er

$$X_1 = (X \cup \{b_{j+1}\}) \backslash \{c_{j+1}\} = \{c_1, \ldots, c_j, b_{j+1}, c_{j+2}, \ldots, c_k\} \in {}^i\Gamma_a^- .$$

Men nu er $c_{j+2} \in X_1 \in {}^i\Gamma_a^-$, og $b_{j+2} \in V_i \backslash (X_1 \cup \{a\})$, så ved brug af lemma 4.1.3 igen fås

$$X_2 = (X_1 \cup \{b_{j+2}\}) \backslash \{c_{j+2}\} = \{c_1, \ldots, c_j, b_{j+1}, b_{j+2}, c_{j+3}, \ldots, c_k\} \in {}^i\Gamma_a^- .$$

Denne procedure kan gentages $k - j$ gange, indtil man har

$$X_{k-j} = \{c_1, \ldots, c_j, b_{j+1}, \ldots, b_k\} \in {}^i\Gamma_a^-,$$

dvs. $X_{k-j} \cup \{a\}$ er en cykel gennem a indeholdt i V_i. Men da $k \leq m$, er $X_{k-j} \cup \{a\} \subseteq Y \cup \{a\}$, hvilket på grund af minimaliteten af cykler kun kan lade sig gøre, hvis $k = m$. Alle cykler indeholdt i V_i gennem a har derfor samme størrelse.

Resultatet skal nu udvides til at vise, at alle cykler indeholdt i V_i har samme størrelse. Lad $a, b \in V_i$ med $a \neq b$ og lad $X \in {}^i\Gamma_a^-$. Hvis $b \in X$, er $X \cup \{a\}$ en cykel gennem både a og b. Som det lige er vist ovenfor, må alle cykler gennem a, b have samme størrelse. Hvis $b \notin X$, findes der iflg. lemma 4.1.3 for alle $c \in X$ en cykel $C = (X \cup \{a, b\}) \backslash \{c\}$ gennem a, b med $|C| = |X \cup \{a\}|$. Så alle cykler indeholdt i V_i gennem ethvert par af punkter $a, b \in V_i$ har samme størrelse, og da $\mathcal{M}$ desuden er sammenhængende, har alle cykler indeholdt i V_i dermed samme størrelse. Lad denne længde af cyklerne være $k + 1$.

Omvendt må det nu vises, at enhver delmængde af V_i af kardinalitet $k + 1$ er en cykel. Lad derfor $X \subseteq V_i$ med $|X| = k + 1$ og antag, at X ikke er en cykel. Så indeholder X enten en ægte delmængde C, som er en cykel, eller også er X uafhængig, dvs. indeholdt i en cykel C. Men da alle cykler i V_i har længde $k + 1$ er $X = C$ og X er dermed selv en cykel. □

De uniforme matroider $\mathcal{M}_i = \mathcal{M}|_{V_i}$, som $\mathcal{M}$ siges at *dekomponere* i, kaldes også for $\mathcal{M}$'s *stærke sammenhængskomponenter*.

4.2 Dekomposition af ideelle access-strukturer

Jeg skal lige kort forlade de rene matematiske overvejelser om matroider og se, hvordan resultaterne kan bruges til at sige noget om ideelle access-strukturer. I forrige afsnit sås, hvordan sammenhængende matroider generelt dekomponerer under stærk sammenhæng. Dette resultat er i sig selv interessant ud fra et matematisk synspunkt, men det kan ikke overraskende også anvendes til at udlede en slags dekomposition for ideelle access-strukturer. Denne rækkefølge er logisk set omvendt i forhold til, hvordan tingene bliver behandlet i [Ng, Walker]. Jeg gør det på denne måde, fordi jeg mener, at dekomposition

af matroider dybest set er det matematiske grundlag, som access-strukturerne arver deres dekomposition fra. Desuden bruger [Ng, Walker]'s bevis nogle lidt trælse hjælpesætninger om informationsteori. Det kræver noget arbejde at vise disse hjælpesætninger, og jeg mener ikke, de er specielt interessante i sig selv. Desuden synes jeg, at resultatet i sidste ende følger noget mere elegant af matroidedekompositionen. Dog bliver det ene af disse lemmaer brugt kortvarigt i et senere bevis, så jeg vil opskrive det her. Det er [Ng, Walker], lemma 2:

Lemma 4.2.1. *Hvis $A \in \Gamma_s^-$, så er $H(A) = \sum_{a \in A} H(a)$.*

Betragt et ideelt secret sharing scheme M over access-strukturen Γ_{p_0} med associeret matroide $\mathcal{M} = \mathcal{T}(M) = (V, C)$, hvor $V = \mathcal{P} \cup \{p_0\}$ er mængden af personer i schemet inklusiv dealeren, og hvor C er mængden af cykler. Som det sås i forrige afsnit, dekomponerer $\mathcal{M}$ under stærk sammenhæng i N uniforme sammenhængskomponenter $\mathcal{M}_1, \ldots, \mathcal{M}_N$. Da er $\mathcal{M}_i$ en uniform matroide $\mathcal{U}_{k_i, n_i}$, og cyklerne i $\mathcal{M}_i$ er da præcis de mængder, som har kardinalitet $k_i + 1$. Ifølge sætning 4.1.4 er C_i også givet ved

$$C_i = \bigcup_{a \in V_i} \left\{ A \cup \{a\} \,\middle|\, A \in {}^i\Gamma_a^- \right\}.$$

$\mathcal{M}_i$ er derfor den associerede matroide $\mathcal{T}(\Gamma_a)$, $a \in V_i$, til et ideelt $(k_i + 1, n_i)$-threshold scheme på V_i. Dette ses her:

Hvis nemlig Γ_a er et $(k_i + 1, n_i)$-threshold scheme på V_i med $a \in V_i$, så giver ombytningsegenskaben, korollar 3.1.12 på side 51, at $\mathcal{T}(\Gamma_a)$ er matroiden karakteriseret ved, at cyklerne præcis er mængderne af kardinalitet $k_i + 1$. På grund af entydigheden af den associerede matroide $\mathcal{T}(\Gamma_a)$ givet i hovedsætning 2, sætning 3.2.3 på side 52, er så $\mathcal{T}(\Gamma_a) = \mathcal{M}_i = (V_i, C_i)$.

[Ng, Walker] definerer størrelsen Δ_a som basen for den ideelle access-struktur Γ_a hørende til schemet med dealeren a. Desuden definerer de for $a \notin A$ størrelsen $\Delta_a(b) = \{A \in \Delta_a \mid b \notin A\}$. For at bevare konsistent notation, vil jeg dog betegne Δ_a som Γ_a^- og for $a \notin A$ definere $\Gamma_a^-(b) = \{A \in \Gamma_a^- \mid b \notin A\}$.

På baggrund af ombytningsegenskaben defineres den såkaldte *stærke sammenhæng* imellem to personer i et SSS:

Definition 4.2.2. To personer $a, b \in V = \mathcal{P} \cup \{p_o\}$ siges at være *stærkt sammenhængende*, hvis $\Gamma_a^-(b) = \Gamma_b^-(a)$. Da skrives $a \sim b$.

Som det netop er vist, dekomponerer enhver ideel access-struktur Γ i et antal threshold-strukturer $\Gamma_1, \ldots, \Gamma_N$. Stærk sammenhæng defineret for personer i et SSS er altså også en ækvivalensrelation. Klasserne Γ_i svarer præcis til matroidekomponenterne $\mathcal{M}_i$. Threshold-strukturer kan altså på denne måde siges at være "primitive komponenter" eller "byggesten" for alle andre ideelle access-strukturer.

Dette kan som nævnt også vises uden brug af ækvivalensrelationen på matroider. Sådan er det faktisk oprindeligt gjort i [Ng, Walker]. De viser følgende lemma:

Lemma 4.2.3. *Stærk sammenhæng "$\sim$" er en ækvivalensrelation på $V = \mathcal{P} \cup \{p_0\}$.*

Beviset i [Ng, Walker] baserer sig da på definitioner i samme stil som dem fra forrige afsnit. Derudover er det nødvendigt at vise de førnævnte lidt trælse informationsteoretiske hjælpesætninger ([Ng, Walker], Lemma 1, Lemma 2, Theorem 1) angående entropien af delmængder af V. Lad $V_1, \ldots, V_N$ være de stærke sammenhængs-ækvivalensklasser på V. I stil med begreberne fra forrige afsnit kan der for alle $a \in V_i$ defineres

$$ {}^{i}\Gamma_a^- = \{A \in \Gamma_a^- \mid A \subseteq V_i\} \tag{4.4} $$

som den delmængde af basen Γ_a^-, der er indeholdt i klassen V_i. Definér også foreningen

$$ {}^{i}\Gamma^- = \bigcup_{a \in V_i} {}^{i}\Gamma_a^-, \tag{4.5} $$

som er mængden af delmængder A indeholdt i V_i, der er autoriserede i forhold til en person $a \in V_i \setminus A$. Jeg bruger her samme notation for begreberne i ligning (4.4) og (4.5), som blev brugt i forrige afsnit i ligning (4.2) og (4.3).

[Ng, Walker] benytter sig af en type af koder, som kaldes MDS-koder. For en ordens skyld vil jeg lige definere, hvad det er, da de viser sig at være tæt knyttede til cyklerne i de uniforme sammenhængskomponenter.

Definition 4.2.4. Lad C være en kode af længde n over et alfabet af størrelse q og antag, at to kodeord er forskellige, hvis de afviger på mindst d koordinatpositioner. Da siges koden C at have *minimum distance* d.

En kode C af længde n over et alfabet af størrelse q og med minimum distance d har højst q^{n-d+1} forskellige elementer (eller kodeord). Hvis der nemlig ses bort fra f.eks. de sidste $d-1$ koordinatpositioner i alle forskellige kodeord, er de alle stadig forskellige, og $d-1$ er pr. definition 4.2.4 det højeste antal med denne egenskab. Der er dermed højst $q^{n-(d-1)} = q^{n-d+1}$ forskellige kodeord. En kode, som har det maksimale antal elementer, kaldes maximal distance separable. Dette giver følgende definition:

Definition 4.2.5. En kode C af længde n over et alfabet af størrelse q og med minimum distance d, og som har det maksimale antal q^{n-d+1} forskellige elementer, kaldes en *MDS-kode*.

For en MDS-kode gælder det altså åbenbart, at for enhver mængde af $n-d+1$ koordinatpositioner og enhver mængde af $n-d+1$ alfabetelementer findes der et entydigt kodeord med netop disse alfabetelementer på netop disse positioner. Sæt $t = n-d+1$. Denne størrelse har åbenbart en vigtig betydning, og mængderne af sådanne $t = n-d+1$ koordinatpositioner kaldes *minimum information sets*. MDS-koden kan også defineres på følgende måde med parametrene (r, t, q):

Definition 4.2.6. Lad C være en kode af længde r over et alfabet $\mathcal{A}$ med $|\mathcal{A}| = q$. C siges at være en *MDS-kode*, hvis der findes et t, så det for alle t positioner $i_1, \ldots, i_t$ og for alle følger af t elementer $a_1, \ldots, a_t \in \mathcal{A}$ (ikke nødvendigvis forskellige) gælder, at der findes præcis ét kodeord $c = (c_1, \ldots, c_r) \in C$ med $c_{i_j} = a_j$ for alle $j = 1, \ldots, t$. En sådan MDS-kode siges at have parametre (r, t, q).

Ifølge [Ng, Walker], findes der en ideel (k, n)-threshold access-struktur med $|\mathcal{S}| = q$, hvis og kun hvis der findes en MDS-kode af længde $n + 1$ over et q-alfabet, hvor alle MIS'er (minimum information sets) har størrelse k. Men [Ng, Walker] viser ikke dette. De henviser i stedet bl.a. til [Mitchell, Walker, Wild], Thm. 3.4, men denne artikel viser faktisk en sætning for authentication schemes:

Sætning 4.2.7 (Sætning A.2.7). *Lad $C = C(\mathcal{A})$ være den associerede kode til et N-perfekt authentication scheme $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$. Så er C en MDS-kode med parametre $(|\mathcal{S}|, N + 1, q)$, hvor $q = |(s)|$ for alle $s \in \mathcal{S}$.*

Hvis omvendt C er en MDS-kode med parametre $(r, N + 1, q)$, så er $C = C(\mathcal{A})$ for et N-perfekt authentication scheme $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ med $|\mathcal{S}| = r$ og q krypteringer af hver kildetekstbesked.

De nærmere omstændigheder omkring denne sætning har jeg valgt at henlægge til appendiks A.

I virkeligheden er det jo en sammenhæng mellem MDS-koder og *threshold-strukturer*, der ønskes. Sammenhængen mellem N-perfekte authentication schemes og ideelle threshold schemes er nemlig ikke nødvendigvis helt triviel. Den ønskede direkte sammenhæng mellem MDS-koder og ideelle threshold-strukturer har jeg derfor selv forsøgt at etablere ved denne sætning:

Sætning 4.2.8 (Sætning B.1.1). *Der findes en ideel (t, n)-threshold-access-struktur, hvor $|\mathcal{K}| = |\mathcal{S}| = q$, hvis og kun hvis der findes en MDS-kode med parametre $(n + 1, t, q)$.*

Jeg beviser selv sætningen i appendiks B. [Ng, Walker] viser nu følgende sætning:

Sætning 4.2.9. *Koden C_i er en MDS-kode, hvor ${}^i\Gamma^-$ er mængden af MIS'er, dvs. elementerne i ${}^i\Gamma^-$ er alle af kardinalitet $H(V_i)/H(s)$, og enhver delmængde af V_i af denne kardinalitet tilhører ${}^i\Gamma^-$.*

Bevis. Lad $A \in {}^i\Gamma^-$. Så er $A \in \Gamma_a^-$ for et $a \in V_i \backslash A$, og da V_i er en stærk ækvivalensklasse, gælder det, at $A \in \Gamma_a^-$ for alle $a \in V_i \backslash A$. Så $H(V_i \backslash A \mid A) = 0$, og

$$H(V_i) = H(V_i \backslash A \mid A) + H(A) = H(A).$$

Iflg. lemma 4.2.1 er $H(V_i) = H(A) = \sum_{a \in A} H(a) = \sum_{a \in A} H(s) = |A| \cdot H(s)$, hvilket giver $|A| = H(V_i)/H(s)$, så A har den ønskede kardinalitet. Da A desuden er minimal med $H(A) = H(V_i)$, er A et MIS.

Lad nu $X \subseteq V_i$ med $|X| = H(V_i)/H(s)$ og lad $X' \subseteq X$ være maksimal med den egenskab, at

$$H(X') = \sum_{x \in X'} H(x).$$

Det skal så vises, at $X' = X$. Antag derfor $X' \neq X$ og lad $x \in X \setminus X'$. Så er

$$H(x \mid X') = H(X' \cup \{x\}) - H(X'),$$

Men da enten $H(x \mid X') = 0$ eller $H(x \mid X') = H(x)$, er $H(x \mid X') = 0$ på grund af minimaliteten af X'. Men så findes en $X'' \subseteq X'$, så $X'' \in {}^{i}\Gamma^{-}_{x}$, og $|X''| < |X| = H(V_i)/H(s)$. Men det er jo i bevisets første del vist, at

$$X'' \in {}^{i}\Gamma^{-} \Longrightarrow |X''| = \frac{H(V_i)}{H(s)},$$

så det er en modstrid, og dermed er $X' = X$. Enhver delmængde $X \subseteq V_i$ med $|X| = H(V_i)/H(s)$ er derfor i ${}^{i}\Gamma^{-}$. □

Koden C_i er åbenbart MDS med mængden af MIS'er ${}^{i}\Gamma^{-}$ bestående af mængder af en bestemt kardinalitet $k = H(V_i)/H(s)$, dvs. der findes en ideel $(k, |V_i| - 1)$-threshold accessstruktur på V_i.

Jeg har således karakteriseret strukturen af de minimale autoriserede delmængder, som ligger indenfor en stærk ækvivalensklasse, idet Γ dekomponerer i threshold-strukturerne $\Gamma_1, \ldots, \Gamma_N$. Hermed er karakteriseringen af cyklerne indenfor hver stærk sammenhængskomponent $\mathcal{M}_i$ klaret. Men der er jo også cykler, som ikke er indeholdt i en enkelt stærk sammenhængskomponent, og disse mangler man at få styr på for at kunne karakterisere alle cykler i matroiden $\mathcal{M}$. Disse cykler, som snitter flere sammenhængskomponenter, skal nu undersøges. Dog kun i det specielle tilfælde $N = 2$.

4.3 Matroider med to uniforme komponenter

Dette afsnit er i forlængelse af afsnit 4.1 og fortsætter behandlingen af matroiders dekomposition i uniforme komponenter ved ækvivalensrelationen "stærk sammenhæng".

Antag, at en matroide $\mathcal{M}$ dekomponerer i N stærke sammenhængsklasser $V_1, \ldots, V_N$ hver med uniform matroidestruktur, så det giver matroiderne $\mathcal{U}_{k_1,n_1}, \ldots, \mathcal{U}_{k_N,n_N}$. Spørgsmålet, der ønskes besvaret, er, hvordan ser cyklerne i $\mathcal{M}$ ud? Dette undersøges for $N = 2$.

Lad nu $\mathcal{M} = (V, C)$ være en sammenhængende matroide med sammenhængsklasser V_1, V_2, så $V = V_1 \cup V_2$ med $\mathcal{M}|_{V_1} = \mathcal{U}_{k_1,n_1}$, $\mathcal{M}|_{V_2} = \mathcal{U}_{k_2,n_2}$ med $k_i \geq 1, k_i < n_i$, og lad C_i være restriktionen af C til V_i. Lad $X \subseteq V$ med $|X \cap V_1| = m$ og $|X \cap V_2| = n$. Da defineres *typen* af X til at være (m, n). Dermed er f.eks. C_1 netop mængden af delmængder af type $(k_1 + 1, 0)$.

Der skal nu vises en hel del lemmaer, som til sammen beviser sætning 4.3.11. Resten af karakteriseringen følger i sætningerne 4.3.12 og 4.3.13. Disse sætninger kombineres til dette afsnits hovedresultat, korollar 4.3.14 på side 93.

Lemma 4.3.1. *Hvis $\mathcal{M}$ har en cykel af type (m,n) med $mn \neq 0$, så er $m \leq k_1$ og $n \leq k_2$.*

Bevis. Antag at $\mathcal{M}$ indeholder en cykel C med $m > k_1$. Så er $m \geq k_1 + 1$, og C indeholder da en delmængde af type $(k_1 + 1, 0)$, men dette er en cykel i $\mathcal{U}_{k_1,n_1}$ og dermed også i $\mathcal{M}$, hvilket er en modstrid med minimaliteten af cyklen C. Beviset er tilsvarende for n. □

Lemma 4.3.2. *Hvis $\mathcal{M}$ har en cykel af type (m,n), så er alle delmængder af V af denne type cykler i $\mathcal{M}$.*

Bevis. Antag at $\mathcal{M}$ har en cykel $C = \{x_1, \ldots, x_m, y_1, \ldots, y_n\}$ af type (m,n) med $mn \neq 0$ og antag med $x_i \in V_1$ og $y_i \in V_2$. Lad $C' = \{x'_1, \ldots, x'_m, y'_1, \ldots, y'_n\}$ være en anden delmængde af type (m,n) med $x'_i \in V_1$ og $y'_i \in V_2$. Lad $x'_i \in C' \backslash C$ og $x_j \in C \backslash C'$. Da $x'_i, x_j \in V_1$ er i den samme sammenhængsklasse, er $\Gamma^-_{x'_i}(x_j) = \Gamma^-_{x_j}(x'_i)$. Da er $C \setminus \{x_j\} \in \Gamma^-_{x_j}(x'_i) = \Gamma^-_{x'_i}(x_j)$, dvs. $(C \cup \{x'_i\}) \backslash \{x_j\}$ er en cykel i $\mathcal{M}$ af type (m,n). Dette argument kan gentages indtil samtlige elementer fra $C \backslash C'$ er erstattet af elementerne fra $C' \backslash C$. Til sidst fås, at C' også er en cykel i $\mathcal{M}$. □

Bemærk at beviset for lemma 4.3.2 ikke benytter nogen antagelse om, at $n_i > k_i$, så lemmaet må også gælde for dekomposition i frie matroider, dvs. hvor $n_i = k_i$.

Lemma 4.3.3. *Hvis $\mathcal{M}$ har cykler af type (m,n) og (m',n'), så er enten $m' = m$, $n' = n$, eller $m' < m$, $n' > n$, eller $m' > m$, $n' < n$.*

Bevis. Antag først at $m' < m$ og $n' \leq n$. Så vil en cykel af type (m,n) indeholde en mængde af type (m',n'), hvilket er en cykel. Men dette er en modstrid. Argumentet kan gentages i alle andre tilfælde på nær netop de tre nævnte. □

Lemma 4.3.4. *$\mathcal{M}$ har ingen cykler af type (m,n), hvor $m + n > k_1 + k_2$ eller $m + n \leq k_1$.*

Bevis. Ifølge lemma 4.3.1 er $m \leq k_1$ og $n \leq k_2$, og dermed er $m + n \leq k_1 + k_2$. Beviset for, at der ikke findes cykler med $m + n \leq k_1$, er et induktionsbevis, hvor det n'te trin $P(n)$ er udsagnet "der er ingen cykler af type (m,n) med $m + n \leq k_1$".

$P(1)$ siger, at der ingen cykler er af type $(m,1)$ med $m + 1 \leq k_1$. Denne påstand skal nu vises. Antag derfor, at der findes en cykel af type $(m,1)$ med $m + 1 \leq k_1$. Iflg. lemma 4.3.2 er alle mængder af denne type cykler i $\mathcal{M}$. Lad C_1, C_2 være forskellige cykler af type $(m,1)$ med

$$C_1 = \{x_1, x_2, \ldots, x_m, y\} \quad \text{og} \quad C_2 = \{x'_1, x_2, \ldots, x_m, y\},$$

hvor $x'_1, x_i \in V_1, y \in V_2, x'_1 \neq x_1$. Så er $y \in C_1 \cap C_2$, og iflg. proposition 1.1.6 på side 9 findes en cykel

$$C_3 \subseteq (C_1 \cup C_2) \backslash \{y\} = \{x'_1, x_1, \ldots, x_m\}.$$

C_3 er altså af type $(m',0)$ for et $m' \leq m + 1$. Men pr. antagelse er $m + 1 \leq k_1$, så $m' \leq k_1$, hvilket betyder, at C_3 er indeholdt i en mængde af type $(k_1 + 1, 0)$, men en sådan er en cykel, og det giver en modstrid. Så $P(1)$ er sand.

Antag nu, at $P(n)$ holder for alle $1 \leq n \leq k$, dvs. der er ingen cykel af type (m,n), hvis $m + n \leq k_1$ for alle $1 \leq n \leq k$. Man skal så vise udsagnet $P(k+1)$, nemlig at der heller

ikke findes cykler af type $(m, k+1)$, hvis $m+k+1 \leq k_1$. Beviset kører i samme stil som det for $P(1)$. Antag derfor at C_1, C_2 er forskellige cykler af denne type med

$$C_1 = \{x_1, x_2, \ldots, x_m, y_1, \ldots, y_{k+1}\} \quad \text{og} \quad C_2 = \{x_1', x_2, \ldots, x_m, y_1, \ldots, y_{k+1}\},$$

hvor $x_1', x_i \in V_1, y_i \in V_2, x_1' \neq x_1$. Så er $y_{k+1} \in C_1 \cap C_2$, og der findes en cykel C_3, så

$$C_3 \subseteq (C_1 \cup C_2) \backslash \{y_{k+1}\} = \{x_1', x_1, x_2, \ldots, x_m, y_1, \ldots, y_k\}.$$

C_3 er nu af type (m', n'), hvor $m' \leq m+1$ og $n' \leq k$. Så er $m'+n' \leq m+1+k \leq k_1$, og pr. induktionsantagelse er der ingen cykler af type (m', n'), så det er en modstrid. Disse C_1, C_2 kan derfor ikke findes, og der er derfor ingen cykler af type $(m, k+1)$, hvis $m+k+1 \leq k_1$. □

Lemma 4.3.5. *Hvis $\mathcal{M}$ har en cykel af type (m, n), hvor $m+n = k$, så er $k_1+1 \leq k \leq k_1+k_2$, og alle delmængder med $m'+n' = k$, $m' \leq k_1$, $n' \leq k_2$ er cykler i $\mathcal{M}$.*

Bevis. Første del af udsagnet følger klart af lemma 4.3.4. Lad derfor C_1, C_2 være to forskellige cykler af type (m, n), $m+n = k$ med

$$C_1 = \{x_1, \ldots, x_m, y_1, \ldots, y_n\} \quad \text{og} \quad C_1 = \{x_1, \ldots, x_m, y_1, \ldots, y_{n-1}, y_n'\},$$

hvor $x_i \in V_1$ og $y_n', y_i \in V_2, y_n' \neq y_n$. Så er $x_1 \in C_1 \cap C_2$, og der findes en cykel C_3, så

$$C_3 \subseteq (C_1 \cup C_2) \backslash \{x_1\} = \{x_2, \ldots, x_m, y_1, \ldots, y_n, y_n'\}.$$

Da er C_3 af type (m', n'), hvor $m' < m$ Iflg. lemma 4.3.3 er så $n' > n$, og C_3 må være af type $(m', n+1)$ med $m' \leq m-1$.

Hvis i stedet

$$C_1 = \{x_1, x_2, \ldots, x_m, y_1, \ldots, y_n\} \quad \text{og} \quad C_2 = \{x_1', x_2, \ldots, x_m, y_1, \ldots, y_n\}$$

med $x_1' \neq x_1$, så findes en cykel $C_4 \subseteq (C_1 \cup C_2) \backslash \{y_n\}$ af type (m', n') med $m' \leq m+1$ og $n' \leq n-1$. Dvs. C_4 er af type $(m+1, n')$ med $n' \leq n-1$. Cyklen C_4 er så af type $(m+1, n')$ med $n' \leq n-1$ igen som følge af lemma 4.3.3.

Det er dermed vist, at hvis der findes en cykel af type (m, n), så må der findes cykler af type $(m+1, n')$ og $(m', n+1)$ med $m' \leq m-1$ og $n' \leq n-1$.

Dette kan så benyttes således, at cykler af type $(m+1, n')$ giver anledning til cykler af type $(m'', n'+1)$, hvor $m'' \leq m$ og $n'+1 \leq n$. Dette kan iflg. lemma 4.3.3 kun lade sig gøre, hvis $m'' = m$ og $n'+1 = n$, dvs. $n' = n-1$. Dette argument kan også bruges på cyklerne af type $(m', n+1)$ til at vise, at $m' = m-1$.

Argumentet kan gentage så længe kravene fra lemma 4.3.1 stadig er opfyldt. Det er altså vist, at hvis der findes cykler af type (m, n) med $mn \neq 0$, så er der også cykler af type $(m+h, n-h)$ med $m+h \leq k_1, n-h \leq k_2$ samt cykler af type $(m-h, n+h)$ med $m-h \leq k_1, n+h \leq k_2$. Og nu da der findes cykler af ovennævnte typer, er iflg. lemma 4.3.2 alle mængder med disse egenskaber cykler i $\mathcal{M}$. □

Lemma 4.3.6. *Der findes m, n med $mn \neq 0$, så der eksisterer cykler af type (m, n).*

Bevis. Da $\mathcal{M}$ er sammenhængende, er ethvert par af elementer indeholdt i en cykel. Der kan derfor laves cykler, som indeholder mindst ét element fra hver af V_1, V_2. □

Lemma 4.3.7. *Hvis der findes cykler af type (m, n) og type (m', n') med $mn \neq 0$, og $m'n' \neq 0$, så er $m + n = m' + n'$.*

Bevis. Antag at der findes cykler type (m, n) og type (m', n') med $m+n = k$ og $m'+n' = k'$ og antag, at $k > k'$. Iflg. lemma 4.3.3 er enten $m' > m$, $n' < n$ eller $m' < m$, $n' > n$.

Antag $m' > m$, $n' < n$ med $m' = m + s$, $n' = n - t$, hvor $s, t > 0$. Idet $k > k'$, er $m + n > m + s + n - t$, så der skal gælde $s < t$. Iflg. lemma 4.3.5 findes der cykler af type $(m + s, n - s)$. Men da $n - s > n - t$, vil en cykel af type $(m + s, n - s)$ indeholde en mængde af type $(m + s, n - t) = (m', n')$, hvilket iflg. lemme 4.3.2 er en cykel. Men dette er en modstrid, så der kan ikke gælde $k > k'$.

På samme måde vises det, at der ikke kan gælde $k' > k$. □

Lemma 4.3.8. *Hvis $k_1 = k_2$, så opfylder alle cykler af type (m, n) med $mn \neq 0$, at $m + n > k_1 + 1$.*

Bevis. Iflg. lemma 4.3.5 er $k_1+1 \leq m+n$. antag at $m+n = k_1+1 = k_2+1$. Iflg. lemma 4.3.5 igen er så alle mængder af kardinalitet k_1+1 cykler i $\mathcal{M}$, dvs. $\mathcal{M}$ er den uniforme matroide $\mathcal{U}_{k_1,|V|}$. Men i en uniform matroide kan ethvert par af elementer ombyttes, således at $\mathcal{M}$ består af præcis én stærk sammenhængsklasse. Så hvis $\mathcal{M}$ har to sammenhængsklasser, er $m + n > k_1 + 1$. □

Iflg. lemma 4.3.6 findes der m, n, så der eksisterer cykler af type (m, n) med $mn \neq 0$. Ved at sammenfatte de resterende lemmaer fra 4.3.1 til 4.3.8 fås, at cyklerne af type (m, n) med $m + n = k$ opfylder

1. $m \leq k_1$,
2. $n \leq k_2$,
3. $k_1 + 1 \leq k \leq k_1 + k_2$, hvis $k_1 > k_2$,
4. $k_1 + 1 < k \leq k_1 + k_2$, hvis $k_1 = k_2$.

Jeg ønsker at vise sætning 4.3.11 og skal derfor nu vise, at $V = V_1 \cup V_2$ under kravene fra sætning 4.3.11 giver en matroide, som dekomponerer under stærk sammenhæng i netop de stærke sammenhængsklasser V_1, V_2.

Lemma 4.3.9. *Lad $V = V_1 \cup V_2$ være en disjunkt forening med $|V_1| = n_1$ og $|V_2| = n_2$ og lad C være familien af delmængder af V bestående af*

(a) alle delmængder af kardinalitet $k_1 + 1$, som er indeholdt i V_1, dvs. alle delmængder af type $(k_1 + 1, 0)$,

(b) alle delmængder af kardinalitet $k_2 + 1$, som er indeholdt i V_2, dvs. alle delmængder af type $(0, k_2 + 1)$,

(c) alle delmængder af type (m, n), hvor $0 < m \leq k_1$, $0 < n \leq k_2$, og $m + n = k$, hvor

$$\begin{cases} k_1 + 1 \leq k \leq k_1 + k_2, & \text{hvis } k_1 > k_2, \\ k_1 + 1 < k \leq k_1 + k_2, & \text{hvis } k_1 = k_2. \end{cases}$$

Så er $\mathcal{C}$ mængden af cykler i en matroide på V.

Bevis. Lad $\mathcal{C}$ være en familie af mængder, som opfylder kravene fra lemmaet og lad $C_1, C_2 \in \mathcal{C}$ være to forskellige mængder. Beviset deles nu op i seks tilfælde, som vises separat ved brug af en matroides cykel-karakterisering (sætning 1.1.9 på side 11):

(i) C_1 og C_2 opfylder begge kravet fra pkt. (a): Kravet (C1) fra sætning 1.1.9 er klart opfyldt, da der umuligt kan gælde $C_1 \subseteq C_2$, hvis $C_1 \neq C_2$ er af samme type. Lad $C_1 \neq C_2$ med $z \in C_1 \cap C_2$, så er $|(C_1 \cup C_2) \backslash \{z\}| \geq k_1 + 1$. Der må derfor være indeholdt en delmængde $C_3 \subseteq (C_1 \cup C_2) \backslash \{z\}$ med $|C_3| = k_1 + 1$ af type $(k_1, 0)$. Dermed er også (C2) opfyldt.

(ii) C_1 og C_2 opfylder begge kravet fra pkt. (b): Beviset fra pkt. (i) ovenfor kan gentages blot med type $(0, k_2 + 1)$ i stedet. Man arbejder da bare i V_2 i stedet for V_1, men det gør ingen forskel i forhold til argumentationen i dette bevis.

(iii) C_1 og C_2 opfylder begge kravet fra pkt. (c): Lad C_1 være en mængde af type (m_1, n_1) og C_2 en mængde af type (m_2, n_2) med $m_1 + n_1 = m_2 + n_2 = k$ iflg. lemma 4.3.7, hvor $k_1 + 1 \leq k \leq k_1 + k_2$. (C1) er klart opfyldt, da begge C_1, C_2 har samme kardinalitet k.

Antag først at $m_1 = m_2 = m$ og $n_1 = n_2 = n$. Lad $C_1 \neq C_2$ være af type (m, n) og antag WLOG at $x \in (C_1 \cap C_2) \cap V_1$. Lad desuden $C' = (C_1 \cup C_2) \setminus \{x\}$. Hvis nu $C_1 \cap V_2 = C_2 \cap V_2$, så er $C_1 \cap V_1 \neq C_2 \cap V_1$, da $C_1 \neq C_2$, og C' er en mængde af type (m', n) med $m' \geq m$. Altså indeholder C' en mængde af type (m, n), dvs. (C2) er opfyldt. Hvis $C_1 \cap V_2 \neq C_2 \cap V_2$, er C' en mængde af type (m', n') med $m' \geq m - 1$ og $n' \geq n + 1$. C' indeholder da en mængde af type $(m - 1, n + 1)$, som dermed også er omfattet af pkt. (c). Dette opfylder derfor (C2).

Antag nu $m_1 > m_2$ og $n_1 < n_2$ og lad

$$C_1 = \{x_1, \ldots, x_{m_1}, y_1, \ldots, y_{n_1}\} \quad \text{og} \quad C_2 = \{x'_1, \ldots, x'_{m_2}, y'_1, \ldots, y'_{n_2}\}.$$

Hvis $x_1 = x'_1 \in C_1 \cap C_2$, så er mængden på formen

$$C_3 = \{x_2, \ldots, x_{m_2+1}, y'_1, \ldots, y'_{n_2}\}$$

af type (m_2, n_2) indeholdt i $(C_1 \cup C_2) \setminus \{x_1\}$, hvilket opfylder (C2). Hvis i stedet $y_1 = y'_1 \in C_1 \cap C_2$, er mængden på formen

$$C_3 = \{x_1, \ldots, x_{m_1}, y'_2, \ldots, y'_{n_1+1}\}$$

af type (m_1, n_1) indeholdt i $(C_1 \cup C_2) \setminus \{y_1\}$. Hvis endelig $m_1 < m_2$ og $n_1 > n_2$, kan argumentet fra før vendes og bruges igen.

(iv) C_1 er af type som i (a), C_2 er af type som i (b): Da er $C_1 \cap C_2 = \emptyset$, og både (C1) og (C2) opfyldes.

(v) $C1$ er af type som i (a), C_2 er af type som i (c): Antag at C_2 er af type (m, n) med $m + n = k$, hvor k opfylder kravene i (c). (C1) er klart opfyldt. Lad $x \in V_1$ med $x \in C_1 \cap C_2$ og lad $C' = (C_1 \cup C_2) \setminus \{x\}$. Da C_1 er af type $(k_1+1, 0)$ er $|C' \cap V_1| \geq k_1 \geq m$, og så findes der en mængde $C_3 \subseteq C'$ med $|C_3 \cap V_1| = m$ og $|C_3 \cap V_2| = n$, dvs. C_3 er af type (c). Dermed er (C2) opfyldt.

(vi) C_1 er af type som i (b), C_2 er af type som i (c): Et lignende argument som det for (v) kan bruges her.

Hermed er hele beviset for lemmaet færdigt. □

Lemma 4.3.10. *Lad $\mathcal{M}$, V, V_1, V_2 og C være som i lemma 4.3.9. Så er V_1 og V_2 de stærke sammenhængsklasser i $\mathcal{M}$.*

Bevis. Her skal det vises, at $a \sim b$, hvis og kun hvis a, b begge er indeholdt i enten V_1 eller V_2. Antag derfor først at $a, b \in V_1$. Så består $\Gamma_a^-(b)$ af

- alle delmængderne af $A \subseteq V_1$ med $|A| = k_1$ og $a, b \notin A$, dvs. mængderne af type $(k_1, 0)$, som ikke indeholder a, b (lemma 4.3.9 (a)),
- mængderne af type $(m - 1, n)$, som ikke indeholder a, b, dvs. mængderne B med $|B| = k - 1$, $a, b \notin B$ og $|B \cap V_1| = m - 1$ og $|B \cap V_2| = n$ (lemma 4.3.9 (c)).

Men det er præcis mængderne i $\Gamma_b^-(a)$, da begge $a, b \in V_1$. Så $a \sim b$. På samme måde kan det vises for $a, b \in V_2$.

Antag nu at $a \in V_1$ og $b \in V_2$. Det skal så vises, at $a \nsim b$. Med A_0 betegnes nu familien af delmængder af V_1 af kardinalitet k_1, som ikke indeholder a, b. Lad $A_{m,n}$ være familien af mængder af kardinalitet $k-1$, som ikke indeholder a, b, og som er af type $(m-1, n)$. Lad ligeledes B_0 betegne familien af delmængder af V_2 af kardinalitet k_2, som ikke indeholder a, b samt $B_{m,n}$ mængderne af kardinalitet $k - 1$, som ikke indeholder a, b, og som er af type $(m, n - 1)$. Så er

$$\Gamma_a^-(b) = A_0 \cup \left(\bigcup_{m+n=k} A_{m,n} \right) \quad \text{og} \quad \Gamma_b^-(a) = B_0 \cup \left(\bigcup_{m+n=k} B_{m,n} \right).$$

Hvis $\Gamma_a^-(b) \subseteq \Gamma_b^-(a)$, er $A_0 \subseteq B_{m_0,n_0}$ for nogle m_0, n_0 med $m_0 + n_0 = k$, da der jo gælder $A_0 \notin B_0$. Da $A_0 \subseteq V_1$, er så $n_0 - 1 = 0$, $m_0 = k_1$ og $k - 1 = k_1$. Så er $k = k_1 + 1$.

Hvis $\Gamma_a^-(b) \supseteq \Gamma_b^-(a)$, så kan en tilsvarende argumentation som før bruge til at indse, at $B_0 \subseteq A_{m',n'}$ for nogle m', n' med $m' + n' = k$. Det må så gælde, at $m' - 1 = 0$, $k - 1 = k_2$ og $n' = k_2$, så $k = k_2 + 1$. Så hvis $a \sim b$, skal der altså gælde $\Gamma_a^-(b) = \Gamma_b^-(a)$, dvs. $k_1 = k_2$ og $k = k_1 + 1$. Men dette er i modstrid med den antagelse, der blev gjort i lemma 4.3.9, som siger, at $k > k_1 + 1$, hvis $k_1 = k_2$. Der må derfor gælde $a \nsim b$. □

Ovenstående lemmaer viser tilsammen følgende sætning:

Sætning 4.3.11. *Lad $\mathcal{M}$ være en sammenhængende matroide på V. Hvis $\mathcal{M}$ har netop to sammenhængs-klasser V_1, V_2 med $\mathcal{M}|_{V_1} = \mathcal{U}_{k_1,n_1}$, $\mathcal{M}|_{V_2} = \mathcal{U}_{k_2,n_2}$ med $k_i \geq 1$, $n_i \geq k_i$ og $k_1 \geq k_2$. Så består mængden af cykler i $\mathcal{M}$ af*

(a) alle mængder af type $(k_1 + 1, 0)$,

(b) alle mængder af type $(0, k_2 + 1)$,

(c) alle mængder af type (m, n), så $m \leq k_1$, $n \leq k_2$, og $m + n = k$, hvor

$$\begin{cases} k_1 + 1 \leq k \leq k_1 + k_2, & \text{hvis } k_1 > k_2, \\ k_1 + 1 < k \leq k_1 + k_2, & \text{hvis } k_1 = k_2. \end{cases}$$

Indtil nu har jeg jo antaget, at $k_i < n_i$, men hvad nu, hvis en sammenhængende matroide $\mathcal{M}$ dekomponerer i to matroider $\mathcal{M}_1, \mathcal{M}_2$, hvor den ene eller begge de to er frie matroider $\mathcal{U}_{n,n}$, hvor alle delmængder er uafhængige. Dette spørgsmål svarer de to næste sætninger på. Først må jeg dog lige vise nogle lemmaer, som svarer til lemmaerne 4.3.1–4.3.10. Disse ekstra lemmaer er ikke vist i [Ng, Walker]. De skriver bare, at det kan vises, at de gælder, så derfor vil jeg nu vise dem. De er for ordens skyld nummereret lemma (4.3.1*) — lemma (4.3.10*), så man kan sammenligne med de beslægtede lemmaer, de skal ligne.

Lad i det følgende $\mathcal{M} = (V, \mathcal{I})$ være en sammenhængende matroide med stærke sammenhængsklasser V_1, V_2 med

$$\mathcal{M}_1 = \mathcal{M}|_{V_1} = \mathcal{U}_{k_1,n_1}, 1 \leq k_1 < n_1,$$
$$\mathcal{M}_2 = \mathcal{M}|_{V_2} = \mathcal{U}_{k_2,n_2}, 1 \leq k_2 = n_2,$$

dvs. $\mathcal{M}_2$ er en fri matroide på V_2.

Lemma (4.3.1*). *Hvis $\mathcal{M}$ har en cykel af type (m, n) med $mn \neq 0$, så er $m \leq k_1$ og $n \leq k_2$.*

Bevis. Antag at $\mathcal{M}$ har en cykel C af type (m, n) med $m > k_1$. Så er $m \geq k_1 + 1$, og C indeholder derfor en delmængde af type $(k_1 + 1, 0)$, hvilket er en cykel, og det er en modstrid.

Da $n \leq n_2 = k_2$, er $n \leq k_2$. □

Lemma (4.3.2*). *Hvis $\mathcal{M}$ har en cykel af type (m, n), så er enhver delmængde af V af type (m, n) en cykel i V.*

Bevis. Præcis samme bevis som for lemma 4.3.2. □

Lemma (4.3.3*). *Hvis $\mathcal{M}$ har en cykel af type (m, n) og (m', n'), så er enten $m' = m, n' = n$, eller $m' < m, n' > n$, eller $m' > m, n' < n$.*

Bevis. Præcis samme bevis som for lemma 4.3.3. □

Lemma (4.3.4*). *Der er ingen cykler af type (m, n), hvor $m + n > k_1 + k_2$ eller $m + n \leq k_1$ eller $m + n \leq k_2$.*

Bevis. Ifølge lemma 4.3 er $m + n \leq k_1 + k_2$. Det skal nu vises, at der ikke findes cykler af type (m, n) med $m + n \leq k_1$. Jeg laver et induktionsbevis, hvor $P(n)$ er udsagnet "Der findes ingen cykler af type (m, n) med $m + n \leq k_1$."

Først bevises $P(1)$. Antag at der findes en cykel af type $(m, 1)$ med $m + 1 \neq k_1$. Iflg. lemma 4.3 er da alle mængder af denne type cykler i $\mathcal{M}$. Lad da C_1, c_2 være to forskellige cykler af type $(m, 1)$, hvor

$$C_1 = \{x_1, x_2, \ldots, x_m, y\},$$
$$C_2 = \{x_1', x_2, \ldots, x_m, y\},$$

hvor $x_1', x_i \in V_1$, $y \in V_2$, $x_1' \neq x_1$. Så er $y \in C_1 \cap C_2$, og der må findes en cykel $C_3 \subseteq (C_1 \cup C_2)\backslash\{y\} = \{x_1', x_1, x_2, \ldots, x_m\}$. Men da er C_3 af type $(m', 0)$ for et $m' \leq m + 1$. Men pr. antagelse er $m + 1 \leq k_1$, så $m' \leq k_1$, og dermed er C_3 indeholdt i en mængde af type $(k_1, 0)$, hvilket er en modstrid.

Antag nu at $P(n)$ gælder for alle $1 \leq n \leq k$. Dvs. der er ingen cykler af type (m, n) med $m + n \leq k_1$ for alle $1 \leq n \leq k$. Antag at C_1, C_2 er to forskellige cykler af type $(m, k + 1)$ med $m + k + 1 \leq k_1$, hvor

$$C_1 = \{x_1, x_2, \ldots, x_m, y_1, \ldots, y_{k+1}\},$$
$$C_1 = \{x_1', x_2, \ldots, x_m, y_1, \ldots, y_{k+1}\},$$

hvor $x_1' \neq x_1$, $x_1', x_i \in V_1$, $y_j \in V_2$. Så er $y_{k+1} \in C_1 \cap C_2$, og der findes derfor en cykel $C_3 \subseteq (C_1 \cup C_2)\backslash\{y_{k+1}\} = \{x_1', x_1, x_2, \ldots, x_m, y_1, \ldots, y_k\}$. Så må C_3 være af type (m', n'), hvor $m' \leq m+1$, $n' \leq k$, og dermed er $m'+n' \leq m+1+k \leq k_1$. Men pr. induktionsantagelse findes ingen sådan cykel C_3, og derfor findes cyklerne C_1, C_2 heller ikke.

Tilsvarende induktionsbevis kan foretages med induktion i m. Alt forløber tilsvarende, når det skal vises, at $m + n > k_2$. □

Lemma (4.3.5*). *Hvis $\mathcal{M}$ har en cykel af type (m, n), hvor $m + n = k$, så er $k_1 + 1 \leq k \leq k_1 + k_2$, og alle delmængder af type (m', n') med $m' + n' = k$, $0 < m' \leq k_1$, $n' \leq k_2$ er også cykler i $\mathcal{M}$.*

Bevis. Samme bevis som for lemma 4.3.5. Blot skal $m' > 0$, da der ikke findes cykler af type $(0, n')$, fordi $\mathcal{M}_2$ er uniform. □

Lemma (4.3.6*). *Der findes cykler af type (m, n) med $mn \neq 0$.*

Bevis. Som lemma 4.3.6: Da $\mathcal{M}$ er sammenhængende, er hvert par af punkter indeholdt i en cykel. □

Lemma (4.3.7*). *Hvis der findes cykler af type (m, n) og (m', n') med $mn \neq 0$, $m'n' \neq 0$, så er $m + n = m' + n'$.*

Bevis. Samme bevis som for lemma 4.3.7. □

Lemma (4.3.8*). *Hvis $k_1 = k_2$, så opfylder alle cykler af type (m, n) med $mn \neq 0$, at $m + n > k_1 + 1$.*

Bevis. Samme bevis som for lemma 4.3.8. □

Lemma (4.3.9*). *Lad $V = V_1 \cup V_2$ være en disjunkt forening med $|V_1| = n_1$ og $|V_2| = n_2$ og lad C være familien af delmængder af V bestående af*

(a) alle delmængder af kardinalitet $k_1 + 1$, som er indeholdt i V_1, dvs. alle delmængder af type $(k_1 + 1, 0)$,

(b) alle delmængder af type (m, n), hvor $0 < m \leq k_1$, $0 < n \leq k_2$, og $m + n = k$, hvor

$$\begin{cases} k_1 + 1 \leq k \leq k_1 + k_2, & \text{hvis } k_1 > k_2, \\ k_1 + 1 < k \leq k_1 + k_2, & \text{hvis } k_1 = k_2. \end{cases}$$

Så er C mængden af cykler i en matroide på V.

Bevis. Det skal vises, at ethvert par af mængder C_1, C_2 af type (a) eller (b) opfylder betingelserne for at hver cykler i en matroide. Der er tre tilfælde:

(i) C_1, C_2 er begge af type (a): Samme bevis som (i) i beviset for lemma 4.3.9.

(ii) C_1, C_2 er begge af type (b): Lad C_1 være en mængde af type (m_1, n_1) og C_2 en mængde af type (m_2, n_2) med $m_1 + n_1 = m_2 + n_2 = k$ iflg. lemma (4.3.7*), hvor $k_1 + 1 \leq k \leq k_1 + k_2$. (C1) er klart opfyldt, da begge C_1, C_2 har samme kardinalitet k.

Antag først $m_1 = m_2 = m$ og $n_1 = n_2 = n$ og lad C_1, C_2 være to forskellige cykler af type (m, n). Antag at $x \in (C_1 \cap C_2) \cap V_1$. Lad desuden $C' = (C_1 \cup C_2) \setminus \{x\}$. Hvis nu $C_1 \cap V_2 = C_2 \cap V_2$, så er $C_1 \cap V_1 \neq C_2 \cap V_1$, da $C_1 \neq C_2$, og C' er en mængde af type (m', n) med $m' \geq m$. altså indeholder C' en mængde af type (m, n), dvs. (C2) er opfyldt. Hvis $C_1 \cap V_2 \neq C_2 \cap V_2$, er C' en mængde af type (m', n') med $m' \geq m - 1$ og $n' \geq n + 1$. Da indeholder C' en mængde af type $(m - 1, n + 1)$, som dermed også er omfattet af pkt. (c). Dette opfylder derfor (C2). Samme argument kan bruges, hvis $x \in (C_1 \cap C_2) \cap V_2$.

Antag nu $m_1 > m_2$ og $n_1 < n_2$ og lad

$$C_1 = \{x_1, \ldots, x_{m_1}, y_1, \ldots, y_{n_1}\} \quad \text{og} \quad C_2 = \{x'_1, \ldots, x'_{m_2}, y'_1, \ldots, y'_{n_2}\}.$$

Hvis $x_1 = x'_1 \in C_1 \cap C_2$, så er mængden på formen

$$C_3 = \{x_2, \ldots, x_{m_2+1}, y'_1, \ldots, y'_{n_2}\}$$

af type (m_2, n_2) indeholdt i $(C_1 \cup C_2) \setminus \{x_1\}$, hvilket opfylder (C2). Hvis i stedet $y_1 = y'_1 \in C_1 \cap C_2$, er mængden på formen

$$C_3 = \{x_1, \ldots, x_{m_1}, y'_2, \ldots, y'_{n_1+1}\}$$

af type (m_1, n_1) indeholdt i $(C_1 \cup C_2) \setminus \{y_1\}$. Hvis endelig $m_1 < m_2$ og $n_1 > n_2$, kan argumentet fra før vendes og bruges igen.

(iii) C_1 er af type (a), og C_2 er af type (b): Som (v) i beviset for lemma (4.3.9*).

□

Lemma (4.3.10*). *Lad $\mathcal{M}$, V, V_1, V_2 og C være som i lemma (4.3.9*). Så er V_1 og V_2 de stærke sammenhængsklasser i $\mathcal{M}$.*

Bevis. Her skal det vises, at $a \sim b$, hvis og kun hvis a, b begge er indeholdt i enten V_1 eller V_2.

Antag derfor først at $a, b \in V_1$. Så består $\Gamma_a^-(b)$ af

- alle delmængderne af $A \subseteq V_1$ med $|A| = k_1$ og $a, b \notin A$, dvs. mængderne af type $(k_1, 0)$, som ikke indeholder a, b (lemma 4.3.9 (a)),
- mængderne af type $(m-1, n)$, som ikke indeholder a, b, dvs. mængderne B med $|B| = k-1$, $a, b \notin B$ og $|B \cap V_1| = m-1$ og $|B \cap V_2| = n$ (lemma 4.3.9 (c)).

Men det er præcis mængderne i $\Gamma_b^-(a)$, da begge $a, b \in V_1$. Så $a \sim b$.

Hvis $a, b \in V_2$, så er $\Gamma_a^-(b) = \Gamma_b^-(a) = \emptyset$, og dermed er $a \sim b$.

Hvis $\Gamma_a^-(b) \supseteq \Gamma_b^-(a)$, så kan man bruge tilsvarende argumentation som før til at indse, at $B_0 \subseteq A_{m',n'}$ for nogle m', n' med $m' + n' = k$. Der må så gælde $m' - 1 = 0$, $k - 1 = k_2$ og $n' = k_2$, så $k = k_2 + 1$. Så hvis $a \sim b$, skal der altså gælde $\Gamma_a^-(b) = \Gamma_b^-(a)$, dvs. $k_1 = k_2$ og $k = k_1 + 1$. Men dette er i modstrid med den antagelse, der blev gjort i lemma 4.3.9, som siger, at $k > k_1 + 1$, hvis $k_1 = k_2$. Derfor må det gælde, at $a \nsim b$. □

Sætning 4.3.12. *Lad $\mathcal{M}$ være en sammenhængende matroide på V, som dekomponerer i to sammenhængsklasser V_1, V_2 med*

$$\begin{aligned} \mathcal{M}_1 &= \mathcal{M}|_{V_1} = \mathcal{U}_{k_1,n_1}, \quad n_1 > k_1 \geq 1 \\ \mathcal{M}_2 &= \mathcal{M}|_{V_2} = \mathcal{U}_{k_2,n_2}, \quad n_2 = k_2 \geq 1, \qquad \textit{dvs. } \mathcal{M}_2 \textit{ er en fri matroide.} \end{aligned}$$

Så består mængden C af cykler i $\mathcal{M}$ af

(a) alle mængder af type $(k_1 + 1, 0)$,

(b) alle mængder af type (m, n), hvor $1 \leq m \leq k_1$ og $1 \leq n \leq k_2$ med

$$\begin{cases} k_1 + 1 < k \leq k_1 + k_2, & \text{hvis } k_1 \geq k_2 \\ k_2 < k \leq k_1 + k_2, & \text{hvis } k_1 < k_2. \end{cases}$$

Hvis omvendt $V = V_1 \cup V_2$ er en disjunkt forening af to mængder med $|V_1| = n_1$, $|V_2| = n_2$, og hvis C er en familie af delmængder af V bestående af mængder, som opfylder (a) og (b) ovenfor, så er C mængden af cykler i en sammenhængende matroide på V med stærke sammenhængsklasser V_1, V_2.

Bevis. Beviset deles op i fem dele efter udelukkelsesmetoden:

(i) Der er ingen cykler af type $(0,k)$ for alle $1 \leq k \leq k_2$, idet alle delmængder af V_2 er uafhængige.

(ii) Der er ingen cykler af type $(k,0)$ for alle $1 \leq k \leq k_1$, da en mængde af type $(k,0)$ er indeholdt i en cykel af type $(k_1+1,0)$.

(iii) Der er ingen cykler af type (k_1+1,k) for alle $1 \leq k \leq k_2$, da en mængde af type (k_1+1,k) indeholder en cykel af type $(k_1+1,0)$.

(iv) Der er ingen cykler af type (m,n) med $m+n = k_1+1$, hvis $k_1 \geq k_2$, for i så fald ville iflg. lemma 4.3.5 alle mængder af kardinalitet k_1+1 være cykler, og $\mathcal{M}$ ville være en uniform matroide.

(v) Der er ingen cykler af type (m,n) med $m+n = k_2$, hvis $k_1 < k_2$. For da ville der også være cykler af type $(1,k_2-1)$. Lad C_1, C_2 være to cykler af type $(1,k_2-1)$ med

$$C_1 = \{x, y_1, \ldots, y_{k_2-1}\} \quad \text{og} \quad C_2 = \{x, y_1, \ldots, y_{k_2-2}, y'_{k_2-1}\},$$

hvor $x \in V_1$ og $y_i, y'_{k_2-1} \in V_2$. Da $x \in C_1 \cap C_2$, må der findes en cykel $C_3 \subseteq (C_1 \cup C_2)\backslash\{x\} = V_2$, hvilket er en modstrid, da alle delmængder af V_2 er uafhængige.

Så er alle cykler i $\mathcal{M}$ altså af type som i (a) eller (b).

Hvis man omvendt betragter mængderne af type som i (a) eller (b), så definerer de iflg. lemma (4.3.9*) og (4.3.10*) cyklerne i en matroide, som dekomponerer i netop de stærke sammenhængsklasser, der ønskes. □

Sætning 4.3.13. *Der findes ingen sammenhængende matroide $\mathcal{M}$, hvor både $\mathcal{M}_1$ og $\mathcal{M}_2$ er frie matroider.*

Bevis. Antag at der findes en sammenhængende matroide $\mathcal{M}$ på V, som har stærke sammenhængs-klasser V_1, V_2 med $\mathcal{M}_1 = \mathcal{M}|_{V_1} = \mathcal{U}_{k_1,n_1}$, $\mathcal{M}_2 = \mathcal{M}|_{V_2} = \mathcal{U}_{k_2,n_2}$ og $k_i = n_i \geq 1$, $k_1 \geq k_2$, dvs. $\mathcal{M}_1, \mathcal{M}_2$ er frie. Lad C være mængden af cykler i $\mathcal{M}$. Da både $\mathcal{M}_1$ og $\mathcal{M}_2$ er frie, er der iflg. lemma 4.3.2 ingen cykler af type $(k,0)$ for $1 \leq k \leq k_1$ eller af type $(0,k)$ for $1 \leq k \leq k_2$. Der er heller ingen cykler af type $(1,k)$ for $1 \leq k < k_2$, for i så fald ville iflg. lemma 4.3.2 alle mængder af denne type være cykler. Lad nemlig

$$C_1 = \{x_1, y_1, \ldots, y_k\} \quad \text{og} \quad C_2 = \{x_1, y_1, \ldots, y'_k\}, \quad k < k_2.$$

Da $x \in C_1 \cap C_2$, må der findes en cykel $C_3 \subseteq (C_1 \cup C_2)\backslash\{x\} = \{y_1, \ldots, y_k, y'_k\}$. Men det er en modstrid. Af samme grund er der heller ingen cykler af type $(k,1)$ for $1 \leq k \leq k_1$. Iflg. lemma 4.3.3 og lemma 4.3.5 så er der ingen cykler af type (m,n) med $m+n \leq k_1$. Hvis $m+n = k$, må der derfor gælde, at $k_1+1 \leq k \leq k_1+k_2$. Men så er alle mængder af kardinalitet k cykler i $\mathcal{M}$ iflg. lemma 4.3.5, hvilket betyder, at $\mathcal{M}$ er uniform og derfor har netop én stærk sammenhængsklasse. Dette er en modstrid, så $\mathcal{M}$ kan ikke have nogen cykler, og kan derfor heller ikke være sammenhængende. □

De foregående tre sætninger kan kombineres til følgende korollar, som karakteriserer cyklerne i en sammenhængende matroide med netop to stærke sammenhængsklasser:

Korollar 4.3.14. *Hvis $\mathcal{M}$ har to stærke sammenhængsklasser V_1, V_2 med $\mathcal{M}|_{V_1} = \mathcal{M}_1 = \mathcal{U}_{k_1,n_1}$ og $\mathcal{M}|_{V_2} = \mathcal{M}_2 = \mathcal{U}_{k_2,n_2}$, så gælder enten (a) eller (b):*

(a) $n_1 > k_1$, $n_2 > k_2$, $k_1 \geq k_2 \geq 1$, *og cyklerne i $\mathcal{M}$ består af mængderne af type*

(i) $(k_1 + 1, 0)$,

(ii) $(0, k_2 + 1)$,

(iii) (m, n), $1 \leq m \leq k_1$, $1 \leq n \leq k_2$, $m + n = k$, *hvor*

$$\begin{cases} k_1 + 1 \leq k \leq k_1 + k_2, & k_1 > k_2 \\ k_1 + 2 \leq k \leq k_1 + k_2, & k_2 = k_2. \end{cases}$$

(b) $n_1 > k_1$, $n_2 = k_2$, *og cyklerne i $\mathcal{M}$ består af mængderne af type*

(i) $(k_1 + 1, 0)$,

(ii) (m, n), $1 \leq m \leq k_1$, $1 \leq n \leq k_2$, $m + n = k$, *hvor*

$$\begin{cases} k_1 + 2 \leq k \leq k_1 + k_2, & k_1 \geq k_2 \\ k_2 + 1 \leq k \leq k_1 + k_2, & k_1 = k_2. \end{cases}$$

Hvis omvendt $V = V_1 \cup V_2$ er en disjunkt forening med $|V_1| = n_1$, $|V_2| = n_2$, og hvis C er familien af delmængder af V, som opfylder enten (a) eller (b), så er C mængden af cykler i en sammenhængende matroide på V med stærke sammenhængsklasser V_1, V_2. Man skriver da $\mathcal{M} = \mathcal{U}_{k_1,n_1} \oplus^k \mathcal{U}_{k_2,n_2}$.

Hermed er klassen af matroider med netop to stærke sammenhængskomponenter karakteriseret ud fra antallet af cykler af de forskellige typer. Karakteriseringen kan også formuleres ved hjælp af de basen af maksimale uafhængige mængder, som det er gjort i [Ng]:

Sætning 4.3.15. *Lad $\mathcal{M} = \mathcal{U}_{k_1,n_1} \oplus^k \mathcal{U}_{k_2,n_2}$. Så er basen for $\mathcal{M}$ netop mængderne af typerne*

$$\begin{gathered} (k_1, k - k_1 - 1) \\ (k_1 - 1, k - k_1) \\ (k_1 - 2, k - k_1 + 1) \\ \vdots \\ (k - k_2 - 1, k_2). \end{gathered}$$

Bevis. Her benyttes "basis-aksiomet" fra sætning 1.1.11 på side 11. Lad $\mathcal{B}$ være familien af mængder af ovennævnte typer og lad $B_1, B_2 \in \mathcal{B}$ med $B_1 \neq B_2$, og antag at B_1 og B_2 er af samme type (m, n). Lad desuden $x \in B_1 \backslash B_2$. Der gælder også $x \in V_i$ for et $i \in \{1, 2\}$. Da B_1 og B_2 er af samme type, er $|B_1 \cap V_i| = |B_2 \cap V_i|$, og på grund af x's egenskaber må der

findes et element $y \in V_i$ med $y \in B_2 \setminus B_1$. Mængden $(B_1 \cup \{y\}) \setminus \{x\}$ er også af type (m, n) og må derfor være et element i $\mathcal{B}$.

Antag nu at B_1 og B_2 er af forskellige typer, så B_1 er af type (m_1, n_1), og B_2 er af type (m_2, n_2). Antag desuden WLOG at $m_1 > m_2$. Iflg. lemma 4.3.3 er da $n_2 > n_1$, og pr. definition af familien $\mathcal{B}$ er

$$k - k_2 \leq m_1 \leq k_1 \quad \text{samt} \quad k - k_1 - 1 \leq n_1 \leq k_2 - 1.$$

Lad $x \in B_1 \setminus B_2$ og antag, at $x \in V_1$. Da $n_2 > n_1$, findes der et element $y \in V_2$ med $y \in B_2 \setminus B_1$. Mængden $(B_1 \cup y) \setminus \{x\}$ er da af type $(m_1 - 1, n_1 + 1)$, og da

$$m_1 \geq k - k_2 \quad \text{og} \quad n_1 \leq k_2 - 1,$$

er $(B_1 \cup y) \setminus \{x\} \in \mathcal{B}$. Antag nu at $x \in V_2$. Da $n_2 > n_1$, findes der et element $y \in V_2$ med $y \in B_2 \setminus B_1$. Mængden $(B_1 \cup \{y\}) \setminus \{x\}$ er igen af type (m_1, n_1) og tilhører dermed $\mathcal{B}$. Dvs. elementerne i $\mathcal{B}$ opfylder "basis-aksiomet", og $\mathcal{B}$ er derfor mængden af baser for $\mathcal{M}$. □

Endelig tæller [Ng, Walker] antallet af ikke-isomorfe sammenhængende matroider med to uniforme sammenhængskomponenter:

Sætning 4.3.16. *Der er ialt $\kappa(k_1, n_1; k_2, n_2)$ sammenhængende matroider $\mathcal{M}$ på V, som har stærke sammenhængsklasser V_1, V_2 med $\mathcal{M}|_{V_1} = \mathcal{U}k_1, n_1, \mathcal{M}|_{V_2} = \mathcal{U}_{k_2,n_2}$, hvor*

$$\kappa(k_1, n_1; k_2, n_2) = \begin{cases} k_2 - 1 & \text{hvis } k_1 = k_2, \\ \min(k_1, k_2) & \text{hvis } n_i > k_i,\ i = 1, 2, \\ k_j - 1 & \text{hvis } k_i \geq k_j,\ n_i > k_i,\ n_j = k_j, \\ k_i & \text{hvis } k_i < k_j,\ n_i > k_i,\ n_j = k_j \\ 0 & \text{hvis } n_i = k_i. \end{cases}$$

Og så til dette afsnits hovedresultat, som siger, at alle matroider, som dekomponerer i præcis to uniforme sammenhængskomponenter, er secret sharing:

Sætning 4.3.17. *Matroiden $\mathcal{M} = \mathcal{U}_{k_1,n_1} \oplus^k \mathcal{U}_{k_2,n_2}$ er secret sharing.*

Resultatet er opført som et korollar i [Ng], men jeg vil ikke gå nærmere ind i beviset, da det kræver en del arbejde i projektiv geometri, hvilket vil føre forvidt i denne sammenhæng. Dog skal en enkelt vigtig detalje om beviset nævnes: I beviset bruges, at alle matroider med to uniforme sammenhængskomponenter er repræsentérbare over legemer, og så giver den tilstrækkelige betingelse, at matroiderne er secret sharing. Dette er selvfølgelig fuldt gyldigt, men det udvider ikke den tilstrækkelige betingelse ved at tilføje flere matroider til dem, som man allerede ved, er secret sharing. Dog giver det en spændende ny metode, som måske i fremtiden kan bruges til netop dette.

4.3.1 Ideelle access-strukturer med to threshold-komponenter

Resultaterne fra det foregående afsnit om dekomposition af matroider kan ikke overraskende bruges til at definere følgende:

$$^{V}\Gamma^{-} = \bigcup_{s \in V} \Gamma_s^-,$$

dvs. mængden af punkterede cykler (dvs. træer) i den associerede matroide eller sagt på en anden måde; mængden af baser for alle mulige access-strukturer på V. Betragt en ideel access-struktur Γ_a for et $a \in V$. Hvis man udskifter dealeren a med $b \in V$, hvor $b \neq a$, så fås ifølge ombytningsegenskaben en ideel access-struktur Γ_b. Hvis nu a, b tilhører samme stærke sammenhængsklasse, vil Γ_a og Γ_b være isomorfe. Hvis derimod a, b tilhører forskellige stærke sammenhængsklasser, så er Γ_a og Γ_b ikke nødvendigvis isomorfe. Faktisk giver [Ng, Walker] følgende eksempel, hvor dette illustreres:

Eksempel: Lad $V = \{a, b, c, d, e\}$. Ifølge [Ng, Walker] er $\Gamma_a = \{\{b, c\}, \{b, d\}, \{b, e\}\}$ access-strukturen for et ideelt SSS med a som dealer. Dette giver en associeret matroide $\mathcal{M}(\Gamma_a)$, hvor i hvert fald mængderne $\{a, b, c\}, \{a, b, d\}, \{a, b, e\}$ er cykler. Ved brug af kravene til en matroides cykler fra cykel-karakteriseringen, sætning 1.1.9, fås at $\mathcal{M}(\Gamma_a)$ har cyklerne $C = \{\{a, b, c\}, \{a, b, d\}, \{a, b, e\}, \{c, d\}, \{c, e\}, \{d, e\}\}$. Det ses iøvrigt, at $\mathcal{M}(\Gamma_a)$ er sammenhængende. For $\mathcal{M}(\Gamma_a)$ gælder desuden

$$\begin{aligned}
a \sim b &\iff \Gamma_a^-(b) = \{\{c\}, \{d\}, \{e\}\} = \Gamma_b^-(a), \\
a \nsim c &\iff \Gamma_a^-(c) = \{\{b, d\}, \{b, e\}\} \neq \Gamma_c^-(a) = \{\{d\}, \{e\}\}, \\
c \sim d &\iff \Gamma_c^-(d) = \{\{a, b\}, \{e\}\} = \Gamma_d^-(c), \\
c \sim e &\iff \Gamma_c^-(e) = \{\{a, b\}, \{d\}\} = \Gamma_e^-(c), \\
d \sim e &\iff \Gamma_e^-(d) = \{\{a, b\}, \{c\}\} = \Gamma_d^-(e),
\end{aligned}$$

så $\mathcal{M}(\Gamma_a)$ dekomponerer i de to stærke sammenhængsklasser $V_1 = \{a, b\}, V_2 = \{c, d, e\}$. Indsættes nu b som dealer i stedet for a, fås access-strukturen $\Gamma_b = \{\{a, c\}, \{a, d\}, \{a, e\}\}$, der som ventet er isomorf med Γ_a.

Indsættes i stedet c som dealer, fås en access-struktur $\Gamma_c = \{\{a, b\}, \{d\}, \{e\}\}$. Denne access-struktur er ikke isomorf med Γ_a. ◇

Ovenstående eksempel illustrerer den næste sætning om antallet af ikke-isomorfe, sammenhængende, ideelle access-strukturer, hvor den associerede matroide dekomponerer i netop to stærke sammenhængskomponenter:

Sætning 4.3.18. *Der er højst $2\kappa(k_1, n_1; k_2, n_2)$ mulige ikke-isomorfe sammenhængende ideelle access-strukturer Γ_s på $V \setminus \{s\}$ for et $s \in V$ sådan, så V dekomponerer i to stærke sammenhængsklasser V_1, V_2 med $|V_i| = n_i$, og $^{V}\Gamma^{-}|_{V_i} = \left\{A \in {}^{V}\Gamma^{-} \mid A \subseteq V_i\right\}$ præcis består af mængderne af kardinalitet k_i.*

4.4 Dekompositions-konstruktionen

I dette afsnit vil jeg gennemgå en konstruktion af en perfekt access-struktur Γ ud fra et antal ideelle access-strukturer $\Gamma_1, \ldots, \Gamma_N$. Denne konstruktion kaldes i [Stinson] for "The Decomposition Construction". Jeg vil så vise, hvordan denne konstruktion på baggrund af stærk dekomposition faktisk kan benyttes til at konstruere en *ideel* access-struktur Γ, og dette minder jo en del om, hvad der blev vist i afsnit 4.2.

Definition 4.4.1. Antag at Γ er en access-struktur med basis Γ_0 over mængden $\mathcal{K}$ af hemmeligheder. En *ideel $\mathcal{K}$-dekomposition* af Γ_0 er en mængde $\{\Gamma_1, \ldots, \Gamma_N\}$, som opfylder

1. $\Gamma_k \subseteq \Gamma_0$ for alle $1 \leq k \leq N$,
2. $\Gamma_0 = \bigcup_{k=1}^{N} \Gamma_k$,
3. For alle $1 \leq k \leq N$ findes et ideelt SSS med basis Γ_k over $\mathcal{K}$ på mængden af personer $\mathcal{P}_k$, hvor $\mathcal{P}_k = \bigcup_{A \in \Gamma_k} A$.

Betragt en access-struktur Γ med basis Γ_0. Antag, at Γ_0 har en ideel $\mathcal{K}$-dekomposition $\{\Gamma_1, \ldots, \Gamma_N\}$. Hver Γ_k er da en ideel access-struktur på mængden af personer $\mathcal{P}_k \subseteq \mathcal{P}$. Man kan da for hver person $p_i \in \mathcal{P}$ definere størrelsen

$$R_i = \left|\{k \mid p_i \in \mathcal{P}_k\}\right|.$$

Følgende sætning giver information rate'en for et perfekt scheme på en access-struktur ud fra denne access-strukturs ideelle $\mathcal{K}$-dekomposition.

Sætning 4.4.2. *Antag at Γ er en access-struktur med basis Γ_0. Lad $\mathcal{K}$ være en mængde, og antag at $\{\Gamma_1, \ldots, \Gamma_N\}$ er en ideel $\mathcal{K}$-dekomposition af Γ_0. Så eksisterer et perfekt SSS over Γ med information rate $\rho = 1/R$, hvor*

$$R = \max\{R_i \mid 1 \leq i \leq |\mathcal{P}|\}.$$

Bevis. På grund af den ideelle $\mathcal{K}$-dekomposition, findes der ideelle schemes over alle Γ_k, $1 \leq k \leq N$ med hemmeligheder fra $\mathcal{K}$. Det k'te af disse ideelle schemes har mængden $\mathcal{F}^k$ af fordelingsfunktioner.

Der ønskes en konstruktion af et perfekt scheme over Γ med hemmeligheder i $\mathcal{K}$, og mængden af dette schemes fordelingsfunktioner, kaldes $\mathcal{F}$. Antag at dealeren p_0 ønsker at dele hemmeligheden s_0. Han vælger da for alle $1 \leq k \leq N$ en fordelingsfunktion $f^k \in \mathcal{F}^k_{s_0}$ og deler de tilhørende shares ud til personerne i $\mathcal{P}_k$.

Det skal nu vises, at dette scheme er perfekt. Det er klart, at enhver autoriseret delmængde vil finde den rigtige værdi for hemmeligheden. Dette skyldes, at alle Γ_k'erne jo specielt er perfekte access-strukturer. Antag nu, $A \subseteq \mathcal{P}$ er en uautoriseret mængde, dvs. $A \notin \Gamma$. Hver person $p_i \in A$ får nu ialt R_i shares, da han tilhører mængder i netop så mange

af baserne $\Gamma_1, \ldots, \Gamma_N$. Men selvom A nu besidder ialt $\sum_{p_i \in A} R_i$ shares i stedet for kun $|A|$, så kan hver share kun bruges i det scheme, hvorfra den blev uddelt, og disse er alle perfekte. Dvs. A har derfor ingen information om s_0.

Nu skal information rate'en så udregnes. Da hvert komponent-scheme er ideelt, er antallet af mulige shares til hver person

$$|S(p_i)| = |\mathcal{K}|^{R_i} \quad \forall p_i \in \mathcal{P},$$

og der fås

$$\rho_i = \frac{\log_2 |\mathcal{K}|}{\log_2 |S(p_i)|} = \frac{\log_{|\mathcal{K}|} |\mathcal{K}|}{\log_{|\mathcal{K}|} |S(p_i)|} = \frac{1}{R_i},$$

så

$$\rho = \min_{p_i \in \mathcal{P}} \{\rho_i\} = \frac{1}{\max\limits_{p_i \in \mathcal{P}} \{R_i\}} = \frac{1}{R}.$$ □

Generelt kunne der jo godt være flere ideelle $\mathcal{K}$-dekompositioner af en access-struktur, så for fuldstændighedens skyld, refererer jeg her nedenfor, hvordan dekompositions-konstruktionen er formuleret i [Stinson], theorem 11.13. Antag her at der er l ideelle $\mathcal{K}$-dekompositioner af en access-struktur. Ideen er at bruge de l dekompositioner til at lave et scheme med hemmeligheder i $\mathcal{K}^l$.

Sætning 4.4.3 (Dekompositions-konstruktionen). *Antag at Γ er en access-struktur med basis Γ_0, og lad $l \geq 1$ være et helt tal. Lad $\mathcal{K}$ være mængden af nøgler og antag for alle $1 \leq j \leq l$, at $\mathcal{D}_j = \left\{\Gamma_{j,1}, \ldots, \Gamma_{j,n_j}\right\}$ er en ideel $\mathcal{K}$-dekomposition af Γ_0. Lad $\mathcal{P}_{j,k}$ betegne mængden af personer i access-strukturen $\Gamma_{j,k}$. For hver person p_i defineres*

$$R_i = \sum_{j=1}^{l} \left|\{k \mid p_i \in \mathcal{P}_{j,k}\}\right|.$$

Så findes et perfekt SSS over Γ med information rate $\rho = l/R$, hvor

$$R = \max\{R_i \mid 1 \leq i \leq |\mathcal{P}|\}.$$

Da jeg ikke skal bruge ovenstående sætning til noget direkte, men bare har den med for fuldstændighed, så vil jeg ikke give beviset men i stedet henvise til [Stinson], p. 355. For at dele hemmeligheden $s_0 = (s_1, \ldots, s_l)$, deler man s_j ud blandt personerne i $\mathcal{P}_{j,k}$. Information rate'en bestemmes som i beviset for sætning 4.4.2.

Hvis man nu kigger tilbage på stærk sammenhæng fra afsnit 4.2, så er denne type dekomposition jo specielt også en ideel $\mathcal{K}$-dekomposition, og derfor må dekompositions-konstruktionen også kunne bruges her.

Betragt en mængde ideelle og disjunkte access-strukturer $\Gamma_1, \ldots, \Gamma_N$. Disse access-strukturer kan opfattes som en ideel $\mathcal{K}$-dekomposition af access-strukturen $\Gamma = \bigcup_i \Gamma_i$, som opfylder definition 4.4.1, idet kravene 1 og 2 er klart opfyldte og 3 opfyldes, fordi

hver komponent i forvejen er en ideel struktur. Her er så $l = 1$. Idet komponenterne er disjunkte, er $R_i = 1$ for alle i. Derfor er også $R = 1$, og information rate'en bliver $\rho = 1$. Dette betyder, at det nye scheme er ideelt.

Hvis man kunne kæde det ovenstående sammen med stærk sammenhæng således, at $\Gamma_1, \ldots, \Gamma_N$ præcis bliver de stærke sammenhængskomponenter for Γ, så har man fundet en måde at opbygge ethvert ideelt SSS af threshold-komponenter.

Kapitel 5

Sammenfatning

I afsnit 5.1 vil jeg forsøge at skabe et overblik over denne rapports vigtigste resultater samt opridse deres betydning og indbyrdes relationer. Jeg medtager ikke definitioner, da de skulle være forholdsvis lette at finde frem til i selve teksten eller i indekset bagest.

I afsnit 5.2 præsenteres en mulig retning for den videre udvikling i arbejdet på at forbedre den tilstrækkelige betingelse fra sætning 3.3.11 på side 59, idet matroide-dekompositionen giver anledning til en klasse af matroider, som er secret sharing. Det viser sig jo i slutningen af forgående kapitel, at klassen af matroider, som dekomponerer i præcis to uniforme sammenhængskomponenter, alle er secret sharing, da de faktisk er repræsentérbare over legemer.

5.1 Opsummering af resultater

Jeg vil nu opsummere de vigtigste resultater fra de forgående kapitler. I parantes er angivet, hvor i teksten de kommer fra. Jeg har vist nogle grundlæggende egenskaber ved relationerne "$\rightarrow$" og "$\rightrightarrows$" i propositionerne 2.4.9 og 2.4.10, hvilket, jeg vurderer, er vigtigt at få med, da jeg i kombination med de alternative definitioner 2.4.4–2.4.6 bl.a. har brugt dem til at simplificere nogle af beviserne i kapitel 3. Overordnet set er det ikke et hovedresultat i karakteriseringen af ideelle secret sharing schemes, så det står ikke opført herunder som et selvstændigt "resultat".

Det første resultat, som knytter ideel secret sharing sammen med matroider, er første hovedsætning. Her konstrueres til ethvert ideelt SSS en familie af mængder, som viser sig at udgøre en matroide på mængden af personer i schemet (inklusiv dealeren). Denne sætning ([Brickell, Davenport], Theorem 1) er faktisk grundlaget for hele arbejdet i denne rapport:

Resultat 1 (Hovedsætning 1, sætning 3.1.4). *Lad M være et sammenhængende ideelt SSS. Da er mængderne i $D(M) = \{A \subseteq \mathcal{P} \mid \exists y \in A \colon A \setminus \{y\} \rightrightarrows y\}$ de afhængige mængder i en sammenhængende matroide.*

En anden meget vigtig egenskab ved et ideelt SSS er den egenskab, jeg har valgt at kalde ombytningsegenskaben. Uvist af hvilken grund er ombytningsegenskaben heller

ikke formuleret som selvstændig sætning i nogen artikel, jeg har læst, men jeg mener, den er vigtig både for forståelsen og til brug i beviser, hvorfor jeg har valgt at formulere og bevise den som et selvstændigt resultat. Navnet er taget fra Ng-Walkers "exchange property", men deres formulering i [Ng, Walker], Lemma 1, illustrerer ikke så tydeligt, hvad det i grunden er for en egenskab.

Resultat 2 (Ombytningsegenskaben, sætning 3.1.12). *Lad $A \in \Gamma^-_{p_0}$, $p_0 \notin A$ med $p_1 \in A$. Da er $(A \cup \{p_0\}) \backslash \{p_1\} \in \Gamma^-_{p_1}$.*

Umiddelbart har dealeren i et SSS ved *realiseringen* af schemet (dvs. i det øjeblik schemet rent faktisk anvendes) en speciel egenskab eller noget speciel information, som sætter denne person i "centrum" i hele schemet. Dealeren vælger jo den bestemte række i matrixrepræsentationen og kender dermed alle shares samt hemmeligheden s_0. Hvis schemet er ideelt og sammenhængende, har dealeren dog ikke nogen speciel egenskab i selve den kombinatoriske struktur – i hvert fald ikke i forhold til de andre medvirkende personer. Det er klart, at dealeren er den eneste person, som kender den specielle share (eller hemmelighed) s_0, men samme matrixrepræsentation kunne bruges til at konstruere et sammenhængende, ideelt SSS med en hvilken som helst anden person som dealer, hvor hemmeligheden så bare er denne persons share. Denne symmetri er det, som ombytningsegenskaben giver.

Følgende er egentlig en uddybning af 1. hovedsætning, idet cyklerne i den associerede matroide til et SSS nu karakteriseres i forhold til basen for schemets access-struktur. Dette lemma bidrager derfor i stor grad til at forstå konstruktionen af den associerede matroide, og det er et nødvendigt resultat i arbejdet med secret sharing-matroider:

Resultat 3 (Lemma 3.2.2). *Cyklerne i den associerede matroide $\mathcal{T}(M)$ gennem et punkt p udgøres netop af mængderne på formen $A \cup \{p\}$, hvor $A \in \Gamma^-_p$.*

Anden hovedsætning gør en i stand til med rette at tale om *den* associerede matroide til et ideelt SSS. Sætningen siger, at den associerede matroide til et ideelt SSS er entydigt bestemt op til isomorfi. Denne egenskab er i kombination med 1. hovedsætning selvsagt nødvendig, når man ønsker at kortlægge mængden af matroider, som er secret sharing. Uden denne sætning ville man først have været nødt til at bestemme samtlige mulige associeret matroide til hver type af SSS, og disse "typer" er ikke engang kategoriserede. Denne kategorisering kan nu i stedet foretages ved at betragte de forskellige klasser af matroider, som er et væsentligt mere veludviklet emne i matematikken. Derfor har jeg ladet sætningen være en "hovedsætning" i denne rapport. Desuden giver sætningen den vigtige erkendelse, at matroiden alene afhænger af det underliggende SSS's access-struktur, dvs. at et ideelt SSS kan opfattes som en rent kombinatorisk konstruktion. Sætningen er vist som et hovedresultat i [Martin].

Resultat 4 (Hovedsætning 2, sætning 3.2.3). *Lad M være et ideelt SSS for Γ. Så er den associerede matroide $\mathcal{T}(M) = \mathcal{T}(\Gamma)$ uafhængig af M og entydigt bestemt ved Γ.*

Nu hvor hvert ideelt SSS giver anledning til en entydig matroide, vil man forsøge at karakterisere de ideelle schemes ved at karakterisere de fremkomne secret sharing-matroider. Her er det i første omgang vigtigt at notere sig, at det ikke er alle matroider, der

er secret sharing. [Seymour] viste ved hjælp af secret sharing-matricer, at f.eks. Vamos-matroiden ikke er secret sharing.

Det blev klargjort, at der desværre var en fejl i Brickell-Davenports banebrydende artikel, [Brickell, Davenport], endda i et af deres hovedresultater ([Brickell, Davenport], Theorem 2). Selve sætningen er som sagt forkert, men netop det er i sig selv et vigtigt resultat, da det er et faktum, der ikke nævnes i mange artikler om emnet. Så hvis man læser [Brickell, Davenport], men ikke får læst [Simonis, Ashikhmin], hvori fejlen rettes, kan man nemt overse, at sætningen *ikke* gælder:

Resultat 5 (Brickell-Davenports fejlsætning, sætning 3.3.2). *Følgende fejlagtige udsagn fra [Brickell, Davenport], Theorem 2 gælder* ikke*:*

> *"Lad $\mathcal{T} = (V, \mathcal{I})$ være en sammenhængende matroide, som er repræsentérbar over et right nearfield R, og lad $v_0 \in V$. Så findes et sammenhængende ideelt secret sharing scheme M, så $R = \mathcal{K}$, $p_0 = v_0$, $\mathcal{P} = V$, og $D(M)$ er de afhængige mængder i $\mathcal{T}$."*

Fejlen i Brickell-Davenports bevis for ovenstående "sætning" blev som nævnt rettet i [Simonis, Ashikhmin], der endvidere kom med det modeksempel, som jeg også gør rede for i afsnit 3.3.3. I denne forbindelse blev secret sharing-matroiderne faktisk karakteriseret som såkaldte næsten-affine koder. Derfor er følgende et vigtigt resultat:

Resultat 6 (sætning 3.3.10). *$\Gamma(C)$ er access-strukturen for et ideelt SSS, hvis og kun hvis $C \subseteq F^{S'}$ er en næsten-affin kode, hvor $M(C)$ er uden løkker, og*

$$\Gamma^{-}(C) = \{A \subseteq S \mid A' \text{ cykel i } M(C)\}.$$

Dette er jo meget interessant, men desværre er disse koder ikke specielt velkendte fra så mange andre steder i matematikken. Men hvis man kan kortlægge de næsten-affine koder, så har man også den ønskede karakterisering af de ideelle secret sharing schemes.

Den eneste fejl, som Brickell-Davenport begik i deres bevis var egentlig implicit at antage, at der gjaldt venstre-distributet i en bestemt ring, som altså ellers antoges at være et right nearfield! Dette betyder faktisk, at det selv samme bevis kan benyttes til at bevise en lidt svagere sætning, som bare gælder for legemer i stedet for disse right nearfields (legemer uden venstre-distributet). Dette bevis giver følgende sætning, som giver en tilstrækkelig betingelse for secret sharing-matroider:

Resultat 7 (Tilstrækkelig betingelse, sætning 3.3.11). *En sammenhængende matroide $\mathcal{T}$ er den associerede matroide til et sammenhængende m-ideelt SSS, hvis $\mathcal{T}$ er repræsentérbar over et legeme eller en algebra af orden m.*

Denne betingelse er meget praktisk til beviser, men den kan, som det nævnes på side 62, ikke også være nødvendig, idet der findes secret sharing-matroider, som ikke er repræsentérbare over noget legeme. Non-Pappus-matroiden er ifølge [Simonis, Ashikhmin] et eksempel på en sådan matroide.

Nu da ikke alle secret sharing-matroider kan karakteriseres, kunne man som et delresultat studere en klasse af secret sharing-matroider, som man rent faktisk *er* i stand til

at bestemme. Det er de matroider, der siges at være universelt ideelle. Dvs. dem som har den egenskab, at der findes ideelle schemes med shares af vilkårlig kardinalitet, som matroiderne associerer til. Følgende karakterisering af [Beimel, Chor] er desuden smuk, fordi den er så enkel at formulere, og fordi den viser, at matroider, som er både binære og tertiære, besidder overraskende stærke egenskaber.

Resultat 8 (Karakterisering af universelt ideelle access-strukturer, sætning 3.4.2). *En access-struktur* Γ *er universelt ideel, hvis og kun hvis* Γ *er* både *2-ideel* og *3-ideel.*

De næste fire resultater udspringer faktisk af en ny tilgang til secret sharing-matroider og faktisk matroider generelt. I [Ng, Walker] udvikles en dekomposition af matroider, som måske kan vise sig at være særdeles nyttig i arbejdet med at karakterisere secret sharing-matroiderne. Dekompositionen bygger på en bestemt ækvivalensrelation kaldet stærk sammenhæng:

Resultat 9 (Lemma 4.1.2). *Lad* $\mathcal{M} = (V, C)$ *være en matroide. Da er stærk sammenhæng en ækvivalensrelation på* V.

Ovenstående ækvivalensrelation inddeler selvfølgelig matroidens punktmængde i et antal disjunkte ækvivalensklasser $V_1, \ldots, V_N$, og hvis matroiden $\mathcal{M}$ restringeres til hver af disse ækvivalensklasser, fås en mængde matroider $\mathcal{M}_1, \ldots, \mathcal{M}_N$, som man kan sige, at $\mathcal{M}$ dekomponerer i. Strukturen af hver af disse såkaldte stærke sammenhængskomponenter $\mathcal{M}_i$ viser sig faktisk ved hjælp af følgende resultat at være uniform:

Resultat 10 (Sætning 4.1.4). *Restriktionen* $\mathcal{M}_i = \mathcal{M}|_{V_i} = (V_i, C_i)$ *er en uniform matroide, og mængden af cykler er*

$$C_i = \{X \in C \mid X \subseteq V_i\} = \bigcup_{a \in V_i} \left\{ A \cup \{a\} \,\middle|\, A \in {}^{i}\Gamma_a^- \right\}.$$

Dette ser umiddelbart smukt ud, for det viser, at der i en vis forstand kan siges at findes en form for primitive strukturer, som alle secret sharing-matroider – og derfor også alle ideelle access-strukturer – er opbygget af. Disse primitive strukturer er altså uniforme matroider eller med andre ord threshold-strukturer:

Resultat 11 (Sætning 4.2.9). *Koden* C_i *er en MDS-kode, hvor* ${}^{i}\Gamma^-$ *er mængden af MIS'er, dvs. elementerne i* ${}^{i}\Gamma^-$ *er alle af kardinalitet* $H(V_i)/H(s)$*, og enhver delmængde af* V_i *af denne kardinalitet tilhører* ${}^{i}\Gamma^-$.

Der er altså en tæt sammenhæng mellem MDS-koder og threshold-strukturer. Jeg fandt, at der gælder følgende resultat, som brugtes undervejs i arbejdet med dekomposition:

Resultat 12 (Sætning B.1.1). *Der findes en ideel* (t, n)*-threshold access-struktur, hvor* $|\mathcal{K}| = |\mathcal{S}| = q$*, hvis og kun hvis der findes en MDS-kode med parametre* $(n + 1, t, q)$.

Dette er en forbedring i forhold til behandlingen i [Mitchell, Walker, Wild], da det er mere direkte det, som ønskes vist, samt da beviset desuden også er simplere.

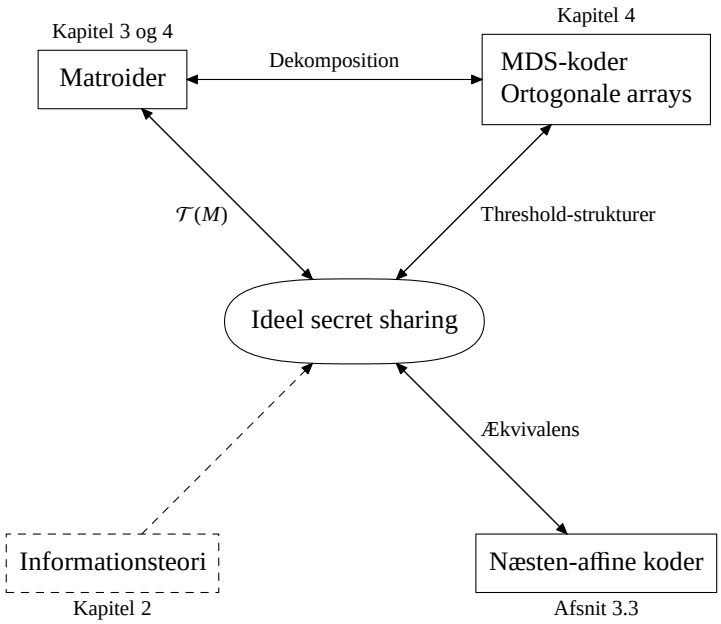
Grunden til, at dekomposition af matroider og secret sharing schemes er spændende, er, at det giver en anderledes måde at opdele matroider på, som ikke blot skelner mellem, om de er repræsentérbare over legemer eller ej. I [Ng] er det i hvert fald anskueliggjort, at dekomposition kan bruges til noget fornuftigt i forhold til at karakterisere de ideelle secret sharing schemes. Dette er iøvrigt det nyeste resultat, jeg har set vedrørende dette emne:

Resultat 13 (Sætning 4.3.17). *Matroiden* $\mathcal{M} = \mathcal{U}_{k_1,n_1} \oplus^k \mathcal{U}_{k_2,n_2}$ *er secret sharing.*

Alle matroider, som dekomponerer i præcis to stærke sammenhængskomponenter er altså secret sharing.

For at danne et overblik og følge op på figuren på side 4 kan man illustrere sammenhængen, jeg er nået frem til, mellem de forskellige matematiske begreber, der er associeret til ideel secret sharing:

Figur 5.1. Begreber relaterede til ideel secret sharing.



Forbindelsen til informationsteori er gjort svagere i figuren for at illustrere, at informationsteorien ikke længere spiller så central en rolle, som den gjorde, før man kendte til korrespondancen mellem ideel secret sharing og matroider og koder samt de alternative definitioner 2.4.5–2.4.6. Når informationsteori stadig er nødvendig fra tid til anden, er det primært til brug i beviser, hvor det kan bruges til at tælle rækker eller shares. Men ved at bruge nogle af resultaterne fra kapitel 3, må dette også kunne gøres helt uden direkte brug af informationsteori.

Jeg vil nu kort opsummere mine egne bidrag til emnet, så det bliver klart for læseren, hvad der er nyt, og hvad der er refereret fra artikler af andre forfattere.

Mine bidrag:

- Eksempel 2.2.3: Dataopbevaring i netværk,
- Ækvivalensen mellem definitionerne 2.4.2–2.4.3 og 2.4.4–2.4.6,
- Formulering og bevis af egenskaberne "punktvis monotoni" og "pseudo-transitivitet" for relationen "$\rightarrow$" samt "punktvis monotoni" og"transitivitet" for relationen "$\rightrightarrows$",
- Formulering og bevis af ombytningsegenskaben, sætning 3.1.12,
- Beviset for ækvivalensen mellem næsten-affin kode-konstruktionen i afsnit 3.3.2 og Brickell-Davenports model for ideel secret sharing.
- Beviserne for lemmaerne (4.3.1*)–(4.3.10*).
- Konstruktion af ideel access-struktur ved hjælp af dekompositions-konstruktionen kombineret med stærk dekomposition.
- Direkte bevis for ækvivalensen mellem ideelle (t, n)-threshold access-strukturer og MDS-koder med parametre $(n + 1, t, q)$.

5.2 Retninger for videre udvikling

Jeg gav i kapitel 3 en tilstrækkelig betingelse for, hvornår en matroide er secret sharing. Den sagde, at en matroide er secret sharing, hvis den er repræsentérbar over et legeme. Denne tilstrækkelige betingelse kan som nævnt ikke også være nødvendig. Man kunne derfor godt tænke sig at udvide mængden af matroider, som er secret sharing – og selvfølgelig helst indtil man har en betingelse, som er både nødvendig og tilstrækkelig, hvorved karakteriseringen er komplet.

Der er dog et par resultater, som udstikker nogle mulige retninger, man kunne gå i det videre arbejde. Det er dels de næsten-affine koder, som [Simonis, Ashikhmin] indførte og så MDS-koder samt dekomposition under stærk sammenhæng, som [Ng, Walker] arbejdede med.

Næsten-affine koder: Det er vist, at et ideelt secret sharing scheme præcis er en næsten-affin kode. Problemet er så bare at karakterisere de matroider, som er næsten-affint repræsentérbare. Dette er et uløst problem, som man passende kunne studere nærmere i fremtiden.

MDS-koder: Det kunne være interessant at studere disse koder lidt mere indgående i forbindelse med secret sharing-matroider, da disse koder åbenbart er uløseligt forbundet med threshold-strukturer, som jo er byggestenene for alle andre sammenhængende ideelle secret sharing schemes. I appendiks A og B redegøres for MDS-kodernes sammenhæng med ideelle threshold-strukturer.

Ortogonale arrays: Gennem appendiks A og B anes det, at der må være tætte bånd mellem de tre objekter, MDS-koder, ortogonale arrays og ideelle threshold-strukturer. Ydermere kunne ortogonale arrays ifølge [Pieprzyk, Xian-Mo 2] være spændende, hvis man vil studere schemes, som skal kunne klare forskellige former for snyd blandt deltagerne eller share recovery.

Dekomposition under stærk sammenhæng: Dekomposition af matroider er et andet emne, som lader til at kunne give nogle brugbare resultater. Jeg har vist, at en matroide, som dekomponerer i N uniforme sammenhængskomponenter under stærk sammenhæng, er secret sharing, hvis $N = 1$, eller $N = 2$. For $N = 1$ er matroiden selv uniform og er dermed repræsentationen af et ideelt threshold-scheme. For $N = 2$ har [Ng] vist, at matroiden er secret sharing. Dette blev opnået ved at vise, at sådanne matroider er repræsentérbare over legemer. Dette resultat udvider jo i sig selv ikke den tilstrækkelige betingelse, men det karakteriserer en spændende klasse af secret sharing-matroider, og det afstikker en ny retning for videre arbejde, idet antallet af stærke sammenhængskomponenter angiver en ny måde at karakterisere matroider.

Det er fortsat et åbent spørgsmål, hvilke egenskaber klassen af matroider med $N = 3$ egentlig har i forhold til det at være secret sharing, så dette bør naturligvis undersøges. For at gøre dette må det klarlægges, hvordan cyklerne i en matroide med tre uniforme sammenhængskomponenter ser ud, og det resultat mangler fortsat. Desuden er uvist, om matroider med tre uniforme sammenhængskomponenter er repræsentérbare over legemer. Vamos-matroiden, som jo var et eksempel på en matroide, som ikke er secret sharing, dekomponerer ifølge [Ng] i fire uniforme sammenhængskomponenter. Det kunne være interessant, hvis der kunne findes uendelige klasser af matroider, som ikke er secret sharing, dvs. hvis man f.eks. kunne vise noget i stil med, at der fandtes et $k > 2$, så ingen matroide med $N \geq k$ er secret sharing. På den måde kunne man måske indskrænke eftersøgningen efter secret sharing-matroider.

Det er også værd at notere sig, at metoden med at undersøge matroiders repræsentérbarhed over legemer ikke i sig selv er nok til at karakterisere secret sharing-matroiderne fuldstændigt, idet der jo findes secret sharing-matroider, som ikke er repræsentérbare over noget legeme. Et nærmere studium i matroider med denne egenskab ville være ønskelig, så man kunne finde frem til, hvilke andre egenskaber disse matroider måtte have tilfælles. På denne måde kunne der måske opstilles en betingelse for, hvornår en matroide, som ikke er repræsentérbar, er secret sharing.

Dekompositions-konstruktion: Som nævnt i afsnit 4.4, så ville det være interessant, hvis der kunne etableres en nærmere sammenhæng imellem ideel $\mathcal{K}$-dekomposition og dekomposition under stærk sammenhæng. Dvs. hvis det ud fra en mængde disjunkte threshold-strukturer $\Gamma_1, \ldots, \Gamma_N$ kunne fastslås, om de også er de stærke sammenhængskomponenter for den ideelle access-struktur Γ, som de giver anledning til ifølge dekompositions-konstruktionen.

Appendiks A

MDS-koder og authentication schemes

Dette appendiks bruges til at vise sætning 4.2.7 på side 81 i afsnit 4.2. Det omhandler authentication schemes, som det er behandlet i [Mitchell, Walker, Wild] og forudsætter en viden om koder. Emnet i appendiksets afsnit A.1 og A.2 hører egentlig sammen med gennemgangen af forbindelsen mellem MDS-koder og access-strukturer i afsnit 4.2, men er af praktiske årsager flyttet og givet sit eget appendiks. Jeg vil nemlig ikke gøre brug af authentication schemes andre steder i rapporten, og det ville bryde afsnit 4.2 på en lidt akavet facon, hvis begrebet skulle defineres og behandles dér. Formålet med dette appendiks er hovedsageligt at bevise sætning 4.2.7, som i dette appendiks benævnes sætning A.2.7.

Afsnit A.3 præsenterer en tæt sammenhæng mellem authentication schemes og ortogonale arrays. Dette kunne være et andet forbindelsesled mellem authentication schemes og MDS-koder, idet de kombinatoriske strukturer i ortogonale arrays og MDS-koder minder meget om hinanden.

A.1 Authentication schemes

Et *authentication scheme* bruges til at sikre ægtheden af beskeder, som modtages over en usikker kanal. Dvs. dels at beskeden har det ægte, oprindelige indhold og dels kommer fra den person, der står som afsender. Følgende scheme kører mellem to personer A og B:

Personerne A og B starter med i hemmelighed at dele en hemmelig nøgle $K \in \mathcal{K}$. Personen A ønsker så at sende en besked med indhold $s \in \mathcal{S}$ til person B. Personerne A og B deler på forhånd en mængde såkaldte authentication rules eller krypteringsregler $\mathcal{E}$, som ved hjælp af nøglen K krypterer alle kildetekstbeskeder, så

$$\forall K \in \mathcal{K}\ \exists e_K \in \mathcal{E},\ \text{så } e_K : \mathcal{S} \to \mathcal{A},$$

hvor $\mathcal{A}$ er mængden af såkaldte *authentication tags*. A sender så beskeden $(s, a) \in \mathcal{S} \times \mathcal{A}$ til B, som verificerer ægtheden ved at kontrollere, at $e_K(s) = a$. På linien kan også sidde en "spoofer" O, som kan opfange alt, hvad der bliver sendt over kanalen, og som også selv kan sende beskeder til B.

Et authentication scheme er altså en tupel $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$, hvis afvikling kan skitseres således:

Afvikling af authentication scheme

1. A og B enes i hemmelighed om en nøgle $K \in \mathcal{K}$.
2. A vælger en kildetekstbesked $s \in \mathcal{S}$, som skal sendes til B. A udregner $a = e_K(s) \in \mathcal{A}$ og sender beskeden $(s, a) \in \mathcal{S} \times \mathcal{A}$ til B.
3. B udregner $a' = e_K(s)$ og accepterer, hvis og kun hvis $a' = a$.

Spooferen O kender dog ikke den hemmelige nøgle K, som A og B deler, og systemet har til formål at forhindre spooferen O i at udføre to typer af angreb:

Impersonation attack O vælger en besked (s', a') og sender denne til B i håb om at få den godkendt som om, at A var afsender.

Substitution attack O opfanger en besked (s, a) afsendt af A. O ændrer denne til (s', a'), hvor $s' \neq s$ og sender denne videre til B i håb om at få den godkendt med A som afsender.

Til hvert af disse angreb kan knyttes en såkaldt *deception probability*, som er defineret som sandsynligheden for, at angrebet lykkes for spooferen O, hvis denne bruger en optimal strategi. Derfor defineres sandsynlighederne Pd_0 for impersonation og Pd_1 for substitution.

[Stinson] definerer følgende generelle deception probability til beregning af Pd_0 og Pd_1. Størrelsen $payoff(s, a)$ for $s \in \mathcal{S}, a \in \mathcal{A}$ er sandsynligheden for, at B accepterer beskeden (s, a):

$$payoff(s, a) \equiv prob(a = e_K(s)) = \sum_{\{K \in \mathcal{K} | e_K(s) = a\}} p_{\mathcal{K}}(K),$$

hvor $p_{\mathcal{K}}$ er sandsynlighedsfordelingen på $\mathcal{K}$. O vil så forsøge at maksimere denne størrelse, så vi får, at

$$Pd_0 = \max\{payoff(s, a) \mid s \in \mathcal{S}, a \in \mathcal{A}\}.$$

Pd_1 er en anelse mere besværlig at beregne. Spooferen opsnapper her en besked (s, a), som han ønsker at substituere med (s', a), hvor $s' \neq s$. Jeg vil ikke gennemgå udregningerne, da de er lidt langtrukne, men iflg. [Stinson] kan Pd_1 findes som

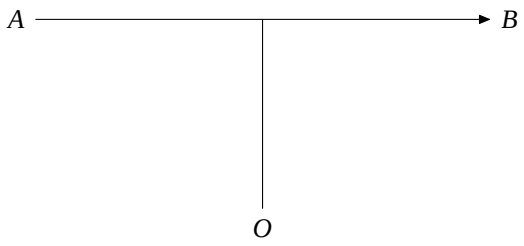
$$Pd_1 = \sum_{(s,a) \in \mathcal{S} \times \mathcal{A}} p_{\mathcal{S}}(s) q_{s,a},$$

hvor

$$q_{s,a} = \max\left\{ \sum_{\{K\in\mathcal{K} | e_K(s)=a, e_K(s')=a'\}} p_{\mathcal{K}}(K) \;\middle|\; s' \in \mathcal{S}, s' \neq s, a' \in \mathcal{A} \right\}.$$

Et authentication scheme kan repræsenteres grafisk som i figur A.1.

Figur A.1. Setup for authentication scheme



Som eksempel på et authentication scheme kan vi betragte følgende matrix, hvor 1. søjle indeholder nøglerne i $\mathcal{K} = \mathbb{Z}_3 \times \mathbb{Z}_3$, og hvor hver af de resterende søjler betegner en kildetekstbesked fra $\mathcal{S} = \mathbb{Z}_3$ med de tilhørende authentication tags:

$$\left[\begin{array}{c|ccc} (0,0) & 0 & 0 & 0 \\ (0,1) & 1 & 1 & 1 \\ (0,2) & 2 & 2 & 2 \\ (1,0) & 0 & 1 & 2 \\ (1,1) & 1 & 2 & 0 \\ (1,2) & 2 & 0 & 1 \\ (2,0) & 0 & 2 & 1 \\ (2,1) & 1 & 0 & 2 \\ (2,2) & 2 & 1 & 0 \\ \hline \mathcal{K} & 0 & 1 & 2 \end{array}\right]$$

Det kan antages, at denne matrix er offentligt kendt blandt både *A, B* og *O*, så det altså kun er nøglen *K*, der er hemmeligt kendt af *A* og *B*.

Antagelser Jeg vil lige gøre et par antagelser om schemets beskaffenhed efter beskrivelsen i [Mitchell, Walker, Wild]. De beskriver et såkaldt "nonsplitting, Cartesian scheme", hvor "nonsplitting" betyder, at authentication tag'et $a \in \mathcal{A}$ til en given kildetekstbesked $s \in \mathcal{S}$ og en given nøgle $K \in \mathcal{K}$ er entydigt bestemt. Givet en nøgle $K \in \mathcal{K}$ kan der altså til enhver kildetekstbesked $s \in \mathcal{S}$ findes et entydigt tag $a = e_K(s) \in \mathcal{A}$. At schemet er kartesisk vil sige, at der til ethvert givet tag a altid kan findes den entydige kildetekstbesked s, som det er en kode af. Også selvom man ikke kender nøglen K, som blev brugt! Til ethvert tag $a \in \mathcal{A}$ findes altså en entydig kildetekstbesked $S(a) \in \mathcal{S}$, hvor $a = e_K(S(a))$ for alle $K \in \mathcal{K}$. ◇

Til et authentication scheme kan der tilordnes en såkaldt *incidence structure* $\mathcal{I} = \mathcal{I}(\mathcal{E}, \mathcal{A}, \|)$, som bygger på en *incidence relation* "$\|$" defineret ved

$$e \| a \iff a = e_K(S(a)).$$

Elementerne i mængden $\mathcal{E}$ kaldes *punkter*, og elementerne i $\mathcal{A}$ kaldes for *blokke*.

Følgende størrelser kan nu defineres:

$$(a) = \{e_K \in \mathcal{E} \mid e_K(S(a)) = a\}$$
$$(e) = \{a \in \mathcal{A} \mid e_K(S(a)) = a\}$$
$$(s) = \{a \in \mathcal{A} \mid S(a) = s\},$$

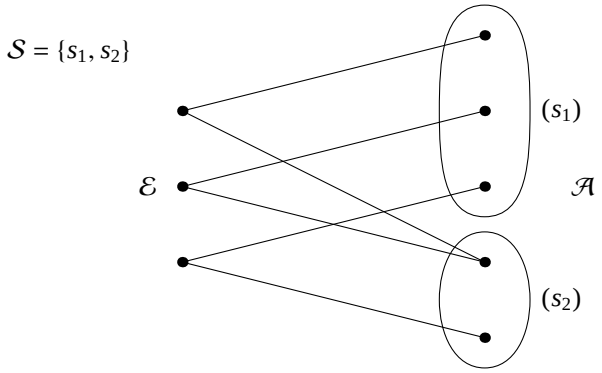
så (a) er mængden af krypteringsregler, som relaterer til a ved relationen "$\|$", (e) er mængden af tags, som relaterer til krypteringsreglen e, og (s) betegner mængden af tags, som hører til kildetekstbeskeden s.

For en incidence structure $\mathcal{I}$ gælder det, at $\{(s) \mid s \in \mathcal{S}\}$ deler $\mathcal{A}$ i $|\mathcal{S}|$ disjunkte klasser, hvor hvert element $e_K \in \mathcal{E}$ relaterer til præcis ét element $e_K(s)$ i hver klasse i $\mathcal{A}$. Dvs. $\{(s) \mid s \in \mathcal{S}\}$ er en såkaldt *parallelisme* på $\mathcal{I}$.

Definition A.1.1. En *parallelisme* på en incidence structure $\mathcal{I}(\mathcal{E}, \mathcal{A}, \|)$ er en deling af mængden af blokke i klasser med den egenskab, at hvert punkt er relateret til præcis én blok i hver klasse ved relationen "$\|$".

Inddelingen beskrevet ovenfor er forsøgt illustreret i figur A.2:

Figur A.2. Eksempel på parallelisme på incidence structure $\mathcal{I}(\mathcal{E}, \mathcal{A}, \|)$



Følgende proposition karakteriserer faktisk de incidence structures, der associerer til et authentication scheme som netop de incidence structures, der har en parallelisme:

Proposition A.1.2. *En incidence structure $\mathcal{I}$ associerer til et authentication scheme, præcis hvis $\mathcal{I}$ har en parallelisme.*

Bevis. Lad først et authentication scheme med incidence structure $\mathcal{I}$ være givet. Det er let at overbevise sig om, at $\{(s) \mid s \in \mathcal{S}\}$ som før nævnt er en parallelisme på $\mathcal{I}$. Det hænger hovedsageligt på, at schemet er nonsplitting.

Lad nu omvendt $\mathcal{I} = \mathcal{I}(P, B, \|)$ være en incidence structure med punktmængde P, blokmængde B og incidence relation "$\|$". Antag at $\mathcal{I}$ har en parallelisme. Antag desuden at der ikke er multible punkter, dvs. antag at der gælder

$$(p) = (p') \Rightarrow p = p'.$$

Der skal konstrueres en krypteringsregel dvs. en afbildning $p : \mathcal{S} \to B$ for hvert $p \in P$. Sæt derfor for hvert $s \in \mathcal{S}$ værdien $p(s)$ til at være den entydigt bestemte blok i klassen (s), som er relateret til p.

Det skal nu checkes, at $(\mathcal{S}, B, \mathcal{K}, P)$ er et authentication scheme med incidence structure $\mathcal{I}(P, B, \mathcal{I})$. Men det er ret simpelt: Det er klart, at hvert tag $p(s)$, dvs. hver blok i B på grund af parallelismen er entydigt bestemt ved s. Eftersom $\{(s) \mid s \in \mathcal{S}\}$ er en parallelisme, og $\mathcal{A}$ som følge deraf opsplitter i disjunkte klasser at tags hørende til hver enkelt kildetekstbesked, så er schemet også kartesisk. □

A.2 Authentication codes

Det kan ofte være nyttigt at repræsentere authentication schemes ved hjælp af koder. Dette gøres i det følgende. Først skal det vises, at der faktisk også kan associeres incidence structures med parallelisme til koder. Lad derfor en kode C af længde r over alfabet $\mathcal{A}$ være givet. Vi kan da konstruere en incidence structure $\mathcal{I}(C)$ med punktmængde bestående af kodeordene i C, og hvor blokkene er tuplerne (i, a), hvor $i \in \{1, \ldots, r\}$ og $a \in \mathcal{A}$. Som med authentication schemes kan der her tænke på en matrix, hvor en række svarer til et punkt/kodeord, og en indgang svarer til en blok. Da defineres incidence relationen mellem et punkt c og en blok (i, a) "$\|$" således:

$$c \| (i, a) \iff c_i = a.$$

Lad så for $j \in \{1, \ldots, r\}$ størrelsen (j) betegne mængden af blokke på formen (j, a). Da er $\{(j) \mid j \in \{1, \ldots, r\}\}$ en parallelisme på $\mathcal{I}(C)$.

Der gælder også den omvendte sammenhæng, idet der til enhver incidence structure $\mathcal{I}$ med en parallelisme kan associeres en kode C med $\mathcal{I}(C) = \mathcal{I}$. Lad derfor $\mathcal{I}(P, B, \|)$ være en incidence structure med parallelisme S. Hvis man sætter $r = |\mathcal{S}|$, kan blokklasserne nummereres $1, \ldots, r$. Der kan arbitrært vælge en passende stor mængde $\mathcal{A}$ således, at der for hver klasse $j \in \{1, \ldots, r\}$ kan laves en injektion $\phi_j : (j) \hookrightarrow \mathcal{A}$. Da ϕ_j er en injektion, kan hver blok $b \in (j)$ nu identificeres som tuplen $\big(j, \phi_j(b)\big)$. For hvert punkt $p \in P$ kan nu defineres et kodeord $(p_1, \ldots, p_r)$, hvor $p_i = \phi_i(b)$, hvor b er den entydigt bestemte blok i klassen i, som er relateret til p. Mængden $C = \{(p_1, \ldots, p_r) \mid p \in P\}$ udgør da en kode af længde r over alfabetet $\mathcal{A}$ med incidence structure $\mathcal{I}(C) = \mathcal{I}$.

Hermed er udledt følgende proposition:

Proposition A.2.1. *En incidence structure $\mathcal{I}$ associerer til en kode C, præcis hvis $\mathcal{I}$ har en parallelisme.*

Da der nu gennem proposition A.1.2 er en korrespondance imellem authentication schemes og incidence structures med parallelismer, og der fra proposition A.2.1 er en korrespondance imellem incidence structures med parallelismer og koder, kan de to propositioner nu kombineres til en sammenhæng imellem authentication schemes og koder:

Korollar A.2.2. *Til ethvert authentication scheme $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ kan tilordnes en kode (*authentication code *i litteraturen) $C(\mathcal{A})$ af længde $|\mathcal{S}|$ bestående af $|\mathcal{E}|$ kodeord over alfabetet $\mathcal{A}$ med $|\mathcal{A}|$ lig med det største antal forskellige tags hørende til en kildetekstbesked $s \in \mathcal{S}$.*

Omvendt kan der til enhver kode C konstrueres et authentication scheme $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ med $C(\mathcal{A}) = C$.

Nu da der er en karakterisering af korrespondancen mellem koder og incidence structures, så vil det være nyttigt at lave en korrespondance imellem MDS-koder[1] og så deres associerede incidence structures.

Jeg vil lige opfriske, hvad en MDS-kode er.

Definition A.2.3. Lad C være en kode af længde r over et alfabet $\mathcal{A}$ med $|\mathcal{A}| = q$. C siges at være en *MDS-kode*, hvis der findes et t, så det for alle t positioner $i_1, \ldots, i_t$ og for alle følger af t elementer $a_1, \ldots, a_t \in \mathcal{A}$ (ikke nødvendigvis forskellige) gælder, at der findes præcis ét kodeord $c = (c_1, \ldots, c_r) \in C$ med $c_{i_j} = a_j$ for alle $j = 1, \ldots, t$. En sådan MDS-kode siges at have parametre (r, t, q).

Notation: Lad desuden $\hat{b} = (b_1, \ldots, b_j)$ være en følge af j blokke fra en incidence structure. Så betegner $\left(\hat{b}\right)$ mængden af punkter, som er relaterede til samtlige blokke $b_1, \ldots, b_j$ fra $\hat{b}$. ◇

Følgende lemma viser, hvordan en MDS-kode $C(\mathcal{I})$ opstår på baggrund af en incidence structure $\mathcal{I}$:

Lemma A.2.4. *Lad C være en MDS-kode med parametre (r, t, q) og lad $\mathcal{I} = \mathcal{I}(C)$ være den associerede incidence structure. Lad desuden $0 \leq j \leq t$ og $\hat{b} = (b_1, \ldots, b_j)$ være en følge af j blokke fra forskellige parallel-klasser. Så er*

$$\left|\left(\hat{b}\right)\right| = q^{t-j}. \tag{A.1}$$

Lad omvendt $\mathcal{I}$ være en incidence structure med en parallelisme, som for et q og et t og for alle $0 \leq j \leq t$ opfylder ligning (A.1). Så er koden $C = C(\mathcal{I})$ en MDS-kode med parametre (r, t, q), hvor r er antallet af parallel-klasser i $\mathcal{I}$.

[1] Se nedenstående definition A.2.3 eller afsnit 4.2

Bevis. Det er relativt simpelt at vise, at ligning (A.1) holder under de givne antagelser. Hvis nemlig $j = t$, så er der pr. definition af MDS-koden præcis 1 mulig vektor (eller kodeord) $\hat{b}$. Hvis $j = t - 1$, vil der nødvendigvis være præcis q forskellige vektorer svarende til antallet af mulige værdier på den sidste position i de kodeord, som $\hat{b}$ er indeholdt i. Og ligeledes hvis $j = t - 2$, så bliver der q^2 muligheder for de to manglende positioner. Dette argument kan fortsættes til $j = 0$ på grund af egenskaben ved MDS-koden.

Lad omvendt $\mathcal{I}$ være en incidence structure med en parallelisme, som for et q og et t og for alle $0 \leq j \leq t$ opfylder ligning (A.1). Lad også $\hat{a} = (a_1, \ldots, a_t)$ være en følge af t blokke fra forskellige parallel-klasser. Så bliver koden $C(\mathcal{I})$ ifølge konstruktionen på side 111 en MDS-kode, når man tæller antallet af kodeord med $j = t$. Man får nemlig, at der i så fald findes præcis én vektor (eller ét kodeord) $\hat{b} = (b_1, \ldots, b_t)$, som har $b_i = a_i$ for alle $i = 1, \ldots, t$. □

Korollar A.2.5. *I en incidence structure, som opfylder betingelserne i lemma A.2.4 ovenfor, indeholder hver parallel-klasse præcis q blokke.*

Bevis. Følger direkte af lemma A.2.4, da ligning (A.1) med $j = t$ kræver, at der er q mulige værdier for hver position, dvs. q forskellige blokke i hver klasse. □

Jeg vil nu gennemgå, hvad et N-perfekt authentication scheme er, for det er den type schemes, dette afsnits hovedresultat drejer sig om. Antag at hver krypteringsregel $e \in \mathcal{E}$ vælges med sandsynlighed $p(e)$, samt at det er tilladt at bruge hver krypteringsregel til at sende højst N beskeder.

Spooferen O observerer n beskeder $(s_1, a_1), \ldots, (s_n, a_n)$ afsendt fra A til B og krypteret med nøglen $e \in \mathcal{E}$, hvor $0 \leq n \leq N$. O skal nu forsøge at konstruere n beskeder $\left(S(a_1), a_1'\right), \ldots, (S(a_n), a_n')$ med $S(a_i) \neq s_i$. Lad $P(n)$ være sandsynligheden for, at dette vil lykkes for O og lad P_N være middelværdien af $P(0), \ldots, P(N)$. I [Walker], Corollary 3 findes en nedre grænse for P_N til at være

$$-\log P_N \leq \frac{H(\mathcal{E})}{N+1} \leq \frac{\log|\mathcal{E}|}{N+1},$$

hvor $H(\mathcal{E})$ er entropien hørende til sandsynlighedsfordelingen $p(e)$.

Et *N-perfekt authentication scheme* kan nu defineres som et scheme med minimal P_N, dvs. hvor der gælder

$$-\log P_N = \frac{\log|\mathcal{E}|}{N+1} \quad \text{eller} \quad P_N = |\mathcal{E}|^{-\frac{1}{N+1}},$$

samt hvor $p(e)$ er den uniforme fordeling.

Følgen af de transmitterede kildetekstbeskeder $s_1 = S(a_1), \ldots, s_n = S(a_n)$ kan af spooferen betragtes som en stokastisk proces $p(s_1, \ldots, s_n)$, hvor $p(s_{n+1} \mid s_1, \ldots, s_n)$ betegner sandsynligheden for, at spooferen efter at have observeret $s_1, \ldots, s_n$ vælger at sende beskeden s_{n+1} i sit angrebsforsøg. Schemet ville være sårbart overfor impersonation attack, hvis man tillod, at den samme besked blev sendt flere gange, idet spooferen da blot behøvede at kopiere en tidligere afsendt besked med tilhørende tag. Man må derfor kræve,

at dette ikke tillades, og det kan derfor antages, at alle kildetekstbeskederne er forskellige. Processen antages altså at opfylde

$$p(s_j \mid s_1, \ldots, s_{j-1}) = 0 \Longleftrightarrow s_j \in \{s_1, \ldots, s_{j-1}\}.$$

Det vil også antages, at udvælgelsen af krypteringsreglen $e_K \in \mathcal{E}$ foregår uafhængigt af den førnævnte kildetekst-udvælgelsesproces. Så sandsynligheden $p(\hat{m})$ for at følgen $\hat{m} = (a_1, \ldots, a_n)$ bliver sendt af A bliver

$$p(\hat{m}) = p(S(\hat{m}))\, p((\hat{m})),$$

hvor

$$\begin{aligned} S(\hat{m}) &= (S(m_a), \ldots, S(m_a)) \\ (\hat{m}) &= \left\{ e_K \in \mathcal{E} \;\middle|\; e_K\left(S(a_j)\right) = a_j,\ j = 1, \ldots, n \right\}. \end{aligned}$$

Hvis desuden $p((\hat{m})) \neq 0$, og $s \in \mathcal{S}$, så kan for alle $a \in (s)$ defineres

$$(s \mid \hat{m}) = \left\{ a \in (s) \;\middle|\; p((a) \mid (\hat{m})) \neq 0 \right\}.$$

Bemærk:

- Mængden $(s \mid \hat{m})$ består af de blokke fra (s), som kan være authentication tags for s, givet at følgen $\hat{m}$ allerede er observeret.
- Hvis $n = 0$, så er $\hat{m}$ den tomme følge, og i så fald består $(s \mid \hat{m})$ af de blokke fra $\mathcal{I}$, der tilhører (s), og som er relaterede til mindst et punkt $e_K \in \mathcal{E}$, hvor $p(e_K) \neq 0$.

Lemma A.2.6. *Et authentication scheme $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ er N-perfekt, hvis og kun hvis der for alle $0 \leq n \neq N$ gælder følgende: Hvis $\hat{m} = (m_1, \ldots, m_n)$ med $p(\hat{m}) \neq 0$, hvis $s \in \mathcal{S}$ med $p(s \mid S(\hat{m})) \neq 0$, og hvis $a \in (s \mid \hat{m})$, så er*

$$\frac{\log|\mathcal{E}|}{N+1} = \frac{H(\mathcal{E})}{N+1} = -\log p((a) \mid (\hat{m})) = \log|(s \mid \hat{m})|. \tag{A.2}$$

Beviset følger af [Walker], Theorem 2, Corollary 3, hvis beviser er baserede på informationsteori.

Sætning A.2.7. *Lad $C = C(\mathcal{A})$ være den associerede kode til et N-perfekt authentication scheme $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$. Så er C en MDS-kode med parametre $(|\mathcal{S}|, N+1, q)$, hvor $q = |(s)|$ for alle $s \in \mathcal{S}$.*

Hvis omvendt C er en MDS-kode med parametre $(r, N+1, q)$, så er $C = C(\mathcal{A})$ for et N-perfekt authentication scheme $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ med $|\mathcal{S}| = r$ og q krypteringer af hver kildetekstbesked.

Bevis. Lad $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ være et N-perfekt authentication scheme og lad $\mathcal{I} = \mathcal{I}(\mathcal{A})$ være dets associerede incidence structure. Benyttes nu lemma A.2.6 med $n = 0$, kan det fastslås, at

$$\log|(s)| = \frac{\log|\mathcal{E}|}{N+1} \qquad \forall s \in \mathcal{S}.$$

Så der er et fast antal q elementer i hver parallel-klasse, hvor $|\mathcal{E}| = q^{N+1}$.

Lad nu $0 \leq j \leq N+1$ og lad $\hat{m} = (a_1, \ldots, a_j)$ være en følge af blokke fra $\mathcal{I}$ hørende til forskellige parallel-klasser. Det skal nu vises, at $|(\hat{m})| = q^{N+1-j}$ ved induktion i j.

Dette er vist for $j = 0$, så antag, at $1 \leq j \leq N+1$ samt, at udsagnet gælder for $j-1$. Lad $(\hat{m}') = (a_1, \ldots, a_{j-1})$. Da udvælgelsen af krypteringsreglerne er uafhængige af beskederne, er

$$p((\hat{m})) = p\left((a_j) \;\middle|\; (\hat{m}')\right) p((\hat{m}')). \tag{A.3}$$

Da sandsynlighedsfordelingen $p(e)$ er uniform, og da $|\mathcal{E}| = q^{N+1}$, er

$$p((\hat{m})) = |(\hat{m})|q^{-(N+1)} \quad \text{og} \quad p((\hat{m}')) = |(\hat{m}')|q^{-(N+1)}.$$

Hvis ligning (A.3) divideres med $q^{-(N+1)}$, får vi $|(\hat{m})| = p\left((a_j) \;\middle|\; (\hat{m}')\right)|(\hat{m}')|$. Ved brug af induktionsantagelsen på $|(\hat{m}')|$ fås

$$|(\hat{m})| = p\left((a_j) \;\middle|\; (\hat{m}')\right) q^{N+1-(j-1)}. \tag{A.4}$$

Nu kan lemma A.2.6 med $n = j-1$ benyttes på $\hat{m}'$ og $s = S(a_j)$, så

$$\log\left|\left(S(a_j) \mid \hat{m}'\right)\right| = \frac{\log|\mathcal{E}|}{N+1} = \log q.$$

Og da $|(S(a_j))| = q$, så er $\left(S(a_j) \mid \hat{m}'\right) = (S(a_j))$. Så er $a_j \in \left(S(a_j) \mid \hat{m}'\right)$, og iflg. lemma A.2.6 er da

$$-\log p\left((a_j) \;\middle|\; (\hat{m}')\right) = \log q,$$

hvilket giver $p\left((a_j) \;\middle|\; (\hat{m}')\right) = q^{-1}$. Dette kan nu indsættes i ligning (A.4), så vi får $|(\hat{m})| = q^{N+1-j}$, hvorved induktionsbeviset er tilendebragt. Det er altså nu vist, at hvis $0 \leq j \leq N+1$, og hvis $\hat{m} = (a_1, \ldots, a_j)$ er en følge af blokke fra $\mathcal{I}$ hørende til forskellige parallel-klasser, så er $|(\hat{m})| = q^{N+1-j}$, og iflg. lemma A.2.4 er $C(\mathcal{I})$ en MDS-kode.

Lad nu omvendt $\mathcal{I}(C)$ være en incidence structure associeret til en MDS-kode C og lad $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ være authentication schemet, som er associeret til $\mathcal{I}$. Lad $p(e)$ være den uniforme sandsynlighedsfordeling på mængden $\mathcal{E}$ af punkter i $\mathcal{I}$. Lad desuden $p(s_1, \ldots, s_n)$ være en stokastisk proces defineret på mængden $\mathcal{S}$ af parallel-klasser i $\mathcal{I}$, hvor

$$p(s_j \mid s_1, \ldots, s_{j-1}) = 0 \Longleftrightarrow s_j \in \{s_1, \ldots, s_{j-1}\}.$$

Lad $0 \leq n \leq N+1$ og $\hat{m} = (a_1, \ldots, a_n)$ med $p(\hat{m}) \neq 0$. Lad også $s \in \mathcal{S}$ med $p\left(s \;\middle|\; S(\hat{m})\right) \neq 0$, hvor $S(\hat{m}) = (S(a_1), \ldots, S(a_n))$ og lad $a \in (s \mid \hat{m})$. Da $p(\hat{m}) = p(S(\hat{m}))\, p((\hat{m})) \neq 0$, er alle klasserne $S(a_1), \ldots, S(a_n)$ forskellige. Da desuden $p\left(s \;\middle|\; S(\hat{m})\right) \neq 0$, er klassen s forskellig fra alle $S(a_1), \ldots, S(a_n)$. Så er iflg. lemma A.2.4

$$|(\hat{m})| = q^{N+1-n} \qquad \text{og} \qquad |(\hat{m}, a)| = q^{N+1-n-1},$$

og dermed

$$p\left((a) \;\middle|\; (\hat{m})\right) = \frac{|(\hat{m}, a)|}{|(\hat{m})|} = q^{-1}.$$

Da er $(s \mid \hat{m}) = (s)$. Da $p(e)$ er uniform, er $H(\mathcal{E}) = \log|\mathcal{E}|$, og iflg. lemma A.2.4 er $|\mathcal{E}| = q^{N+1}$, og $|(s)| = q$ iflg. korollar A.2.5. Hermed er betingelserne fra ligning (A.2) i lemma A.2.6 opfyldt, og $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ er et N-perfekt authentication scheme. □

Som nævnt er formålet med dette appendiks at skabe sammenhæng mellem MDS-koder og threshold-strukturer, men sætning A.2.7 handler om authentication schemes, og det er som nævnt i kapitel 4 ikke umiddelbart trivielt, at N-perfekte authentication schemes og ideelle threshold-strukturer er ækvivalente konstruktioner. Et forbindelsesled mellem disse kunne være ortogonale arrays, som beskrives meget kort i afsnit A.3.

A.3 Ortogonale arrays

Authentication schemes repræsenteret som matricer giver en naturlig anledning til at studere de såkaldte ortogonale arrays[2], som defineres således:

Definition A.3.1. Et *ortogonalt array* $OA(q, r, \lambda, t)$ er en $\lambda q^t \times r$-matrix over q symboler, hvor det gælder, at enhver $\lambda q^t \times t$-delmatrix indeholder hver af de q^t mulige rækkervektorer præcis λ gange.

Bemærk, at et ortogonalt array $OA(q, r, 1, 2)$ også er en MDS-kode med parametre $(r, 2, q)$. I eksemplet på et authentication scheme på side 109 indgår f.eks. det ortogonale array $OA(3, 3, 1, 2)$ over $\mathbb{Z}_3$, men det er forholdsvis simpelt at konstruere andre eksempler:

$$OA(3,3,1,2) = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{bmatrix} \quad OA(2,4,2,2) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \quad OA(2,3,1,2) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

De følgende sætninger, som er bevist i [Stinson], giver en karakterisering af authentication schemes ved hjælp af ortogonale arrays:

Sætning A.3.2. *Antag at der findes et ortogonalt array* $OA(q, r, \lambda, 2)$. *Så findes en authentication code* $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ *med* $|\mathcal{S}| = r$, $|\mathcal{A}| = q$, $|\mathcal{K}| = \lambda q^2$, *og* $Pd_0 = Pd_1 = 1/q$.

Og den omvendte sætning:

Sætning A.3.3. *Antag at* $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ *er en authentication code med* $|\mathcal{A}| = q$ *og* $Pd_1 = 1/q$. *Så er* $|\mathcal{K}| = r^2$, *hvis og kun hvis der findes et ortogonalt array* $OA(q, r, 1, 2)$, *hvor* $|\mathcal{S}| = r$, *og* $p_{\mathcal{K}}(K) = 1/q^2$ *for alle nøgler* $K \in \mathcal{K}$.

Denne formuleres også mere generelt i [Stinson]:

[2] Ortogonale arrays er kombinatorisk set ækvivalente med transversale designs og ortogonale latin squares, hvilket jeg ikke vil uddybe.

Sætning A.3.4. *Antag at* $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ *er en authentication code med* $|\mathcal{S}| = r$, $|\mathcal{A}| = q$, *og* $Pd_0 = Pd_1 = 1/q$. *Så er* $|\mathcal{K}| \geq r(q-1)+1$, *hvis og kun hvis der findes et ortogonalt array* $OA(q, r, \lambda, 2)$ *med* $\lambda = \frac{r(q-1)+1}{q^2}$, *og* $p_{\mathcal{K}}(K) = \frac{1}{r(q-1)+1}$ *for alle* $K \in \mathcal{K}$.

Da disse resultater ikke rigtigt ligger i kerneområdet af denne rapport, har jeg ikke givet nogen beviser. Resultaterne er medtaget blot for at påpege, at en sammenhæng mellem de nævnte objekter eksisterer.

Den særligt interesserede læser vil i [Pieprzyk, Xian-Mo 2] kunne finde mere om ortogonale arrays og særligt om deres sammenhæng med ideelle threshold access-strukturer. [Pieprzyk, Xian-Mo 2], Thm. 1 siger f.eks. følgende, hvis bevis jeg ikke vil komme ind på:

Sætning A.3.5. *Et ortogonalt array* $OA(q, n+1, 1, t)$ *udgør en matrixrepræsentation for et ideelt* (t, n)*-threshold scheme.*

Hermed er ortogonale arrays kædet sammen med både N-perfekte authentication schemes og ideelle threshold access-strukturer. Det ville dog føre for vidt at udforske denne forbindelse til bunds i dette speciale. Især da det tyder på, at der er enklere måder at vise, den ønskede ækvivalens mellem threshold-strukturer og MDS-koder. Se appendiks B.

Appendiks B

MDS-koder og threshold-strukturer – et alternativt bevis

I afsnit B.1 studeres sammenhængen mellem threshold-strukturer og MDS-koder. Denne sammenhæng, som den er beskrevet i appendiks A, kan godt virke lidt uigennemskuelig, da hovedparten af afsnittet handler om authentication schemes og strukturer relaterede hertil. Jeg vil derfor her forsøge at vise denne sammenhæng på en mere direkte måde ved hjælp af matrixrepræsentationer. Dette appendiks har til formål at vise sætning 4.2.8 på side 81, som i appendikset her kaldes sætning B.1.1.

B.1 MDS-koder og threshold-strukturer

Dette afsnit har til formål at bevise et brugbart resultat, som bl.a. benyttes i afsnit 4.2. Det drejer sig følgende ækvivalens mellem threshold-strukturer og MDS-koder:

Sætning B.1.1. *Der findes en ideel* (t, n)*-threshold access-struktur, hvor* $|\mathcal{K}| = |\mathcal{S}| = q$*, hvis og kun hvis der findes en MDS-kode med parametre* $(n + 1, t, q)$*.*

Bevis. Lad en MDS-kode C med parametre $(n + 1, t, q)$ være defineret over et alfabet $\mathcal{S}$, som så har $|\mathcal{S}| = q$. Da gælder det pr. definition, at der for alle t positioner $i_1, \ldots, i_t$ og for alle følger $s_1, \ldots, s_t \in \mathcal{S}$, at der findes præcis ét kodeord $c = (c_1, \ldots, c_{n+1})$ med $c_{i_j} = s_j$ for alle $j = 1, \ldots, t$. Betragt en $q^t \times (n + 1)$-matrixrepræsentation M af koden, hvor hvert kodeord er en række i matricen, og hvor hver koordinatposition er en søjle, der opfattes som et element i søjlemængden $\mathcal{P}^* = \mathcal{P} \cup \{p_0\}$, hvor den første søjle benævnes p_0, og søjlerne i $\mathcal{P}$ kaldes $p_1, \ldots, p_n$. Det skal nu vises, at dette er et (t, n)-threshold scheme med M som matrixrepræsentation. I dette scheme skal man tænke på hver søjle i M som en person i $\mathcal{P}^*$ og hver blok i koden/indgang i M som en share. Da $\mathcal{K} = \mathcal{S}$, skal det vises, at schemet er perfekt med den rigtige access-struktur.

Lad derfor $A \subseteq \mathcal{P}$. Hvis $|A| \geq t$, vil enhver delmængde af t personer/koordinatpositioner $\{p_{i_1}, \ldots, p_{i_t}\} \subseteq A$ med deres shares fastlægge en entydig række/kodeord, og dermed er specielt den første position i dette kodeord (svarende til p_0's share) entydigt bestemt.

Antag nu, at $|A| = t - 1$, og lad $p' \in \mathcal{P}^* \setminus A$. Da der for alle share-distributioner $(s_1, \ldots, s_{|A|}) \in S(A)$ til A og for alle mulige shares $s(p') \in S(p') = \mathcal{S}$ til p' findes præcis én række med share-distribution $(s_1, \ldots, s_{|A|}, s(p')) \in S(A \cup \{p'\})$, må det gælde, at der for hver given share-distribution til A findes ialt $|\mathcal{S}| = q$ mulige shares til p'. Der gælder derfor $A \nrightarrow p'$. Dette argument kan gøres generelt, hvis der antages $|A| = t - k$, for $0 \leq k \leq t$. Da finder man, at der for alle $p'_1, \ldots, p'_k \in \mathcal{P}^* \setminus A$ findes q^k mulige forskellige share-distributioner

$$\left(s_1, \ldots, s_{|A|}, s(p'_1), \ldots, s(p'_k)\right) \in S(A \cup \{p'_1, \ldots, p'_k\}),$$

hvilket giver $A \nrightarrow \{p'_1, \ldots, p'_k\}$. Schemet er derfor perfekt. Access-strukturen er således en ideel (t, n)-threshold-struktur.

Lad M være et (t, n)-threshold scheme med p_0 som dealer og $|\mathcal{S}| = |\mathcal{K}| = q$. Man skal også her tænke på M som schemets matrixrepræsentation. Betragt en delmængde af personer $A \subseteq \mathcal{P}$ med $|A| = t$, og antag WLOG at $A = \{p_1, \ldots, p_t\}$. Da er $A \in \Gamma^-_{p_0}$, og iflg. lemma 3.1.7 er så $|S(A)| = q^{|A|}$. Dette betyder, at der for alle følger af t elementer $s_1, \ldots, s_t \in \mathcal{S}$ findes en række i M med $s(p_j) = s_j$ for $j = 1, \ldots, t$.

For at vise, at M repræsenterer en MDS-kode, skal det vises, at der ikke kan være mere end én række med denne egenskab. Antag derfor at der er to sådanne rækker, samt at de adskiller sig ved værdierne i position $p' \in \mathcal{P} \setminus A$. Da $A \in \Gamma^-_{p_0}$, er rækkernes værdi i koordinatposition p_0 entydigt bestemt. Dette kan også formuleres således, at enhver share-distribution $(s_1, \ldots, s_{|A|}) \in S(A)$ til A fastlægger en entydig værdi s_0 for p_0's share. Dvs. i alle de rækker, hvor $s(p_j) = s_j$ for $j = 1, \ldots, |A|$, er også $s(p_0) = s_0$. Så $s(p_j) = s_j$ for $j = 0, 1, \ldots, |A|$.

Da M er et threshold scheme, er f.eks.

$$(A \cup \{p'\}) \setminus \{p_1\} \in \Gamma^-_{p_0},$$

og på grund af ombytningsegenskaben, korollar 3.1.12 på side 51, så kan p_0 og p' ombyttes, så der fås

$$(A \cup \{p_0\}) \setminus \{p_1\} \in \Gamma^-_{p'}.$$

Men hvis der er to mulige værdier for $s(p')$ givet share-distributionen $(s_0, s_2, \ldots, s_t) \in S((A \setminus \{p_1\}) \cup \{p_0\})$, så er $s(p')$ ikke entydigt bestemt, hvilket er i modstrid med, at access-strukturen $\Gamma_{p'}$ iflg. ombytningsegenskaben er ideel. □

Litteratur

[Beimel, Chor] Amos Beimel, Benny Chor, *Universally Ideal Secret Sharing Schemes*, http://www.cs.bgu.ac.il/~beimel/pub.html, IEEE Trans. on Info. Theory, 40(3), pp. 786–794, 1994. Extended abstract i *Advances in Cryptology – Crypto '92 proceedings*, Lecture Notes in Computer Science, vol. 740, Springer Verlag (1993), pp. 183–195.

[Benaloh, Leichter] J. Benaloh, J. Leichter, *Generalized secret sharing and monotone funcitons*, Advances in Cryptology – Crypto '88, Lecture Notes in Computer Science, vol. 403, Springer Verlag (1990), pp. 27–35.

[Brickell, Davenport] Ernest F. Brickell, Daniel M. Davenport, *On the Classification of Ideal Secret Sharing Schemes*, J. Cryptology (1991) 4, pp. 123–134.

[Golić] Jovan Dj. Golić, *On Matroid Characterization of Ideal Secret Sharing Schemes*, J. Cryptology (1998) 11, pp. 75–86.

[Jackson, Martin] Wen-Ai Jackson, Keith M. Martin, *Combinatorial models for perfect secret sharing schemes*, J. Combinatorial Mathematics and Combinatorial Computing, 28 (1998), pp. 249–265.

[Martin] Keith Murray Martin, *Discrete Structures in the Theory of Secret Sharing*, Ph.d. thesis, University of London.

[Mitchell, Walker, Wild] Chris Mitchell, Michael Walker, Peter Wild, *The Combinatorics of Perfect Authentication Schemes*, Siam Journal of Discrete Mathematics, vol. 7, No. 1 (1994), pp. 102–107.

[Ng] Siaw-Lynn. Ng, *A Representation of a Family of Secret Sharing Matroids*, Designs, Codes and Cryptography, 30 (2003), pp. 5–19.

[Ng, Walker] Siaw-Lynn. Ng, Michael Walker, *On the Composition of Matroids and Ideal Secret Sharing Schemes*, Designs, Codes and Cryptography, 24 (2001), pp. 49–67.

[Oxley] James G. Oxley, *Matroid Theory*, Oxford University Press, (1997).

[Pieprzyk, Xian-Mo 1] Josef Pieprzyk, Xian-Mo Zhang, *Ideal Threshold Schemes from MDS Codes*, Proceedings of The 5th International Conference on Information Security and Cryptography (ICISC 2002), November 28-29, 2002, Seoul, Korea, 269-279, `http://www.ics.mq.edu.au/~xianmo/icisc02.ps`.

[Pieprzyk, Xian-Mo 2] Josef Pieprzyk, Xian-Mo Zhang, *Ideal Threshold Schemes from Orthogonal Arrays*, 4th International Conference on Information and Communications Security, ICICS'02, Lecture Notes in Computer Science, 2531, Springer - Verlag, Berlin, Heidelbeg, New York, 2002, 469-479, `http://www.ics.mq.edu.au/~xianmo/icics02.ps`.

[Seymour] P. D. Seymour, *On Secret-Sharing Matroids*, J. Combinatorial Theory, Series B 56, pp. 69–73 (1992).

[Shamir] A. Shamir, *How to share a secret*, Communications of the ACM, 22 (1979), pp. 612–613.

[Shannon1] C. E. Shannon, *A mathematical theory of communication*, Bell Systems Technical Journal, 27 (1948), pp. 379–423, 623–656.

[Shannon2] C. E. Shannon, *Communication theory of secret systems*, Bell Systems Technical Journal, 28 (1949), pp. 656–715.

[Simonis, Ashikhmin] Juriaan Simonis, Alexei Ashikhmin, *Almost affine codes*, Designs, Codes and Cryptography, 14 (1998), pp. 179-197.

[Stinson] Douglas R. Stinson, *Cryptography Theory and Practice*, The CRC Press Series on Discrete Mathematics and Its Applications.

[Tutte] W. T. Tutte, *A Homotopy Theorem for Matroids II*, Transactions of the American Mathematical Society, 88, 1, pp. 161–174 (1958).

[Walker] Michael Walker, *Information-Theoretic Bounds for Authentication Schemes*, J. Cryptology, 2 (1990), pp. 131–143.

[Welsh] D. J. A. Welsh, *Matroid Theory*, Academic Press (1976).

Notation

$\mathcal{A}$	Mængden af authentication tags i et authentication scheme	107
BD(Γ)	Familien af fordelingsfunktioner til BD-ideelle schemes på Γ	40
BS(Γ)	Familien af fordelingsfunktioner til BS-ideelle schemes på Γ	40
C^*	Cocykel i graf	14
C_X	Projektionen af den lineære kode $C \subseteq F^S$ ned på $X \subseteq S$	56
$C(\mathcal{A})$	Authentication code	112
$C(\mathcal{I})$	Koden associeret til incidence structure $\mathcal{I}$	112
D	Dealer i et secret sharing scheme	19
$D(M)$	Delmængderne af personer med en indbyrdes afhængighed	45
$D(\mathcal{T})$	Delmængderne af punkter med en indbyrdes afhængighed i matroiden associeret til et ideelt secret sharing scheme	49
$\mathcal{E}$	Mængden af krypteringsregler i et authentication scheme	107
$G = (V, E)$	Graf med punktmængde V og kantmængde E	13
$H(X)$	Entropien af den stokastiske variabel X	16
$H(XY)$	Entropien af den simultane fordeling på stokastiske variable X, Y	16
$H(X \mid Y)$	Entropien af den stokastiske variabel X givet stokastisk variabel Y	16
$\mathcal{I}$	Familien af uafhængige delmængder i matroiden $\mathcal{T} = (V, \mathcal{I})$	8
$\mathcal{I}\|_A$	Familien af uafhængige delmængder i restringerede matroide $\mathcal{T}\|_A$	9
$\mathcal{I}(\mathcal{E}, \mathcal{A}, \|\|)$	Incidence structure	110
$\mathcal{I}(C)$	Incidence structure associeret til koden C	112
IT(Γ)	Familien af fordelingsfunktioner til IT-ideelle schemes på Γ	40
$\mathcal{K}$	Mængden af hemmeligheder i et secret sharing scheme	19
	Mængden af nøgler i et authentication scheme	107
$\mathcal{M}(C)$	Matroiden som er repræsentérbar over den næsten-affine kode C	56
$\mathcal{M}(G)$	Den grafiske matroide associeret til grafen G	15
$\mathcal{M}^*(G)$	Den cografiske matroide associeret til grafen G	15
$\mathcal{M}_i$	Matroiden $\mathcal{M}$'s i'te uniforme sammenhængskomponent	78
$M(i, p)$	Matrix-elementet $M(i, p)$ i schemets matrixrepræsentation	*Se* $s_{i,p}$
$M(i, A)$	Fordelingerne til $A \subseteq \mathcal{P}$, som stemmer med s_A i række i	*Se* $s_{i,A}$
$n(i, p, X)$	Indgangene i søjle p fra rækker, som stemmer med fordelingen $s_{i,X}$	53
$OA(q, r, \lambda, t)$	Ortogonalt array	116

$\mathcal{P}$	Mængden af personer i et secret sharing scheme	19
$\mathcal{P}^*$	Den "udvidede access-struktur" $\mathcal{P} \cup p_0$ med dealeren p_0	
$payoff(s,a)$	Sandsynligheden for at (s,a) accepteres i et authentication scheme	108
Pd_0	Impersonation probability i authentication scheme	108
Pd_1	Substitution probability i authentication scheme	108
$r(X)$	Dimensionen af projektionen C_X af den lineære kode C ned på X	56
$\mathcal{S}$	Mængden af shares i et secret sharing scheme	19
	Mængden af kildetekstbeskeder i et authentication scheme	107
$s_p \in \mathcal{S}$	Share til person p når rækken er underforstået	19
$s_{i,p} \in \mathcal{S}$	Share til person p i række i	33
$s_A \in S(A)$	Share-fordeling til delmængden $A \subseteq \mathcal{P}$ når rækken er underforstået	33
$s_{i,A} \in \mathcal{S}(A)$	Share-fordeling til delmængden $A \subseteq \mathcal{P}$ i rækken i	33
$S(p) \subseteq \mathcal{S}$	Mængden af mulige shares til person $p \in \mathcal{P}$	32
$S(A) \subseteq \mathcal{S}$	Mængden af mulige shares til delmængden $A \subseteq \mathcal{P}$ af personer	33
$\mathcal{T} = (V, C)$	Matroiden på punktmængden V og mængden af cykler C	11
$\mathcal{T} = (V, \mathcal{I})$	Matroide på punktmængden V og familie af uafhængige delmgd. $\mathcal{I}$	8
$\mathcal{T}\|_A$	$\mathcal{T}\|_A = (A, \mathcal{I}\|_A)$ er matroiden $\mathcal{T} = (V, \mathcal{I})$ restringeret til $A \subseteq V$	9
$\mathcal{T}(M)$	Den associerede matroide til det ideelle scheme M	50
$\mathcal{T}(\Gamma)$	Den associerede matroide til den ideelle access-struktur Γ	53
$\mathcal{U}_{k,n}$	Uniform matroide af rang k	79
$\mathbb{Z}_n$	Restklasseringen $\mathbb{Z}/n\mathbb{Z}$ for $n \in \mathbb{N}$.	

Græske symboler

Γ	Access-struktur i secret sharing scheme med dealeren underforstået	19
Γ^-	Basis for access-strukturen Γ	20
Γ_a^-	Basis for access-strukturen Γ med personen a som dealer	44
	Mængden af a-punkterede cykler i en matroide på V med $a \in V$	76
$\Gamma_a^-(b)$	Mængden af a-punkterede cykler fra Γ_a^-, som ikke indeholder $b \in V$	76
	Mængden af delmængder fra Γ_a^-, som ikke indeholder $b \in \mathcal{P}$	79
${}^i\Gamma_a^-$	Delmængden af basen Γ_a^-, indeholdt i den stærke klasse V_i	77
	Mængden af a-punkterede cykler fra Γ_a^-, indeholdt i klassen V_i	80
${}^i\Gamma^-$	Foreningen af ${}^i\Gamma_a^-$'erne over alle $a \in V_i$	77
	Delmængderne af V_i, som er autoriserede i forhold til en $a \in V_i \setminus A$	80
${}^V\Gamma^-$	Mængden af maksimale træer (punkterede cykler) i den associerede matroide. Mængden af baser for alle mulige access-strukturer på V	95
$\Gamma(C)$	Access-strukturen for schemet over den næsten-affine kode C	58
$\Gamma^-(C)$	Basis for access-strukturen $\Gamma(C)$ over den næsten-affine kode C	58
$\Gamma(G)$	Den grafiske access-struktur hørende til grafen G	63
ρ	Rangfunktion på V i en matroide $\mathcal{T} = (V, \mathcal{I})$	9
$\rho(X)$	Rangen af en delmængde $X \subseteq V$ i en matroide $\mathcal{T} = (V, \mathcal{I})$	8
ρ_i	Information rate for person $p_i \in \mathcal{P}$	31

Indeks