MASTER I ALGEBRA/ALGEBRAISK GEOMETRI

Matroider og lineære koder

Ann-Hege Larsen

1. juni 2005

Matematisk institutt
Universitetet i Bergen
Johannes Bruns gate 12
N-5008 Bergen

Forord

Da var tiden inne til å levere fra seg et halvt års arbeid. Jeg vil aller først takke professor Trygve Johnsen for at han takket ja til å være veilederen min. Han fortjener en stor takk for sitt engasjement og sin evne til å motivere.

Dernest vil jeg rette en spesiell takk til Hege Marie Mandt for å ha gjort oppholdet mitt i Bergen ekstra trivelig.

Framfor alt vil jeg takke min kjære Thomas Opsahl for all støtte, hjelp og omsorg. Til slutt vil jeg takke familie og venner for oppmuntrende ord og støtte.

Bergen, 01.06.05

Ann-Hege Larsen

Innhold

Figurer

Kapittel 1

Innledning

Denne masteroppgaven består i å beskrive grunnleggende teori for lineære koder og for matroider, ved hjelp av eksisterende litteratur. Videre observerer vi og beskriver litt om hvordan de to feltene er knyttet sammen. Det finnes også sammenhenger mellom teori for matroider og for grafer. Grafer utgjør derfor et naturlig eksempelmateriale i beskrivelser av matroider.

Whitney introduserte matroider i 1935 som en abstrakt generalisering av en matrise. De tidligste artiklene om matroider var motivert av lineær algebra, med litt inspirasjon fra grafteorien.

I kapittel 1 lister vi opp definisjoner, begreper og resultater fra grafteori som vi bruker i oppgaven.

Kapittel 2 handler først om grunnleggende teori for matroider. Vi gir eksempler på matroider som kommer fra både matriser og grafer. Rangbegrepet for matroider blir definert. Vi definerer også isomorfe matroider. Det viser seg at to ikke-isomorfe grafer kan få isomorfe matroider. Vi studerer duale matroider. Videre definerer vi matroideoperasjoner som generaliserer operasjoner for grafer. Noen klasser av matroider blir også beskrevet i dette kapitlet. Videre defineres Tuttepolynomet for matroider. Dette polynomet inneholder mye informasjon om matroider. Vi skal dessuten bevise MacWilliams Teorem om vektenumeratoren for koder ved hjelp av Tuttepolynomet.

I kapittel 3 beskriver vi først grunnleggende teori for koder. Vi definerer duale koder. Vi gir MacWilliams Teorem som gir en relasjon mellom vektenumeratorene for en lineær kode og dualkoden. Deretter studerer vi MDS koder. Motivert av applikasjoner i kryptografi definerte Wei i en artikkel i 1991 det generaliserte Hamming vekthierarkiet til en lineær kode. Vi gir Weis generaliseringer av både Hamming vekten og Singletonbegrensningen.

Kapittel 4 gir noen sammenhenger mellom matroider og lineære koder. Vi definerer vektormatroiden til en lineær kode, og gir et eksempel på ikke-ekvivalente koder som får isomorfe matroider. Vi viser at MDS koder korresponderer til uniforme matroider. Vi skal se at dualitet av koder korresponderer til dualitet av matroider. Siden en lineær kode og en vektormatroide korresponderer med hverandre, kan noen begreper og egenskaper for matroider overføres til koder, og omvendt. Vi studerer noen av disse. Vi gir Greenes Teorem som viser at vektenumeratoren for en lineær kode er en spesialisering av Tuttepolynomet til den korresponderende matroiden. Vi beviser MacWilliams

Teorem ved å bruke Greenes Teorem. Dessuten oversetter vi noen kodebegreper til matroidespråk. Inspirert av Wei definerer vi høyere vekter for en matroide.

Kapittel 2

Grunnleggende begreper og notasjon

Alle bevis og resultater i dette kapitlet finnes i [9], [15] eller [19].

2.1 Mengdeteori og algebraiske strukturer

Alle mengdene i denne oppgaven er endelige hvis ikke annet er oppgitt. Vi betegner kardinaliteten til en mengde S ved $|S|$. Hvis S er en mengde av kardinalitet k, så sier vi at S er en k-mengde. 2^S betegner potensmengden bestående av samtlige delmengder av S. For enkelhets skyld kaller vi delmengdene av 2^S for familier.

Gitt en familie $\mathcal{F}$ av delmengder av S. Maksimale elementer av $\mathcal{F}$ er de elementene av $\mathcal{F}$ som ikke er ekte inneholdt i et annet element av $\mathcal{F}$. Minimale elementer av $\mathcal{F}$ er de elementene av $\mathcal{F}$ som ikke ekte inneholder noen elementer av $\mathcal{F}$.

Med ordet **multimengde** mener vi en mengde av elementer der noen elementer kan opptre flere ganger. For eksempel er $\{a, b, c\}$ en mengde, mens $\{a, a, a, b, c, c\}$ er en multimengde.

$\mathbb{N}$ betegner mengden $\{1, 2, \ldots\}$ av positive heltall. Mengden av ikke-negative heltall, heltall og reelle tall er betegnet ved $\mathbb{N} \cup \{0\}$, $\mathbb{Z}$ og $\mathbb{R}$, respektivt.

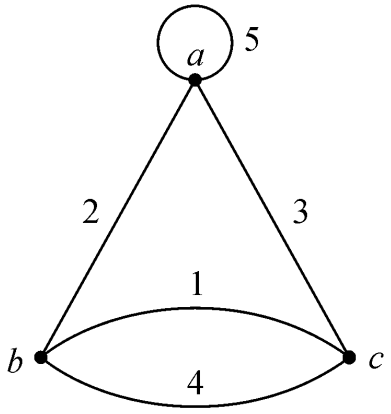
Vi vil betegne en kropp ved $\mathbb{K}$. $\mathbb{F}_q$ betegner den endelige kroppen (opp til isomorfi) med $q = p^m$ elementer, der p er et primtall og $m \in \mathbb{N}$.

Vektorrommet av dimensjon n over $\mathbb{F}_q$ betegnes $\mathbb{F}_q^n$.

2.2 Grafteori

En **graf** er et par $G = (V(G), E(G))$, der $V(G)$ er en ikke-tom endelig mengde av **hjørner** og $E(G)$ er en endelig multimengde av **kanter** som hver består av et *uordnet* par av (ikke nødvendigvis distinkte) hjørner. Figur 2-1 viser en representasjon av en graf som vi skal se mye til senere i oppgaven. Hjørnemengden og kantmengden til denne grafen er $\{a, b, c\}$ og $\{1, 2, 3, 4, 5\}$, respektivt.

La v_1 og v_2 være to hjørner i en graf G. Hvis $e = \{v_1, v_2\}$ er en kant i G, så kaller vi v_1 og v_2 **endepunktene** til e, og vi sier at e er **insident** med v_1 og v_2. Hjørnene v_1 og



Figur 2-1: Grafen G_1.

v_2 er da **naboer** i G. Vi betegner ofte kanten $\{v_1, v_2\}$ ved v_1v_2. En kant med identiske endepunkter er en **løkke**. To kanter med samme endepunkter, som ikke er løkker, sies å være **parallelle** (eller **multiple**). En graf uten løkker og parallelle kanter er **enkel**.

Antall kanter som er insident med et hjørne v kalles **graden til hjørnet** og betegnes $\deg(v)$. Merk at løkker teller dobbelt. Et hjørne med grad 0 kalles **isolert**. En graf G er **regulær** hvis alle hjørnene i G har samme grad.

La G være en graf med m hjørner, $v_1, v_2, \ldots, v_m$, og n kanter, $e_1, e_2, \ldots, e_n$. Vi kan representere G ved en $m \times n$-hjørne-kant insidensmatrise $A_G = [a_{ij}]$, der a_{ij} er antall ganger kanten e_j er insident med v_i. Vi observerer at radene og kolonnene til A_G er indeksert ved henholdsvis hjørnene og kantene i G. Legg merke til at $\deg(v_i)$ er summen av elementene i den i-te raden til A_G. En hjørne-kant insidensmatrise til grafen G_1 i Figur 2-1 er slik:

$$A_{G_1} = \begin{array}{c} \\ a \\ b \\ c \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 0 & 2 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix} \end{array} \tag{2.1}$$

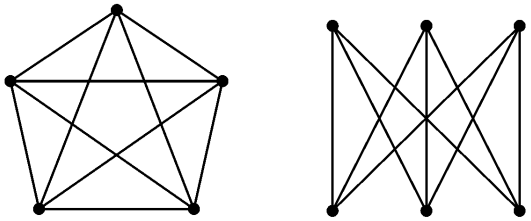
Vi kan få en annen hjørne-kant insidensmatrise til G_1 ved å stokke om elementene i kantmengden eller hjørnemengden.

To grafer G og G' er **isomorfe**, skrevet $G \cong G'$, hvis det eksisterer bijeksjoner $\phi : V(G) \to V(G')$ og $\theta : E(G) \to E(G')$ slik at hjørnet v og kanten e i G er insidente hvis og bare hvis $\phi(v)$ er insident med $\theta(e)$ i G'. To isomorfe grafer betraktes ofte som den samme grafen.

Vi sier at to grafer G og G' er **homeomorfe** hvis det eksisterer en graf H slik at vi kan få (opp til isomorfi) både G og G' fra H ved å sette inn nye hjørner av grad 2 på kantene i H.

En **komplett graf** er en enkel graf der alle mulige hjørnepar er naboer. Den komplette grafen med n hjørner betegnes ved K_n. Vi sier at en enkel graf G er **todelt** (eller **bipartit**) hvis mengden av hjørner kan fordeles i to disjunkte delmengder V_1 og

V_2 slik at hver kant i G forbinder et hjørne i V_1 med et hjørne i V_2. En todelt graf der hvert hjørne i V_1 er forbundet med alle hjørnene i V_2, og omvendt, kalles en **komplett todelt graf**. Vi betegner en slik graf $K_{m,n}$, der $m = |V_1|$ og $n = |V_2|$.



Figur 2-2: a) Grafen K_5. b) Grafen $K_{3,3}$.

En graf H er en **delgraf** av en graf G hvis $V(H) \subseteq V(G)$ og $E(H) \subseteq E(G)$. Hvis $V(H) = V(G)$, så er H en **utspennende delgraf** av G. **Unionen** av to grafer G og G' er grafen $G \cup G'$ med hjørnemengde $V(G) \cup V(G')$ og kantmengde $E(G) \cup E(G')$. Hvis $V(G)$ og $V(G')$ er disjunkte, så er også $E(G)$ og $E(G')$ disjunkte, og vi sier at G og G' er **disjunkte grafer**.

En **sti** i en graf G er en følge $v_0e_1v_1e_2 \cdots v_{k-1}e_kv_k$ der $v_0, v_1, \ldots, v_k$ er distinkte hjørner i G og $e_i = v_{i-1}v_i \in E(G)$ for $i = 1, 2, \ldots, k$. **Lengden** til en sti er antallet kanter på stien. En **krets** av lengde r i G er en følge $v_0e_1v_1e_2 \cdots v_{r-1}e_rv_r$ slik at $v_0e_1v_1e_2 \cdots v_{r-1}$ er en sti, $v_0 = v_r$ og $e_r = v_{r-1}v_r \in E(G)$. Legg merke til at enhver løkke eller ethvert par av parallelle kanter er en krets. En kantmengde $F \in E(G)$ sies å være **uavhengig** hvis F ikke inneholder noen av kretsene i G.

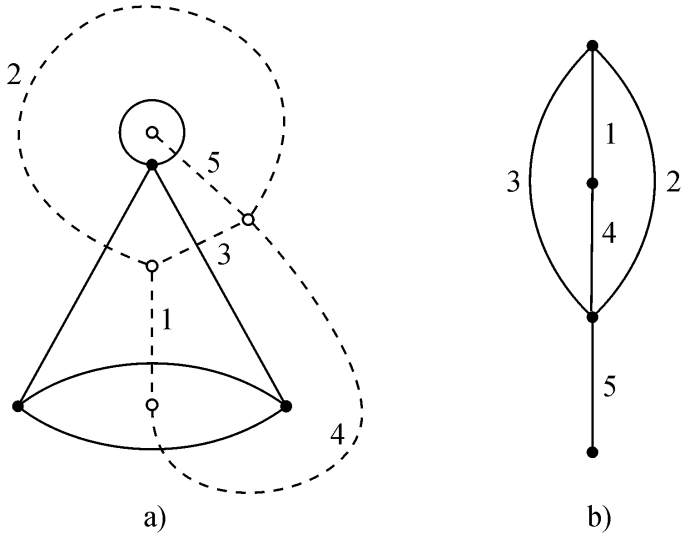
En graf er **sammenhengende** hvis hvert par av distinkte hjørner er forbundet av en sti. En graf som ikke er sammenhengende kalles **usammenhengende**. En **komponent** til en graf G er en maksimal sammenhengende delgraf av G. Merk at vi teller isolerte hjørner som komponenter.

La G være en graf. Hvis $e \in E(G)$, så betegner $G \setminus \{e\}$ delgrafen vi får ved å fjerne e. Tilsvarende kan vi fjerne en mengde F av kanter i G. Denne delgrafen betegnes $G \setminus F$. Hvis $G \setminus F$ har flere komponenter enn G, kalles F en **separerende kantmengde** til G. Merk at en separerende kantmengde til en sammenhengende graf G er en kantmengde slik at hvis den fjernes blir G usammenhengende. En minimal separerende kantmengde kalles en **kokrets** i G. Når en kokrets består av bare en kant, kaller vi denne kanten en **bro**.

Hvis e er en kant i G, så er **kontraksjonen** av e fra G, betegnet ved $G/\{e\}$, grafen vi får ved å fjerne kanten $e = v_1v_2$ og identifisere endepunktene v_1 og v_2 slik at det resulterende hjørnet er insident med de resterende kantene som opprinnelig var insident med v_1 eller v_2. Merk at hvis e er en løkke, så er $G/\{e\} = G \setminus \{e\}$. Hvis $F \subseteq E(G)$, så betegner G/F grafen vi får ved å kontraktere F, det vil si fjerne kantene i F og identifisere hvert par av endepunktene til kantene i F. En graf H sies å være **kontraktibel** til en annen graf G hvis vi kan få G av H ved å suksessivt kontraktere en følge av kanter i H.

En **skog** er en graf som ikke inneholder noen kretser. Legg merke til at hver av kantene i en skog er en bro. En skog med n hjørner og k komponenter har $n-k$ kanter. Et **tre** er en sammenhengende skog. Gitt en sammenhengende graf G. Da er et **utspennende tre** for G en delgraf T av G slik at T er et tre og $V(T) = V(G)$. Et slikt utspennende tre må ha nøyaktig $|V(G)|-1$ kanter. En **utspennende skog** for en vilkårlig graf er den skogen vi får ved å ta et utspennende tre for hver av komponentene i G.

En **planar graf** G er en graf som vi kan tegne i planet uten at noen kanter skjærer hverandre. En slik tegning kaller vi en **plan tegning** (eller **planar representasjon**) av G. Merk at i litteraturen brukes ofte betegnelsen *plan graf* for en plan tegning av en planar graf. Enhver plan tegning av G deler planet inn i et endelig antall **regioner**. To viktige ikke-planare grafer er K_5 og $K_{3,3}$. Kuratowski beviste i 1930 at en graf G er planar hvis og bare hvis den ikke inneholder noen delgraf homeomorf med K_5 eller $K_{3,3}$. Et annet resultat i grafteorien sier at en graf er planar hvis og bare hvis den ikke inneholder noen delgraf som er kontraktibel til K_5 eller $K_{3,3}$.

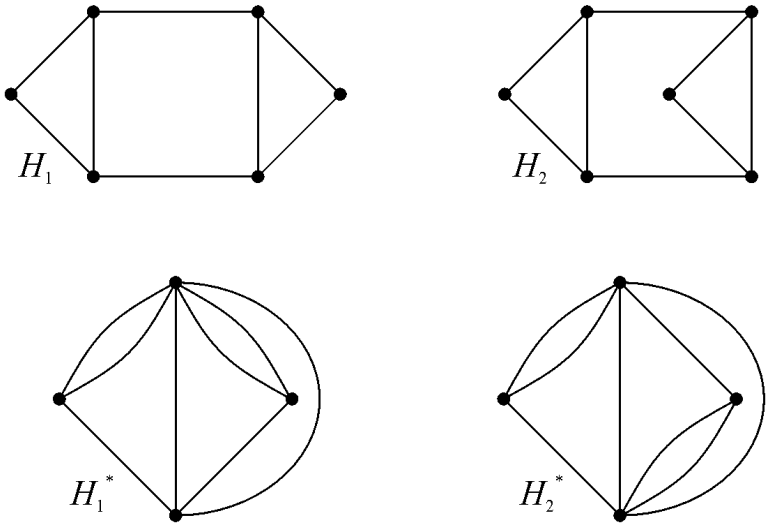


Figur 2-3: a) Konstruksjon av dualen G_1^* til G_1. b) Grafen G_1^*.

La H være en plan tegning av en planar graf G med minst én kant. Vi kan konstruere **den geometriske dualen** til H, betegnet ved H^*, slik:

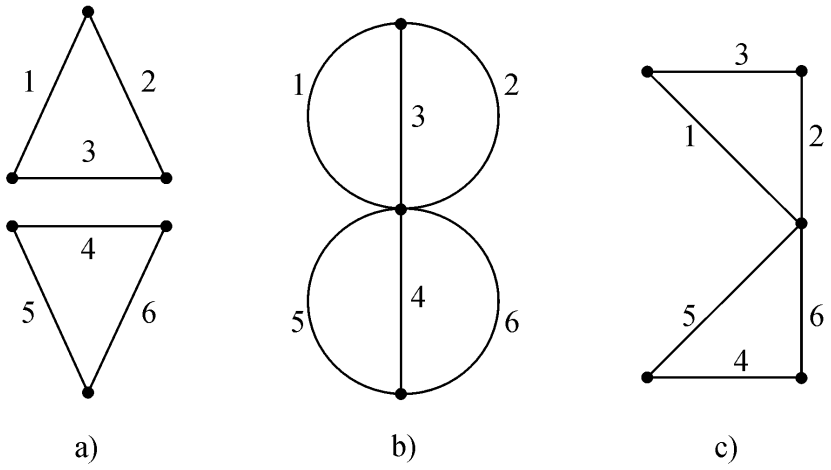
1. Vi setter inn et hjørne $v_R \in V(H^*)$ i hver region R til H.

2. For hver kant e i H gjør vi følgende: Hvis e er en del av grensen mellom to regioner R og R', så forbinder vi v_R og $v_{R'}$ med en kant som krysser ingen andre kanter i H enn e. Hvis e ikke er en del av grensen mellom to regioner, så må den befinne seg i en region R. Da adderer vi en løkke i v_R som krysser e men ingen andre kanter i H eller H^*. Vi gir hver kant i H^* samme betegnelse som kanten den krysser i H. Denne konstruksjonen er illustrert i Figur 2-3 for G_1 i Figur 2-1.



Figur 2-4: En graf kan ha ikke-isomorfe geometriske dualer.

Gitt en planar graf G. En geometrisk dual til G, betegnet ved G^*, er da den geometriske dualen til en plan tegning av G. Merk at siden vi kan ha mange plane tegninger av G, så kan G ha ikke-isomorfe geometriske dualer. Et eksempel som illustrerer dette er gitt i Figur 2-4, der H_1 og H_2 er plane tegninger av den samme grafen, men H_1^* og H_2^* er helt tydelig ikke-isomorfe (H_1^* har et hjørne med grad 6, det har ikke H_2^*).



Figur 2-5: a) H_3. b) H_3^*. c) $(H_3^*)^*$.

Hvis G er sammenhengende, så er $(G^*)^* \cong G$. Dersom G^* er en geometrisk dual til den planare grafen G, så eksisterer det en bijeksjon $\phi : E(G) \to E(G^*)$ slik at X er en krets i G hvis og bare hvis $\phi(X)$ er en kokrets i G^*. Vi antar nå at en slik bijeksjon eksisterer for en vilkårlig graf G^*. Da kalles G^* en **abstrakt dual** til G. Hvis G er en planar graf og G^* er en geometrisk dual til G, så er G^* også en abstrakt dual til G.

Men en abstrakt dual til G trenger ikke å være en geometrisk dual. Av Figur 2-5 kan vi observere at H_3^* er den geometriske dualen til H_3 og at $(H_3^*)^*$ er den geometriske dualen til H_3^*. H_3 er derimot ikke den geometriske dualen til H_3^*, siden $(H_3^*)^* \ncong H_3$. Men siden enhver krets i H_3^* er en kokrets i H_3, så er H_3 en abstrakt dual til H_3^*. Dersom G^* er en abstrakt dual til G, så er G en abstrakt dual til G^*. Welsh beviser i [15] at en graf er planar hvis og bare hvis den har en abstrakt dual.

En **digraf** består av en ikke-tom endelig hjørnemengde $V(D)$ og en endelig multimengde $E(D)$ av *ordnede* par av (ikke nødvendigvis distinkte) hjørner. La v_1 og v_2 være to hjørner i en digraf. Hvis e er en kant som går fra v_1 til v_2, så kalles v_1 og v_2 henholdsvis **start-** og **slutthjørnet**. Vi angir en slik rettet kant (v_1, v_2). Gitt en digraf $D = (V(D), E(D))$. Da kalles grafen $G = (V(G), E(G))$ med $V(G) = V(D)$ og $E(G) = \{\{v_1, v_2\} | (v_1, v_2) \in E(D)\}$ den **underliggende grafen** til D. I dette tilfellet sier vi at D er en **orientering** av G.

Kapittel 3

Matroider

En matroide er en abstrakt mengdeteoretisk konstruksjon. To fundamentale klasser av matroider kommer fra matriser og grafer. Mesteparten av matroideterminologien er bygd på disse to.

Det finnes mange forskjellige, men ekvivalente, måter å definere en matroide på. Vi tar utgangspunkt i en definisjon som kan betraktes som en generalisering av både begrepet lineær uavhengighet kjent fra lineær algebra og uavhengighetsbegrepet kjent fra grafteori. Andre definisjoner vil vi kommentere senere i kapitlet der det er naturlig.

Vi kommer til å definere hva som menes med base og rang for en matroide. Disse begrepene generaliserer basis- og rangbegrepet fra lineær algebra. Motivert av grafteorien definerer vi kretser, løkker og parallelle elementer i en matroide.

Videre skal vi selvfølgelig definere hva vi mener med isomorfe matroider. Vi skal studere duale matroider, samt definere matroideoperasjonene sletting og kontraksjon. Vi skal se nærmere på noen klasser av matroider. Til slutt definerer vi Tuttepolynomet til en matroide.

3.1 Definisjon og noen eksempler

Definisjon 3.1 *La S være en mengde. En **matroide** M på S er et par $(S, \mathcal{I})$, der $\mathcal{I}$ er en familie av delmengder av S med følgende egenskaper:*

(*I1*) $\varnothing \in \mathcal{I}$.

(*I2*) *Hvis $I \in \mathcal{I}$ og $I' \subseteq I$, så er $I' \in \mathcal{I}$.*

(*I3*) *Hvis $I_1, I_2 \in \mathcal{I}$ med $|I_1| < |I_2|$, så eksisterer et element $e \in I_2 - I_1$ slik at $I_1 \cup \{e\} \in \mathcal{I}$.*

*Elementene i $\mathcal{I}$ er de **uavhengige mengdene** til M, og en delmengde av S som ikke er element i $\mathcal{I}$ er **avhengig**. Vi kaller S **grunnmengden** til M.*

Proposisjon 3.2 *Den tredje egenskapen i definisjonen ovenfor, (I3), kan erstattes med følgende ekvivalente egenskap:*

($I3'$) *Hvis $T \subseteq S$, så har alle maksimale delmengder I av T med $I \in \mathcal{I}$ samme kardinalitet.*

Bevis La $\mathcal{I}$ være de uavhengige mengdene til en matroide M. Anta at ($I3$) holder, og anta at I_1 og I_2 er maksimale uavhengige delmengder av $T \subseteq S$. Vi antar, uten tap av generalitet, at $|I_1| < |I_2|$. Da impliserer ($I3$) at det finnes et element $e \in I_2 - I_1$ slik at $I_1 \cup \{e\} \in \mathcal{I}$, men $I_1 \subset I_1 \cup \{e\} \subseteq T$. Dette motsier at I_1 er maksimal. Altså er $|I_1| \geq |I_2|$. Tilsvarende kan vi vise at $|I_2| \geq |I_1|$. Dermed er $|I_1| = |I_2|$. Så ($I3'$) holder.

Anta nå at ($I3'$) holder, og anta at $I_1, I_2 \in \mathcal{I}$ med $|I_1| < |I_2|$. La $T = I_1 \cup I_2$. Siden alle maksimale delmengder av $I_1 \cup I_2$ vil ha den samme kardinaliteten ifølge ($I3'$), kan ikke I_1 være maksimal i T. Det må da finnes elementer $e_i \in T$ slik at $I_1 \cup \{e_i\} \in \mathcal{I}$ er maksimal, og disse e_i-ene er elementer i $I_2 - I_1$ ved kontruksjon. Så ($I3$) holder. ■

Vi skal nå se nærmere på to spesielle typer matroider; vektormatroidene og de uniforme matroidene. La oss starte med matroider som kommer fra vektorer.

Definisjon 3.3 *La $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n$ være vektorer i et vektorrom V. La $S = \{1, 2, \ldots, n\}$, og la $I \subseteq S$ være inneholdt i $\mathcal{I}$ hvis og bare hvis $\{\underline{v}_i \,|i \in I\}$ er lineært uavhengig i V. Da er $M = (S, \mathcal{I})$ en* ***vektormatroide****.*

Bemerkning 3.4 *Legg merke til at konstruksjonen i Definisjon 3.3 ikke krever at $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n$ er distinkte vektorer.*

Det er lett å sjekke at aksiomene for en matroide holder for en vektormatroide. Vi skal nå se at hvis vektorrommet V er mengden $\mathbb{K}^m$ av alle m-tupler av elementer av $\mathbb{K}$ (skrevet som kolonnevektorer), så kan vi representere elementene til matroiden som kolonnene til en $m \times n$-matrise over $\mathbb{K}$.

Proposisjon 3.5 *La A være en $m \times n$-matrise over en kropp $\mathbb{K}$. La S være mengden $\{1, 2, \ldots, n\}$ av indekser for kolonnene til A, og la $\mathcal{I}$ være familien av delmengder I av S slik at multimengden av kolonner med indekser i I er lineært uavhengig i vektorrommet $\mathbb{K}^m$. Da er $(S, \mathcal{I})$ en matroide, som vi kaller vektormatroiden til A og betegner $M[A]$.*

Bevis Dette er Proposisjon 1.1.1 i [9]. Her står også beviset. ■

Eksempel 3.6 *Gitt følgende matrise over $\mathbb{R}$:*

$$A = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

La $S = \{1, 2, 3, 4, 5\}$ være indeksmengden til kolonnene til A. Da er:

$$\mathcal{I} = \{\varnothing, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}.$$

$M[A] = (S, \mathcal{I})$ er vektormatroiden til A. De avhengige mengdene til denne matroiden er:

$$2^S - \mathcal{I} = \{\{5\}, \{1, 4\}, \{1, 5\}, \{2, 5\}, \{3, 5\}, \{4, 5\}\} \cup \{X \subseteq S \,||X| \geq 3\}.$$

En annen viktig matroide defineres slik:

Definisjon 3.7 *La k og n være heltall med $0 \leq k \leq n$. La S være en n-mengde, og la $\mathcal{I} = \{I \subseteq S \,||I| \leq k\}$. Paret $(S, \mathcal{I})$ er en matroide, kalt* ***den uniforme matroiden*** *og betegnet ved $U_{k,n}$.*

Bemerkning 3.8 *$U_{0,0} = (S, \mathcal{I})$, der $S = \varnothing$ og $\mathcal{I} = \{\varnothing\}$ er den unike matroiden på $\varnothing$.*

3.2 Baser

Å definere en matroide M ved å spesifisere alle uavhengige mengder er ikke særlig effektivt. Da er det bedre å liste opp bare de maksimale uavhengige mengdene, så vi introduserer begrepet base.

Definisjon 3.9 *La $M = (S, \mathcal{I})$ være en matroide. En* ***base*** *for M er en maksimal uavhengig delmengde av S.*

Vi betegner familien av baser ved $\mathcal{B}$ eller $\mathcal{B}(M)$. Legg merke til at fra $(I3')$ følger at alle basene for en matroide på S har den samme kardinaliteten.

Eksempel 3.10 *La $M[A] = (S, \mathcal{I})$ være vektormatroiden fra Eksempel 3.6. Da er*

$$\mathcal{B}(M[A]) = \{\{1,2\},\{1,3\},\{2,3\},\{2,4\},\{3,4\}\}.$$

Eksempel 3.11 *Gitt den uniforme matroiden $U_{k,n}$. Det er klart at:*

$$\mathcal{B}(U_{k,n}) = \{X \subseteq S \,||X| = k\}.$$

Definisjon 3.12 *La M være en matroide på grunnmengden S, og la $T \subseteq S$. Vi sier at T er* ***utspennende*** *i M hvis og bare hvis T inneholder en base.*

Det er mulig å definere en matroide ved sin familie av baser, noe som følgende teorem bekrefter.

Teorem 3.13 *La S være en mengde. En ikke-tom familie $\mathcal{B}$ av delmengder av S er mengden av baser til en matroide på S hvis og bare hvis $\mathcal{B}$ har følgende egenskap:*

(B1) Hvis $B_1, B_2 \in \mathcal{B}$ og $x \in B_1 - B_2$, så eksisterer $y \in B_2 - B_1$ slik at $(B_1 \cup \{y\}) - \{x\} \in \mathcal{B}$.

Bevis Dette er Teorem 1.2.1 i [15]. Bevis finnes i [15]. ■

Vi betegner matroiden i Teorem 3.13 $(S, \mathcal{B})$.

3.3 Kretser

Som skrevet er begrepene uavhengighet og base motivert av lineær algebra. Paralleller mellom grafer og matroider er likeledes en kilde til flere begreper i matroideteorien. Et av disse er krets.

Definisjon 3.14 *La $M = (S, \mathcal{I})$ være en matroide. En **krets** i M er en minimal avhengig delmengde av S.*

Vi betegner familien av kretser ved $\mathcal{C}$ eller $\mathcal{C}(M)$.

Eksempel 3.15 *La $M[A]$ være vektormatroiden fra Eksempel 3.6. Da er:*

$$\mathcal{C}(M[A]) = \{\{5\}, \{1,4\}, \{1,2,3\}, \{2,3,4\}\}.$$

Eksempel 3.16 *Gitt den uniforme matroiden $U_{k,n}$. Det er klart at:*

$$\mathcal{C}(U_{k,n}) = \begin{cases} \varnothing & \text{når } k = n, \\ \{X \subseteq S \,||X| = k+1\} & \text{når } k < n. \end{cases}$$

Kjennskap til kretsene, i tillegg til grunnmengden S, er nok til å karakterisere en matroide på S. Følgende resultat kan vi finne som korollar 1.1.5 i [9].

Korollar 3.17 *La $\mathcal{C}$ være en familie av delmengder av en mengde S. Da er $\mathcal{C}$ familien av kretser til en matroide på S hvis og bare hvis $\mathcal{C}$ har følgende egenskaper:*

(C1) $\varnothing \notin \mathcal{C}$.

(C2) Hvis $C_1, C_2 \in \mathcal{C}$ og $C_1 \subseteq C_2$, så er $C_1 = C_2$.

(C3) Hvis $C_1 \neq C_2 \in \mathcal{C}$ og $e \in C_1 \cap C_2$, så eksisterer $C_3 \in \mathcal{C}$ slik at $C_3 \subseteq (C_1 \cup C_2) - \{e\}$.

Bevis Oxley har bevist dette i [9]. Han beviser at disse kretsaksiomene er ekvivalente med uavhengighetsaksiomene i vår Definisjon 3.1. ■

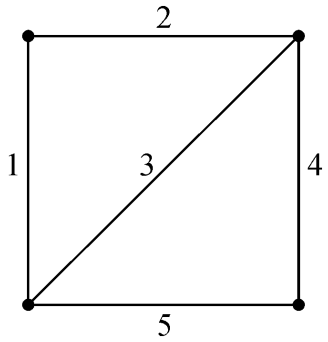
Vi betegner denne matroiden $(S, \mathcal{C})$. For en grafteoretiker er det nok mest naturlig å definere en matroide ved disse kretsaksiomene. Vi er nå klar til å se hvordan vi kan konstruere en matroide fra en graf.

Proposisjon 3.18 *La G være en graf med kantmengde $E(G)$, og la $\mathcal{C}$ være familien av kantmengder til kretser i G. Da er $\mathcal{C}$ mengden av kretser til en matroide på $E(G)$.*

Bevis Vi må vise at $\mathcal{C}$ oppfyller *(C1)*-*(C3)*. Det er klart at $\mathcal{C}$ har egenskapene *(C1)* og *(C2)*. Vi skal nå vise at $\mathcal{C}$ har egenskapen *(C3)*. La C_1 og C_2 være kantmengdene til to distinkte kretser i G som har en felles kant $e = v_1v_2$. Vi skal nå vise at det eksisterer en krets i $C_1 \cup C_2$ som ikke inneholder e. La S_1 være stien mellom v_1 og v_2 i G som har kantmengde $C_1 - \{e\}$, og la S_2 være stien mellom v_1 og v_2 med kantmengde $C_2 - \{e\}$. Vi starter i hjørne v_1 og traverserer så S_1 mot v_2. Vi lar v_3 være det første hjørnet som er med i både S_1 og S_2 og som er slik at den neste kanten i S_1 ikke er med i S_2. Fra

v_3 fortsetter vi å traversere S_1 mot v_2 til vi første gang kommer til et hjørne v_4 ($\neq v_3$) som er med i S_2. Siden både S_1 og S_2 ender i v_2, må det eksistere et slik hjørne. Vi forbinder nå delen av S_1 fra v_3 til v_4 med delen av S_2 fra v_4 til v_3. Resultatet er en krets C_3, og kantmengden til C_3 er inneholdt i $(C_1 \cup C_2) - \{e\}$. Dermed har vi at $\mathcal{C}$ oppfyller (*C3*). ■

Siden $\mathcal{C}$ oppfyller kretsaksiomene (*C1*)-(*C3*) er paret $(E(G), \mathcal{C})$ en matroide. Denne matroiden kalles **kretsmatroiden** til grafen G. Vi betegner den $M(G)$. Det er klart at $I \subseteq E(G)$ er uavhengig i $M(G)$ hvis og bare hvis I er en skog i G. Hvis G er en sammenhengende graf, så er basene for $M(G)$ kantmengdene til utspennende trær for G. Hvis G er usammenhengende, så er basene kantmengdene til utspennende skoger for G.



Figur 3-1: Grafen G_2.

Eksempel 3.19 *La G_2 være grafen vist i Figur 3-1. Kretsmatroiden til G_2 er da $M(G_2) = (S, \mathcal{C})$, der $S = \{1,2,3,4,5\}$ og $\mathcal{C} = \{\{1,2,3\}, \{3,4,5\}, \{1,2,4,5\}\}$.*

3.4 Løkker og parallelle elementer

Begrepene løkke og parallelle kanter kjenner vi fra grafteori. Vi skal nå definere dem for matroider.

Definisjon 3.20 *La $M = (S, \mathcal{I})$ være en matroide. En **løkke** i M er et element $x \in S$ slik at $\{x\}$ er en avhengig mengde. To elementer $x, y \in S$ er **parallelle** hvis $\{x, y\}$ er en avhengig mengde og verken x eller y er løkker.*

Eksempel 3.21 *La M være matroiden gitt i Eksempel 3.6. Da er 5 en løkke i M, siden $\{5\} \notin \mathcal{I}$. 1 og 4 er parallelle elementer, siden $\{1\}, \{4\} \in \mathcal{I}$, mens $\{1,4\} \notin \mathcal{I}$.*

Bemerkning 3.22 *I en vektormatroide er indeksen j en løkke hvis og bare hvis den j-te vektoren er nullvektoren.*

Eksempel 3.23 *Hvis $M(G)$ er kretsmatroiden til en graf G, så korresponderer løkker og parallelle elementer i $M(G)$ til løkker og parallelle kanter i G.*

Vi gir noen enkle resultater om løkker og parallelle elementer:

1. x er en løkke hvis og bare hvis $\{x\}$ er en krets.
2. x er en løkke hvis og bare hvis x ikke er inneholdt i noen baser.
3. Hvis x er en løkke og $x \in T$, så er T avhengig.
4. Distinkte elementer x og y er parallelle hvis og bare hvis $\{x, y\}$ er en krets.
5. Hvis x er parallell med y og y er parallell med z, og $x \neq z$, så er x parallell med z.
6. Hvis T inneholder to parallelle elementer, så må T være avhengig.

Definisjon 3.24 *En **enkel matroide** er en matroide som ikke har noen løkker eller parallelle elementer.*

Eksempel 3.25 *Kretsmatroiden til en enkel graf er et eksempel på en enkel matroide.*

Eksempel 3.26 *Den uniforme matroiden $U_{k,n}$ er enkel for $k \geq 2$.*

3.5 Rangfunksjonen på en matroide

Som en generalisering av rangen til en matrise skal vi nå definere rangen til en matroide. Rangfunksjonen får vi mye bruk for senere i oppgaven.

Definisjon 3.27 *La $M = (S, \mathcal{I})$ være en matroide, og la $T \subseteq S$. **Rangfunksjonen** på M er funksjonen $r : 2^S \to \mathbb{N} \cup \{0\}$ gitt ved*

$$r(T) = \max(|I| \,|\, I \subseteq T, I \in \mathcal{I}).$$

*Vi kaller $r(T)$ **rangen** til T.*

Eksempel 3.28 *Rangen til den tomme mengden er $r(\varnothing) = 0$.*

Bemerkning 3.29 *x er en løkke hvis og bare hvis $r(\{x\}) = 0$. x og y er parallelle hvis og bare hvis $r(\{x\}) = r(\{y\}) = r(\{x, y\}) = 1$.*

Eksempel 3.30 *La A være en $m \times n$-matrise over kroppen $\mathbb{K}$, og la $M[A]$ være matroiden på indeksmengden til kolonnene til A. Da er $r(T)$ rangen til $m \times |T|$-undermatrisen til A som består av de kolonnene til A som har indekser i T. Ekvivalent, $r(T)$ er dimensjonen av underrommet av $\mathbb{K}^m$ som er utspent av kolonnene til A med indekser i T.*

Eksempel 3.31 *La $U_{k,n}$ være den uniforme matroiden på n-mengden S, og la $T \subseteq S$. Da er:*

$$r(T) = \begin{cases} |T| & \text{når } |T| < k, \\ k & \text{når } |T| \geq k. \end{cases}$$

Definisjon 3.32 ***Rangen til en matroide*** *M, betegnet ved $r(M)$, er lik rangen til grunnmengden S.*

Eksempel 3.33 *Vi studerer igjen matroiden M fra Eksempel 3.6. Rangen til M er:*

$$r(M) = \max(|I| \, | \, I \subseteq S, I \in \mathcal{I}) = 2.$$

Bemerkning 3.34 *Rangen til en vektormatroide $M[A]$ er lik rangen til matrisen A.*

Eksempel 3.35 *Rangen til den uniforme matroiden $U_{k,n}$ er lik k.*

Eksempel 3.36 *La $G = (V(G), E(G))$ være en graf. Rangen til matroiden $M(G)$ er $|V(G)| - k(G)$, der $k(G)$ er antallet komponenter til G.*

Vi skal nå se at vi kan karakterisere uavhengige mengder og baser ved hjelp av rangfunksjonen r.

Proposisjon 3.37 *La M være en matroide på S, og la r være rangfunksjonen på M. Anta at $T \subseteq S$. Da har vi følgende:*

i) T er uavhengig hvis og bare hvis $|T| = r(T)$.

ii) T er en base hvis og bare hvis $|T| = r(T) = r(M)$.

Bevis La M være en matroide på S, og anta at $T \subseteq S$. Vi antar at T er uavhengig. Da er $r(T) = \max(|I| \, | \, I \subseteq T, I \in \mathcal{I}) = |T|$. Anta nå at $|T| = r(T)$. Da må $T \in \mathcal{I}$, så T er uavhengig. Dette fullfører beviset av i). Anta at T er en base. Da er $T \in \mathcal{I}$ og T er en maksimal uavhengig delmengde av S. Dermed er $r(M) = \max(|I| \, | \, I \subseteq S, I \in \mathcal{I}) = |T| = r(T)$. Anta at $|T| = r(T) = r(M)$. Siden $r(T) = |T|$, så må $T \in \mathcal{I}$. Siden $r(M) = |T|$, så må T være en maksimal uavhengig delmengde av S. Dermed er T en base. ii) er nå bevist. ■

Det neste teoremet har vi hentet fra [19] (Teorem 30.1).

Teorem 3.38 *En matroide består av en mengde S og en funksjon $r : 2^S \to \mathbb{N} \cup \{0\}$ slik at:*

(R1) $0 \leq r(X) \leq |X|$ *for alle* $X \subseteq S$.

(R2) Hvis $X \subseteq Y \subseteq S$, så er $r(X) \leq r(Y)$.

(R3) Hvis $X, Y \subseteq S$, så er $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$.

Bevis Dette er bevist i [19]. ■

Wilsons bevis av dette teoremet viser at disse rangaksiomene er ekvivalente med aksiomene i Definisjon 3.1, så vi kan altså definere en matroide ved hjelp av denne rangfunksjonen r. Vi betegner en slik matroide (S, r). Welsh gir i Teorem 1.2.2 i [15] følgende alternative rangaksiomer.

Teorem 3.39 *La S være en mengde. En funksjon $r : 2^S \to \mathbb{N} \cup \{0\}$ er rangfunksjonen på en matroide på S hvis og bare hvis følgende er oppfylt for $X \subseteq S$, $x, y \in S$:*

$(R1')$ $r(\varnothing) = 0$.

$(R2')$ $r(X) \leq r(X \cup \{x\}) \leq r(X) + 1$.

$(R3')$ *Hvis $r(X \cup \{x\}) = r(X \cup \{y\}) = r(X)$, så er $r(X \cup \{x\} \cup \{y\}) = r(X)$.*

Bevis Vi finner beviset i [15]. ■

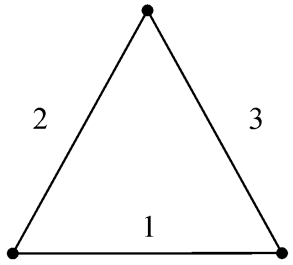
3.6 Isomorfi

Vi skal nå se at to matroider har den samme strukturen hvis det finnes en uavhengighetsbevarende bijeksjon mellom matroidenes grunnmengder.

Definisjon 3.40 *La $M_1 = (S_1, \mathcal{I}_1)$ og $M_2 = (S_2, \mathcal{I}_2)$ være to matroider. M_1 og M_2 er **isomorfe**, betegnet ved $M_1 \cong M_2$, hvis det eksisterer en bijeksjon $\phi : S_1 \to S_2$ slik at $X \in \mathcal{I}_1$ hvis og bare hvis $\phi(X) \in \mathcal{I}_2$ for alle $X \subseteq S_1$.*

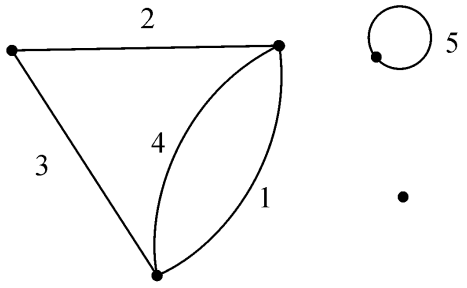
Denne definisjonen er ekvivalent med at det eksisterer en kretsbevarende eller en rangbevarende bijeksjon mellom S_1 og S_2 [15].

Eksempel 3.41 *La G_1 være grafen i Figur 2-1, og la $M(G_1)$ være kretsmatroiden til G_1. Da er $M(G_1) = (S, \mathcal{C})$, der $S = \{1, 2, 3, 4, 5\}$ og $\mathcal{C} = \{\{5\}, \{1, 4\}, \{1, 2, 3\}, \{2, 3, 4\}\}$. Sammenligner vi $M(G_1)$ med matroiden $M[A]$ i Eksempel 3.6, ser vi at, under bijeksjonen $\phi : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ definert ved $\phi(i) = i$, en mengde X er en krets i $M[A]$ hvis og bare hvis $\phi(X)$ er en krets i $M(G_1)$. Ekvivalent, en mengde Y er uavhengig i $M[A]$ hvis og bare hvis $\phi(Y)$ er uavhengig i $M(G_1)$. Vi har altså at $M[A] \cong M(G_1)$.*



Figur 3-2: Den komplette grafen K_3.

Eksempel 3.42 *La K_3 være den komplette grafen vist i Figur 3-2. Da er kretsmatroiden $M(K_3)$ isomorf med den uniforme matroiden $U_{2,3}$.*



Figur 3-3: Grafen G_3.

Vi skal nå se at to ikke-isomorfe grafer kan ha isomorfe kretsmatroider.

Eksempel 3.43 *Grafene i Figur 2-1 og Figur 3-3 er to ikke-isomorfe grafer som har identiske kretsmatroider;* $M(G_1) = M(G_3)$. *Vi kan altså ikke ut fra kretsmatroiden avgjøre om en graf er sammenhengende eller om den har noen isolerte hjørner. Matroideisomorfi trenger heller ikke å bevare antall hjørner i grafen eller gradene til hjørnene.*

Definisjon 3.44 *En matroide* M *er* ***grafisk*** *hvis det eksisterer en graf* G *slik at* M *er isomorf med kretsmatroiden* $M(G)$.

Eksempel 3.45 *Vektormatroiden* $M[A]$ *i Eksempel 3.6 er grafisk.*

Følgende resultat er Proposisjon 1.2.8 i [9].

Proposisjon 3.46 *La* M *være en grafisk matroide. Da er* $M \cong M(G)$ *for en sammenhengende graf* G.

Bevis Dette er bevist i [9]. ■

Definisjon 3.47 *La* $\mathbb{K}$ *være en kropp. Vi sier at en matroide* M *er* ***representabel over*** $\mathbb{K}$ *(eller* $\mathbb{K}$***-representabel***) *hvis* M *er isomorf med vektormatroiden til en matrise* A *over* $\mathbb{K}$. *Matrisen* A *kalles en* ***representasjon*** *for* M ***over*** $\mathbb{K}$ *(eller en* $\mathbb{K}$***-representasjon*** *for* M*).*

Eksempel 3.48 *Kretsmatroiden* $M(G_1)$ *i Eksempel 3.41 er* $\mathbb{R}$*-representabel. Matrisen* A *i Eksempel 3.6 er en representasjon for* $M(G_1)$ *over* $\mathbb{R}$.

Eksempel 3.49 *La* n *være et heltall som er større enn* 1. *Da er* $U_{2,n}$ *representabel over en kropp* $\mathbb{K}$ *hvis og bare hvis* $|\mathbb{K}| \geq n-1$. *(Dette er hentet fra Proposisjon 6.5.2 i [9].)*

La A være en $m \times n$-matrise over kroppen $\mathbb{K}$, og la $M[A]$ være vektormatroiden til A. Da er grunnmengden til $M[A]$ lik indeksmengden for kolonnene til A. Vi kan ikke bestemme en unik A fra $M[A]$. Isomorfiklassen til $M[A]$ forblir uforandret hvis vi utfører følgende operasjoner på A:

r1. Permutasjon av rader.

r2. Multiplikasjon av en rad med en skalar$\neq 0$.

r3. Addisjon av en skalarmultippel av en rad til en annen rad.

c1. Permutasjon av kolonner.

c2. Multiplikasjon av en kolonne med en skalar$\neq 0$.

d1. Fjerne en rad av 0-ere (med mindre dette er den eneste raden).

Vi kaller operasjonene r1.-r3. for elementære radoperasjoner og c1.-c2. for elementære kolonneoperasjoner. Ved å utføre slike elementære operasjoner kan vi redusere A til en matrise på formen $\begin{bmatrix} I_r & B \end{bmatrix}$, der I_r er $r \times r$-identitetsmatrisen og B er en $r \times (n-r)$-matrise over $\mathbb{K}$. Matrisen $\begin{bmatrix} I_r & B \end{bmatrix}$ kalles en **standard representasjon** for vektormatroiden. Merk at permutasjon av kolonnene til B vil gi en standard representasjon for en isomorf vektormatroide. Vi har altså ikke en unik standard representasjon for isomorfiklassen til en vektormatroide.

Definisjon 3.50 *En matroide som er representabel over $\mathbb{F}_2$ og $\mathbb{F}_3$ kalles **binær** og **ternær**, respektivt.*

Eksempel 3.51 *Den uniforme matroiden $U_{2,4}$ er ikke binær, men den er ternær. Vi skal nå se grunnen til dette. Anta at $U_{2,4}$ er representert over en kropp $\mathbb{K}$ ved en matrise A. Siden den største uavhengige mengden i $U_{2,4}$ har to elementer, så har kolonnerommet til A, vektorrommet utspent av kolonnene til A, dimensjon 2. Et 2-dimensjonalt vektorrom over $\mathbb{F}_2$ har nøyaktig 4 elementer, der tre av dem er forskjellig fra 0. Så hvis $\mathbb{K} = \mathbb{F}_2$, så har ikke A fire distinkte kolonner forskjellig fra 0. Dermed har A en mengde av to kolonner som er lineært avhengig, og A er derfor ikke en representasjon for $U_{2,4}$ over $\mathbb{F}_2$. Vi har at $U_{2,4}$ ikke er binær. Matrisen*

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix}$$

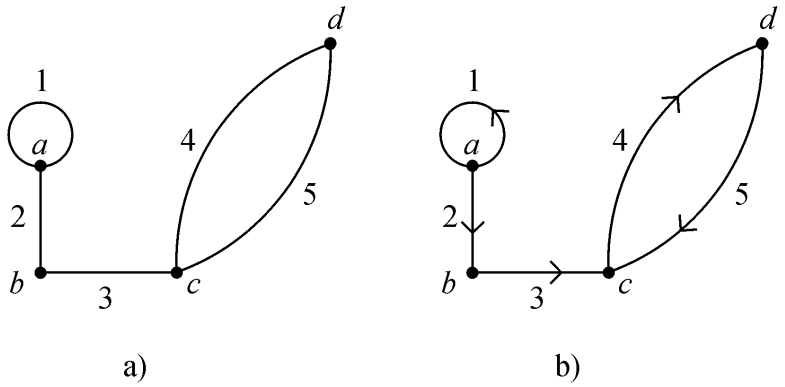
er en representasjon for $U_{2,4}$ over $\mathbb{F}_3$ siden hvert par av kolonner til denne matrisen er lineært uavhengig. Derfor er $U_{2,4}$ ternær.

Eksempel 3.52 *Alle grafiske matroider er binære. Hvis G er en graf med m hjørner og n kanter, så er en $\mathbb{F}_2$-representasjon for kretsmatroiden $M(G)$ $m \times n$-hjørne-kant insidensmatrisen til G, der vi har redusert hvert element modulo 2.*

Gitt en graf G med m hjørner og n kanter. Da kan vi konstruere en digraf $D(G)$ fra G ved å tilegne en vilkårlig retning til hver kant. Vi kan deretter representere $D(G)$ ved en $m \times n$-hjørne-kant insidensmatrise $A_{D(G)} = [a_{ij}]$ etter følgende regler:

$$a_{ij} = \begin{cases} 1 & \text{hvis } i \text{ er starthjørnet til en rettet kant } j \text{ som ikke er en løkke,} \\ -1 & \text{hvis } i \text{ er slutthjørnet til en rettet kant } j \text{ som ikke er en løkke,} \\ 0 & \text{ellers.} \end{cases}$$

Da er $A_{D(G)}$ en representasjon for kretsmatroiden $M(G)$ over enhver kropp $\mathbb{K}$; la $+1$ være den multiplikative identiteten i $\mathbb{K}$ og la -1 være den additive inversen til denne $+1$.



Figur 3-4: a) Grafen G_4. b) En orientering $D(G_4)$ av G_4.

Eksempel 3.53 *La G_4 være grafen i Figur 3-4 a), og la $D(G_4)$ være digrafen vist i Figur 3-4 b). Da er $A_{D(G_4)}$ gitt ved:*

$$A_{D(G_4)} = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 & -1 \\ 0 & 0 & 0 & -1 & 1 \end{bmatrix} \end{array}.$$

Vi har følgende resultat fra Proposisjon 5.1.2 i [9].

Proposisjon 3.54 *Hvis G er en graf, så er $M(G)$ representabel over enhver kropp.*

Bevis Oxley beviser dette i [9]. ■

Eksempel 3.55 *Den uniforme matroiden $U_{2,4}$ er ikke grafisk, siden $U_{2,4}$ ikke er binær og enhver grafisk matroide er binær.*

Definisjon 3.56 *En matroide sies å være **regulær** hvis den kan representeres ved en matrise over $\mathbb{R}$ der alle kvadratiske undermatriser har determinanter i $\{0, 1, -1\}$.*

Som neste resultat viser, så er klassen av regulære matroider identisk lik klassen av matroider som er representabel over alle kropper.

Teorem 3.57 *Følgende er ekvivalent for en matroide M:*

i) M er regulær.

ii) M er representabel over enhver kropp.

iii) M er binær og $\mathbb{K}$-representabel for en kropp $\mathbb{K}$ av karakteristikk $\neq 2$.

Bevis Se Teorem 6.6.3 i [9]. ■

Merk at en konsekvens av Teorem 3.57 er at klassen av regulære matroider er snittet av klassene av binære og ternære matroider.

Proposisjon 3.58 *Hvis G er en graf, så er $M(G)$ regulær.*

Bevis Dette følger direkte fra Proposisjon 3.54 og Teorem 3.57. ■

3.7 Duale matroider

Vi skal nå se hva vi mener med duale matroider. I grafteorien møter vi begrepet abstrakt dual, som er en generalisering av den geometriske dualen og som gir en karakterisering av planare grafer. Det viser seg at definisjonen av en abstrakt dual er en direkte konsekvens av matroidedualitet.

Vi starter med å gjengi Teorem 2.1.1 i [15].

Teorem 3.59 *Hvis $\{B_i \,|i \in I\}$ er mengden av baser til en matroide M på S, så er $\{S - B_i \,|i \in I\}$ mengden av baser til en matroide M^* på S.*

Bevis Welsh har bevist dette i [15]. ■

Matroiden M^* i teoremet ovenfor kalles **dualen** til M. Legg merke til at $\mathcal{B}(M^*) = \mathcal{B}^*(M) = \{S - B \,|B \in \mathcal{B}(M)\}$. Siden $(\mathcal{B}^*(M))^* = \mathcal{B}(M)$, så er $(M^*)^* = M$.

Bemerkning 3.60 *I motsetning til en planar graf, så har en matroide én unik dual.*

Proposisjon 3.61 *Dualen til den uniforme matroiden $U_{k,n}$ er den uniforme matroiden $U_{n-k,n}$.*

Bevis Anta at $U_{k,n}$ er den uniforme matroiden på en n-mengde S. Basene for $U_{k,n}$ er alle k-delmengdene av S. $\mathcal{B}^*(U_{k,n})$ består da av alle $(n-k)$-delmengdene av S, så vi har at $U^*_{k,n} = U_{n-k,n}$. ■

M^* har følgende egenskaper:

1. En delmengde $I \subseteq S$ er uavhengig i M^* hvis og bare hvis $S - I$ er utspennende i M.

2. Et element $e \in S$ er en løkke i M hvis og bare hvis e er element i enhver base for M^*.

Rangfunksjonen på M^* betegner vi ved r^*. Vi kaller r^* den **duale rangfunksjonen** på M. Vi har altså at $r(M^*) = r^*(M)$ og

$$r(M) + r^*(M) = |S|. \tag{3.1}$$

(3.1) er et spesialtilfelle av følgende:

Teorem 3.62 *La M og M^* være matroider på grunnmengden S, og la $T \subseteq S$. Rangfunksjonene r og r^* til M og M^*, respektivt, er tilknyttet ved:*

$$r^*(S-T) = |S| - r(S) - |T| + r(T).$$

Bevis Dette er Teorem 2.1.2 i [15]. Beviset står der. ■

Proposisjon 3.63 *For alle delmengder X av grunnmengden S til en matroide M, har vi:*

$$r^*(X) = |X| - r(S) + r(S-X).$$

Bevis La M være en matroide på S. Anta at $X \subseteq S$. Da er $S-X$ også en delmengde av S. Ved å bruke Teorem 3.62, får vi:

$$\begin{aligned} r^*(X) &= r^*(S-(S-X)) \\ &= |S| - r(S) - |S-X| + r(S-X) \\ &= |S| - r(S) - |S| + |X| + r(S-X) \\ &= |X| - r(S) + r(S-X) \end{aligned}$$

■

En **kobase** for M er en base for M^*, en **kokrets** i M er en krets i M^* og en **koløkke** i M er en løkke i M^*. En koløkke i M er altså et element $e \in S$ som ikke er inneholdt i noen baser for M^*. e er da inneholdt i enhver kobase for M^*, det vil si e er med i enhver base for M.

Eksempel 3.64 *La $G = (V(G), E(G))$ være en graf. Da er $e \in E(G)$ en koløkke i kretsmatroiden $M(G)$ hvis og bare hvis e er en bro i G.*

Eksempel 3.65 *I en vektormatroide er indeksen j en koløkke hvis og bare hvis den j-te vektoren ikke er en lineær kombinasjon av de andre vektorene.*

Eksempel 3.66 *La $U_{k,n}$ være den uniforme matroiden på en n-mengde S. Kokretsene til $U_{k,n}$ er alle $(n-k+1)$-delmengdene av S.*

Siden M^* er den unike dualen til matroiden M på S, så er kjennskap til kobasene, kokretsene eller den duale rangfunksjonen nok til å karakterisere matroiden M. Vi kan dermed definere en matroide ved hjelp av disse begrepene. Generelt er det slik at det til ethvert utsagn om en matroide finnes et dualt utsagn.

Vi skal nå studere dualen til kretsmatroiden til en graf. Vi starter med å se på et eksempel.

Eksempel 3.67 *La oss betrakte grafen G_1 i Figur 2-1. Siden G_1 er sammenhengende, så er basene for $M(G_1)$ lik kantmengdene til utspennende trær for G_1. Vi har at:*

$$\mathcal{B}(M(G_1)) = \{\{1,2\},\{1,3\},\{2,3\},\{2,4\},\{3,4\}\}.$$

Se nå på grafen G_1^* i Figur 2-3 b). Utspennende trær for denne grafen er kantmengdene på formen $\{5\} \cup X$, der X er element i følgende mengde:

$$\{\{1,2\},\{1,3\},\{1,4\},\{2,4\},\{3,4\}\}.$$

Vi observerer at utspennende trær for G_1^* er komplementene av utspennende trær for G_1. Basene for $M(G_1^*)$ er altså:

$$\mathcal{B}(M(G_1^*)) = \mathcal{B}^*(M(G_1)).$$

Dermed er $M(G_1)$ og $M(G_1^*)$ duale matroider. I dette eksemplet har vi altså at $(M(G_1))^* = M(G_1^*)$, der G_1^* er den geometriske dualen til G_1. Som vi skal se litt senere, så gjelder dette for enhver planar graf. La oss nå se på mengden av kretser til $M(G_1^*)$:

$$\mathcal{C}(M(G_1^*)) = \mathcal{C}^*(M(G_1)) = \{\{2,3\},\{1,2,4\},\{1,3,4\}\}.$$

Vi ser av Figur 2-1 at disse mengdene korresponderer til kokretsene i G_1.

Vi har følgende resultat:

Teorem 3.68 *La G være en graf, og la $\mathcal{C}^*$ betegne familien av kantmengder til kokretser i G. Da er $\mathcal{C}^*$ mengden av kretser til en matroide $M^*(G)$ på $E(G)$ og*

i) $M^*(G) = (M(G))^*$,

ii) $M(G) = (M^*(G))^*$.

Bevis Dette er bevist i [15] (se Teorem 2.4.1 og Teorem 2.4.2). ■

Matroiden $M^*(G)$ i Proposisjon 3.68 kalles **kokretsmatroiden** til G.

Eksempel 3.69 *La G_2 være grafen vist i Figur 3-1. Kokretsmatroiden til G_2 er da $M^*(G_2) = (S, \mathcal{C}^*)$, der $S = \{1,2,3,4,5\}$ og*

$$\mathcal{C}^* = \{\{1,2\},\{4,5\},\{1,3,4\},\{1,3,5\},\{2,3,4\},\{2,3,5\}\}.$$

Definisjon 3.70 *En matroide som er isomorf med kokretsmatroiden $M^*(G)$ til en graf G kalles **kografisk**.*

Eksempel 3.71 *La K_3 være den komplette grafen i Figur 3-2. Siden $M(K_3) \cong U_{2,3}$, så er $M^*(K_3) \cong U_{2,3}^* = U_{1,3}$. Den uniforme matroiden $U_{1,3}$ er altså en kografisk matroide.*

Vi skal se på noen resultater om planare grafer. Vi gjengir nå Lemma 2.3.7 i [9].

Lemma 3.72 *Hvis G^* er en geometrisk dual til den planare grafen G, så er:*

$$M(G^*) \cong M^*(G).$$

Bevis Oxley beviser dette i [9]. ■

Eksempel 3.73 *Selv om H_1^* og H_2^* i Figur 2-4 er to ikke-isomorfe geometriske dualer til den samme planare grafen, så har de isomorfe kretsmatroider.*

Vi har følgende resultat fra [9]:

Teorem 3.74 *Følgende er ekvivalent for en graf G:*

i) G er planar.

ii) $M^*(G)$ er grafisk.

iii) G har en abstrakt dual.

Bevis Se beviset til Teorem 5.2.2 i [9]. ■

Det gjenstår nå å se hvordan vi kan konstruere dualen til en vektormatroide.

Teorem 3.75 *La M være en matroide på $S = \{e_1, e_2, \ldots, e_n\}$, og la rangen til M være lik r med $0 < r < n$. Hvis M har standard representasjonen*

$$\begin{matrix} e_1 \ldots e_r & e_{r+1} \ldots e_n \end{matrix}$$
$$\begin{bmatrix} I_r & B \end{bmatrix},$$

så har M^* representasjonen

$$\begin{matrix} e_1 \ldots e_r & e_{r+1} \ldots e_n \end{matrix}$$
$$\begin{bmatrix} -B^T & I_{n-r} \end{bmatrix},$$

der I_k er $k \times k$-identitetsmatrisen og B^T er den transponerte matrisen til B.

Bevis Dette beviset finnes i [9] (se Teorem 2.2.8). ■

Eksempel 3.76 *La G_1 være grafen vist i Figur 2-1. En standard representasjon for $M(G_1)$ med hensyn på basen $\{1, 2\}$ over $\mathbb{F}_2$ er gitt ved:*

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix}$$
$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

$M^*(G_1)$ har derfor følgende representasjon med hensyn på basen $\{3, 4, 5\}$ over $\mathbb{F}_2$:

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix}$$
$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Siden $M^*(G_1) \cong M(G_1^*)$, der G_1^* er grafen i 2-3 b), så er også den siste matrisen en $\mathbb{F}_2$-representasjon for $M(G_1^*)$.

Bemerkning 3.77 *I Teorem 3.75 antok vi at rangen r til matrisen $\begin{bmatrix} I_r & B \end{bmatrix}$ verken er 0 eller n. Hvis $r = 0$, er $M \cong U_{0,n}$, så $M^* \cong U_{n,n} \cong M[I_n]$. Hvis $r = n$, så er $M \cong U_{n,n}$. Dermed er $M^* \cong U_{0,n} \cong M[0_n]$, der 0_n er $n \times n$-nullmatrisen.*

Teorem 3.75 og bemerkningen ovenfor gir oss følgende resultat.

Korollar 3.78 *Hvis M er representabel over kroppen $\mathbb{K}$, så er også dualen M^* representabel over $\mathbb{K}$.*

Neste resultat finnes som Proposisjon 2.2.22 i [9].

Proposisjon 3.79 *Dualen til en regulær matroide er regulær.*

Bevis Se [9]. ■

Proposisjon 3.80 *Hvis G er en graf, så er $M^*(G)$ regulær.*

Bevis Denne proposisjonen følger direkte fra Proposisjon 3.58 og Proposisjon 3.79. ■

Definisjon 3.81 *En matroide som både er grafisk og kografisk kaller vi **planar-grafisk**.*

Teorem 3.74 forteller oss at en matroide M er både grafisk og kografisk hvis og bare hvis M er kretsmatroiden til en planar graf (ekvivalent kokretsmatroiden til en planar graf). Vi avslutter dette delkapitlet med Proposisjon 5.2.6 i [9].

Proposisjon 3.82 *Følgende er ekvivalent for en graf G:*

i) G er en planar graf.

ii) $M(G)$ er en planar-grafisk matroide.

3.8 Minorer

Gitt en graf G med kantmengden $E(G)$. Vi kan fjerne eller kontraktere en delmengde $F \subseteq E(G)$. Vi skal nå definere matroideoperasjoner som generaliserer disse to operasjonene for grafer.

Definisjon 3.83 *La $M = (S, \mathcal{I})$ være en matroide, og la $T \subseteq S$.*

*i) Matroiden $M \setminus T = (S - T, \mathcal{I}(M \setminus T))$, der $\mathcal{I}(M \setminus T) = \{I \subseteq S - T \,|\, I \in \mathcal{I}(M)\}$ kalles **slettingen** av T fra M.*

*ii) Matroiden $M/T = (M^* \setminus T)^*$ på grunnmengden $S - T$ kalles **kontraksjonen** av T fra M.*

Definisjon 3.84 *En **minor** til en matroide M er en matroide som er fått fra M ved slettinger og/eller kontraksjoner.*

Vi starter med et eksempel hentet fra [9].

Eksempel 3.85 *La S være en n-mengde, og la T være en t-delmengde av S. Da er:*

$$U_{k,n}/T \cong \begin{cases} U_{0,n-t} & \text{hvis } n \geq t \geq k, \\ U_{k-t,n-t} & \text{når } t < k. \end{cases} \quad \text{og}$$

$$U_{k,n} \setminus T \cong \begin{cases} U_{n-t,n-t} & \text{hvis } n \geq t \geq n-k, \\ U_{k,n-t} & \text{når } t < n-k. \end{cases}$$

Vi ser at enhver minor til en uniform matroide er uniform.

Vi skal nå se på minorer til kretsmatroiden.

Eksempel 3.86 *La G_1 være grafen vist i Figur 2-1. Kretsmatroiden til G_1 er $M(G_1) = (S, \mathcal{C}(M(G_1)))$, der $S = \{1,2,3,4,5\}$ og $\mathcal{C}(M(G_1)) = \{\{5\},\{1,4\},\{1,2,3\},\{2,3,4\}\}$. Fra Eksempel 3.41 vet vi at de uavhengige mengdene til $M(G_1)$ er:*

$$\mathcal{I}(M(G_1)) = \{\varnothing,\{1\},\{2\},\{3\},\{4\},\{1,2\},\{1,3\},\{2,3\},\{2,4\},\{3,4\}\}.$$

Slettingen av $\{3\}$ fra $M(G_1)$ er matroiden $M(G_1) \setminus \{3\} = (S', \mathcal{I}(M(G_1) \setminus \{3\}))$, der $S' = \{1,2,4,5\}$ og

$$\mathcal{I}(M(G_1) \setminus \{3\}) = \{I \subseteq S' \,|\, I \in \mathcal{I}(M(G_1))\} = \{\varnothing,\{1\},\{2\},\{4\},\{1,2\},\{2,4\}\}.$$

$\mathcal{I}(M(G_1) \setminus \{3\})$ består altså av de elementene i $\mathcal{I}(M(G_1))$ som ikke inneholder 3. De avhengige mengdene til $M(G_1) \setminus \{3\}$ er:

$$\{\{5\},\{1,4\},\{1,5\},\{2,5\},\{4,5\},\{1,2,4\},\{1,2,5\},\{1,4,5\},\{2,4,5\},\{1,2,4,5\}\}.$$

Kretsene i $M(G_1) \setminus \{3\}$ er da mengden $\{\{5\},\{1,4\}\}$. Figur 3-5 a) viser slettingen av kanten 3 fra grafen G_1. Vi ser fra denne figuren at $M(G_1) \setminus \{3\} = M(G_1 \setminus \{3\})$.

Ofte kan det være mer naturlig å definere matroidene M/T og $M \setminus T$ ut fra sine kretser. Vi karakteriserer derfor kretsene til disse matroidene.

Proposisjon 3.87 *La $M = (S, \mathcal{C})$ være en matroide, og la $T \subseteq S$. Da er kretsene til $M \setminus T$ lik mengden*

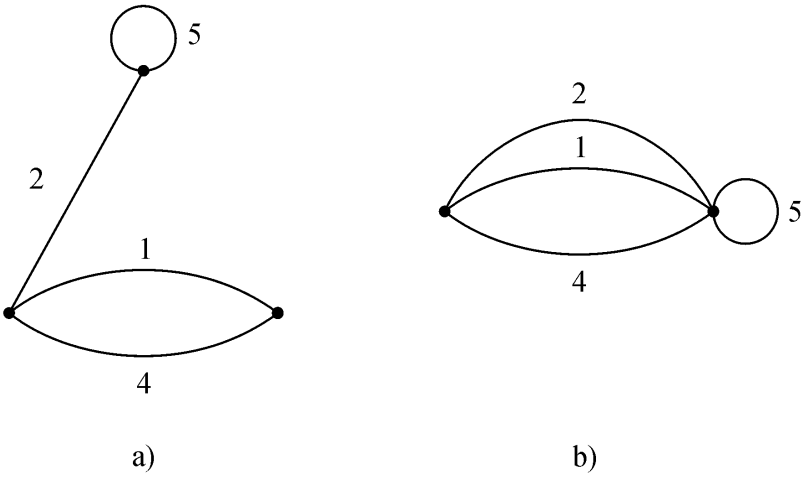
$$\mathcal{C}(M \setminus T) = \{C \subseteq S - T \,|\, C \in \mathcal{C}(M)\} = \{C \in \mathcal{C}(M) \,|\, C \cap T = \varnothing\}.$$

Bevis Dette følger direkte fra Definisjon 3.83 i). ■

Proposisjon 3.1.11 i [9] lar oss karakterisere kretsene til M/T.

Proposisjon 3.88 *Kretsene til M/T består av de minimale ikke-tomme elementene til $\{C - T \,|\, C \in \mathcal{C}(M)\}$.*

Bevis Denne proposisjonen er bevist i [9]. ■



Figur 3-5: a) Grafen $G_1 \setminus \{3\}$. b) Grafen $G_1 / \{3\}$.

Eksempel 3.89 *La G_1 være grafen i forrige eksempel. Fra Proposisjon 3.88 har vi da at kretsene til matroiden $M(G_1) / \{3\}$ er:*

$$\mathcal{C}(M(G_1) / \{3\}) = \{\{5\}, \{1,2\}, \{1,4\}, \{2,4\}\}.$$

Det er klart at når $E(G)$ er kantmengden til en graf G og $T \subseteq E(G)$, så har vi:

$$M(G \setminus T) = M(G) \setminus T. \tag{3.2}$$

La oss nå se hva som skjer når vi kontrakterer $\{3\}$ fra kretsmatroiden $M(G_1)$ i forrige eksempel.

Eksempel 3.90 *La $M(G_1)$ være kretsmatroiden til grafen G_1 i Figur 2-1. Da er:*

$$M(G_1) / \{3\} = (M^*(G_1) \setminus \{3\})^*.$$

Siden G_1 er en planar graf, har vi fra Lemma 3.72 at:

$$(M^*(G_1) \setminus \{3\})^* \cong (M(G_1^*) \setminus \{3\})^*,$$

der G_1^* er en geometrisk dual til G_1. Videre har vi fra (3.2) at:

$$(M(G_1^*) \setminus \{3\})^* = (M(G_1^* \setminus \{3\}))^*.$$

Men

$$(M(G_1^* \setminus \{3\}))^* = M^*(G_1^* \setminus \{3\}) \cong M((G_1^* \setminus \{3\})^*)$$

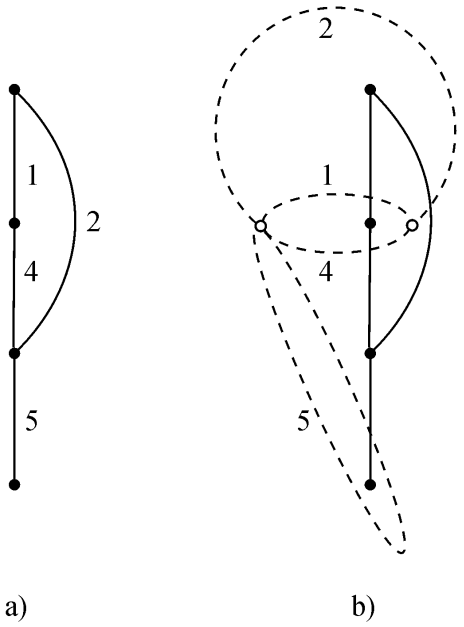
fra Lemma 3.72, så

$$M(G_1) / \{3\} \cong M((G_1^* \setminus \{3\})^*).$$

Figur 2-3 b) viser G_1^*. Konstruksjonen av $(G_1^* \setminus \{3\})^*$ er illustrert i Figur 3-6. Vi ser

at $(G_1^* \setminus \{3\})^* \cong G_1/\{3\}$*, der* $G_1/\{3\}$ *er grafen i Figur 3-5 b). Vi har derfor at*

$$M(G_1)/\{3\} = M(G_1/\{3\}).$$



Figur 3-6: a) $G_1^* \setminus \{3\}$. b) Konstruksjon av $(G_1^* \setminus \{3\})^*$.

Vi gjengir Proposisjon 3.2.1 i [9].

Proposisjon 3.91 *Hvis* G *er en graf, så er*

$$M(G)/T = M(G/T)$$

for alle delmengder T *av* $E(G)$*.*

Bevis Oxley beviser denne proposisjonen i [9]. ■

Siden $M(G)/T = M(G/T)$ og $M(G) \setminus T = M(G \setminus T)$ for alle delmengder $T \subseteq E(G)$, får vi følgende resultat:

Proposisjon 3.92 *Enhver minor til en grafisk matroide er grafisk.*

La r være rangfunksjonen på en matroide M, og la $r_{M\setminus T}$ og $r_{M/T}$ betegne rangfunksjonene på matroidene $M \setminus T$ og M/T, respektivt. Anta at $T \subseteq S$. Da gir Oxley i [9] følgende sammenhenger som gjelder for alle $X \subseteq S - T$:

$$r_{M\setminus T}(X) = r(X), \tag{3.3}$$

$$r_{M/T}(X) = r(X \cup T) - r(T). \tag{3.4}$$

Proposisjon 3.93 *La M være en matroide på S. Hvis T_1 og T_2 er disjunkte delmengder av S, så er:*

$$(M \setminus T_1)/T_2 = (M/T_2) \setminus T_1.$$

Bevis Anta at T_1 og T_2 er disjunkte delmengder av grunnmengden S til en matroide M. Det holder å vise at $(M \setminus T_1)/T_2$ og $(M/T_2) \setminus T_1$ har den samme rangfunksjonen. Hvis $X \subseteq S - (T_1 \cup T_2)$, så er $r_{(M/T_2)\setminus T_1}(X) = r_{M/T_2}(X)$ fra (3.3). Videre så har vi fra (3.4) at $r_{M/T_2}(X) = r(X \cup T_2) - r(T_2)$. Fra (3.3) har vi så at $r(X \cup T_2) - r(T_2) = r_{M\setminus T_1}(X \cup T_2) - r_{M\setminus T_1}(T_2)$. Men $r_{M\setminus T_1}(X \cup T_2) - r_{M\setminus T_1}(T_2) = r_{(M\setminus T_1)/T_2}(X)$ fra (3.4), så vi har derfor at $r_{(M/T_2)\setminus T_1}(X) = r_{(M\setminus T_1)/T_2}(X)$. ■

Proposisjon 3.94 *$M \setminus T = M/T$ hvis og bare hvis $r(T) + r(S - T) = r(M)$.*

Bevis Dette er Proposisjon 3.1.24 i [9], og beviset finnes i [9]. ■

Vi får følgende resultat (Korollar 3.1.25 i [9]):

Korollar 3.95 *$M \setminus \{e\} = M/\{e\}$ hvis og bare hvis e er en løkke eller en koløkke i M.*

Vi illustrerer dette korollaret ved et eksempel.

Eksempel 3.96 *La M være en matroide på $S = \{1,2,3\}$ med $\mathcal{I}(M) = \{\varnothing, \{2\}\}$. Da er $\mathcal{B}(M) = \{\{2\}\}$. Elementet $1 \in S$ er en løkke i M, siden $\{1\} \notin \mathcal{I}(M)$. Sletter vi $\{1\}$ fra M får vi matroiden $M \setminus \{1\} = (\{2,3\}, \mathcal{I}(M \setminus \{1\}))$, der*

$$\mathcal{I}(M \setminus \{1\}) = \{I \subseteq \{2,3\} \,|\, I \in \mathcal{I}(M)\} = \{\{2\}\}.$$

Familien av baser til denne matroiden er da $\mathcal{B}(M \setminus \{1\}) = \{\{2\}\}$. Vi skal nå konstruere matroiden $M/\{1\}$ som er lik $(M^* \setminus \{1\})^*$ per definisjon. Dualen til M er matroiden $M^* = (\{1,2,3\}, \mathcal{B}(M^*))$, der

$$\mathcal{B}(M^*) = \{\{1,2,3\} - B \,|\, B \in \mathcal{B}(M)\} = \{\{1,3\}\}.$$

De uavhengige mengdene til M^* er da $\mathcal{I}(M^*) = \{\varnothing, \{1\}, \{3\}, \{1,3\}\}$. Vi konstruerer matroiden vi får fra M^* ved å slette $\{1\}$; $M^* \setminus \{1\} = (\{2,3\}, \mathcal{I}(M^* \setminus \{1\}))$, der

$$\mathcal{I}(M^* \setminus \{1\}) = \{I \subseteq \{2,3\} \,|\, I \in \mathcal{I}(M^*)\} = \{\varnothing, \{3\}\}.$$

Basene for $M^* \setminus \{1\}$ er da $\mathcal{B}(M^* \setminus \{1\}) = \{\{3\}\}$. Vi dualiserer $M^* \setminus \{1\}$ og får matroiden $(M^* \setminus \{1\})^* = (\{2,3\}, \mathcal{B}((M^* \setminus \{1\})^*))$, der

$$\mathcal{B}((M^* \setminus \{1\})^*) = \{\{2,3\} - B \,|\, B \in \mathcal{B}(M^* \setminus \{1\})\} = \{\{2\}\}.$$

Vi har altså at $\mathcal{B}((M^* \setminus \{1\})^*) = \mathcal{B}(M \setminus \{1\})$. Matroidene $M/\{1\}$ og $M \setminus \{1\}$ har samme grunnmengde og samme familie av baser. Dermed er $M/\{1\} = M \setminus \{1\}$. La oss nå se verifisere at $M \setminus \{e\} = M/\{e\}$ når e er en koløkke i M. Elementet $2 \in S$ er en koløkke i M, siden $\{2\}$ er inneholdt i basen for M. Sletter vi $\{2\}$ fra M får vi matroiden $M \setminus \{2\} = (\{1,3\}, \mathcal{I}(M \setminus \{2\}))$, der

$$\mathcal{I}(M \setminus \{2\}) = \{I \subseteq \{1,3\} \,|\, I \in \mathcal{I}(M)\} = \{\varnothing\}.$$

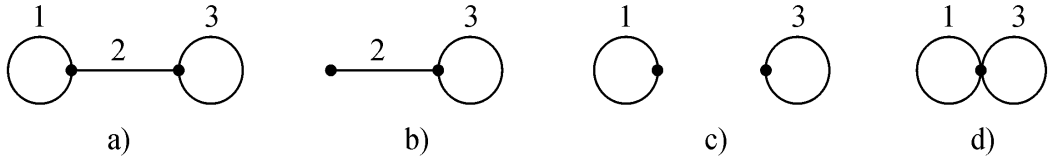
Da er $\mathcal{B}(M \setminus \{2\}) = \{\varnothing\}$. *Vi skal nå konstruere matroiden* $M/\{2\} = (M^* \setminus \{2\})^*$. *Matroiden* $M^* \setminus \{2\} = (\{1,3\}, \mathcal{I}(M^* \setminus \{2\}))$, *der*

$$\mathcal{I}(M^* \setminus \{2\}) = \{I \subseteq \{1,3\} \,|\, I \in \mathcal{I}(M^*)\} = \{\varnothing, \{1\}, \{3\}, \{1,3\}\}.$$

Da er $\mathcal{B}(M^* \setminus \{2\}) = \{\{1,3\}\}$. *Vi dualiserer* $M^* \setminus \{2\}$ *og får matroiden* $(M^* \setminus \{2\})^* = (\{1,3\}, \mathcal{B}((M^* \setminus \{2\})^*))$, *der*

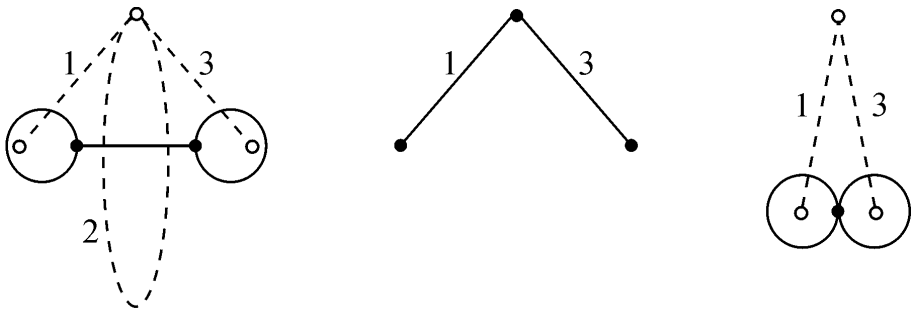
$$\mathcal{B}((M^* \setminus \{2\})^*) = \{\{1,3\} - B \,|\, B \in \mathcal{B}(M^* \setminus \{2\})\} = \{\varnothing\}.$$

Vi har altså at $\mathcal{B}((M^* \setminus \{2\})^*) = \mathcal{B}(M \setminus \{2\})$. *Dermed er* $M/\{2\} = M \setminus \{2\}$. *Matroiden* M *i dette eksemplet er isomorf med kretsmatroiden* $M(G_5)$ *til grafen* G_5 *vist i Figur 3-7 a). Fra Figur 3-7 b)-d) ser vi at* $M(G_5 \setminus \{1\}) = M(G_5/\{1\})$ *og* $M(G_5 \setminus \{2\}) = M(G_5/\{2\})$.



Figur 3-7: a) Grafen G_5. b) $G_5 \setminus \{1\} = G_5/\{1\}$. c) $G_5 \setminus \{2\}$. d) $G_5/\{2\}$.

For grafer er det en sammenheng mellom sletting og kontraksjon gjennom dualitet. Et eksempel på dette er vist i Figur 3-8. Denne sammenhengen gjelder også for matroider.



Figur 3-8: $G_5^* \setminus \{2\} = (G_5/\{2\})^*$

Teorem 3.97 *La* M *være en matroide på* S, *og la* $T \subseteq S$. *Da er:*

i) $(M \setminus T)^* = M^*/T$, *og*

ii) $(M/T)^* = M^* \setminus T$.

Bevis Anta at T er en delmengde av grunnmengden S til en matroide M. i) Det holder å vise at $(M \setminus T)^*$ og M^*/T har den samme rangfunksjonen. Hvis $X \subseteq S - T$, så er

$$\begin{aligned} r_{(M\setminus T)^*}((S-T)-X) &= |S-T| - r_{M\setminus T}(S-T) - |X| + r_{M\setminus T}(X) \\ &= |S| - |T| - r(S-T) - |X| + r(X) \end{aligned}$$

ved Teorem 3.62 og (3.3). Fra (3.4) får vi at:

$$\begin{aligned} r_{M^*/T}((S-T)-X) &= r^*(((S-T)-X)\cup T) - r^*(T) \\ &= r^*(S-X) - r^*(T). \end{aligned}$$

Men fra Teorem 3.62 og Proposisjon 3.63 har vi at:

$$\begin{aligned} r^*(S-X) - r^*(T) &= |S| - r(S) - |X| + r(X) - (|T| - r(S) + r(S-T)) \\ &= |S| - |X| + r(X) - |T| - r(S-T). \end{aligned}$$

Så

$$\begin{aligned} r_{M^*/T}((S-T)-X) &= |S| - |X| + r(X) - |T| - r(S-T) \\ &= r_{(M\setminus T)^*}((S-T)-X) \end{aligned}$$

Vi har dermed vist at i) holder. Ved å sette inn M istedenfor M^* i i) og ta dualer får vi ii). ■

Proposisjon 3.98 *Enhver minor til en kografisk matroide er kografisk.*

Bevis La $M^*(G)$ vær en matroide, og la $T \subseteq E(G)$. La oss først vise at $M^*(G)/T$ er kografisk. Fra Teorem 3.97 har vi at

$$M^*(G)/T = (M(G) \setminus T)^*,$$

men

$$(M(G) \setminus T)^* = (M(G \setminus T))^*$$

fra Proposisjon 3.92 og

$$(M(G \setminus T))^* = M^*(G \setminus T)$$

fra Teorem 3.68. Vi har at $M^*(G)/T = M^*(G \setminus T)$, så $M^*(G)/T$ er kografisk. Vi har tilsvarende at $M^*(G) \setminus T$ er kografisk, siden

$$M^*(G) \setminus T = (M(G)/T)^* = (M(G/T))^* = M^*(G/T).$$

Dermed er enhver minor til en kografisk matroide også kografisk. ■

Vi skal nå vise at klassen av $\mathbb{K}$-representable matroider også er minor-lukket.

Proposisjon 3.99 *La $\mathbb{K}$ være en kropp. Enhver minor til en $\mathbb{K}$-representabel matroide er $\mathbb{K}$-representabel.*

Bevis La A være en matrise over $\mathbb{K}$, og la T være en delmengde av indeksmengden til kolonnene til A. $A \backslash T$ er matrisen fått fra A ved å slette alle kolonnene som har indekser i T. Det er klart at $M[A] \setminus T = M[A \setminus T]$, så enhver sletting av en $\mathbb{K}$-representabel matroide er $\mathbb{K}$-representabel. Siden dualen til en $\mathbb{K}$-representabel matroide også er $\mathbb{K}$-representabel, så har vi fra definisjonen av kontraksjon at enhver kontraksjon av en $\mathbb{K}$-representabel matroide er $\mathbb{K}$-representabel. Så en $\mathbb{K}$-representabel matroide er minor-lukket. ■

Siden en matroide M er $\mathbb{K}$-representabel hvis og bare hvis alle minorene til M er $\mathbb{K}$-representabel, kan vi karakterisere klassen av $\mathbb{K}$-representable matroider ved å liste opp minorene som ikke er $\mathbb{K}$-representable. Klassen av $\mathbb{K}$-representable matroider er lukket under dualitet, så vi har følgende resultat (Lemma 6.5.1 i [9]):

Lemma 3.100 *Hvis minoren M ikke er representabel over $\mathbb{K}$, så er heller ikke dualen M^* det.*

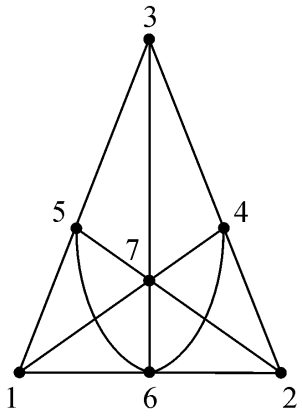
Fra Eksempel 3.49 og Lemma 3.100 følger dette resultatet for alle endelige kropper $\mathbb{F}_q$:

Korollar 3.101 *Matroidene $U_{2,q+2}$ og $U_{q,q+2}$ er ikke $\mathbb{F}_q$-representabel.*

Dette korollaret finnes som Korollar 6.5.3 i [9].

Eksempel 3.102 *$U_{2,5}$ er ikke representabel over $\mathbb{F}_3$. Heller ikke $U_{2,5}^* = U_{3,5}$ er $\mathbb{F}_3$-representabel.*

Vi skal straks gjengi noen viktige resultater. Men først definerer vi en ny matroide.



Figur 3-9: Fanomatroiden F_7.

Diagrammet i Figur 3-9 er en geometrisk representasjon av matroiden på $S = \{1, 2, \ldots, 7\}$ med familien av baser bestående av alle delmengder av S av kardinalitet 3, med unntak av $\{1,2,6\}$, $\{1,4,7\}$, $\{1,3,5\}$, $\{2,3,4\}$, $\{2,5,7\}$, $\{3,6,7\}$ og $\{4,5,6\}$. Vi ser at basene er nøyaktig de 3-mengdene som ikke ligger på en linje. Denne matroiden kaller vi **Fanomatroiden** og betegner den ved F_7. Kretsene til F_7 er linjer,

slik som $\{1,2,6\}$, og komplementene av linjene, slik som $\{3,4,5,7\}$. Kokretsene til F_7 er $\{1,2,3,7\}$, $\{1,2,4,5\}$, $\{1,3,4,6\}$, $\{1,5,6,7\}$, $\{2,3,5,6\}$, $\{2,4,6,7\}$ og $\{3,4,5,7\}$. Kobasene til F_7 er alle delmengder med 4 elementer som inneholder en linje, slik som $\{1,2,4,6\}$.

Fanomatroiden F_7 (og dermed også dualen F_7^*) er binær. En representasjon for F_7 over $\mathbb{F}_2$ er:

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix} \qquad (3.5)$$
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} .$$

Proposisjon 6.5.5 i [9] forteller oss følgende:

Proposisjon 3.103 *La $\mathbb{K}$ være en kropp av karakteristikk $\neq 2$. Da er F_7 og F_7^* minorer som ikke er representabel over $\mathbb{K}$.*

Bevis Oxley beviser dette i [9]. ■

Vi gjengir nå Teoremene 6.5.4, 6.5.7, 6.6.4, 6.6.5 og 6.6.5 i [9]. Alle bevisene finnes i [9].

Teorem 3.104 *En matroide M er binær hvis og bare hvis M ikke har noen minor $U_{2,4}$-minor.*

Teorem 3.105 *En matroide M er ternær hvis og bare hvis M ikke har noen minor isomorf med noen av matroidene*

$$U_{2,5},\ U_{3,5},\ F_7 \text{ og } F_7^*.$$

Teorem 3.106 *En matroide M er regulær hvis og bare hvis M ikke har noen minor isomorf med noen av matroidene*

$$U_{2,4},\ F_7 \text{ og } F_7^*.$$

Teorem 3.107 *En matroide M er grafisk hvis og bare hvis M ikke har noen minor isomorf med noen av matroidene*

$$U_{2,4},\ F_7,\ F_7^*,\ M^*(K_5) \text{ og } M^*(K_{3,3}).$$

Teorem 3.108 *En matroide M er kografisk hvis og bare hvis M ikke har noen minor isomorf med noen av matroidene*

$$U_{2,4},\ F_7,\ F_7^*,\ M(K_5) \text{ og } M(K_{3,3}).$$

Fra disse teoremene ser vi blant annet at en binær matroide M er regulær hvis og bare hvis M ikke har F_7 eller F_7^* som minorer. En matroide M er planar-grafisk hvis og bare hvis M er regulær og ikke har minorer isomorf med $M(K_5)$, $M(K_{3,3})$ eller deres dualer. Neste resultat finnes som Korollar 6.6.6 i [9]:

Korollar 3.109 *Følgende er ekvivalent for en matroide M:*

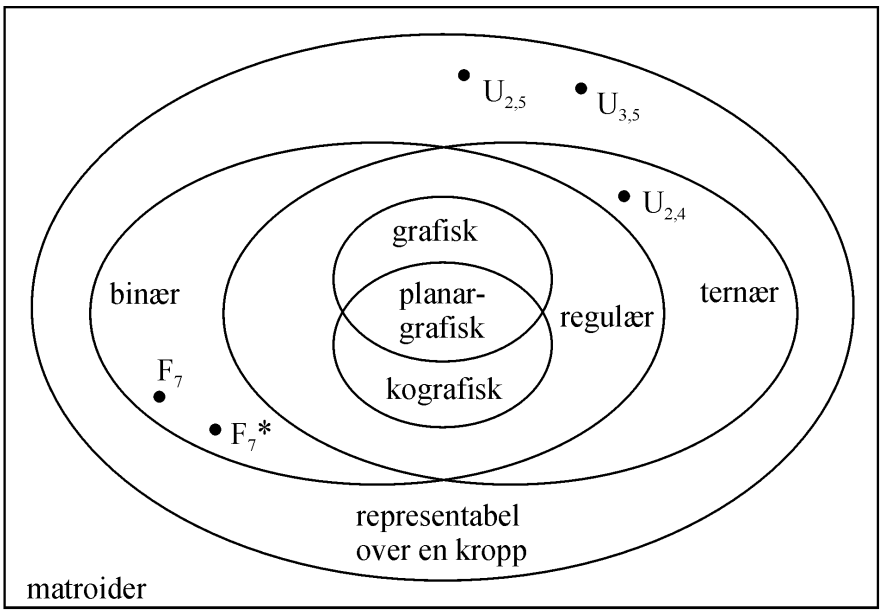
i) $M \cong M(G)$ *for en planar graf* G.

ii) M *er både grafisk og kografisk.*

iii) M *ikke har noen minor isomorf med noen av matroidene*

$$U_{2,4},\ F_7,\ F_7^*,\ M(K_5),\ M^*(K_5),\ M(K_{3,3}) \text{ og } M^*(K_{3,3}).$$

Vi avslutter dette delkapitlet med en figur som viser sammenhenger mellom noen klasser av matroider.



Figur 3-10: Noen klasser av matroider.

3.9 Tuttepolynomet til en matroide

Definisjon 3.110 *En matroide* ***isomorfi invariant*** *er en funksjon f på klassen av alle matroider slik at*

$$f(M_1) = f(M_2) \text{ når } M_1 \cong M_2.$$

La M være en matroide på S, og la $e \in S$. Med $M(\{e\})$ mener vi undermatroiden av M på $\{e\}$. Vi lar $\mathfrak{K}$ betegne en klasse av matroider som er lukket under isomorfi og matroideoperasjonene sletting og kontraksjon.

Definisjon 3.111 *En funksjon f på $\mathfrak{K}$ kalles en* ***Tutte-Grothendieck*** *(eller* ***T-G****)* ***invariant*** *hvis f er en isomorfi invariant slik at følgende gjelder for alle $e \in S$:*

$$f(M) = \begin{cases} f(M \setminus \{e\}) + f(M/\{e\}) & \text{hvis } e \text{ verken er en løkke eller en koløkke i } M, \\ f(M(\{e\}))\, f(M \setminus \{e\}) & \text{ellers.} \end{cases}$$

Definisjon 3.112 *La M være en matroide på S, og la $T \subseteq S$.* ***(Whitney) rang-generatorfunksjonen*** *på M er gitt ved:*

$$R(M; x, y) = \sum_{T \subseteq S} x^{r(S)-r(T)} y^{r^*(S)-r^*(S-T)}, \tag{3.6}$$

der r, r^* er rangfunksjonene på M, M^* respektivt.

Fra tidligere vet vi at $r^*(S) = |S| - r(S)$. Ved å bruke dette, samt relasjonen mellom r og r^*, gitt i Teorem 3.62, kan vi omskrive 3.6 til:

$$\begin{aligned} R(M; x, y) &= \sum_{T \subseteq S} x^{r(S)-r(T)} y^{r^*(S)-r^*(S-T)} \\ &= \sum_{T \subseteq S} x^{r(S)-r(T)} y^{(|S|-r(S))-(|S|-r(S)-|T|+r(T))} \\ &= \sum_{T \subseteq S} x^{r(S)-r(T)} y^{|T|-r(T)}. \end{aligned}$$

Proposisjon 3.113 *La M være en matroide. Da er:*

$$R(M^*; x, y) = R(M; y, x).$$

Bevis Ved å bruke at $r^*(S) = |S| - r(S)$ sammen med Proposisjon 3.63, får vi:

$$\begin{aligned} R(M^*; x, y) &= \sum_{T \subseteq S} x^{r^*(S)-r^*(T)} y^{|T|-r^*(T)} \\ &= \sum_{T \subseteq S} x^{|S|-r(S)-(|T|-r(S)+r(S-T))} y^{|T|-(|T|-r(S)+r(S-T))} \\ &= \sum_{T \subseteq S} x^{|S|-|T|-r(S-T)} y^{r(S)-r(S-T)} = \sum_{U \subseteq S} x^{|U|-r(U)} y^{r(S)-r(U)} \\ &= R(M; y, x). \end{aligned}$$

Bidraget av en mengde T til $R(M; y, x)$ er identisk med bidraget av den komplemente mengden $U = S - T$ til $R(M^*; x, y)$. ■

Proposisjon 3.114 *La M være en matroide på $\{e\}$.*

i) Hvis e er en løkke i M, så er $R(M(\{e\}); x, y) = y + 1$.

ii) Hvis e er en koløkke i M, så er $R(M(\{e\}); x, y) = x + 1$.

Bevis Anta at $S = \{e\}$. Da er det nøyaktig to matroider, M_1 og M_2, på S, en har $\mathcal{I} = \{\varnothing\}$ og den andre har $\mathcal{I} = \{\varnothing, \{e\}\}$. Vi ser nå på den første matroiden. Siden $\{e\} \notin \mathcal{I}$, er e en avhengig mengde til M_1, det vil si at e er en løkke i M_1. Dermed er $r(S) = r(\{e\}) = 0$. Vi vet også at $r(\varnothing) = 0$. Da er:

$$\begin{aligned} R(M(\{e\}); x, y) &= \sum_{T \subseteq S} x^{r(S)-r(T)} y^{|T|-r(T)} \\ &= x^{r(S)-r(\varnothing)} y^{|\varnothing|-r(\varnothing)} + x^{r(S)-r(\{e\})} y^{|\{e\}|-r(\{e\})} \\ &= 1 + y. \end{aligned}$$

Så i) holder. Vi betrakter så matroiden M_2 med $\mathcal{I} = \{\varnothing, \{e\}\}$. Vi ser at $\{e\} \in \mathcal{I}$, så e er en koløkke i M_2. Da er e en løkke i M_2^* og $r(\{e\}) = |\{e\}| - r^*(\{e\}) = 1 - 0 = 1$ fra (3.1). Vi har at $r(S) = r(\{e\}) = 1$. Rangen til $\varnothing$ er lik 0. Vi får:

$$\begin{aligned} R(M(\{e\}); x, y) &= \sum_{T \subseteq S} x^{r(S)-r(T)} y^{|T|-r(T)} \\ &= x^{r(S)-r(\varnothing)} y^{|\varnothing|-r(\varnothing)} + x^{r(S)-r(\{e\})} y^{|\{e\}|-r(\{e\})} \\ &= x + 1. \end{aligned}$$

Så ii) holder. ■

Lemma 3.115 *$R(M; x, y)$ er en T-G invariant for klassen av alle matroider.*

Bevis La M være en matroide på S, og la $e \in S$. Det er klart at:

$$R(M; x, y) = \sum_{\substack{T \subseteq S \\ e \notin T}} x^{r(S)-r(T)} y^{|T|-r(T)} + \sum_{\substack{T \subseteq S \\ e \in T}} x^{r(S)-r(T)} y^{|T|-r(T)}. \tag{3.7}$$

Vi betrakter det første leddet på høyre siden av 3.7. Det er klart at dette er lik:

$$\sum_{T \subseteq S - \{e\}} x^{r(S)-r(T)} y^{|T|-r(T)}.$$

Siden

$$r(S) = \begin{cases} r(S - \{e\}) + 1 \text{ hvis } e \text{ er en koløkke,} \\ r(S - \{e\}) \text{ ellers.} \end{cases}$$

får vi:

$$\begin{aligned} \sum_{\substack{T \subseteq S \\ e \notin T}} x^{r(S)-r(T)} y^{|T|-r(T)} &= \begin{cases} \sum\limits_{T \subseteq S - \{e\}} x^{r(S-\{e\})+1-r(T)} y^{|T|-r(T)} \text{ hvis } e \text{ er en koløkke,} \\ \sum\limits_{T \subseteq S - \{e\}} x^{r(S-\{e\})-r(T)} y^{|T|-r(T)} \text{ ellers.} \end{cases} \\ &= \begin{cases} x \sum\limits_{T \subseteq S - \{e\}} x^{r(S-\{e\})-r(T)} y^{|T|-r(T)} \text{ hvis } e \text{ er en koløkke,} \\ \sum\limits_{T \subseteq S - \{e\}} x^{r(S-\{e\})-r(T)} y^{|T|-r(T)} \text{ ellers.} \end{cases} \end{aligned}$$

Vi har derfor at:

$$\sum_{\substack{T\subseteq S\\ e\notin T}} x^{r(S)-r(T)}y^{|T|-r(T)} = \begin{cases} xR\left(M\setminus\{e\};x,y\right) & \text{hvis } e \text{ er en koløkke,}\\ R\left(M\setminus\{e\};x,y\right) & \text{ellers.}\end{cases} \tag{3.8}$$

Vi ser nå på det andre leddet på høyre siden av 3.7. Dette er lik:

$$\sum_{U\subseteq S-\{e\}} x^{r((S-\{e\})\cup\{e\})-r(U\cup\{e\})}y^{|U\cup\{e\}|-r(U\cup\{e\})}.$$

La r' betegne rangfunksjonen på $M/\{e\}$. Fra (3.4) får vi at følgende gjelder for alle $U\subseteq S-\{e\}$:

$$r'(U) = \begin{cases} r\left(U\cup\{e\}\right) & \text{hvis } e \text{ er en løkke,}\\ r\left(U\cup\{e\}\right)-1 & \text{ellers.}\end{cases}$$

Så:

$$\begin{aligned}\sum_{\substack{T\subseteq S\\ e\in T}} x^{r(S)-r(T)}y^{|T|-r(T)} &= \begin{cases} \sum\limits_{U\subseteq S-\{e\}} x^{r'(S-\{e\})-r'(U)}y^{|U|+1-r'(U)} & \text{hvis } e \text{ er en løkke,}\\ \sum\limits_{U\subseteq S-\{e\}} x^{r'(S-\{e\})+1-(r'(U)+1)}y^{|U|+1-(r'(U)+1)} & \text{ellers.}\end{cases}\\ &= \begin{cases} y\sum\limits_{U\subseteq S-\{e\}} x^{r'(S-\{e\})-r'(U)}y^{|U|-r'(U)} & \text{hvis } e \text{ er en løkke,}\\ \sum\limits_{U\subseteq S-\{e\}} x^{r'(S-\{e\})-r'(U)}y^{|U|-r'(U)} & \text{ellers.}\end{cases}\end{aligned}$$

Dermed er:

$$\sum_{\substack{T\subseteq S\\ e\in T}} x^{r(S)-r(T)}y^{|T|-r(T)} = \begin{cases} yR\left(M/\{e\};x,y\right) & \text{hvis } e \text{ er en løkke,}\\ R\left(M/\{e\};x,y\right) & \text{ellers.}\end{cases} \tag{3.9}$$

Vi setter 3.8 og 3.9 inn i 3.7 og får:

$$R(M;x,y) = \begin{cases} R\left(M\setminus\{e\};x,y\right)+yR\left(M/\{e\};x,y\right) & \text{hvis } e \text{ er en løkke i } M,\\ xR\left(M\setminus\{e\};x,y\right)+R\left(M/\{e\};x,y\right) & \text{hvis } e \text{ er en koløkke i } M,\\ R\left(M\setminus\{e\};x,y\right)+R\left(M/\{e\};x,y\right) & \text{ellers.}\end{cases}$$

Siden $M/\{e\} = M\setminus\{e\}$ når e er en løkke eller en koløkke i M, har vi nå at:

$$R(M;x,y) = \begin{cases} (1+y)\,R\left(M\setminus\{e\};x,y\right) & \text{hvis } e \text{ er en løkke i } M,\\ (x+1)\,R\left(M\setminus\{e\};x,y\right) & \text{hvis } e \text{ er en koløkke i } M,\\ R\left(M\setminus\{e\};x,y\right)+R\left(M/\{e\};x,y\right) & \text{ellers.}\end{cases}$$

Men

$$R\left(M\left(\{e\}\right);x,y\right) = \begin{cases} y+1 & \text{når } e \text{ er en løkke i } M,\\ x+1 & \text{når } e \text{ er en koløkke i } M.\end{cases}$$

Dermed er:

$$R(M;x,y)=\begin{cases} R(M(\{e\});x,y)\,R(M\setminus\{e\};x,y) & \text{hvis } e \text{ er en løkke i } M,\\ R(M(\{e\});x,y)\,R(M\setminus\{e\};x,y) & \text{hvis } e \text{ er en koløkke i } M,\\ R(M\setminus\{e\};x,y)+R(M/\{e\};x,y) & \text{ellers.}\end{cases}$$

Så $R(M;x,y)$ er en T-G invariant. ■

Definisjon 3.116 *La $M=(S,r)$ være en matroide. **Tuttepolynomet** til M er gitt ved:*

$$T(M;x,y)=R(M;x-1,y-1).$$

Bemerkning 3.117 *Ikke-isomorfe matroider kan ha samme Tuttepolynom.*

Eksempel 3.118 *La $U_{2,3}$ være den uniforme matroiden på $S=\{1,2,3\}$. Eksempel 3.31 gir oss rangen til $T\subseteq S$:*

$$\begin{aligned} r(\varnothing) &= 0,\ r(\{1\})=r(\{2\})=r(\{3\})=1,\\ r(\{1,2\}) &= r(\{1,3\})=r(\{2,3\})=r(S)=2.\end{aligned}$$

Tuttepolynomet til $U_{2,3}$ er:

$$\begin{aligned} T(U_{2,3};x,y) &= R(U_{2,3};x-1,y-1)\\ &= \sum_{T\subseteq S}(x-1)^{r(S)-r(T)}(y-1)^{|T|-r(T)}\\ &= (x-1)^{r(S)-r(\varnothing)}(y-1)^{|\varnothing|-r(\varnothing)}\\ &\quad +(x-1)^{r(S)-r(\{1\})}(y-1)^{|\{1\}|-r(\{1\})}\\ &\quad +(x-1)^{r(S)-r(\{2\})}(y-1)^{|\{2\}|-r(\{2\})}\\ &\quad +(x-1)^{r(S)-r(\{3\})}(y-1)^{|\{3\}|-r(\{3\})}\\ &\quad +(x-1)^{r(S)-r(\{1,2\})}(y-1)^{|\{1,2\}|-r(\{1,2\})}\\ &\quad +(x-1)^{r(S)-r(\{1,3\})}(y-1)^{|\{1,3\}|-r(\{1,3\})}\\ &\quad +(x-1)^{r(S)-r(\{2,3\})}(y-1)^{|\{2,3\}|-r(\{2,3\})}\\ &\quad +(x-1)^{r(S)-r(S)}(y-1)^{|S|-r(S)}\\ &= (x-1)^2(y-1)^0+3(x-1)(y-1)^0+3(x-1)^0(y-1)^0\\ &\quad +(x-1)^0(y-1)\\ &= (x-1)^2+3(x-1)+3+(y-1)\\ &= x^2+x+y.\end{aligned}$$

Proposisjon 3.119 *La M være en matroide. Da er:*

$$T(M^*;x,y)=T(M;y,x).$$

Bevis Vi har at

$$T(M^*;x,y)=R(M^*;x-1,y-1)=R(M;y-1,x-1)=T(M;y,x).$$

■

Teorem 3.120 *La M være en matroide på S, og la $e \in S$. Da er:*

i) $T(U_{0,0}; x, y) = 1$.

ii) $T(M(\{e\}); x, y) = \begin{cases} y & \text{hvis } e \text{ er en løkke i } M, \\ x & \text{hvis } e \text{ er en koløkke i } M. \end{cases}$

iii) $T(M; x, y) = \begin{cases} T(M(\{e\}); x, y)\, T(M \setminus \{e\}; x, y) & \text{hvis } e \text{ er løkke eller koløkke i } M, \\ T(M \setminus \{e\}; x, y) + T(M/\{e\}; x, y) & \text{ellers.} \end{cases}$

Bevis i) $U_{0,0}$ er den unifome matroiden med $S = \varnothing$ og $\mathcal{I} = \{\varnothing\}$. Siden $r(\varnothing) = 0$, får vi:

$$\begin{aligned} T(U_{0,0}; x, y) &= R(U_{0,0}; x-1, y-1) \\ &= (x-1)^{r(\varnothing)-r(\varnothing)} (y-1)^{|\varnothing|-r(\varnothing)} = (x-1)^0 (y-1)^0 = 1. \end{aligned}$$

ii) Siden $T(M; x, y) = R(M; x-1, y-1)$, så holder ii) fra Proposisjon 3.114. iii) Siden $T(M; x, y) = R(M; x-1, y-1)$, så holder iii) fra Lemma 3.115. ■

Det er altså mulig å beregne Tuttepolynomet ved hjelp av matroideoperasjonene sletting og kontraksjon. Vi skal nå beregne Tuttepolynomet til matroiden i forrige eksempel på nytt.

Eksempel 3.121 *La $U_{2,3}$ være matroiden fra Eksempel 3.118 med $S = \{1, 2, 3\}$. Vi skal beregne Tuttepolynomet til $U_{2,3}$ ved hjelp av Teorem 3.120. Vi ser at for eksempel elementet $1 \in S$ ikke er en løkke i $U_{2,3}$, siden $\{1\} \in \mathcal{I}(U_{2,3}) = \{I \subseteq S \,||I| \leq 2\}$. $\mathcal{B}(U_{2,3}) = \{I \subseteq S \,||I| = 2\}$, så 1 er heller ikke en koløkke i $U_{2,3}$ siden $\{1\}$ ikke er inneholdt i basen $\{2, 3\}$ for $U_{2,3}$. Tuttepolynomet til $U_{2,3}$ er da gitt ved:*

$$T(U_{2,3}; x, y) = T(U_{2,3} \setminus \{1\}; x, y) + T(U_{2,3}/\{1\}; x, y).$$

$U_{2,3} \setminus \{1\}$ har grunnmengden $\{2, 3\}$ og fra eksempel 3.85 har vi at:

$$U_{2,3} \setminus \{1\} \cong U_{2,2}.$$

Fra Eksempel 3.31 ser vi at rangen til delmengdene T av $\{2, 3\}$ er da:

$$r(\varnothing) = 0,\ r(\{2\}) = r(\{3\}) = 1,\ \text{og } r(\{2, 3\}) = 2.$$

Tuttepolynomet til $U_{2,3} \setminus \{1\}$ er:

$$\begin{aligned} T(U_{2,3} \setminus \{1\}; x, y) &= R(U_{2,3} \setminus \{1\}; x-1, y-1) \\ &= \sum_{T \subseteq \{2,3\}} (x-1)^{r(\{2,3\})-r(T)} (y-1)^{|T|-r(T)} \\ &= (x-1)^2 + 2(x-1) + 1 \\ &= x^2. \end{aligned}$$

$U_{2,3}/\{1\}$ har også grunnmengden $\{2,3\}$ og fra Eksempel 3.85 får vi at:

$$U_{2,3}/\{1\} \cong U_{1,2}.$$

Eksempel 3.31 gir oss at rangen til $T \subseteq \{2,3\}$ er:

$$r(\varnothing) = 0, \text{ og } r(\{2\}) = r(\{3\}) = r(\{2,3\}) = 1.$$

Tuttepolynomet til $U_{2,3}/\{1\}$ er:

$$\begin{aligned} T(U_{2,3}/\{1\}; x, y) &= R(U_{2,3}/\{1\}; x-1, y-1) \\ &= \sum_{T \subseteq \{2,3\}} (x-1)^{r(\{2,3\})-r(T)} (y-1)^{|T|-r(T)} \\ &= (x-1) + 2 \cdot 1 + (y-1) \\ &= x + y. \end{aligned}$$

Tuttepolynomet til $U_{2,3}$ er da:

$$\begin{aligned} T(U_{2,3}; x, y) &= T(U_{2,3} \setminus \{1\}; x, y) + T(U_{2,3}/\{1\}; x, y) \\ &= x^2 + x + y, \end{aligned}$$

som er det samme vi fant i Eksempel 3.118.

Proposisjon 3.122 *Tuttepolynomet til den uniforme matroiden $U_{k,n}$ er gitt ved:*

$$T(U_{k,n}; x, y) = \sum_{i=0}^{k-1} \binom{n}{i} (x-1)^{k-i} + \sum_{i=k}^{n} \binom{n}{i} (y-1)^{i-k}.$$

Bevis Anta at $U_{k,n}$ er den uniforme matroiden på n-mengden S, og la $T \subseteq S$. Da er $r(S) = k$ og:

$$r(T) = \begin{cases} |T| & \text{når } |T| < k, \\ k & \text{når } |T| \geq k. \end{cases}$$

Vi får:

$$\begin{aligned}
T\left(U_{k,n};x,y\right) &= R\left(U_{k,n};x-1,y-1\right)\\
&= \sum_{T\subseteq S}\left(x-1\right)^{r(S)-r(T)}\left(y-1\right)^{|T|-r(T)}\\
&= \sum_{\substack{T\subseteq S\\|T|<k}}\left(x-1\right)^{r(S)-r(T)}\left(y-1\right)^{|T|-r(T)}\\
&\quad+\sum_{\substack{T\subseteq S\\|T|\geq k}}\left(x-1\right)^{r(S)-r(T)}\left(y-1\right)^{|T|-r(T)}\\
&= \sum_{\substack{T\subseteq S\\|T|<k}}\left(x-1\right)^{k-|T|}\left(y-1\right)^{|T|-|T|}+\sum_{\substack{T\subseteq S\\|T|\geq k}}\left(x-1\right)^{k-k}\left(y-1\right)^{|T|-k}\\
&= \sum_{\substack{T\subseteq S\\|T|<k}}\left(x-1\right)^{k-|T|}+\sum_{\substack{T\subseteq S\\|T|\geq k}}\left(y-1\right)^{|T|-k}\\
&= \left(x-1\right)^{k-0}+n\left(x-1\right)^{k-1}+\binom{n}{2}\left(x-1\right)^{k-2}\\
&\quad+\cdots+\binom{n}{k-1}\left(x-1\right)^{k-(k-1)}\\
&\quad+\binom{n}{k}\left(y-1\right)^{k-k}+\binom{n}{k+1}\left(y-1\right)^{k+1-k}+\cdots+\binom{n}{n}\left(y-1\right)^{n-k}\\
&= \left(x-1\right)^{k-0}+n\left(x-1\right)^{k-1}+\binom{n}{2}\left(x-1\right)^{k-2}\\
&\quad+\cdots+\binom{n}{k-1}\left(x-1\right)^{k-(k-1)}\\
&\quad+\binom{n}{k}\left(y-1\right)^{0}+\binom{n}{k+1}\left(y-1\right)^{1}+\cdots+\binom{n}{n}\left(y-1\right)^{n-k}\\
&= \sum_{i=0}^{k-1}\binom{n}{i}\left(x-1\right)^{k-i}+\sum_{i=k}^{n}\binom{n}{i}\left(y-1\right)^{i-k}.
\end{aligned}$$

■

Proposisjon 3.122 gir oss en ny måte å beregne Tuttepolynomet til $U_{k,n}$ på.

Eksempel 3.123 *Vi beregner Tuttepolynomet til $U_{2,3}$ ved hjelp av Proposisjon 3.122.*

$$\begin{aligned} T(U_{2,3};x,y) &= \sum_{i=0}^{1}\binom{3}{i}(x-1)^{2-i}+\sum_{i=2}^{3}\binom{3}{i}(y-1)^{i-2} \\ &= \binom{3}{0}(x-1)^2+\binom{3}{1}(x-1)^1+\binom{3}{2}(y-1)^0+\binom{3}{3}(y-1)^1 \\ &= (x-1)^2+3(x-1)+3+y-1 \\ &= x^2+x+y, \end{aligned}$$

som vi ser stemmer med Tuttepolynomet vi fant i Eksempel 3.118.

Vi skal nå se at Tuttepolynomet inneholder mye informasjon om matroiden.

Proposisjon 3.124 *La M være en matroide på grunnmengden S. Da gjelder følgende:*

i) Antall baser for M er lik $T(M;1,1)=R(M;0,0)$.

ii) Antall uavhengige mengder til M er lik $T(M;2,1)=R(M;1,0)$.

iii) Antall utspennende mengder til M er lik $T(M;1,2)=R(M;0,1)$.

iv) $T(M;2,2)=R(M;1,1)=2^{|S|}$.

Bevis Fra definisjonen på Tuttepolynomet har vi at $T(M;x,y)=R(M;x-1,y-1)$. Rang-generatorfunksjonen er definert som en sum over delmengder $T\subseteq S$. De eneste delmengdene som bidrar til $R(M;0,0)$ er de med $|T|=r(T)=r(S)$, det vil si basene til M. Så i) holder. De eneste delmengdene som bidrar til $R(M;1,0)$ er de med $|T|=r(T)$, det vil si uavhengige mengder til M og vi har ii). Vi skal nå bevise iii). Vi vet at antall utspennende mengder til M er lik antall uavhengige mengder til M^*. Så fra ii) har vi at antall utspennende mengder til M er lik $T(M^*;2,1)$. Fra Proposisjon 3.119 vet vi at $T(M^*;2,1)=T(M;1,2)$ og iii) følger. Til slutt har vi at $R(M;1,1)=\sum_{T\subseteq S}1^{r(S)-r(T)}1^{|T|-r(T)}=2^{|S|}$. ■

Eksempel 3.125 *La $U_{2,3}$ være matroiden fra Eksempel 3.118. Antallet baser for $U_{2,3}$ er da:*

$$\begin{aligned} T(U_{2,3};1,1) &= R(U_{2,3};0,0) \\ &= \sum_{T\subseteq S}0^{r(\{1,2,3\})-r(T)}0^{|T|-r(T)} \\ &= 0^20^0+3\cdot 0^10^0+3\cdot 0^00^0+0^00^1 \\ &= 3. \end{aligned}$$

Antallet uavhengige mengder for $U_{2,3}$ er lik:

$$\begin{aligned} T\left(U_{2,3};2,1\right) &= R\left(U_{2,3};1,0\right) \\ &= \sum_{T\subseteq S} 1^{r(\{1,2,3\})-r(T)} 0^{|T|-r(T)} \\ &= 1^2 0^0 + \left(1^1 0^0\right)\cdot 3 + \left(1^0 0^0\right)\cdot 3 + 1^0 0^1 \\ &= 1+3+3=7. \end{aligned}$$

Kapittel 4

Koder

4.1 Lineære koder

La n være et positivt heltall, og la Q være en q-mengde, kalt **alfabetet**. Mengden av n-tupler over Q betegnes Q^n. En q-ær blokk-kode C av lengde n er en ikke-tom delmengde av Q^n. Elementene i C kalles kodeord. Hvis $|C| = 1$, kaller vi koden triviell.

Definisjon 4.1 *La* $\underline{x} = (x_1, x_2, \ldots, x_n) \in Q^n$ *og* $\underline{y} = (y_1, y_2, \ldots, y_n) \in Q^n$. ***Hammingavstanden*** $d\left(\underline{x}, \underline{y}\right)$ *mellom* $\underline{x}$ *og* $\underline{y}$ *er gitt ved:*

$$d\left(\underline{x}, \underline{y}\right) = \left|\{i \,|x_i \neq y_i, i = 1, \ldots, n\}\right|.$$

Hammingavstanden mellom $\underline{x}$ og $\underline{y}$ er altså antall koordinater der $\underline{x}$ og $\underline{y}$ er forskjellige. Hammingavstanden er en metrikk på Q^n.

Definisjon 4.2 ***Hammingvekten*** $w\left(\underline{x}\right)$ *til et kodeord* $\underline{x} = (x_1, x_2, \ldots, x_n)$ *er:*

$$w\left(\underline{x}\right) = \left|\{i \,|x_i \neq 0, i = 1, \ldots, n\}\right| = d\left(\underline{x}, \underline{0}\right),$$

det vil si antall koordinater forskjellig fra 0 *i* $\underline{x}$.

Definisjon 4.3 ***Minimumsavstanden*** *til en ikke-triviell kode* C *er gitt ved:*

$$d = d\left(C\right) = \min\left\{d\left(\underline{x}, \underline{y}\right) \left|\underline{x}, \underline{y} \in C, \underline{x} \neq \underline{y}\right.\right\}.$$

En kode av lengde n, med M kodeord og med minimumsavstand d refereres til som en (n, M, d)-kode.

Definisjon 4.4 ***Minimumsvekten*** *til en kode* C *er gitt ved:*

$$w\left(C\right) = \min\left\{w\left(\underline{c}\right) |\underline{c} \in C - \{\underline{0}\}\right\},$$

det vil si den minste vekten forskjellig fra 0 *i* C.

Teorem 4.5 (Singletonbegrensningen) *La* C *være en* q*-ær* (n, M, d)*-kode. Da er:*

$$M \leq q^{n-d+1}.$$

Bevis Se [12] (Teorem 2.1.8) for bevis. ■

La Q være kroppen $\mathbb{F}_q$. Da er Q^n et n-dimensjonalt vektorrom, nemlig $\mathbb{F}_q^n$.

Definisjon 4.6 *En q-ær **lineær kode** av lengde n og dimensjon k er et k-dimensjonalt underrom av $\mathbb{F}_q^n$.*

En kode C er altså lineær hvis $\underline{x} + \underline{y} \in C$ når $\underline{x}, \underline{y} \in C$. Legg merke til at en lineær kode alltid må inneholde ordet $\underline{0}$. For hvis C skal være lineær, så må summen $\underline{x} + (-1)\,\underline{x} = \underline{0}$ være et kodeord siden C er lukket under addisjon og multiplikasjon med -1. Vi bruker $[n, k, d]$-kode som notasjon for en k-dimensjonal lineær kode av lengde n med minimumsavstand d. Merk at en q-ær $[n, k, d]$-kode er også en q-ær $\left(n, q^k, d\right)$-kode, men ikke alle $\left(n, q^k, d\right)$-koder er en $[n, k, d]$-kode. Noen ganger sløyfer vi parameteren d i notasjonene (n, M, d) og $[n, k, d]$.

Teorem 4.7 *La C være en lineær kode. Da er minimumsavstanden til C lik minimumsvekten til C:*

$$d\left(C\right) = w\left(C\right).$$

Bevis Se [7] (Teorem 3.2.3). ■

Definisjon 4.8 *La C være en $[n, k, d]$-kode. En **generatormatrise** G for C er en $k \times n$-matrise der radene er en basis for C.*

Bemerkning 4.9 *Merk at en generatormatrise for C må ha rang lik k.*

Siden C er et k-dimensjonalt underrom, så har C en basis $\{\underline{c}_1, \underline{c}_2, \ldots, \underline{c}_k\}$ slik at ethvert kodeord $\underline{c} \in C$ kan representeres som en lineær kombinasjon av elementene i basisen:

$$\underline{c} = u_1\underline{c}_1 + u_2\underline{c}_2 + \ldots + u_k\underline{c}_k, \tag{4.1}$$

der $u_i \in \mathbb{F}_q$. Ligning 4.1 kan skrives som:

$$\underline{c} = \underline{u}G,$$

der $\underline{u} = (u_1, \ldots, u_k) \in \mathbb{F}_q$ og

$$G = \begin{bmatrix} \underline{c}_1 \\ \underline{c}_2 \\ \vdots \\ \underline{c}_k \end{bmatrix} = \begin{bmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,n} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{k,1} & c_{k,2} & \cdots & c_{k,n} \end{bmatrix}$$

er en generatormatrise for C.

To lineære koder C og C' av lengde n over $\mathbb{F}_q$ er **ekvivalente** hvis den ene koden kan fåes fra den andre ved å permutere koordinatene og ved å multiplisere koordinater med skalarer $\neq 0$. Vi gir nå Teorem 5.5 i [5]:

Teorem 4.10 *La G være en generatormatrise for en $[n,k]$-kode. Da kan vi ved å utføre elementære rad- og kolonneoperasjoner omforme G til* ***standard form***

$$\begin{bmatrix} I_k & B \end{bmatrix},$$

der I_k er $k \times k$-identitetsmatrisen og B er en $k \times (n-k)$-matrise.

Bevis Hill beviser dette i [5]. ■

Bemerkning 4.11 *Elementære radoperasjoner bevarer den lineære uavhengigheten mellom radene til en generatormatrise og bytter en basis ut med en annen for den samme koden. De elementære kolonneoperasjonene konverterer generatormatrisen til en generatormatrise for en ekvivalent kode. Legg også merke til at standard formen $\begin{bmatrix} I_k & B \end{bmatrix}$ til en generatormatrise ikke er unik. Permutasjon av kolonnene til B vil gi en generatormatrise for en ekvivalent kode.*

Hvis C er en $[n,k]$-kode med generatormatrise G på standard form, så kalles de første k symbolene i kodeordet $\underline{c} = \underline{u}G$ informasjonssymboler, siden de danner ordet $\underline{u}$ i $\mathbb{F}_q^k$. De siste $r = n-k$ symbolene i $\underline{c} = \underline{u}G$ kalles **redundansen** til koden.

Definisjon 4.12 *La C være en $[n,k]$-kode. En* ***paritetssjekkmatrise*** *H for C er en $(n-k) \times n$-matrise slik at:*

$$\underline{c} \in C \iff \underline{c}H^T = \underline{0},$$

der H^T er den transponerte av H.

Teorem 4.13 *La C være en $[n,k]$-kode. Hvis $G = \begin{bmatrix} I_k & B \end{bmatrix}$ er en generatormatrise på standard form for C, så er $H = \begin{bmatrix} -B^T & I_{n-k} \end{bmatrix}$ en paritetssjekkmatrise for C.*

Bevis Se [13], side 314-315. ■

Legg merke til at $GH^T = [0]$, der $[0]$ er en $k \times (n-k)$ 0-matrise. Indreproduktet $\underline{x} \cdot \underline{y}$ av vektorene $\underline{x} = (x_1, x_2, \ldots, x_n)$ og $\underline{y} = (y_1, y_2, \ldots, y_n)$ i $\mathbb{F}_q^n$ er definert som $\underline{x} \cdot \underline{y} = \sum_{i=1}^{n} x_i y_i$. Hvis $\underline{x} \cdot \underline{y} = 0$, så er $\underline{x}$ og $\underline{y}$ **ortogonale**.

Definisjon 4.14 *La C være en $[n,k]$ -kode.* ***Dualkoden*** *til C, betegnet ved $C^\perp$, er mengden av vektorer som er ortogonal med alle kodeordene i C:*

$$C^\perp = \left\{ \underline{x} \in \mathbb{F}_q^n \,|\, \underline{x} \cdot \underline{c} = 0 \ \forall \underline{c} \in C \right\}.$$

Proposisjon 4.15 *Hvis C er en $[n,k]$ -kode med generatormatrise $G = \begin{bmatrix} I_k & B \end{bmatrix}$, så er $C^\perp$ en $[n, n-k]$-kode med generatormatrise $H = \begin{bmatrix} -B^T & I_{n-k} \end{bmatrix}$. G er en paritetssjekkmatrise for $C^\perp$.*

Bevis Se [13], side 318. ■

Vi har følgende viktige resultat (Teorem 8.4 i [5]):

Teorem 4.16 *Anta at C er en $[n,k]$-kode over $\mathbb{F}_q$ med paritetssjekkmatrise H. Da er minimumsavstanden for C lik d hvis og bare hvis alle valg av $d-1$ kolonner fra H er lineært uavhengige, og minst en mengde av d kolonner fra H er lineært avhengig.*

Bevis Hill beviser dette i [5]. ■

Definisjon 4.17 *La C være en lineær kode av lengde n, og la A_i være antall kodeord i C av vekt i.* ***Vektenumeratoren*** *for C er gitt ved:*

$$W_C(z) = \sum_{i=0}^{n} A_i z^i = \sum_{\underline{c} \in C} z^{w(\underline{c})}.$$

Bemerkning 4.18 *Forskjellige koder kan ha den samme vektenumeratoren.*

Eksempel 4.19 *La C være koden med generatormatrise over $\mathbb{F}_2$ gitt ved*

$$G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

Da er $C = \{000, 101, 011, 110\}$. C har ett kodeord av vekt 0 og tre kodeord av vekt 2, så vektenumeratoren for C er:

$$W_C(z) = 1 + 3z^2.$$

Eksempel 4.20 *Den q-ære repetisjonskoden av lengde n har vektenumeratoren*

$$W_C(z) = 1 + (q-1)\, z^n,$$

det vil si ett kodeord av vekt 0 og $(q-1)$ kodeord av vekt n.

Neste teorem gir en relasjon mellom vektenumeratorene for en lineær kode C og dualkoden $C^\perp$.

Teorem 4.21 (MacWilliams) *La C være en $[n,k]$ -kode over $\mathbb{F}_q$ med vektenumerator $W_C(z)$. Da er vektenumeratoren for $C^\perp$ gitt ved:*

$$W_{C^\perp}(z) = \frac{1}{|C|}\left(1 + (q-1)\, z\right)^n W_C\left(\frac{1-z}{1+(q-1)\, z}\right).$$

Bevis Greenes Teorem (Teorem 5.10 i denne oppgaven) viser at vektenumeratoren for en lineær kode er en spesialisering av Tuttepolynomet til den korresponderende matroiden. Så beviset av MacWilliams Teorem kommer etter at vi har introdusert Greenes Teorem i delkapitlet som omhandler matroideegenskaper for koder. ■

Fra Definisjon 4.17 og Teorem 4.21 ser vi at vektenumeratoren for $C^\perp$ kan omskrives som:

$$\begin{aligned} W_{C^\perp}(z) &= \frac{1}{|C|}(1+(q-1)z)^n W_C\left(\frac{1-z}{1+(q-1)z}\right) \\ &= \frac{1}{q^k}(1+(q-1)z)^n \sum_{i=0}^{n} A_i \left(\frac{1-z}{1+(q-1)z}\right)^i \\ &= q^{-k}\sum_{i=0}^{n} A_i (1-z)^i (1+(q-1)z)^{n-i}. \end{aligned}$$

Eksempel 4.22 *La C være koden $C = \{000, 101, 011, 110\}$ fra Eksempel 4.19. C er en $[3, 2]$ -kode over $\mathbb{F}_2$ med vektenumeratoren:*

$$W_C(z) = 1 + 3z^2.$$

Ved å bruke MacWilliams Teorem er vektenumeratoren for dualkoden $C^\perp = \{000, 111\}$ gitt ved:

$$\begin{aligned} W_{C^\perp}(z) &= 2^{-2}(1+z)^3 W_C\left(\frac{1-z}{1+z}\right) \\ &= \frac{1}{4}(1+z)^3\left(1+\frac{3(1-z)^2}{(1+z)^2}\right) \\ &= \frac{1}{4}\left((1+z)^3 + 3(1+z)(1-z)^2\right) \\ &= \frac{1}{4}\left(z^3+3z^2+3z+1+3z^3-3z^2-3z+3\right) \\ &= 1+z^3. \end{aligned}$$

Eksempel 4.23 *La C være den q-ære repetisjonskoden av lengde n. Siden vektenumeratoren for C er*

$$W_C(z) = 1 + (q-1)z^n,$$

så har dualkoden vektenumeratoren:

$$\begin{aligned} W_{C^\perp}(z) &= \frac{1}{|C|}(1+(q-1)z)^n W_C\left(\frac{1-z}{1+(q-1)z}\right) \\ &= \frac{1}{q}(1+(q-1)z)^n\left(1+(q-1)\frac{(1-z)^n}{(1+(q-1)z)^n}\right) \\ &= \frac{1}{q}\left((1+(q-1)z)^n + (q-1)(1-z)^n\right). \end{aligned}$$

4.2 MDS koder

Vi starter med å gi en lineær"versjon av Teorem 4.5.

Teorem 4.24 *En $[n, k, d]$-kode over $\mathbb{F}_q$ oppfyller:*

$$k \leq n - d + 1.$$

Bevis Dette følger direkte fra Teorem 4.5. ■

Definisjon 4.25 *En $[n, k, d]$-kode med $d = n - k + 1$ kalles en **MDS kode**.*

En MDS kode C har altså minimumsavstand lik $d = r + 1$, der $r = n - k$ er redundansen til C.

Teorem 4.26 *La C være en $[n, k]$-kode med paritetssjekkmatrise H. Da er C en MDS kode hvis og bare hvis alle valg av $n - k$ kolonner fra H er lineært uavhengige.*

Bevis Dette følger direkte fra definisjonen av MDS kode og Teorem 4.16. ■

Det at alle valg av r kolonner fra en paritetssjekkmatrise er lineært uavhengige kaller vi ofte for MDS-egenskapen.

Teorem 4.27 *La C være en $[n, k]$-kode med paritetssjekkmatrise $H = \begin{bmatrix} B^T & I_{n-k} \end{bmatrix}$. Da er C en MDS kode hvis og bare hvis alle kvadratiske undermatrise av B^T er ikke-singulær.*

Bevis For bevis, se Teorem 15.6 i [5]. ■

Teorem 4.28 *La C være en MDS $[n, k]$-kode. Da er dualkoden $C^\perp$ en MDS $[n, n - k]$-kode.*

Bevis Anta at C er en $[n, k]$-kode med paritetssjekkmatrise $\begin{bmatrix} B^T & I_{n-k} \end{bmatrix}$. Da er C en MDS kode hvis og bare hvis enhver kvadratiske undermatrise av B^T er ikke-singulær. Men da har B den samme egenskapen (siden $\det A = \det A^T$ for enhver kvadratisk matrise A). Så koden $C^\perp$ med paritetssjekkmatrise $\begin{bmatrix} I_k & -B \end{bmatrix}$ er MDS. ■

Teorem 4.29 *La C være en $[n, k]$-kode med generatormatrise G. Da er C MDS hvis og bare hvis alle valg av k kolonner fra G er lineært uavhengig.*

Bevis Fra Teorem 4.28 har vi at en kode C er en MDS $[n, k]$-kode hvis og bare hvis $C^\perp$ er en MDS $[n, n - k]$-kode. Vi har videre fra Teorem 4.26 at $C^\perp$ er MDS hvis og bare hvis alle valg av k kolonner fra en paritetssjekkmatrise for $C^\perp$ er lineært uavhengig. Men en paritetssjekkmatrise for $C^\perp$ er en generatormatrise for C, så C er MDS hvis og bare hvis alle valg av k kolonner fra en generatormatrise for C er lineært uavhengig. ■

Vi skal nå se på koder som ikke oppfyller likhet i Singletonbegrensningen, men som nesten gjør det.

Definisjon 4.30 *La C være en $[n, k, d]$-kode. **Singletondefekten** til C er gitt ved:*

$$s(C) = n - k + 1 - d.$$

Eksempel 4.31 *Singletondefekten til en MDS kode C er $s(C) = 0$.*

Definisjon 4.32 *En kode C med Singletondefekt $s(C) = 1$ kalles **nesten-MDS**.*

En nesten-MDS kode har altså minimumsavstanden $d = n - k$.

Bemerkning 4.33 *Hvis C er nesten-MDS, så trenger ikke $C^\perp$ å være det.*

Definisjon 4.34 *En kode C med $s(C) = s\left(C^\perp\right) = 1$ kalles **nær-MDS**.*

4.3 Høyere vekter for lineære koder

Vi skal nå utvide Hammingvektbegrepet. Motivert av applikasjoner i kryptografi definerte Wei i sin artikkel [14] i 1991 det generaliserte Hamming vekthierarkiet til en lineær kode. Vi avgrenser oss til binære koder.

Definisjon 4.35 *La $N \subseteq \mathbb{F}_q^n$. **Støtten** til N, betegnet ved $\chi(N)$, er:*

$$\chi(N) = \{i \,|\exists \underline{c} = (c_1, c_2, \ldots, c_n) \in N, c_i \neq 0\}.$$

Sagt med ord er $\chi(N)$ mengden av posisjoner der ikke alle vektorer i N er 0.

Eksempel 4.36 *La C være den binære koden med følgende generatormatrise:*

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Da er for eksempel:

$$\begin{aligned} \chi(\{00000, 10010\}) &= \{1, 4\}, \\ \chi(\{10010, 01011, 11001\}) &= \{1, 2, 4, 5\} \text{ og} \\ \chi(C) &= \{1, 2, 3, 4, 5\}. \end{aligned}$$

Definisjon 4.37 ***Støttevekten*** *til N er kardinaliteten til mengden $\chi(N)$.*

Definisjon 4.38 *Den h-te **generaliserte Hammingvekten** til C er*

$$d_h(C) = \min\{|\chi(D_h)| \,|D_h \subseteq C\}$$

for D_h et h-dimensjonalt underrom av C.

Bemerkning 4.39 *Legg merke til at*

$$\begin{aligned} d_1(C) &= \min\{|\chi(D_1)| \,|D_1 \subseteq C\} = \min\{|\chi(\underline{c})| \,|\underline{c} \in C - \{\underline{0}\}\} \\ &= \min\{w(\underline{c}) \,|\underline{c} \in C - \{\underline{0}\}\} = d, \end{aligned}$$

som er den tradisjonelle minimumsavstanden til en kode C.

Eksempel 4.40 *Vi betrakter koden C fra forrige eksempel. Vi ser at $d_1(C) = 2$ er lik minimumsavstanden til C. Vi får $d_2(C)$ ved å ta den laveste støttevekten til alle 2-dimensjonale underrom av C. Vi får at $d_2(C) = \min\{|\chi(D_2)|\} = 4$. Vi ser at $d_3(C) = 5$, siden det finnes kodeord i C som er $\neq 0$ i de fem posisjonene.*

Definisjon 4.41 ***Vekthierarkiet*** *til en $[n, k]$-kode C er mengden av heltall*

$$\{d_h(C) \,|1 \leq h \leq k\}.$$

Teorem 4.42 *For en $[n,k]$-kode C med $k>0$, har vi:*

$$1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n.$$

Bevis Se [14], side 1412. ■

Teorem 4.24, som er en lineær"versjon av Singletonbegrensningen, sier at $d \leq n-k+1$ for en $[n,k,d]$-kode over $\mathbb{F}_q$. Wei generaliserer dette i [14].

Korollar 4.43 (Generalisert Singletonbegrensning) *For en $[n,k]$-kode C, har vi:*

$$d_h(C) \leq n-k+h.$$

Bemerkning 4.44 *Når $h=1$, er dette Singletonbegrensningen.*

La H være en paritetssjekkmatrise for en $[n,k]$-kode C. Da sier Teorem 4.16 at $d=d_1$ er det minste antallet t slik at t av kolonnene i H er lineært avhengige. Vi omskriver dette til at d_1 er det minste antallet t slik at det eksisterer t kolonner i H som spenner ut et rom av dimensjon høyst $t-1$. Wei gir følgende generalisering av Teorem 4.16 i [14]. Vi lar $\langle H_i \,|i \in I\rangle$ være rommet generert av kolonnevektorene H_i, $1 \leq i \leq n$. Vi betegner rangen til $\langle H_i \,|i \in I\rangle$ ved $rg\left(\langle H_i \,|i \in I\rangle\right)$.

Teorem 4.45 *For alle $h \leq k$,*

$$d_h(C) = \min\left\{|I| \,\middle|\, |I| - rg\left(\langle H_i \,|i \in I\rangle\right) \geq h\right\}.$$

Bevis Se [14], side 1413. ■

Med andre ord har C generalisert Hammingvekt $d_h(C)=d$ hvis og bare hvis det eksisterer d kolonner i H som spenner ut et rom av dimensjon høyst $d-h$. Altså er d det minste heltallet slik at H har d kolonner med rang høyst lik $d-h$. Teorem 4.45 gir oss en alternativ måte å beregne de generaliserte Hammingvektene.

Eksempel 4.46 *Vi betrakter koden C fra Eksempel 4.36. Vi ser at $G=\begin{bmatrix} I_3 & B \end{bmatrix}$, der*

$$B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}, \text{ så}$$

$$H = \begin{bmatrix} B^T & I_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

er en paritetssjekkmatrise for C. La $I \subseteq \{1,2,\ldots,5\}$. Vi betrakter underrommet generert av kolonnene H_i for $i \in I$. Vi skal finne I som er slik at $|I|$ er det minste heltallet som oppfyller betingelsen $rg\left(\langle H_i \,|i \in I\rangle\right) \leq |I|-h$. For $h=1$ ser vi at de minste mengdene av kolonner som tilfredsstiller betingelsen $rg\left(\langle H_i \,|i \in I\rangle\right) \leq |I|-1$ er $I=\{1,4\}$ eller $I=\{3,5\}$. Så $d_1(C)=2$. Likeledes, den minste mengden av kolonner som oppfyller den gitte betingelsen for $h=2$ har kardinalitet $|I|=4$ ($I=\{1,2,3,4\}$ er en slik mengde). Så $d_2(C)=4$. Til slutt, $d_3(C)=5$.

Neste teorem gir en sammenheng mellom vekthierarkiene til en kode C og dualkoden $C^{\perp}$. Vi betegner vekthierarkiet til den duale koden ved $\left\{d_h\left(C^{\perp}\right)|1 \leq h \leq n-k\right\}$.

Teorem 4.47 *La C være en $[n,k]$-kode. Da er:*

$$\left\{d_h\left(C\right)|1 \leq h \leq k\right\} = \left\{1,2,\ldots,n\right\} - \left\{n+1-d_h\left(C^{\perp}\right)|1 \leq h \leq n-k\right\}.$$

Bevis Se [14], side 1413. ■

Eksempel 4.48 *Vi ser på H fra forrige eksempel som en generatormatrise for den duale koden til C. Da er paritetsjekkmatrisen for $C^{\perp}$ lik generatormatrisen for C:*

$$H_{C^{\perp}} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Vi bruker Teorem 4.45 og beregner de generaliserte Hammingvektene til $C^{\perp}$:

$$d_1\left(C^{\perp}\right) = 3 \text{ og } d_2\left(C^{\perp}\right) = 5.$$

Vi konstruerer så mengden

$$\left\{6-d_h\left(C^{\perp}\right)|1 \leq h \leq 2\right\} = \left\{1,3\right\}$$

og ser at dette er komplementet til vekthierarkiet til C.

Raddum gir i [10] beskrivelser av MDS, nesten- og nær-MDS ved hjelp av høyere vekter. La C være en MDS $[n,k]$-kode. Setter vi opp tallene

$$\left\{n+1-d_h\left(C^{\perp}\right)|1 \leq h \leq n-k\right\} \cup \left\{d_h\left(C\right)|1 \leq h \leq k\right\} = \left\{1,2,\ldots,n\right\} \qquad (4.2)$$

i stigende rekkefølge vil følgen bli:

$$n+1-d_{n-k}\left(C^{\perp}\right),\ldots,n+1-d_1\left(C^{\perp}\right),d_1\left(C\right),\ldots,d_k\left(C\right).$$

Ingen av tallene $n+1-d_h\left(C^{\perp}\right)$ kan stå blant tallene $d_1\left(C\right),\ldots,d_k\left(C\right)$, siden vi da ville få $d_1\left(C\right) < n-k+1$.

La nå C være nesten-MDS. Vi kan beskrive C ved at tallene i 4.2 stilt opp i rekkefølge vil danne følgen:

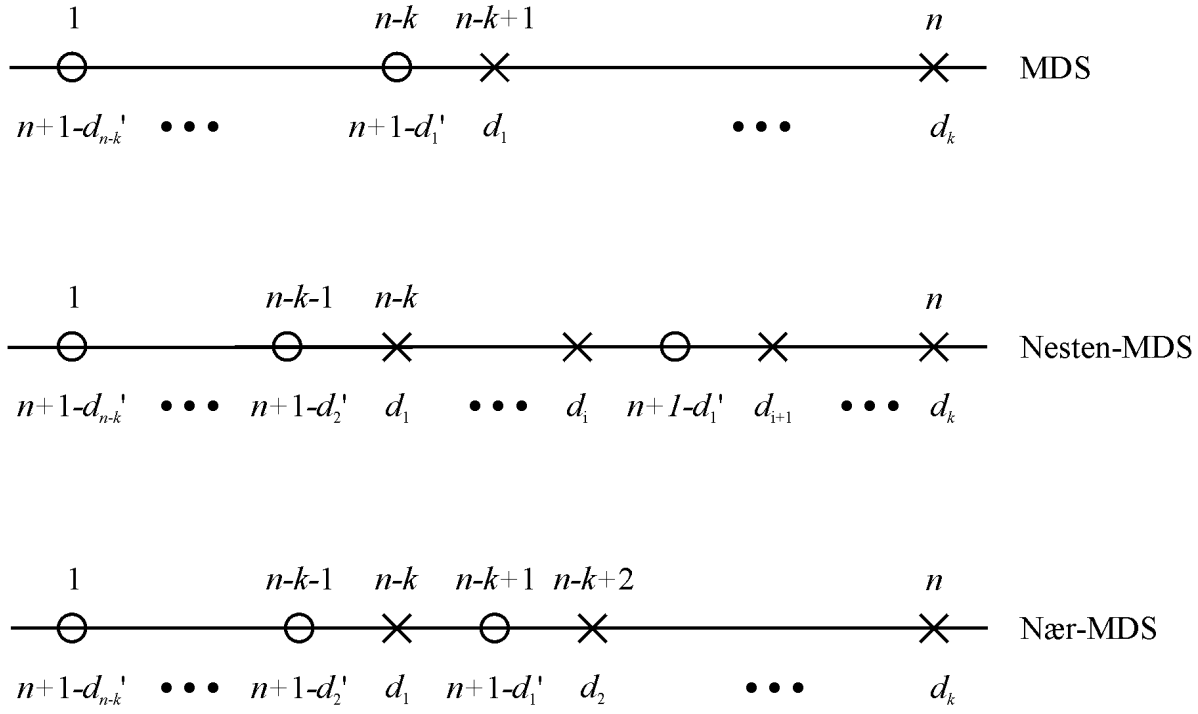
$$n+1-d_{n-k}\left(C^{\perp}\right),\ldots,n+1-d_2\left(C^{\perp}\right),d_1\left(C\right),\ldots,d_i\left(C\right),n+1-d_1\left(C^{\perp}\right),d_{i+1}\left(C\right),\ldots,d_k\left(C\right).$$

Siden $d_1\left(C\right) = n-k$, må nøyaktig ett av tallene $n+1-d_h\left(C^{\perp}\right)$ stå blant $\left\{d_h\left(C\right)|1 \leq h \leq k\right\}$. Vi vet at $d_1\left(C^{\perp}\right) < \cdots < d_{n-k}\left(C^{\perp}\right)$, så $n+1-d_1\left(C^{\perp}\right)$ er det største tallet blant $n+1-d_h\left(C^{\perp}\right)$ og må derfor tallet som finnes blant $d_h\left(C\right)$-ene.

Hvis C er nær-MDS, så kan C karakteriseres ved at tallene i 4.2 stilt opp i rekkefølge vil danne følgen:

$$n+1-d_{n-k}\left(C^{\perp}\right),\ldots,n+1-d_2\left(C^{\perp}\right),d_1\left(C\right),n+1-d_1\left(C^{\perp}\right),d_2\left(C\right),\ldots,d_k\left(C\right).$$

Tallet $n+1-d_1\left(C^{\perp}\right)$ må stå blant $d_h\left(C\right)$-ene siden C er nesten-MDS. $C^{\perp}$ skal også være nesten-MDS, det vil si $d_1\left(C^{\perp}\right)=n-(n-k)=k$. Dermed er $n+1-d_1\left(C^{\perp}\right)=n-k+1$ og $n+1-d_1\left(C^{\perp}\right)$ må stå på plassen etter $d_1\left(C\right)=n-k$. Vi ser at det å være nær-MDS er et spesialtilfelle av det å være nesten-MDS. Figur 4-1 illustrerer Raddums beskrivelse av MDS, nesten- og nær-MDS. I figuren er $d_i\left(C\right)$-ene betegnet ved d_i og illustrert ved et kryss, mens $n+1-d_i\left(C\right)$ er betegnet ved $n+1-d_i'$ og er illustrert ved en sirkel.



Figur 4-1: En illustrasjon av MDS, nesten- og nær-MDS ved hjelp av høyere vekter

Definisjon 4.49 *En h-MDS kode er en kode der h er det minste tallet slik at $d_h=n-k+h$.*

Bemerkning 4.50 *Merk at hvis $d_h=n-k+h$, så er $d_i=n-k+i$ for $h<i\leq k$. Legg også merke til at en MDS kode er 1-MDS.*

Fra Definisjon 4.49 og Teorem 4.45 ser vi at h-MDS betyr at det det eksisterer $n-k+h$ kolonner i paritetssjekkmatrisen H (generatormatrise for $C^{\perp}$) med rang $\leq(n-k+h)-h=n-k$, og hver gang vi velger $n-k+h-1$ kolonner er rangen $\geq n-k+h-1-(h-1)=n-k$. h er altså det minste tallet slik at hver gang vi velger $r+h-1$ kolonner, så har disse rang $\geq r$, der $r=n-k$ er redundansen til koden. Vi vet at en paritetssjekkmatrise H for en kode C er en $(n-k)\times n$-matrise, så en kode er h-MDS hvis og bare hvis alle valg av $n-k+h-1$ kolonner fra H danner en matrise med full rang.

Vi gjengir Proposisjon 3.1.6 og Proposisjon 3.1.7 i [10].

Proposisjon 4.51 *C er nær-MDS hvis og bare hvis C og $C^{\perp}$ begge er 2-MDS.*

Bevis Bevis finnes i [10]. ■

Proposisjon 4.52 *En kode C er nær-MDS hvis og bare hvis den er nesten-MDS og 2-MDS.*

Bevis Se [10]. ■

Kapittel 5

Noen sammenhenger mellom matroider og koder

5.1 Vektormatroiden til en lineær kode

La G være en $k \times n$-matrise over $\mathbb{F}_q$ med lineært uavhengige rader. Fra G kan vi danne følgende to konstruksjoner:

1. Radrommet til G er en $[n, k]$-kode C over $\mathbb{F}_q$.
2. Vi kan definere en vektormatroide $M[G]$ av rang k på indeksmengden $\{1, 2, \ldots, n\}$ for kolonnene til G.

Definisjon 5.1 *La C være en $[n, k]$-kode over $\mathbb{F}_q$. Da er **vektormatroiden til** C matroiden $M[G]$, der G er en generatormatrise for C.*

Generatormatrisen G er en $\mathbb{F}_q$-representasjon for $M[G]$. Vi sier at $M[G]$ er matroiden som korresponderer til den lineære koden C, eller at C korresponderer til $M[G]$. Vi betegner ofte denne vektormatroiden M_C.

Som tidligere nevnt, så endrer ikke elementære radoperasjoner på G den lineære koden. Isomorfiklassen til vektormatroiden forandres heller ikke, siden disse operasjonene ikke endrer på hvilke kolonner som er lineært uavhengige. Likeledes forblir isomorfiklassen til en matroide $M[G]$ uforandret selv om bytter ut C (og G) med (generatormatrisen til) en ekvivalent kode. Multiplikasjon av en kolonne til G med en skalar $\neq 0$ gir heller ikke noen endringer på hvilke kolonner som er lineært uavhengige, så vektormatroiden blir uforandret. Permutasjon av kolonner til G bytter bare på kolonneindeksene slik at vektormatroiden vi får er isomorf med den opprinnelig. Isomorfiklassen bevares altså under kolonnepermutasjon. Disse to kolonneoperasjonene gir en ekvivalent kode. Så vektormatroiden til en lineær kode er veldefinert, siden ethvert par av generatormatriser for C er relatert ved disse rad- og kolonneoperasjonene og slik gir isomorfe matroider.

Eksempel 5.2 *En standard representasjon for den uniforme matroiden $U_{1,3}$ over $\mathbb{F}_2$ er gitt ved:*

$$\begin{bmatrix} 1 & 1 & 1 \end{bmatrix}.$$

Dette er en generatormatrise for den binære repetisjonskoden av lengde 3, som også er Hammingkoden $Ham\,(2,2)$. Så $Ham\,(2,2)$ korresponderer til $U_{1,3}$.

Eksempel 5.3 *En generatormatrise for den duale Hammingkoden $Ham\,(3,2)^{\perp}$ er gitt ved:*

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Fra (3.5) har vi at denne matrisen er en representasjon for Fanomatriden F_7 over $\mathbb{F}_2$. Vi har altså at $M_{Ham(3,2)^{\perp}} = M\,[G] = F_7$.

Bemerkning 5.4 *Merk at ifølge Britz i [3] inneholder koden C mer informasjon enn matroiden M_C. En matroide M kan være vektormatroiden til flere ikke-ekvivalente lineære koder over den samme kroppen.*

Eksempel 5.5 *La*

$$G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \text{ og } G' = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \end{bmatrix}$$

være generatormatriser for henholdsvis kodene C og C' over $\mathbb{F}_3$. Da er C og C' ikke-ekvivalente koder som har isomorfe vektormatroider; $M\,[G] \cong M\,[G']$.

Neste resultat forteller oss at den duale matroiden korresponderer til den duale koden.

Proposisjon 5.6 *Hvis matroiden M korresponderer til $[n,k]$-koden C, så korresponderer den duale matroiden M^* til dualkoden $C^{\perp}$.*

Bevis Anta at C er en $[n,k]$-kode med en generatormatrise G, og at vektormatroiden $M\,[G]$ korresponderer til den lineære koden C. Generatormatrisen G er da en $\mathbb{F}_q$-representasjon for $M\,[G]$. Vi kan redusere G til formen $\begin{bmatrix} I_k & B \end{bmatrix}$, der I_k er en $k \times k$-identitetsmatrise og B er $k \times (n-k)$-matrise. Da har vi fra Teorem 3.75 at en representasjon for den duale matroiden M^* er gitt ved matrisen $\begin{bmatrix} -B^T & I_{n-k} \end{bmatrix}$, der B^T er den transponerte matrisen til B og I_{n-k} er $(n-k) \times (n-k)$-identitetsmatrisen. Fra Proposisjon 4.15 vet vi at matrisen $H = \begin{bmatrix} -B^T & I_{n-k} \end{bmatrix}$ er en generatormatrise for den duale koden $C^{\perp}$, så det finnes en vektormatroide $M\,[H]$ som korresponderer til $C^{\perp}$. Siden $(M\,[G])^* = M\,[H]$, har vi at $M_C^* = M_{C^{\perp}}$ og resultatet følger. ■

Vi har altså at en $[n,k]$-kode C over $\mathbb{F}_q$ har en generatormatrise G som er en representasjon for matroiden M over $\mathbb{F}_q$. C har en paritetssjekkmatrise H slik at $GH^T = [0]$, der $[0]$ er en $k \times (n-k)$ 0-matrise. Den duale koden $C^{\perp}$ har H som generatormatrise. H er en representasjon for den duale matroiden M^* over $\mathbb{F}_q$. Matrisen G er en paritetssjekkmatrise for $C^{\perp}$.

5.2 MDS koder og uniforme matroider

Vi skal nå se hva MDS betyr på matroidenivå.

La C være en MDS kode. Da har C minimumsavstand $d = r + 1$, der $r = n - k$ er redudansen til C. Vi vet at alle valg av r kolonner fra en paritetssjekkmatrise for C er lineært uavhengige. Fra matroideteorien husker vi at den uniforme matroiden $U_{n-k,n}$ har rang lik $n - k$. Alle delmengdene av grunnmengden til $U_{n-k,n}$ som har kardinalitet $\leq n - k$ er dermed uavhengige mengder til $U_{n-k,n}$.

Proposisjon 5.7 *En $[n, k]$-kode C er MDS hvis og bare hvis M_C^* er den uniforme matroiden $U_{n-k,n}$.*

Bevis Anta at C er en $[n, k]$-kode med paritetssjekkmatrise H, og anta at C er MDS. Da har C minimumsavstand $d = n - k + 1$. Vi bruker Teorem 4.26 som sier at C er en MDS kode hvis og bare hvis alle valg av $n - k$ kolonner fra en paritetssjekkmatrise H er lineært uavhengig. (Alle valg av $n - k + 1$ kolonner er selvsagt avhengige.) H er en generatormatrise for $C^\perp$, så vi kan konstruere vektormatroiden $M[H] = M_{C^\perp}$. Denne vektormatroiden er isomorf med den uniforme matroiden $U_{n-k,n}$. Dermed blir MDS-egenskapen ekvivalent med at $M_{C^\perp} = M_C^*$ er den uniforme matroiden $U_{n-k,n}$. ■

Notasjon 5.8 *Med en r-uniform matroide mener vi den uniforme matroiden $U_{r,n}$ av rang r.*

Proposisjon 5.7 gir oss et nytt bevis for Teorem 4.28.
Skissering av et alternativ bevis for Teorem 4.28: Proposisjon 5.7 sier at C er en MDS kode hvis og bare hvis M_C^* er den uniforme matroiden $U_{n-k,n}$. Dualen til den uniforme matroiden $U_{n-k,n}$ er også uniform; $U_{n-k,n}^* = U_{n-(n-k),n} = U_{k,n}$. Vi har at $U_{k,n}$ er matroiden $M_{C^\perp}^*$, så $C^\perp$ er MDS. ■

Vi oppsummerer nå situasjonen gjennom følgende:

Teorem 5.9 *La C være en $[n, k]$-kode over $\mathbb{F}_q$. Da er følgende ekvivalent:*

i) C er MDS.

ii) $C^\perp$ er MDS.

iii) M^* er uniform.

iv) M er uniform.

Bevis Vi har fra Teorem 4.28 har vi at i) er ekvivalent med ii). Teorem 4.26 gir oss at i) er ekvivalent med iii). Til slutt har vi at iii) er ekvivalent med iv) fra Proposisjon 3.61. ■

5.3 Matroideegenskaper for koder

Siden den lineære koden C og vektormatroiden M_C korresponderer til hverandre, kan noen egenskaper for matroider overføres til koder, og omvendt. Vi starter med å se på noen matroideegenskaper for koder.

Greene ga følgende viktige resultat som viser at vektenumeratoren for en lineær kode C er en spesialisering av Tuttepolynomet til den korresponderende matroiden M_C.

Teorem 5.10 (Greene) *Hvis C er en $[n,k]$-kode over $\mathbb{F}_q$ og M_C er den korresponderende matroiden til C, så er:*

$$W_C(z) = (1-z)^k z^{n-k} T\left(M_C; \frac{1+(q-1)z}{1-z}, \frac{1}{z}\right).$$

Bevis Dette er bevist i [18] (se Proposisjon 6.5.1). ■

Eksempel 5.11 *La C være koden fra Eksempel 4.19. Da er den korresponderende matroiden til C lik $M_C = U_{2,3}$. Fra Eksempel 3.118 vet vi at Tuttepolynomet til $U_{2,3}$ er:*

$$T(x,y) = x^2 + x + y.$$

Ved Teorem 5.10 og Proposisjon 3.122 har C vektenumeratoren:

$$W_C(z) = (1-z)^2 z T\left(U_{2,3}; \frac{1+z}{1-z}, \frac{1}{z}\right),$$

der

$$\begin{aligned}
T\left(U_{2,3}; \frac{1+z}{1-z}, \frac{1}{z}\right) &= \sum_{i=0}^{1}\binom{3}{i}\left(\frac{1+z}{1-z}-1\right)^{2-i} + \sum_{i=2}^{3}\binom{3}{i}\left(\frac{1}{z}-1\right)^{i-2} \\
&= \binom{3}{0}\left(\frac{1+z}{1-z}-1\right)^2 + \binom{3}{1}\left(\frac{1+z}{1-z}-1\right)^1 \\
&\quad + \binom{3}{2}\left(\frac{1}{z}-1\right)^0 + \binom{3}{3}\left(\frac{1}{z}-1\right)^1 \\
&= \left(\frac{1+z}{1-z}-1\right)^2 + 3\left(\frac{1+z}{1-z}-1\right) + 3 + \left(\frac{1}{z}-1\right) \\
&= \left(\frac{2z}{1-z}\right)^2 + \frac{6z}{1-z} + 2 + \frac{1}{z}.
\end{aligned}$$

Vi får:

$$\begin{aligned}
W_C(z) &= (1-z)^2 z T\left(U_{2,3}; \frac{1+z}{1-z}, \frac{1}{z}\right) \\
&= (1-z)^2 z\left(\left(\frac{2z}{1-z}\right)^2 + \frac{6z}{1-z} + 2 + \frac{1}{z}\right) \\
&= 4z^3 + 6z^2(1-z) + 2z(1-z)^2 + (1-z)^2 \\
&= 4z^3 + 6z^2 - 6z^3 + 2z - 4z^2 + 2z^3 + 1 - 2z + z^2 \\
&= 3z^2 + 1,
\end{aligned}$$

som stemmer med at koden har tre kodeord av vekt 2 og ett av vekt 0.

Ved å bruke Greenes Teorem kan vi bevise MacWilliams identiteten (Teorem 4.21)

som sier at vektenumeratoren for $C^{\perp}$ er gitt ved:

$$W_{C^{\perp}}(z) = \frac{1}{|C|}(1+(q-1)z)^n W_C\left(\frac{1-z}{1+(q-1)z}\right),$$

der $W_C(z)$ er vektenumeratoren for C.

Bevis av Teorem 4.21 (MacWilliams) La C være en lineær kode, og la M være den korresponderende matroiden til C. Vi gir et bevis av Teorem 4.21 ved å bruke Greenes Teorem. Siden $T(M;x,y) = T(M^*;y,x)$ og M^* korresponderer til $C^{\perp}$ (og siden $C^{\perp}$ har dimensjon $n - \dim(C)$), har vi:

$$\begin{aligned}
& \frac{1}{|C|}(1+(q-1)z)^n W_C\left(\frac{1-z}{1+(q-1)z}\right) \\
= \; & \frac{1}{q^k}(1+(q-1)z)^n \left(1-\frac{1-z}{1+(q-1)z}\right)^k \left(\frac{1-z}{1+(q-1)z}\right)^{n-k} \\
& T\left(M; \frac{1+\frac{(q-1)(1-z)}{1+(q-1)z}}{1-\frac{1-z}{1+(q-1)z}}, \frac{1}{\frac{1-z}{1+(q-1)z}}\right) \\
= \; & (1+(q-1)z)^{n-k-(n-k)}(1-z)^{n-k} z^k T\left(M; \frac{1}{z}, \frac{1+(q-1)z}{1-z}\right) \\
= \; & (1+(q-1)z)^0 (1-z)^{n-k} z^k T\left(M; \frac{1}{z}, \frac{1+(q-1)z}{1-z}\right) \\
= \; & (1-z)^{n-k} z^k T\left(M; \frac{1}{z}, \frac{1+(q-1)z}{1-z}\right) \\
= \; & (1-z)^{n-k} z^k T\left(M^*; \frac{1+(q-1)z}{1-z}, \frac{1}{z}\right) \\
= \; & W_{C^{\perp}}(z).
\end{aligned}$$

■

Vi skal nå se hva matroidebegrepene løkke og koløkke korresponderer til i kodeteorien.

La C være en lineær kode. Koordinat j til C er en løkke hvis og bare hvis den j-te koordinaten er 0 i hvert kodeord. La G være en generatormatrise for C. Anta at vi utfører elementære radoperasjoner slik at den j-te kolonnen til G er $(1,0,\ldots,0)^T$. Den j-te koordinaten til C er da en koløkke hvis og bare hvis de andre elementene i den første raden til G er 0. Den j-te koordinaten til en lineær kode er en løkke eller en koløkke hvis og bare hvis j er en løkke eller en koløkke i den korresponderende matroiden.

Vi skal nå fortolke matroideoperasjonene sletting og kontraksjon for lineære koder.

Definisjon 5.12 *Hvis koordinat j til den lineære koden C ikke er en koløkke, så sier vi at vi* ***punkterer*** *C i koordinat j hvis vi fjerner denne koordinaten fra hvert kodeord. Hvis den j-te koordinaten ikke er en løkke,* ***forkorter*** *vi C i den j-te koordinaten hvis vi beholder bare de kodeordene i C som har 0 i koordinat j og så fjerner denne koordinaten.*

Fra [12] har vi at hvis C er en $[n,k,d]$-kode med $d \geq 2$, så får vi ved å punktere en

koordinat j koden $C \setminus \{j\}$ med parametrene $n_{C\setminus\{j\}} = n-1$, $k_{C\setminus\{j\}} = k$ og $d_{C\setminus\{j\}} \geq d-1$. En forkortet kode $C/\{j\}$ derimot har $n_{C/\{j\}} = n-1$, $k_{C/\{j\}} \geq k-1$ og $d_{C/\{j\}} \geq d$.

Eksempel 5.13 *La*

$$A = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

være matrisen fra Eksempel 3.6, og la A være en generatormatrise for en lineær kode C over $\mathbb{F}_2$. Da er:

$$C = \{00000, 10110, 01100, 11010\}.$$

Punktering av koordinat 3 fra C gir oss følgende kode

$$C \setminus \{3\} = \{0000, 1010, 0100, 1110\}$$

med generatormatrise

$$A_{C\setminus\{3\}} = \begin{array}{c} \begin{matrix} 1 & 2 & 4 & 5 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \end{array}.$$

Vi ser at vi kunne fått denne matrisen direkte fra A ved å fjerne kolonne 3. Vi kan danne matroiden $M\left[A_{C\setminus\{3\}}\right] = (S', \mathcal{I})$, der $S' = \{1,2,4,5\}$ er indeksmengden for kolonnene til $A_{C\setminus\{3\}}$ og

$$\mathcal{I} = \{\varnothing, \{1\}, \{2\}, \{4\}, \{1,2\}, \{2,4\}\}.$$

Fra Eksempel 3.86 ser vi at $M\left[A_{C\setminus\{3\}}\right] = M(G_1) \setminus \{3\}$, som vi vet er isomorf med $M[A] \setminus \{3\}$ (fra Eksempel 3.41). Punktering av koordinat 3 korresponderer altså til sletting av $\{3\}$ fra matroiden $M[A]$. Vi skal nå se hva som skjer når vi forkorter C i koordinat 3. Den forkortede koden er:

$$C/\{3\} = \{0000, 1110\}$$

med generatormatrise

$$A_{C/\{3\}} = \begin{array}{c} \begin{matrix} 1 & 2 & 4 & 5 \end{matrix} \\ \begin{bmatrix} 1 & 1 & 1 & 0 \end{bmatrix} \end{array}.$$

Vi kan danne matroiden $M\left[A_{C/\{3\}}\right] = (S'', \mathcal{I}'')$, der $S'' = \{1,2,4,5\}$ og

$$\mathcal{I}'' = \{\varnothing, \{1\}, \{2\}, \{4\}\}.$$

Dette er matroiden $M(G_1)/\{3\}$ fra Eksempel 3.89, og vi har at $M(G_1)/\{3\} \cong M[A]/\{3\}$. Dermed ser vi at forkorting av koordinat 3 tilsvarer kontraksjonen av $\{3\}$ fra matroiden $M[A]$. La oss nå se hvordan vi kunne fått en generatormatrise for $C_{C/\{3\}}$ direkte fra

A. Vi ser at A er på formen $\begin{bmatrix} I_2 & B \end{bmatrix}$*, der*

$$B = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

Vi kan danne en paritetssjekkmatrise H for C som er lik

$$H = \begin{bmatrix} -B^T & I_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

over $\mathbb{F}_2$*. Vi fjerner så kolonne* 3 *fra H og får:*

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} D & I_3 \end{bmatrix},$$

der $D = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$*. Dette gir:*

$$\begin{bmatrix} I_1 & -D^T \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 \end{bmatrix} = A_{C/\{3\}}.$$

En paritetssjekkmatrise for C er en generatormatrise for $C^\perp$*. Vi har altså at* $\left(C^\perp \setminus \{3\}\right)^\perp = C/\{3\}$*. Dette stemmer helt overens med definisjonen av kontraksjon for matroider.*

Hvis en lineær kode C korresponderer til en vektormatroide M_C, så har vi at kodeoperasjonen punktering tilsvarer sletting av det korresponderende elementet i matroiden, og kodeoperasjonen forkorting, med hensyn på symbolet 0, tilsvarer matroideoperasjonen kontraksjon.

5.4 Kodeegenskaper for matroider

Vi skal nå se på noen kodebegreper som vi kan oversette til matroidespråk. Inspirert av Teorem 4.45 skal vi konstruere høyere vekter for en matroide.

Definisjon 5.14 *La M være en matroide på S, og la* $T \subseteq S$*. Vi definerer den h-te* ***høyere vekten*** *for M til å være*

$$d_h(M) = \min\{|T| \,|\, r(T) = |T| - h\},$$

det vil si det minste heltallet t slik at det eksisterer en mengde T med $|T| = t$ *og* $r(T) = t - h$*.*

Definisjon 5.15 ***Vekthierarkiet*** *til en matroide M er mengden av heltall*

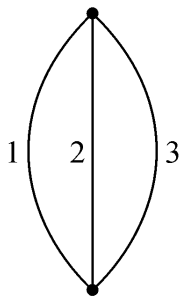
$$\{d_h(M) \,|\, 1 \leq h \leq n - r\}.$$

Vi skal nå gi noen eksempler på konstruksjon av de høyere vektene for noen matroider.

Eksempel 5.16 *La K_3 være den komplette grafen vist i Figur 3-2, og la $M(K_3)$ være kretsmatroiden til K_3 med grunnmengden $S = \{1,2,3\}$. Fra Eksempel 3.42 har vi at $M(K_3) \cong U_{2,3}$. Rangen til $M(K_3)$ er lik $r(U_{2,3}) = 2$, så vi skal konstruere $d_h(M(K_3))$ for $h = 1$. La $T \subseteq S$. Da er:*

$$r(T) = \begin{cases} |T| & \text{når } |T| < 2, \\ k & \text{når } |T| \geq 2. \end{cases}$$

Så $r(\varnothing) = 0$, $r(\{1\}) = r(\{2\}) = r(\{3\}) = 1$, $r(\{1,2\}) = r(\{1,3\}) = r(\{2,3\}) = r(S) = 2$. $d_1(M)$ er det minste antallet t av elementer i T med rang lik $t-1$. Vi ser at $d_1(M(K_3)) = \min\{|T| \, | \, r(T) = |T| - 1\} = |\{1,2,3\}| = 3$.



Figur 5-1: Grafen G_6.

Eksempel 5.17 *La G_6 være grafen i Figur 5-1, og la $M(G_6) = (S, \mathcal{I})$, der $S = \{1,2,3\}$ og $\mathcal{I} = \{\varnothing, \{1\}, \{2\}, \{3\}\}$. Da er $M(G_6) \cong U_{1,3}$, så $r(M(G_6)) = r(U_{1,3}) = 1$. Vi skal finne $d_h(M(G_6))$ for $h = 1,2$. La $T \subseteq S$. Da er $r(T) = 1$ for alle ikke-tomme delmengder T og $r(\varnothing) = 0$. Vi får at $d_1(M(G_6)) = \min\{|T| \, | \, r(T) = |T| - 1\} = 2$ og $d_2(M(G_6)) = \min\{|T| \, | \, r(T) = |T| - 2\} = 3$. Vi går nå tilbake til Eksempel 5.16. Matroiden $M(K_3) \cong U_{2,3}$ i Eksempel 5.16 er den duale matroiden til $M(G_6)$. Vi ser at*

$$\{d_1(M(G_6)), d_2(M(G_6))\} = \{1,2,3\} - \{n+1-d_1(M^*(G_6))\},$$

så $\{d_h(M(G_6)) \, | \, 1 \leq h \leq 2\}$ er komplementet til vekthierarkiet til $M^*(G_6)$.

Vi har følgende resultat, som tilsvarer Teorem 4.47 for koder.

Proposisjon 5.18 *La M være en matroide. Da er:*

$$\{d_h(M) \, | \, 1 \leq h \leq n-r\} \cup \{n+1-d_h(M^*) \, | \, 1 \leq h \leq r\} = \{1,2,\ldots,n\}.$$

Bevis La M være en matroide på en n-mengde S, og la rangen til M være lik $r(S) = r$. La $T \subseteq S$. Da er vekthierarkiet til M og den dualematroiden M^* henholdsvis mengdene

$$\{d_h(M) \,|1 \leq h \leq n-r\}, \text{ der } d_h(M) = \min\{|T| \,||T| - r(T) = h\} \text{ og}$$
$$\{d_h(M^*) \,|1 \leq h \leq r\}, \text{ der } d_h(M^*) = \min\{|T| \,||T| - r^*(T) = h\}.$$

Vi ser på hvilke mengder som beregner de høyere vektene og ser om vi kan finne et mønster. Vi har: $|\varnothing| - r(\varnothing) = 0$, $|S| - r(S) = n - r$, $r^*(S) = |S| - r(S) = n - r$ (fra (3.1)), $|\varnothing| - r^*(\varnothing) = 0$ og $|S| - r^*(S) = n - (n-r) = r$. La $F(T) = |T| - r(T)$ og $F^*(T) = |T| - r^*(T)$. Fra 3.62 har vi at $F(T) = |T| - r(T) = |S| - r(S) - r^*(S-T)$. Vi har videre at:

$$\begin{aligned} F(T) &= |S| - r(S) - r^*(S-T) \\ &= |S| - r(S) + |S-T| - r^*(S-T) - |S-T| \\ &= n - r + F^*(S-T) - |S-T|. \end{aligned}$$

La nå T være den tomme mengden. Da er:

$$\begin{aligned} F(\varnothing) &= n - r + F^*(S) - |S| \\ 0 &= n - r + n - r^*(S) - n. \end{aligned}$$

$T = S$ gir:

$$\begin{aligned} F(S) &= n - r + F^*(\varnothing) - |\varnothing| \\ n - r &= n - r + 0 - 0 \end{aligned}$$

La nå $h(x) \in \mathbb{Z}$ være gitt ved:

$$h(x) = \max F(T) \text{ for } T \subseteq S \text{ og } |T| = x.$$

Da er:

$$\begin{aligned} h(x) &= n - r + h^*(n-x) - n + x \\ &= h^*(n-x) - r + x \end{aligned}$$

$x = 0$ gir:

$$h(0) = h^*(n) - r = 0,$$

siden $h^*(n) = \max F^*(n) = n - (n-r) = r$. Vi har:

$$\begin{aligned} d_1(M) &= \min\{|T| \,||T| - r(T) = 1\} = \min\{x \,|h(x) = 1\} \\ d_2(M) &= \min\{|T| \,||T| - r(T) = 2\} = \min\{x \,|h(x) = 2\} \\ &\vdots \\ d_{n-r}(M) &= \min\{|T| \,||T| - r(T) = n-r\} = \min\{x \,|h(x) = n-r\}. \end{aligned}$$

d_i-ene er lik $\{x \,|h(x) - h(x-1) = 1\}$. Vi ser at d_i-ene gjør et sprang. La oss nå se på h^*:

$$\begin{aligned} h(x) - h(x-1) &= h^*(n-x) - r + x - h^*(n-x+1) + r - x + 1 \\ &= h^*(n-x) - h^*((n+1)-x) + 1 \\ &= 1 - (h^*((n+1)-x) - h^*(n-x)). \end{aligned}$$

Videre har vi at:

$$h(x) - h(x-1) = \begin{cases} 0 \text{ hvis } d_i\text{-ene ikke gjør noen sprang} \\ 1 \text{ hvis } d_i\text{-ene gjør et sprang} \end{cases}$$

Så:

$$h(x) - h(x-1) = 0 \iff (h^*((n+1)-x) - h^*(n-x)) = 1.$$

Vi har:

$$x = d_i \text{ passe } i \iff (n+1) - x \text{ ikke er } d_j^{\perp} \text{ for noen } j.$$

Resultatet følger. ■

Vi illustrerer Proposisjon 5.18 ved følgende eksempel.

Eksempel 5.19 *La G_2 være grafen vist i Figur 3-1. Kretsmatroiden til G_2 er da $M(G_2) = (S, \mathcal{I}(M(G_2)))$, der $S = \{1,2,3,4,5\}$ og*

$$\mathcal{I}(M(G_2)) = \left\{ \begin{array}{l} \varnothing, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{1,2\}, \{1,3\}, \{1,4\}, \{1,5\}, \{2,3\}, \\ \{2,4\}, \{2,5\}, \{3,4\}, \{3,5\}, \{4,5\}, \{1,2,4\}, \{1,2,5\}, \\ \{1,3,4\}, \{1,3,5\}, \{1,4,5\}, \{2,3,4\}, \{2,3,5\}, \{2,4,5\} \end{array} \right\}$$

Rangen til $M(G_2)$ er lik $r(M(G_2)) = 3$. Vi skal konstruere de høyere vektene $d_h(M(G_2))$ for h opp til $n - r(M(G_2)) = 2$. La $T \subseteq S$. $d_1(M(G_2))$ er kardinaliteten til den minste avhengige mengden, så $d_1(M(G_2)) = 3$. Da vet vi at $d_2(M(G_2))$ er 4 eller 5. $d_2(M(G_2)) = \min\{|T| \,|r(T) = |T| - 2\} = 5$. Vi skal beregne de høyere vektene $d_h(M^*(G_2))$ for h opp til $r(M(G_2)) = 3$. Vi konstruerer kokretsmatroiden til G_2. Vi ser at basene for $M(G_2)$ er mengden

$$\mathcal{B}(M(G_2)) = \{\{1,2,4\}, \{1,2,5\}, \{1,3,4\}, \{1,3,5\}, \{1,4,5\}, \{2,3,4\}, \{2,3,5\}, \{2,4,5\}\}.$$

Da er $M^*(G_2) = (S, \mathcal{B}(M^*(G_2)))$, der $S = \{1,2,3,4,5\}$ og

$$\begin{aligned} \mathcal{B}(M^*(G_2)) &= \{S - B \,|B \in \mathcal{B}(M(G_2))\} \\ &= \{\{1,3\}, \{1,4\}, \{1,5\}, \{2,3\}, \{2,4\}, \{2,5\}, \{3,4\}, \{3,5\}\}. \end{aligned}$$

Rangen til $M^*(G_2)$ er lik $r^*(M(G_2)) = 2$. Vi har at $d_1(M^*(G_2))$ er kardinaliteten til den minste avhengige mengden, så $d_1(M^*(G_2)) = |\{1,2\}| = 2$. Videre har vi at $d_2(M^*(G_2)) = \min\{|T| \,|r^*(T) = |T| - 2\} = 4$. Siden $d_3(M^*(G_2))$ må være større

enn 4 *har vi at* $d_3\left(M^*\left(G_2\right)\right) = 5$. *Da har vi at:*

$$\begin{aligned} & \left\{d_h\left(M\left(G_2\right)\right) | 1 \leq h \leq 2\right\} \cup \left\{n+1-d_h\left(M^*\left(G_2\right)\right) | 1 \leq h \leq 3\right\} \\ = \; & \{3,5\} \cup \{6-2, 6-4, 6-5\} = \{1,2,3,4,5\}. \end{aligned}$$

5.5 Litt om veien videre

Vi vet at en lineær kode C er MDS hvis og bare hvis M^* er uniform. C har redundans r og er MDS hvis og bare hvis M^* er r-uniform, der r er rangen til matroiden. C har redundans r og er h-MDS hvis og bare hvis M^* er (r,h)-uniform. At en matroide er (r,h)-uniform betyr at matroiden har rang lik r og at alle mengdene i M^* av kardinalitet $r+h-1$ har rang r. Vi kan definere og studere hva h-MDS, nær- og nesten-MDS betyr for matroider. Vi kan oversette begrepene om høyere vekter, h-MDS, nær- og nesten-MDS for grafer, samt studere den grafteoretiske fortolkningen av uniform.

Bibliografi

[1] A. Barg, *The Matroid of Supports of A Linear Code*, AAECC 8, s. 165-172, 1997.

[2] L. Beineke og R. Wilson, *Graph Connections*, Oxford University Press, Oxford, 1997.

[3] T. Britz, *MacWilliams identities and matroid polynomials*, Electronic Journal of Combinatorics 9, 2002, #R19, 16 sider.

[4] R. L. Graham, M. Grötschel og L. Lovász, ed., *Handbook of Combinatorics*, Vol. I, Elsevier, Amsterdam, 1995.

[5] R. Hill, *A First Course in Coding Theory*, Oxford University Press, Oxford, 1986.

[6] D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger og J. R. Wall, *Coding Theory*, Marcel Dekker, New York, 1991.

[7] J. H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, New York, 1999.

[8] F. J. MacWilliams og N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Elsevier Science Publishers B. V., North Holland, 1977.

[9] J. G. Oxley, *Matroid Theory*, Oxford University Press, Oxford, 1992.

[10] H. Raddum, *MDS-formodningen og vekthierarkiet for sterkt algebraisk-geometriske koder*, hovedfagsoppgave, Universitetet i Bergen, 1999.

[11] S. Roman, *Coding and Information Theory*, Springer-Verlag, New York, 1992.

[12] H. van Tilborg, *Error-correcting Codes - a first course*, Studentlitteratur, Lund, 1993.

[13] W. Trappe og L. C. Washington, *Introduction to Cryptography with Coding Theory*, Prentice Hall, Upper Saddle River, New Jersey, 2002.

[14] V. K. Wei, Generalized Hamming Weights for Linear Codes, *IEEE Transactions on Information Theory*, Vol. 37, No. 5, s. 1412-1418, 1991.

[15] D. J. A. Welsh, *Matroid Theory*, Academic Press, London, 1976.

[16] N. White, ed., *Theory of Matroids*, Cambridge University Press, Cambridge, 1986.

[17] N. White, ed., *Combinatorial Geometries*, Cambridge University Press, Cambridge, 1987.

[18] N. White, ed., *Matroid Applications*, Cambridge University Press, Cambridge, 1992.

[19] R. J. Wilson, *Introduction to Graph Theory*, Longman, Harlow, 1996.