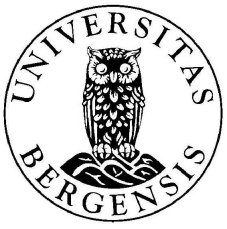
Sammenhenger mellom koder, matroider, grafer og simplisielle komplekser

Masteroppgave i
algebra

Bård Heiseldal

Matematisk Institutt
Universitetet i Bergen



Våren 2008

Forord

Denne masteroppgaven handler hovedsakelig om å studere sammenhenger mellom ulike emner innen algebra og kombinatorikk. De matematiske konseptene som studeres, er lineære koder, matroider, grafer og simplisielle komplekser, og vi forsøker blant annet å vise hvordan konstruksjoner definert innenfor en av disse grenene også kan gi mening innenfor en annen.

Kodeteori handler om å finne gode metoder for å sende informasjon gjennom en kanal der det kan forekomme forstyrrelser. Hovedproblemet i kodeteori er tredelt: For det første er det ønskelig med koder som er raske å sende, for det andre er det viktig at koden er stor nok til å sende alle de ulike informasjonsbitene og for det tredje må koden være robust mot forstyrrelser i kanalen. En kode består generelt av tupler av elementer fra en definert mengde kalt alfabetet. I denne oppgaven konsentrerer vi oss om lineære blokk-koder, og i dette tilfellet er tuplene elementer i et vektorrom over en kropp. Lineære blokk-koder er spesifisert ved en generatormatrise eller paritetssjekkmatrise, matriser der radene danner en basis for henholdsvis koden og dualkoden, som er det ortogonale komplementet til koden. Særlig vil vi studere såkalte MDS-koder, en klasse av lineære koder med spesielt gode egenskaper i forhold til det tredelte problemet skissert ovenfor, samt klasser av koder som i en viss forstand nesten er MDS.

Grafteori er et velkjent emne med røtter tilbake til Euler på 1700-tallet og med et bredt spekter av anvendelser, særlig innen informatikk. En graf er et enkelt konsept, bestående av en mengde hjørner og en mengde (uordnede) par av hjørner kalt kanter. I denne oppgaven tillater vi både flere kanter for hvert par av hjørner og at disse parene ikke nødvendigvis består av distinkte hjørner, altså det som ofte betegnes som en multigraf. Dersom kantene består av ordnede hjørnepar, har vi en rettet graf eller digraf. En trellis er et spesialtilfelle av en digraf, der kantene i tillegg er vektede og hjørnene er inndelt i lag. Trelliser er mye brukt i kodeteori, og da særlig innen dekoding.

En matroide er en konstruksjon bestående av en (endelig) grunnmengde og en mengde av uavhengige elementer, der disse er elementer i potensmengden til grunnmengden som oppfyller bestemte krav. Denne konstruksjonen generaliserer til en viss grad avhengighetsbegreper både for matriser og grafer, på følgende måter: Dersom grunnmengden i matroiden består av kolonnevektorene i en matrise, så er en delmengde av grunnmengden uavhengig i matroiden hvis og bare hvis kolonnevektorene i delmengden er lineært uavhengige. Dersom grunnmengden i matroiden i stedet består av kantmengden til en graf, så er en delmengde av grunnmengden uavhengig i matroiden hvis og bare hvis ingen av kantene i delmengden danner en krets i grafen. Videre er som nevnt lineære blokk-koder spesifisert ved matriser, og i denne oppgaven studerer vi konsepter innen kode- og grafteori som kan generaliseres til matroider.

Et simplisielt kompleks defineres på lignende måte som en matroide (faktisk kan vi si at en matroide er et spesialtilfelle av et simplisielt kompleks), med en grunnmengde kalt hjørnemengden og en mengde elementer fra potensmengden til hjørnemengden kalt fjes, der

mengden av fjes er lukket under inklusjon. Det er en nær sammenheng mellom simplisielle komplekser og kvadratfrie monomialidealer, og Stanley-Reisner-idealet og -ringen til et simplisielt kompleks defineres ut fra denne sammenhengen. Videre kan vi konstruere et Stanley-Reisner-ideal fra de maksimale uavhengige elementene til en matroide, og i denne oppgaven spesialiserer vi denne konstruksjonen fra matroider til grafer. Særlig studerer vi den minimale frie resolusjonen av Stanley-Reisner-ringer som oppstår på denne måten.

Oppgaven deles naturlig i tre hoveddeler som utgjør kapitlene 2−4, i tillegg til kapittel 1 som hovedsakelig gjengir standarddefinisjoner og -resultater innen graf-, matroide- og kodeteori.

I kapittel 2 gjør vi bruk av den nevnte sammenhengen mellom graf- og kodeteori, via matroider. Vi ser hvordan vekthierarkiet til en kode kun avhenger av matroidestrukturen til paritetssjekkmatrisen og definerer derfor vekthierarkiet også for matroider og grafer. Vi viser hvordan MDS-egenskapene til en kode bestemmes av vekthierarkiet til koden og studerer hvilken betydning MDS-egenskaper har på matroide- og grafnivå. Videre klassifiserer vi noen matroider og grafer med gitte MDS-egenskaper og gir en del telleresultater i denne forbindelse.

I kapittel 3 ser vi på trelliser fra lineære koder, og da særlig den minimale trellisen til en kode. Vi viser at størrelsen til den minimale trellisen er gitt ved matroidestrukturen til generatormatrisen for koden og studerer øvre og nedre grenser for denne størrelsen. Videre ser vi hvordan vi innenfor ekvivalensklassen til en kode kan ha minimale trelliser av ulik størrelse og studerer derfor hvordan vi ved å bruke ekvivalente koder kan redusere størrelsen på den minimale trellisen. Også i dette kapittelet ser vi på MDS-egenskapene til en kode, og vi studerer hvordan disse har betydning for trellis-størrelsen. Til slutt beskriver vi Viterbi-algoritmen, en trellisalgoritme som fungerer bedre jo mindre trellisen er.

I kapittel 4 konstruerer vi simplisielle komplekser fra grafer, som nevnt ovenfor, og vi studerer sammenhenger mellom grafen og det tilhørende simplisielle komplekset. Videre ser vi på hvilke egenskaper ved en graf som har betydning for den minimale frie resolusjonen av Stanley-Reisner-ringen til det tilhørende simplisielle komplekset, og vi viser hvordan vi kan bestemme denne resolusjonen direkte fra grafen.

Dersom resultater eller konstruksjoner som gis i denne oppgaven ikke er nye, men kun er del av en tilrettelagt oversikt over materiale hentet fra allerede eksisterende litteratur, vil refereranser til disse kildene oppgis underveis.

I arbeidet med denne oppgaven er det mange som på ulike måter har bidratt. Mine veiledere, Trygve Johnsen og Gunnar Fløystad, fortjener en stor takk for omfattende og entusiastisk hjelp, i tillegg til at de har gitt gode forslag til retningen på oppgaven. Videre vil jeg takke Nils Henry Rasmussen, Henning Lohne, Alexander Lundervold og Erlend Grong for hjelp med skrivingen i LaTeX og med tegneprogrammet Xfig, samt Jan Magnus Økland for hjelp til å komme igang med Macaulay 2, et program jeg har hatt stor nytte av i forberedelsene til kapittel 4. For øvrig vil jeg takke alle studentene ved Matematisk Institutt for et godt sosialt miljø.

En særlig takk vil jeg rette til kona mi, Grete-Marita, for å ha gjort det mulig for meg å bruke såpass mye tid på å skrive denne oppgaven, midt i barnepass og bleieskift. Takk også for grundig korrekturlesing og mye oppmuntring på veien. Takk til min datter Maria for daglige solstråler og til familie og venner for øvrig. Sist, men ikke minst, takk til Jesus, min Herre og Frelser.

Innhold

Figurer

Kapittel 1

Grunnleggende resultater og teori

I dette kapittelet gjengir vi allerede velkjente definisjoner og hovedresultater fra grafteori, matroideteori og kodeteori som vi trenger videre i oppgaven, i tillegg til mer generelle begreper og notasjon som gis i kapittel 1.1. Mens kapittel 1.2 stort sett kun består i å definere velkjente grafteoretiske begreper, er det i kapitlene 1.3 og 1.4 også gjengitt mange resultater. Som det fremgår av referansene her, er mesteparten av stoffet hentet fra [O] og [H], og vi henviser til disse for en grundigere introduksjon til matroide- og kodeteori. Organiseringen av dette kapittelet gjenspeiler at det ofte er tatt utgangspunkt i [L].

1.1 Begreper og notasjon

Alle mengdene i denne oppgaven er endelige, så sant annet ikke fremgår av sammenhengen. Kardinaliteten til en mengde S betegnes $|S|$, og potensmengden, bestående av alle delmengder av S, betegnes $\mathcal{P}(S)$. Vi kaller ofte delmengdene av $\mathcal{P}(S)$ for familier. Vi kaller elementer i en familie $\mathcal{F} \subseteq \mathcal{P}(S)$ **maksimale** hvis de ikke er ekte inneholdt i noe annet element av $\mathcal{F}$, og **minimale** hvis de ikke ekte inneholder noen elementer av $\mathcal{F}$.

Vi lar $\mathbb{N}$ betegne mengden $\{1, 2, \dots\}$ av positive heltall. (Av praktiske årsaker vil vi inkludere tallet 0 i $\mathbb{N}$ i kapittel 4.)

En kropp betegnes $\mathbb{K}$, mens $\mathbb{F}_q$ betegner den endelige kroppen med $q = p^m$ elementer, der p er et primtall og $m \in \mathbb{N}$. Det er bevist at $\mathbb{F}_q$ er unik, opp til isomorfi. Vektorrommet av dimensjon n over $\mathbb{F}_q$ betegnes $(\mathbb{F}_q)^n$.

Definisjon 1.1.1. *En **multimengde** valgt fra en mengde S er en funksjon $m : S \to \mathbb{N} \cup \{0\}$, og vi skriver (S, m) for denne.*

For eksempel kan $\{a, a, b, b, b, d\}$ betegne multimengden med $S = \{a, b, c, d, e\}$ og $m(a) = 2, m(b) = 3, m(c) = 0, m(d) = 1, m(e) = 0$. Ofte kan vi i praksis se på en multimengde som en mengde der elementer kan opptre flere ganger.

Definisjon 1.1.2. *Dersom mengden S består av elementer i et vektorrom over en gitt kropp $\mathbb{K}$, definerer vi **lineær uavhengighet på en multimengde** (S, m) på følgende måte: $(T, m) \subseteq (S, m)$ er lineært uavhengig hvis T er lineært uavhengig og $m(t) = 1$ for alle $t \in T$.*

Vi bruker notasjonen $\underline{x}$ for vektorer. Hvis A er en matrise, så betegner A^T den transponerte matrisen til A, mens matrisen $(-1)\cdot A$ betegnes $-A$. Vi skriver I_n for $(n \times n)$-identitetsmatrisen

og $\underline{0}$ og $\mathbf{0}$ for henholdsvis en vektor og en matrise der alle entrier er 0; dimensjonene her fremgår oftest av sammenhengen. Altså har vi:

$$I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix}, \text{ og, gitt en } (m \times n)\text{-matrise } A = \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{bmatrix}, \text{ er}$$

$$A^T = \begin{bmatrix} a_{1,1} & \cdots & a_{m,1} \\ \vdots & \ddots & \vdots \\ a_{1,n} & \cdots & a_{m,n} \end{bmatrix} \text{ og } -A = \begin{bmatrix} -a_{1,1} & \cdots & -a_{1,n} \\ \vdots & \ddots & \vdots \\ -a_{m,1} & \cdots & -a_{m,n} \end{bmatrix}.$$

Med notasjonen $\mathrm{rg}(A)$ mener vi rangen til matrisen A, altså dimensjonen til kolonnerommet til A.

Symbolet $\square$ markerer slutten på et bevis, eller eventuelt mangel på bevis, dersom resultatet er trivielt eller bevist tidligere.

1.2 Grafteori

En **graf** $G = (V(G), E(G))$ består av en ikke-tom, endelig mengde $V(G)$ av **hjørner** og en endelig multimengde $E(G)$ valgt fra en mengde **kanter**, som hver består av et uordnet par av (ikke nødvendigvis distinkte) hjørner. Likevel kommer vi i det følgende til å bruke notasjonen $e \in E(G)$. Med dette menes at e er en kant i mengden som multimengden $E(G)$ velges fra, samtidig som funksjonen $E(G)$ med argumentet e gir en funksjonsverdi større enn 0.

En **kantmerket graf** er en graf der kantene er merket med tallene $1, 2, \ldots, n$, der $n = |E(G)|$. En **kantvektet graf** er en graf der hver kant er tilordnet et element fra en endelig mengde. Dette elementet kalles da kantens **vekt**, og ulike kanter kan ha samme vekt. Helt tilsvarende kan vi definere **hjørnemerket graf**, **hjørnevektet graf** og **vekten** til et hjørne i en hjørnevektet graf. Dersom det i det videre er snakk om merkede eller vektede grafer, vil vi presisere dette.

La G være en graf, og $v_1, v_2 \in V(G)$. Hvis $e = \{v_1, v_2\} \in E(G)$, kalles 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 v_2 kalles da **naboer** i G. En kant med identiske endepunkter kalles en **løkke**, og to kanter (som ikke er løkker) med samme endepunkter kalles **parallelle**. Hvis G ikke inneholder noen løkker eller parallelle kanter, sier vi at G er en **enkel graf**. **Graden** til et hjørne er antall kanter som er insident med hjørnet, der løkker teller som to kanter.

Hvis G og H er grafer og $V(H) \subseteq V(G)$ og $E(H) \subseteq E(G)$ sier vi at H er en **delgraf** av G. Spesielt, hvis vi lar $V(X) = \{v \in V(G) \mid v \text{ er insident med } e, \text{ for én } e \in X\}$, der $X \subseteq E(G)$, kaller vi delgrafen $H = (V(X), X)$ **restriksjonen av G til X** og skriver $G|_X$ for denne.

En **sti** i en graf G er en følge $v_0 e_1 v_1 e_2 \cdots v_{k-1} e_k v_k$, der $v_0, v_1, \ldots, v_k \in V(G)$ er distinkte hjørner og $e_i = \{v_{i-1}, v_i\} \in E(G)$ for alle $1 \leq i \leq k$. Hvis vi i tillegg tar med kanten $e_0 = \{v_k, v_0\}$, sier vi at følgen $v_0 e_1 v_1 e_2 \cdots v_{k-1} e_k v_k e_0 v_0$ er en **krets**. Det minste antall kanter i en krets i G kalles **vidden** til G.

En graf G er **sammenhengende** hvis det eksisterer en sti mellom hvert par av hjørner i G, og **usammenhengende** hvis den ikke er sammenhengende. En **komponent** av G er en maksimal sammenhengende delgraf av G.

La $G = (V(G), E(G))$ være en graf, og $X \subseteq E(G)$. Vi definerer **slettingen** av X fra G som grafen vi får ved å fjerne X fra G, og vi skriver $G \setminus X$ for denne. Vi har altså $G \setminus X = (V(G), E(G) \setminus X)$. Dersom $G \setminus X$ har flere komponenter enn G, kaller vi X en **separerende kantmengde** i G. Dersom X i tillegg er minimal, kalles X en **kokrets** i G, og en kokrets bestående av bare én kant, kalles en **bro**. Det minste antall kanter i en kokrets i G kalles **kovidden** til G.

Kontraksjonen av $X \subseteq E(G)$ fra en graf G, betegnet ved G/X, er grafen vi får ved å fjerne X fra G og identifisere endepunktene til kanter i X med hverandre. Hjørnene $v_1, v_2 \in V(G)$ identifiseres altså med hverandre i G/X hvis og bare hvis $e = \{v_1, v_2\} \in X$.

En **skog** er en graf som ikke inneholder noen kretser, og et **tre** er en sammenhengende skog. Legg merke til at en skog ikke har vidde. Et **utspennende tre** for en sammenhengende graf G er et maksimalt tre, altså et tre som inneholder alle hjørnene i G, mens en **utspennende skog** for en (vilkårlig) graf G er en skog som består av ett utspennende tre for hver komponent av G. Hvis T er et tre, har vi $|V(T)| = |E(T)| + 1$, altså har vi $|V(T)| = |E(T)| + i$ hvis T er en skog med i komponenter. Dersom T er en utspennende skog for grafen G, har vi derfor $V(T) = V(G)$ og $|E(T)| = |V(T)| - i = |V(G)| - i$, der i er antall komponenter av G (og dermed også av T).

Kretsrangen til en graf G er det maksimale antall kanter som kan fjernes fra G uten at antall komponenter øker. Vi ser at kretsrangen må være gitt som forskjellen mellom $|E(G)|$ og antall kanter i en utspennende skog for G, altså har vi at kretsrangen er $|E(G)| - |V(G)| + i$, der i er antall komponenter av G.

To grafer G og H kalles **isomorfe** hvis det eksisterer bijeksjoner $\phi : V(G) \to V(H)$ og $\theta : E(G) \to E(H)$ slik at for $v \in V(G)$ og $e \in E(G)$ har vi at e er insident med v hvis og bare hvis $\theta(e)$ er insident med $\phi(v)$ i H.

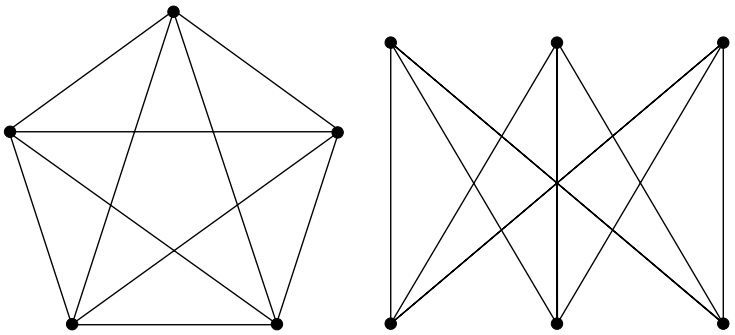
To viktige klasser av grafer er de komplette og komplette bipartite grafene. En graf er **komplett** hvis det mellom hvert hjørnepar eksisterer nøyaktig én kant, og vi skriver K_n for den komplette grafen med n hjørner. En graf kalles **bipartit** hvis hjørnene i grafen kan deles i to mengder V_1 og V_2 slik at hver kant i grafen forbinder et hjørne i V_1 med et hjørne i V_2. Grafen G kalles **komplett bipartit** hvis den er bipartit og det eksisterer nøyaktig én kant mellom hvert hjørnepar $\{v_1, v_2\}$, der $v_1 \in V_1$ og $v_2 \in V_2$. Hvis $|V_1| = m, |V_2| = n$, skriver vi $K_{m,n}$ for G. Merk at for $m, n \in \mathbb{N}$ og $\{m, n\}$ et uordnet par er K_n og $K_{m,n}$ unike, opp til isomorfi. Vi har altså $|V(K_n)| = n$ og $|V(K_{m,n})| = m + n$, og det er lett å vise at $|E(K_n)| = \sum_{i=1}^{n-1} i = \frac{(n-1)n}{2}$ og $|E(K_{m,n})| = m \cdot n$.

Hvis G og H er grafer, sier vi at H er en ***G*-konfigurasjon** hvis H kan fås fra G ved å legge til hjørner langs kanter i G.

Vi sier at en graf er **planar** hvis den kan tegnes i et plan uten at noen kanter skjærer hverandre. En slik tegning kalles en **planar representasjon** av grafen, og enhver planar representasjon deler planet inn i **regioner**. Grafene K_5 og $K_{3,3}$ (se figur 1.1) er to viktige eksempler på ikke-planare grafer, og følgende teorem gjør det lettere å avgjøre om en graf er planar eller ikke:

Teorem 1.2.1. *Følgende er ekvivalent, for en graf G:*

i) G er planar.



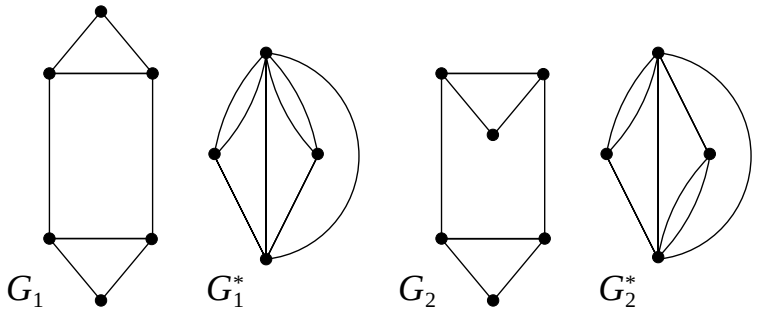
Figur 1.1: Grafene K_5 og $K_{3,3}$.

ii) G inneholder ingen delgraf som er en K_5- eller $K_{3,3}$-konfigurasjon.

Bevis. Kuratowski beviste dette i 1930. Beviset finnes som teorem 9.10 i [BM]. □

Korollar 1.2.2. *La G være en graf med $V(G) < 5$ og/eller $E(G) < 9$. Da er G planar.*

Bevis. Vi merker oss at for en vilkårlig graf G, gjelder $V(G) \leq V(G')$ og $E(G) \leq E(G')$ for enhver G-konfigurasjon G'. Siden $V(K_5) = 5 < V(K_{3,3})$ og $E(K_{3,3}) = 9 < E(K_5)$, følger resultatet umiddelbart fra teorem 1.2.1. □



Figur 1.2: Isomorfe grafer med ikke-isomorfe geometriske dualer.

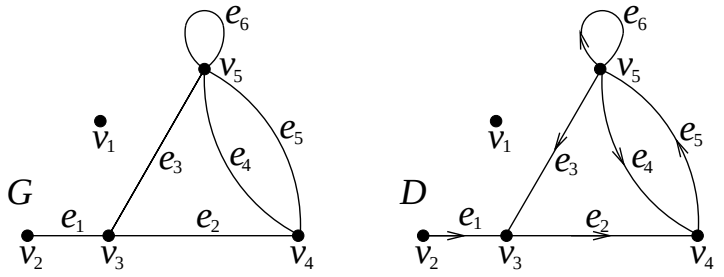
Gitt en planar representasjon G' av en planar graf G, kan vi konstruere en **geometrisk dual** G^* til G på følgende måte: Velg ett punkt v_i^* for hver region r_i' i G'. Disse er hjørnene i G^*. For hvert par $\{v_i^*, v_j^*\}$ av hjørner i G^*, som ligger i henholdsvis region r_i' og r_j' i G', gjør vi følgende: Anta at $\{e_1', e_2', \ldots, e_k'\} \in E(G')$ er kantene som er felles for regionene r_i' og r_j'. Vi forbinder da v_i^* og v_j^* med kanter $e_1^*, e_2^*, \ldots, e_k^* \in E(G^*)$, der e_i^* krysser e_i' og ingen andre kanter i G'. Hvis $e' \in E(G')$ kun grenser til én region r', legger vi til en løkke til det hjørnet i G^* som ligger i r'.

Merk at to forskjellige planare representasjoner av en planar graf kan ha ikke-isomorfe geometriske dualer, noe som er vist på figur 1.2.

Vi merker oss også at vi for en vilkårlig planar graf G har en bijeksjon mellom kretser i G og kokretser i G^* (derav navnet kokrets), der G^* er en geometrisk dual til G. Bijeksjonen er gitt ved at $\{e_1, e_2, \ldots, e_i\} \subseteq E(G)$ er kantmengden til en krets i G hvis og bare hvis

$\{e_1^*, e_2^*, \ldots, e_i^*\} \subseteq E(G^*)$ er kantmengden til en kokrets i G^*, der e_j^* er kanten som krysser $e'_j \in E(G')$, og G' er den planare representasjonen av G som gir G^*. Altså får vi at vidden til G er lik kovidden til G^*.

Gitt en graf G med m hjørner og n kanter, der $V(G) = \{v_1, v_2, \ldots, v_m\}$ og $E(G) = \{e_1, e_2, \ldots, e_n\}$, kan vi representere G ved en $m \times n$ **hjørne-kant-insidensmatrise** $A_G = [a_{i,j}]$, der $a_{i,j}$ er antall ganger kanten e_j er insident med hjørnet v_i.



Figur 1.3: Digrafen D er en orientering av grafen G.

En **rettet graf** eller **digraf** er en graf der kantene er rettet, som vist på figur 1.3 (grafen D). Mer formelt består en digraf $D = (V(D), E(D))$ av en ikke-tom, endelig mengde $V(D)$ av hjørner og en endelig multimengde $E(D)$ valgt fra en mengde **rettede kanter**, som hver består av et *ordnet* par av (ikke nødvendigvis distinkte) hjørner. Vi angir en rettet kant e i D med $e = (v_1, v_2)$ dersom e går fra hjørnet v_1 til hjørnet v_2, og kaller v_1 og v_2 henholdsvis for **starthjørnet** og **slutthjørnet** til e. Grafen G med $V(G) = V(D)$ og $E(G) = \{\{v_i, v_j\} \,|\, (v_i, v_j) \in E(D)\}$ kalles den **underliggende grafen** til D, og vi sier at D er en **orientering** av G.

Vi kan også representere en digraf D ved en $m \times n$ hjørne-kant-insidensmatrise $A_D = [a_{i,j}]$, der

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

Legg merke til at hvis digrafen D er en orientering av grafen G, og vi reduserer matrisene A_D og A_G modulo 2, får vi $A_D = A_G$.

Eksempel 1.2.3. *Digrafen D er en orientering av grafen G på figur* 1.3. *Med nummereringen av hjørnene og kantene som gitt på figuren, har vi*

$$A_G = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 2 \end{bmatrix} \text{ og } A_D = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 & 1 & 0 \\ 0 & 0 & 1 & 1 & -1 & 0 \end{bmatrix}.$$

Dersom et tre er rettet, og det eksisterer et hjørne v, kalt **roten**, slik at det er én unik (rettet) sti fra v til et vilkårlig annet hjørne i treet, kalles det et **rotet tre**. Det er lett å se at hjørnet v er entydig bestemt, for hvis det eksisterte to ulike røtter, v_1 og v_2, så ville det eksistert én rettet sti fra v_1 til v_2 og en annen fra v_2 til v_1, og vi ville ha fått en krets.

1.3 Matroider

En matroide kan defineres på mange forskjellige, men ekvivalente måter, som vi vil se videre i dette kapittelet. Vårt valg av definisjon er som følger:

Definisjon 1.3.1. *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) $\emptyset \in \mathcal{I}$.

(I2) *Hvis $I_1 \in \mathcal{I}$ og $I_2 \subseteq I_1$, så er $I_2 \in \mathcal{I}$.*

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

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

Følgende proposisjon, gitt som oppgave 4 i kapittel 1.1 i [O], gir et alternativt matroide-definerende aksiomsystem, nemlig (I1), (I2) og (I3′):

Proposisjon 1.3.2. *Den tredje egenskapen i definisjon* 1.3.1*,* (I3)*, kan erstattes med følgende ekvivalente egenskap, for $X \subseteq S$:*

(I3′) *Alle maksimale delmengder I av X med $I \in \mathcal{I}$ har samme kardinalitet.*

Bevis. La $\mathcal{I}$ være familien av uavhengige mengder til en matroide M. Anta at (I3) holder for $\mathcal{I}$, og at $I_1, I_2 \in \mathcal{I}$ er maksimale delmengder av $X \subseteq S$ med $|I_1| < |I_2|$. Da medfører (I3) at det eksisterer et element $e \in I_2 \setminus I_1$ slik at $I_1 \cup \{e\} \in \mathcal{I}$. Siden $e \in I_2 \setminus I_1 \subseteq X$ har vi $I_1 \subset I_1 \cup \{e\} \subseteq X$, noe som er en selvmotsigelse, siden I_1 er maksimal i X. Altså har vi $|I_1| \not< |I_2|$. Siden I_1 og I_2 er vilkårlig valgt, har vi også $|I_2| \not< |I_1|$, altså må vi ha $|I_1| = |I_2|$, og (I3′) følger.

Anta så at (I3′) holder for $\mathcal{I}$, og at $I_1, I_2 \in \mathcal{I}$ med $|I_1| < |I_2|$. La $X = I_1 \cup I_2 \subseteq S$. Da gir (I3′) at I_1 ikke er maksimal i X. Da må det eksistere et element $e \in X \setminus I_1$ slik at $I_1 \cup \{e\} \in \mathcal{I}$, og siden $X \setminus I_1 = (I_1 \cup I_2) \setminus I_1 = I_2 \setminus I_1$, følger (I3). □

Proposisjon 1.3.3. *La S være mengden av kolonneindekser til en $m \times n$-matrise A over en kropp $\mathbb{K}$, og la $\mathcal{I} = \{I \subseteq S \mid$ multimengden av kolonner indeksert av I er lineært uavhengig over vektorrommet $\mathbb{K}^m\}$. Da er $(S,\mathcal{I})$ en matroide som vi kaller **vektormatroiden** til A, med betegnelsen $M[A]$.*

Bevis. Se proposisjon 1.1.1 i [O]. □

Definisjon 1.3.4. *La $M = (S,\mathcal{I})$ være en matroide. En **base** for M er en maksimal uavhengig delmengde av S. Vi betegner familien av alle basene for M ved $\mathcal{B}$ eller $\mathcal{B}(M)$.*

Legg merke til at egenskap (I3′) umiddelbart gir at alle basene for M har samme kardinalitet, og egenskap (I2) gir følgende sammenheng:

$$I \in \mathcal{I}(M) \quad \Leftrightarrow \quad I \subseteq B \text{ for én } B \in \mathcal{B}(M).$$

Dette betyr igjen at en matroide er entydig bestemt av $\mathcal{B}$, og vi betegner den $(S,\mathcal{B})$. Følgende proposisjon gir egenskapen en mengde må ha for å være en familie av baser for en matroide:

Teorem 1.3.5. *La $\mathcal{B}$ være en ikke-tom familie av delmengder av en mengde S. Da er $(S, \mathcal{B})$ en matroide hvis og bare hvis $\mathcal{B}$ tilfredsstiller følgende egenskap:*

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

Bevis. Se korollar 1.2.5 i [O]. □

Definisjon 1.3.6. *La $M = (S, \mathcal{I})$ være en matroide. En **krets** i M er en minimal avhengig delmengde av S. Vi betegner familien av alle kretsene til M ved $\mathcal{C}$ eller $\mathcal{C}(M)$.*

Teorem 1.3.7. *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) *$\emptyset \notin \mathcal{C}$.*

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

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

Bevis. Se korollar 1.1.5 i [O]. Oxley beviser her at egenskapene (C1)−(C3) er ekvivalente med (I1)−(I3). □

Siden (C1)−(C3) er ekvivalente med (I1)−(I3), er en matroide M entydig definert av $\mathcal{C}(M)$. Vi skriver $M = (S, \mathcal{C})$ for denne matroiden.

Proposisjon 1.3.8. *La G være en graf med kantmengde $E(G)$, og la $\mathcal{C}$ være familien av kantmengder til kretser i G. Da er $\mathcal{C}$ familien av kretser til en matroide på $E(G)$. Vi kaller denne matroiden **kretsmatroiden** til grafen G, og betegner den med $M(G)$.*

Bevis. Dette er proposisjon 1.1.7 i [O], og beviset står der. □

En delmengde I av $E(G)$ er altså uavhengig hvis og bare hvis den ikke inneholder kantmengden til en krets i G, eller sagt på en annen måte, hvis og bare hvis $G|_I$, restriksjonen av G til I, er en skog. Tilsvarende er en delmengde B av $E(G)$ en base for $M(G)$ hvis og bare hvis $G|_B$ er en utspennende skog for G.

Inspirert av grafterminologi definerer vi også **vidden** til en matroide M som den minste kardinaliteten til en krets i M. Da får vi umiddelbart at vidden til en graf G er lik vidden til matroiden $M(G)$.

Definisjon 1.3.9. *La $M = (S, \mathcal{I})$ være en matroide. **Rangfunksjonen** på M er en funksjon $r : \mathcal{P}(S) \to \mathbb{N} \cup \{0\}$ gitt ved*

$$r(X) \quad = \quad max\,\{|I| \,|\, I \subseteq X, I \in \mathcal{I}\},$$

*for alle $X \subseteq S$. **Rangen** til X er tallet $r(X)$. **Rangen til matroiden** M er lik $r(S)$, og vi skriver $r(M)$ for denne.*

Dersom $M[A] = (S, \mathcal{I})$ er en vektormatroide for en matrise A, har vi altså at for $X \subseteq S$ er $r(X)$ lik rangen til matrisen som utgjøres av kolonnevektorene i A med indekser i X, så rangfunksjonen r er en naturlig generalisering av rangen til en matrise.

La $M(G)$ være kretsmatroiden til en graf G, og la S være grunnmengden til $M(G)$. Som tidligere bemerket, er $X \subseteq E(G)$ uavhengig hvis og bare hvis $G|_X$ er en skog. Derfor har vi, for $X \subseteq S$, at $r(X) = |E(T_X)|$, der T_X er en utspennende skog for restriksjonen av G til kantene i G med indekser i X. Legg merke til at dersom G har i komponenter, og T_G er en utspennende skog for G, har vi $r(M(G)) = |E(T_G)| = |V(T_G)| - i = |V(G)| - i$.

Proposisjon 1.3.10. *La $M = (S, r)$ være en matroide, og la $X \subseteq S$. Da har vi:*

$$X \text{ er uavhengig} \quad \Leftrightarrow \quad |X| = r(X), \tag{1.1}$$

$$X \text{ er avhengig} \quad \Leftrightarrow \quad |X| > r(X), \text{ og} \tag{1.2}$$

$$X \text{ er en base} \quad \Leftrightarrow \quad |X| = r(X) = r(M). \tag{1.3}$$

Bevis. (1.1) Dette følger direkte fra definisjonen av r.

(1.2) Siden $r(X) \leq |X|$ for alle $X \subseteq S$ (også dette direkte fra definisjonen av r), følger dette fra (1.1).

(1.3) Anta først at X er en base. Da er X en maksimal uavhengig delmengde av S, altså har vi $|X| = \max\{|I| \,|\, I \subseteq X, I \in \mathcal{I}\} = r(X) = \max\{|I| \,|\, I \subseteq S, I \in \mathcal{I}\} = r(M)$. Anta så at $|X| = r(X) = r(M)$. Vi har $|X| = r(X)$, som betyr at X må være uavhengig, og dette kombinert med $|X| = r(M)$ gir at X må være en maksimal uavhengig delmengde av S, for hvis ikke, eksisterer $Y \subseteq S$ slik at $Y \in \mathcal{I}(M)$ og $|Y| > |X| = r(M) = \max\{|I| \,|\, I \subseteq S, I \in \mathcal{I}(M)\}$, som er en selvmotsigelse. Altså har vi at X er en base. □

Proposisjon 1.3.10 gir blant annet at $\mathcal{I}(M)$ er entydig bestemt av rangfunksjonen på M, altså er matroiden M også entydig bestemt. Vi skriver $M = (S, r)$ for en matroide på S definert av en rangfunksjon r.

Vi gir så to ekvivalente aksiomsystem som definerer en rangfunksjon på en matroide:

Teorem 1.3.11. *La S være en mengde, og la $X, Y \subseteq S$ og $x, y \in S$. En funksjon $r : \mathcal{P}(S) \to \mathbb{N} \cup \{0\}$ er rangfunksjonen på en matroide på S hvis og bare hvis r har disse egenskapene:*

(R1) $0 \leq r(X) \leq |X|$.

(R2) $r(X) \leq r(Y)$ *hvis* $X \subseteq Y$.

(R3) $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$.

Ekvivalent, hvis og bare hvis r har disse egenskapene:

(R1′) $r(\emptyset) = 0$.

(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 har vi* $r(X \cup \{x\} \cup \{y\}) = r(X)$.

Bevis. Dette er teoremene 1.2.2 og 1.2.3 i [Wel], og bevisene finnes der, i kapittel 1.5. Beviset for aksiomene (R1) – (R3) finnes også i [O] (korollar 1.3.4). □

Definisjon 1.3.12. *To matroider $M_1 = (S_1, \mathcal{I}_1)$ og $M_2 = (S_2, \mathcal{I}_2)$ er **isomorfe** 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 $X \subseteq S_1$. Vi skriver $M_1 \cong M_2$.*

Vi introduserer nå dualitetsbegrepet for matroider, som utgjør et viktig verktøy i matroideteori, og, som vi skal se, korresponderer med dualitetsbegrepet i grafteori.

Teorem 1.3.13. *La $M = (S, \mathcal{B}(M))$ være en matroide. Da er $\mathcal{B}^*(M) = \{S \setminus B \mid B \in \mathcal{B}(M)\}$ familien av baser for en matroide M^* på S, kalt den **duale matroiden** til M.*

Bevis. Se teorem 2.1.1 i [O]. □

Legg merke til at vi fra forrige teorem umiddelbart får at

$$(M^*)^* \quad = \quad M,$$

siden vi har $(\mathcal{B}^*(M))^* = \mathcal{B}(M)$.

Vi kaller de uavhengige mengdene, basene og kretsene til M^* henholdsvis for **kouavhengige mengder**, **kobaser** og **kokretser** til M. Rangfunksjonen på M^* kaller vi den **duale rangfunksjonen** på M, og betegner den med r^*. Merk at en matroide har én unik dual, altså er kjennskap til de kouavhengige mengdene, kobasene, kokretsene eller den duale rangfunksjonen nok til å karakterisere en matroide.

Vi definerer også **kovidden** til M som vidden til M^*.

Hvis G er en graf, betegner vi dualen til kretsmatroiden med $M^*(G)$ og kaller den **kokretsmatroiden** til G. Følgende proposisjon viser at matroidedualitet korresponderer med geometrisk dualitet for planare grafer:

Proposisjon 1.3.14. *Hvis G^* er en geometrisk dual for en planar graf G, har vi*

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

Bevis. Dette er lemma 2.3.7 i [O], og beviset står der. □

Merk at dette gir at alle geometriske dualer til en graf har isomorfe kretsmatroider, selv om, som tidligere bemerket, de kan være ikke-isomorfe på grafnivå.

Vi har også, som forventet, følgende sammmenheng:

Proposisjon 1.3.15. *For en graf G og $X \subseteq E(G)$ har vi*

$$X \text{ er en kokrets i } G \quad \Leftrightarrow \quad X \text{ er en kokrets i } M(G).$$

Bevis. Se proposisjon 2.3.1 i [O]. □

Altså har vi også at kovidden til G er lik kovidden til $M(G)$.

Følgende teorem gir oss en enkel metode for å konstruere dualen til en vektormatroide:

Teorem 1.3.16. *La $A = [I_r \mid P]$ være en matrise på standard form, og la $M[A]$ være vektormatroiden til A. Da er $(M[A])^*$ lik vektormatroiden $M[B]$ til matrisen $B = [-P^T \mid I_{n-r}]$.*

Bevis. Se teorem 2.2.8 i [O]. □

Legg merke til at det motsatte av teorem 1.3.16 også gjelder, for siden $(M^*)^* = M$, har vi

$$(M[B])^* \quad = \quad ((M[A])^*)^* \quad = \quad M[A],$$

der A og B er matrisene fra teorem 1.3.16.

Vi vil nå gi et eksempel på en klasse av matroider som vil få stor betydning senere i oppgaven:

Eksempel 1.3.17. *La r og n være heltall slik at $0 \leq r \leq n$. La $S = \{1, 2, \ldots, n\}$ og la $\mathcal{B} = \{B \subseteq S \,|\, |B| = r\}$. Det er enkelt å sjekke at $(S, \mathcal{B})$ er en matroide, og vi kaller $(S, \mathcal{B})$* ***den uniforme matroiden*** *av rang r på en n-mengde, og betegner den $U_{r,n}$. Videre er*

$$\begin{aligned} \mathcal{I}(U_{r,n}) &= \{I \subseteq S \,|\, |I| \leq r\}, \\ \mathcal{C}(U_{r,n}) &= \begin{cases} \emptyset & \text{hvis } r = n, \\ \{C \subseteq S \,|\, |C| = r+1\} & \text{hvis } r < n, \text{ og} \end{cases} \\ r(X) &= \begin{cases} |X| & \text{hvis } |X| < r, \\ r & \text{hvis } |X| \geq r, \end{cases} \end{aligned}$$

der $X \subseteq S$. Vi har altså $r(M) = r$.

I tillegg er $\mathcal{B}^*(U_{r,n}) = \{B \subseteq S \,|\, |B| = n - r\}$, altså har vi

$$U_{r,n}{}^* \quad = \quad U_{n-r,n}.$$

En matroide på formen $U_{n,n}$ kalles en ***fri matroide****, og den frie matroiden $U_{0,0}$, som er den unike matroiden på $S = \emptyset$, kalles* ***den tomme matroiden****.*

Til slutt i dette kapittelet tar vi for oss noen definisjoner og resultater som omhandler matroider som kommer fra grafer og matriser, altså de to viktigste kildene til matroideeksempler.

Definisjon 1.3.18. *En matroide som er isomorf til kretsmatroiden til en graf G kalles* ***grafisk****, mens en matroide som er isomorf til kokretsmatroiden til G kalles* ***kografisk****. Hvis matroiden M både er grafisk og kografisk, sier vi at M er* ***planar-grafisk****.*

Proposisjon 1.3.19. *La M være en grafisk matroide. Da er $M \cong M(G)$ for en sammenhengende graf G.*

Bevis. Se proposisjon 1.2.8 i [O]. □

Merk at siden matroideisomorfi kun er en bijeksjon på elementene i grunnmengdene, og vi kan navngi kanter i en graf vilkårlig, kan isomorfiene i definisjon 1.3.18 og proposisjon 1.3.19 erstattes med likheter.

Teorem 1.3.20. *Følgende er ekvivalent, for en graf G:*

i) G *er planar.*

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

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

Bevis. Dette er (deler av) teorem 5.2.2 og proposisjon 5.2.6 i [O], og beviset finnes der. □

Definisjon 1.3.21. *Hvis en matroide M er isomorf til vektormatroiden til en matrise A over en kropp $\mathbb{K}$, sier vi at M er* $\mathbb{K}$***-representabel**. Matrisen A kalles en* $\mathbb{K}$***-representasjon** for M.*

De følgende to resultatene viser at det å være grafisk er et sterkere krav til en matroide enn å være representabel over en kropp:

Proposisjon 1.3.22. *La G være en graf, og la D være en vilkårlig orientering av G. La A_D være hjørne-kant-insidensmatrisen til D. La $\mathbb{K}$ være en vilkårlig kropp med karakteristikk q, og la $A_D{}'$ være A_D redusert modulo q. Da er $A_D{}'$ en $\mathbb{K}$-representasjon for $M(G)$, altså har vi $M[A_D{}'] \cong M(G)$.*

Bevis. Se beviset for proposisjon 5.1.2 i [O]. □

Fra dette får vi umiddelbart følgende:

Korollar 1.3.23. *Hvis G er en graf, så er $M(G)$ representabel over enhver kropp.*

Bevis. Se proposisjon 5.1.2 i [O]. □

Det eksisterer matroider som ikke er representable over noen kropp. Faktisk er den såkalte Vámos-matroiden V_8 (se eksempel 2.1.22 i [O]) ikke representabel over noen kropp, selv om grunnmengden bare består av 8 elementer.

1.4 Lineære koder

Før vi definerer lineære koder, gir vi definisjonen av en generell kode, i tillegg til en del begreper som også har mening i det generelle tilfellet:

Definisjon 1.4.1. *La $F_q = \{\lambda_1, \lambda_2, \ldots, \lambda_q\}$ være en mengde av q forskjellige elementer, og la $n \in \mathbb{N}$. En **q-ær blokk-kode** C av lengde n er en ikke-tom delmengde av $(F_q)^n$, der $(F_q)^n$ er mengden av n-tupler over F_q. Mengden F_q kalles kodens **alfabet**, og elementene i C kalles **kodeord**.*

Alle kodene i denne oppgaven er blokk-koder, derfor bruker vi for enkelthets skyld bare betegnelsen kode når vi mener blokk-kode, og spesifiserer de parametrene som er nødvendige i hvert tilfelle.

Definisjon 1.4.2. *La $\underline{x} = (x_1, x_2, \ldots, x_n) \in (F_q)^n$ og $\underline{y} = (y_1, y_2, \ldots, y_n) \in (F_q)^n$. **Hammingavstanden** $d(\underline{x}, \underline{y})$ mellom $\underline{x}$ og $\underline{y}$ er antall posisjoner der $\underline{x}$ og $\underline{y}$ er forskjellige, altså*

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

Korollar 1.4.3. *Hammingavstanden er en metrikk på $(F_q)^n$.*

Bevis. Beviset står på side 5 i [H]. □

Definisjon 1.4.4. ***Minimumsavstanden** til en kode C er gitt ved*

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

Definisjon 1.4.5. ***Hammingvekten*** *$w(\underline{x})$ til $\underline{x} = (x_1, x_2, \ldots, x_n) \in (F_q)^n$ er antall ikke-null koordinater i $\underline{x}$, altså*

$$w(\underline{x}) \quad = \quad |\{i \,|\, x_i \neq 0,\, 1 \leq i \leq n\}|.$$

Definisjon 1.4.6. ***Minimumsvekten*** *til en kode C er gitt ved*

$$w(C) \quad = \quad \min\{w(\underline{x}) \,|\, \underline{x} \in C \setminus \{\underline{0}\}\}.$$

Definisjon 1.4.7. ***Vektenumeratoren*** *til en kode C av lengde n er*

$$W_C(z) \quad = \quad \sum_{i=0}^{n} A_i z^i,$$

der A_i er antall kodeord av (Hamming)vekt i.

Hvis vi lar F_q være kroppen $\mathbb{F}_q$, blir $(F_q)^n$ et n-dimensjonalt vektorrom, nemlig $(\mathbb{F}_q)^n$, og vi kan definere:

Definisjon 1.4.8. *En* ***q-ær lineær kode*** *C av lengde n og dimensjon k er et k-dimensjonalt underrom av $(\mathbb{F}_q)^n$. Hvis $d(C) = d$, sier vi at C er en* ***[n,k,d]-kode****. Hvis vi ikke er interessert i (eller ikke kjenner) parameteren d, skriver vi ofte bare* ***[n,k]-kode****. En annen viktig parameter er* ***redundansen*** *r til C, som er gitt ved $r = n - k$.*

Et standardresultat fra lineær algebra gir at antall kodeord i en q-ær $[n, k]$-kode er q^k. (Se for eksempel teorem 4.3 i [H] for bevis.)

Teorem 1.4.9. *Hvis C er en lineær kode, har vi*

$$d(C) \quad = \quad w(C).$$

Bevis. Dette er teorem 5.2 i [H], og beviset står der. □

Følgende velkjente teorem gir viktige begrensninger for kodeparametrene n, k og d, og vi skal senere generalisere dette i korollar 1.4.23.

Teorem 1.4.10. ***(Singletonbegrensningen)*** *En $[n, k, d]$-kode oppfyller*

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

Bevis. La C være en $[n, k, d]$-kode. Antall kodeord i C er da q^k. La C' være mengden av de tuplene vi får hvis vi fjerner $d - 1$ fikserte koordinater fra hvert kodeord i C. Da er fremdeles alle elementer i C' forskjellige, altså er $|C'| = |C|$, og siden elementene i C' er $(n-d+1)$-tupler over $\mathbb{F}_q$, har vi maksimalt q^{n-d+1} elementer i C'. Altså har vi

$$q^k \quad = \quad |C| \quad = \quad |C'| \quad \leq \quad q^{n-d+1},$$

som igjen gir

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

□

Definisjon 1.4.11. *En **generatormatrise** G for en $[n,k]$-kode C er en $k \times n$-matrise der radene danner en basis for C.*

Definisjon 1.4.12. *To lineære koder over $(\mathbb{F}_q)^n$ kalles **ekvivalente** hvis den ene koden kan fås fra den andre ved å permutere koordinater og/eller multiplisere koordinater med ikke-null skalarer.*

Legg merke til at ekvivalente koder har de samme parametrene n, k og d.

Teorem 1.4.13. *La G være en generatormatrise for en $[n,k]$-kode. Ved å utføre elementære rad- og kolonneoperasjoner på G kan vi omforme G til **standard form**,*

$$[I_k \,|\, A],$$

der A er en $k \times (n-k)$-matrise.

Bevis. Se teorem 5.5 i [H]. □

Elementære radoperasjoner bevarer den lineære avhengigheten mellom radene til G og bytter en basis med en annen basis for den samme koden, mens elementære kolonneoperasjoner omformer G til en generatormatrise for en ekvivalent kode.

Vi definerer **indreproduktet** $\underline{u} \cdot \underline{v}$ mellom vektorer $\underline{u} = (u_1, u_2, \ldots, u_n) \in (\mathbb{F}_q)^n$ og $\underline{v} = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_q)^n$ til å være $\underline{u} \cdot \underline{v} = u_1v_1 + u_2v_2 + \cdots + u_nv_n \in \mathbb{F}_q$. Hvis $\underline{u} \cdot \underline{v} = 0$, sier vi at $\underline{u}$ og $\underline{v}$ er **ortogonale**.

Definisjon 1.4.14. *La C være en $[n,k]$-kode. **Dualkoden** $C^\perp$ til C er mengden av vektorer i $(\mathbb{F}_q)^n$ som er ortogonale til alle vektorer i C, eller*

$$C^\perp \;=\; \{\underline{v} \in (\mathbb{F}_q)^n \,|\, \underline{v} \cdot \underline{c} = 0 \text{ for alle } \underline{c} \in C\}.$$

Følgende setning viser at $C^\perp$ er fullstendig spesifisert ved generatormatrisen for C:

Proposisjon 1.4.15. *La C være en lineær kode med generatormatrise G. Da er*

$$C^\perp \;=\; \{\underline{v} \in (\mathbb{F}_q)^n \,|\, \underline{v}G^T = \underline{0}\}.$$

Bevis. Se lemma 7.2 i [H]. □

Teorem 1.4.16. *Hvis C er en $[n,k]$-kode, så er $C^\perp$ en $[n,n-k]$-kode, og $(C^\perp)^\perp = C$.*

Bevis. Se teoremene 7.3 og 7.5 i [H] for bevis. □

Definisjon 1.4.17. *En **paritetssjekkmatrise** H for en kode C er en generatormatrise for $C^\perp$.*

Proposisjon 1.4.15 og teorem 1.4.16 gir oss da at H er en $(n-k) \times n$-matrise som tilfredsstiller $GH^T = \mathbf{0}$, og at enhver lineær kode C er entydig gitt ved sin paritetssjekkmatrise H, ved sammenhengen

$$C \;=\; \{\underline{c} \in (\mathbb{F}_q)^n \,|\, \underline{c}H^T = \underline{0}\}.$$

Fordi $GH^T = \mathbf{0}$ har vi at dersom C og C' er ekvivalente koder, så vil også $C^\perp$ og $(C')^\perp$ være ekvivalente, og motsatt. Altså har vi, for koder C og C':

$$C \text{ er ekvivalent med } C' \quad \Leftrightarrow \quad C^\perp \text{ er ekvivalent med } (C')^\perp.$$

En paritetssjekkmatrise H sies å være på **standard form** hvis $H = [B \,|\, I_{n-k}]$, der B er en $(n-k) \times k$-matrise. Følgende teorem gir en god grunn for denne definisjonen, og gjør det også enkelt å konstruere en paritetssjekkmatrise for en kode, gitt en generatormatrise på standard form:

Teorem 1.4.18. *Hvis $G = [I_k \,|\, A]$ er en generatormatrise på standard form for en $[n,k]$-kode C, så er $H = [-A^T \,|\, I_{n-k}]$ en paritetssjekkmatrise for C.*

Bevis. Dette er teorem 7.6 i [H], og beviset står der. □

Vi merker oss at siden H er en generatormatrise for $C^\perp$, så gjelder også det omvendte resultatet: Hvis $H = [B \,|\, I_{n-k}]$ er en paritetssjekkmatrise på standard form for en $[n,k]$-kode, så er $G = [I_k \,|\, -B^T]$ en generatormatrise for koden.

Følgende viktige teorem gir oss en måte å bestemme minimumsavstanden d til en kode, kun ut fra lineær uavhengighet mellom kolonnene i paritetssjekkmatrisen for koden. Vi skal senere generalisere dette og bruke det mye videre i oppgaven.

Teorem 1.4.19. *La C være en $[n,k]$-kode over $(\mathbb{F}_q)^n$, og la H være en paritetssjekkmatrise for C. Da er d minimumsdistansen til C hvis og bare hvis ethvert valg av $d-1$ kolonner i H er lineært uavhengige, samtidig som det eksisterer minst ett valg av d lineært avhengige kolonner i H.*

Bevis. Se teorem 8.4 i [H] for bevis. □

I resten av dette kapittelet vil vi ta for oss det såkalte vekthierarkiet til en lineær kode, som er en generalisering av minimumsvekten, eller ekvivalent, minimumsdistansen, jf. teorem 1.4.9. Vekthierarkiet ble først oppdaget av Helleseth, Kløve og Mykkeltveit i 1977, og senere gjenoppdaget i [Wei]. Resultatene her er hentet fra Weis artikkel.

Definisjon 1.4.20. *La $N \subseteq (\mathbb{F}_q)^n$. **Støtten** $\chi(N)$ til N er mengden av posisjoner der ikke alle vektorer i N er 0, altså*

$$\chi(N) \quad = \quad \{i \,|\, \exists\, \underline{x} = (x_1, x_2, \ldots, x_n) \in N \text{ med } x_i \neq 0 \text{ for } 1 \leq i \leq n\}.$$

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

Vi kan se på minimumsvekten $w(C)$ til en kode C som den minste støttevekten til endimensjonale underrom av C, og slik generalisere $w(C)$ til h-dimensjonale underrom av C, for $1 \leq h \leq k$:

Definisjon 1.4.21. *La C være en $[n,k]$-kode. Den **h-te generaliserte Hammingvekten** til C er*

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

*for $1 \leq h \leq k$, der D_h er et h-dimensjonalt underrom av C. Mengden $\{d_h(C) \,|\, 1 \leq h \leq k\}$ kalles **vekthierarkiet** til C.*

Vi har $\chi(\underline{x}) = w(\underline{x})$ for alle kodeord $\underline{x}$, og $d_1(C) = w(C) = d(C)$, ved teorem 1.4.9. Legg også merke til at ekvivalente koder har samme vekthierarki.

Teorem 1.4.22. *For en $[n, k, d]$-kode C har vi*

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

Bevis. Se teorem 1 i [Wei], side 1412. (Artikkelen [Wei] er avgrenset til kun binære koder, men i resultatene som refereres til i denne oppgaven kan alle bevisene direkte generaliseres til generelle lineære koder, altså gjelder resultatene også generelt.) □

Teorem 1.4.22 gir oss umiddelbart følgende:

Korollar 1.4.23. ***(Generalisert Singletonbegrensning)*** *En $[n, k]$-kode C med vekthierarki $\{d_h \mid 1 \leq h \leq k\}$ oppfyller*

$$d_h \leq n - k + h.$$

□

Legg merke til at den vanlige Singletonbegrensningen, teorem 1.4.10, følger direkte fra korollar 1.4.23, siden $d_1(C) = d(C)$.

Vi skal nå se på en alternativ måte å beregne de generaliserte Hammingvektene på, ved å generalisere teorem 1.4.19. Teoremet sier at $d = d_1$ til en kode C er gitt ved det minste antall kolonner i paritetssjekkmatrisen for C som er lineært avhengige. Eller, sagt på en annen måte, $d = d_1$ er det minste tallet t slik at det eksisterer t kolonner i H som danner kolonnene i en matrise med rang høyst lik $t - 1$. Dette kan generaliseres på følgende måte:

Teorem 1.4.24. *La C være en $[n, k]$-kode, og la H være en paritetssjekkmatrise for C. La H_i være kolonnevektorene til H for $i \in S$, der $S = \{1, 2, \ldots, n\}$ er mengden av kolonneindekser til H, og la H_I være matrisen der vektorene H_i utgjør kolonnene for $i \in I \subseteq S$. Da har vi, for alle $1 \leq h \leq k$:*

$$d_h = \min\{|I| \,|\, |I| - \operatorname{rg}(H_I) \geq h, I \subseteq S\}, \tag{1.4}$$

der d_h er den h-te generaliserte Hammingvekten til C.

Bevis. Dette er teorem 2 i [Wei], se der for bevis. □

Proposisjon 1.4.25. *Uttrykket* (1.4) *i teorem* 1.4.24 *kan erstattes med følgende:*

$$d_h = \min\{|I| \,|\, |I| - \operatorname{rg}(H_I) = h, I \subseteq S\}.$$

Bevis. Matriserangen rg er et spesialtilfelle av rangfunksjonen r for matroider, altså gjelder aksiomene (R1)−(R3) og (R1′)−(R3′) også for matriserangen. Spesielt gjelder aksiom (R2′), altså har vi for enhver vektor H_j med $j \notin I$:

$$\operatorname{rg}(H_I) \leq \operatorname{rg}([H_I \,|\, H_j]) \leq \operatorname{rg}(H_I) + 1.$$

Men siden vi også har

$$|I| < |I \cup \{j\}| = |I| + 1,$$

betyr det at funksjonen $f : S \to \mathbb{N} \cup \{0\}$ definert ved at $f(I) = |I| - \operatorname{rg}(H_I)$, øker med maksimalt én for hver ny vektor som legges til. Og siden vi i (1.4) ønsker minst mulig kardinalitet, kan vi ikke ha $|I| - \operatorname{rg}(H_I) > h$ i dette uttrykket. □

Vi kommer til å gjøre bruk av denne formuleringen av teorem 1.4.24 senere i oppgaven.

Hvis vi kjenner vekthierarkiet til en kode C, er det enkelt å finne vekthierarkiet til dualkoden $C^{\perp}$:

Teorem 1.4.26. *La C være en $[n,k]$-kode. Da har vi*

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

Bevis. Se teorem 3 i [Wei]. □

Kapittel 2

MDS-egenskaper og vekthierarki for koder, matroider og grafer

Teorem 1.4.10, Singletonbegrensningen, gir oss en øvre grense for dimensjonen k til en kode, gitt kodens lengde n og minimumsdistanse d, eller alternativt, en øvre grense for d, gitt n og k. Vi skal nå se på koder som oppfyller likhet i Singletonbegrensningen, kalt MDS-koder (Maximum Distance Separable), og koder som nesten gjør det. Vi skal benytte oss av to ulike mål på hvor nær en kode er til å være MDS, og det å angi et av (eller begge) disse målene til en kode, vil vi i det følgende kalle å angi **MDS-egenskaper** ved koden. Vi vil også studere sammenhengen mellom MDS-egenskapene og vekthierarkiet til en kode, noe som tidligere også for en del er gjort i [R] og [L].

I tillegg vil vi studere den allerede kjente overgangen mellom lineære koder og matroider, og bruke denne og teorem 1.4.24 til å definere vekthierarki også for matroider, slik det er gjort i [L]. Videre vil vi introdusere MDS-egenskaper for matroider, og siden matroider i en viss forstand er en generalisering av grafer, definerer vi vekthierarki og MDS-egenskaper også for grafer. Videre studerer vi hvordan resultater om MDS-egenskaper for koder kan overføres til matroider og grafer, og klassifiserer et stykke på vei matroider og grafer med gitte MDS-egenskaper. Til slutt tar vi med noen resultater som omhandler hvor stort antall grafer med gitte MDS-egenskaper som eksisterer, i lys av de tidligere resultatene.

2.1 MDS-egenskaper for koder

2.1.1 Definisjoner

Vi definerer først MDS-koder, og som nevnt er dette koder som oppfyller likhet i Singletonbegrensningen, teorem 1.4.10:

Definisjon 2.1.1. *En **MDS-kode** er en $[n, k, d]$-kode med $d = n - k + 1$.*

Altså har vi $d = r + 1$ for MDS-koder. Som konvensjon sier vi at nullkoden, det vil si koden med $k = 0$, er MDS. Det neste resultatet, som følger umiddelbart fra teorem 1.4.19, forteller hvordan paritetssjekkmatriser for MDS-koder ser ut:

Korollar 2.1.2. *La C være en $[n,k]$-kode, og la H være en paritetssjekkmatrise for C. Da har vi:*

$$C \text{ er MDS} \quad \Leftrightarrow \quad \text{Alle valg av } n-k \text{ kolonner i } H \text{ er lineært uavhengige.}$$

Bevis. La C være en $[n,k]$-MDS-kode. Da er minimumsdistansen $d = n-k+1$, og teorem 1.4.19 gir oss at dette er ekvivalent med at alle valg av $d-1 = n-k$ kolonner i H er lineært uavhengige, og det eksisterer minst ett valg av $d = n-k+1$ lineært avhengige kolonner i H. Men siden $\text{rg}(H) = n-k$, vil alle valg av $n-k+1$ kolonner i H være lineært avhengige, og vi har resultatet. □

Senere vil vi også se hvordan generatormatriser for MDS-koder ser ut.

La oss så introdusere vårt første mål på hvor nær en kode er til å være MDS:

Definisjon 2.1.3. *La C være en $[n,k,d]$-kode. **Singletondefekten** $S(C)$ til C er:*

$$S(C) \quad = \quad n-k+1-d.$$

Som ventet har vi umiddelbart, for en $[n,k,d]$-kode C:

$$C \text{ er MDS} \quad \Leftrightarrow \quad S(C) = 0.$$

Definisjon 2.1.4. *En kode C med Singletondefekt $S(C) = 1$ kalles **nesten-MDS**.*

Som vi skal vise senere, er dualkoden til en MDS-kode også MDS, men denne egenskapen gjelder dessverre ikke for nesten-MDS-koder. Vi illustrerer dette med følgende enkle eksempel:

Eksempel 2.1.5. *La C være $[4,3]$-koden over $\mathbb{F}_2$ med generatormatrise*

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

Vi har $d(C) = 1$, altså er koden C nesten-MDS, siden Singletondefekten er $S(C) = 4-3+1-1 = 1$. Dualkoden $C^\perp$ er en $[4,1]$-kode, fra teorem 1.4.16. Siden G er på standard form, har vi fra teorem 1.4.18 at en paritetssjekkmatrise H for C (som er en generatormatrise for $C^\perp$) ser slik ut:

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

Altså er $C^\perp = \{0000, 1001\}$, og vi har $d(C^\perp) = 2$. Singletondefekten er derfor $S(C^\perp) = 4-1+1-2 = 2$, og $C^\perp$ er ikke nesten-MDS.

Legg også merke til at vekthierarkiet til $C^\perp$ er $\{d_1\} = \{2\}$, siden $k(C^\perp) = 1$ og $d_1 = d$. Ved teorem 1.4.26 er det da enkelt å finne vekthierarkiet til C, som er $\{d_1, d_2, d_3\} = \{1,2,4\}$.

Som følge av dette innfører vi en ny definisjon, med et sterkere krav enn nesten-MDS:

Definisjon 2.1.6. *La C være en lineær kode. Dersom $S(C) = S(C^\perp) = 1$ kalles C **nær-MDS**.*

2.1.2 MDS-egenskaper, vekthierarki og dualkoder

Vi vil nå se på en annen måte å definere MDS-koder på, nemlig ved hjelp av vekthierarkiet til koden. En umiddelbar fordel med dette, er at vi da kan utnytte teorem 1.4.26 til å si noe om dualkoden. Vi vil videre også bruke dette teoremet til å si noe om dualkoder til nesten-MDS-koder.

Lemma 2.1.7. *Følgende er ekvivalent, for en $[n,k]$-kode C med vekthierarki $\{d_h \mid 1 \leq h \leq k\}$:*

i) C *er MDS.*

ii) $d_1 = n - k + 1$.

iii) $d_h = n - k + h$, *for alle* $1 \leq h \leq k$.

iv) $\{d_h(C) \mid 1 \leq h \leq k\} = \{n - k + 1, n - k + 2, \ldots, n\}$.

Bevis. Vi har *i)* $\Leftrightarrow$ *ii)* fra definisjonen av en MDS-kode, siden $d_1(C) = d(C)$. Del *iii)* og *iv)* er logisk sett det samme utsagnet, mens *iii)* $\Rightarrow$ *ii)* er trivielt, så det eneste vi må vise, er *ii)* $\Rightarrow$ *iii)*. Anta at *ii)* holder. Da gir teorem 1.4.22 at $d_h \geq n - k + h$, for alle $1 \leq h \leq k$. Men fra korollar 1.4.23 har vi også $d_h \leq n - k + h$, altså må vi ha $d_h = n - k + h$, for alle $1 \leq h \leq k$, og *iii)* holder. □

Proposisjon 2.1.8. *For en lineær kode C har vi:*

$$C \text{ er MDS} \quad \Leftrightarrow \quad C^{\perp} \text{ er MDS.}$$

Bevis. La C være en $[n,k]$-kode med vekthierarki $\{d_h \mid 1 \leq h \leq k\}$. Lemma 2.1.7 gir at C er MDS hvis og bare hvis vi har

$$\{d_h(C) \mid 1 \leq h \leq k\} \quad = \quad \{n - k + 1, n - k + 2, \ldots, n\}.$$

Ved teorem 1.4.26 er dette ekvivalent med

$$\{n + 1 - d_h(C^{\perp}) \mid 1 \leq h \leq n - k\} \quad = \quad \{1, 2, \ldots, n - k\},$$

som igjen er det samme som

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

Ved å bruke lemma 2.1.7 en gang til, følger resultatet.

(For alternativt bevis, se [H], korollar 15.7.) □

Siden en paritetssjekkmatrise for en kode er en generatormatrise for den duale koden, får vi umiddelbart følgende resultat, ved å kombinere proposisjon 2.1.8 med korollar 2.1.2:

Korollar 2.1.9. *La C være en $[n,k]$-kode, og la G være en generatormatrise for C. Da har vi:*

$$C \text{ er MDS} \quad \Leftrightarrow \quad \textit{Alle valg av } k \textit{ kolonner i } G \textit{ er lineært uavhengige.}$$

□

Vi vil nå definere en kodeegenskap som viser seg å være nært tilknyttet Singletondefekten til koden, og denne vil også være vårt andre mål på hvor nær en kode er til å være MDS:

Definisjon 2.1.10. *En $[n,k]$-kode C med vekthierarki $\{d_h \mid 1 \leq h \leq k\}$ kalles* ***t-MDS*** *hvis t er det minste tallet slik at $d_t = n - k + t$.*

En MDS-kode er dermed 1-MDS. På samme måte som med MDS-koder bruker vi som konvensjon at degenererte $[n,k]$-koder, altså koder med $d_k < n$, er $(k+1)$-MDS.

Hvis vi kombinerer teorem 1.4.22 med korollar 1.4.23, generalisert Singletonbegrensning, får vi umiddelbart følgende resultat:

Korollar 2.1.11. *For en $[n,k]$-kode C med vekthierarki $\{d_h \mid 1 \leq h \leq k\}$ gjelder følgende:*

$$C \text{ er } t\text{-MDS} \quad \Leftrightarrow \quad d_{t-1} < n - k + t - 1 \text{ og } d_h = n - k + h \text{ for alle } t \leq h \leq k.$$

□

Som Raddum gjør i kapittel 3.1.2 i [R], kan vi karakterisere dualen til en nesten-MDS-kode ved hjelp av vekthierarkiet, men vi vil først gi et mer generelt resultat. Karakteriseringen av dualen til en nesten-MDS-kode vil da komme som et korollar av det følgende:

Teorem 2.1.12. *La C være en $[n,k]$-kode. Da har vi:*

$$\text{Singletondefekten } S(C) = t - 1 \quad \Leftrightarrow \quad C^\perp \text{ er } t\text{-MDS.}$$

Bevis. Definisjonen av Singletondefekt gir at

$$S(C) = t - 1 \quad \Leftrightarrow \quad d_1(C) = n - k - t + 2,$$

og gjentatt bruk av teoremene 1.4.22 og 1.4.26 gir oss at følgende er ekvivalent:

i) $d_1(C) = n - k - t + 2$.

ii) $\{1, 2, \ldots, n-k-t+1\} \cap \{d_h(C) \mid 1 \leq h \leq k\} = \emptyset$ og $n-k-t+2 \in \{d_h(C) \mid 1 \leq h \leq k\}$.

iii) $\{1, 2, \ldots, n-k-t+1\} \subseteq \{n+1-d_h(C^\perp) \mid 1 \leq h \leq n-k\}$ og $n-k-t+2 \notin \{n+1-d_h(C^\perp) \mid 1 \leq h \leq n-k\}$.

iv) $\{k+t, k+t+1, \ldots, n\} \subseteq \{d_h(C^\perp) \mid 1 \leq h \leq n-k\}$ og $k+t-1 \notin \{d_h(C^\perp) \mid 1 \leq h \leq n-k\}$.

v) $\{k+t, k+t+1, \ldots, n\} = \{d_h(C^\perp) \mid t \leq h \leq n-k\}$ og $k+t-1 \notin \{d_h(C^\perp) \mid 1 \leq h \leq n-k\}$.

Sagt med andre ord er t det minste tallet slik at $d_t(C^\perp) = k + t$, og siden dimensjonen til $C^\perp$ er $n - k$, er dette det samme som at $C^\perp$ er t-MDS. □

Dermed kan vi gi en karakterisering av dualen til en nesten-MDS-kode:

Korollar 2.1.13. *La C være en lineær kode. Da har vi:*

$$C \text{ er nesten-MDS} \quad \Leftrightarrow \quad C^\perp \text{ er 2-MDS.}$$

Bevis. Dette er teorem 2.1.12, innsatt $t = 2$. □

Siden $(C^\perp)^\perp = C$, har vi også de motsatte resultatene av teorem 2.1.12 og korollar 2.1.13:

$$\begin{aligned} C \text{ er } t\text{-MDS} &\Leftrightarrow S(C^\perp) = t-1, \text{ og} \\ C \text{ er 2-MDS} &\Leftrightarrow C^\perp \text{ er nesten-MDS.} \end{aligned}$$

Legg merke til at proposisjon 2.1.8 følger direkte fra forrige teorem, siden en MDS-kode har Singletondefekt lik 0 og er 1-MDS. Vi får også umiddelbart følgende resultat, som knytter sammen begrepene nær-MDS, nesten-MDS og 2-MDS:

Korollar 2.1.14. *Følgende er ekvivalent, for en lineær kode C:*

i) C *er nær-MDS.*

ii) C *og* $C^\perp$ *er nesten-MDS.*

iii) C *og* $C^\perp$ *er 2-MDS.*

iv) C *er både nesten-MDS og 2-MDS.*

v) $C^\perp$ *er både nesten-MDS og 2-MDS.*

Bevis. Vi har *i)* $\Leftrightarrow$ *ii)* fra definisjonene av nesten-MDS og nær-MDS. Vi har også at C er nesten-MDS hvis og bare hvis $C^\perp$ 2-MDS, og $C^\perp$ er nesten-MDS hvis og bare hvis C er 2-MDS, noe som umiddelbart gir både *ii)* $\Leftrightarrow$ *iii)*, *ii)* $\Leftrightarrow$ *iv)* og *ii)* $\Leftrightarrow$ *v)*. □

Ekvivalensene *i)*$-$*iv)* er også gitt i [R], som proposisjon 3.1.6 og 3.1.7.

I tillegg kan nær-MDS-koder, som koder med andre MDS-egenskaper, entydig bestemmes fra vekthierarkiet:

Korollar 2.1.15. *Følgende er ekvivalent, for en lineær kode C:*

i) C *er nær-MDS.*

ii) $d_1 = n-k$ *og* $d_2 = n-k+2$.

iii) $\{d_h(C) \mid 1 \leq h \leq k\} = \{n-k, n-k+2, \ldots, n\}$.

Bevis. Siden nær-MDS-koder også er 2-MDS, gjelder høyresiden av ekvivalensen i korollar 2.1.11, med $t = 2$, for nær-MDS-koder. I tillegg har nær-MDS-koder Singletondefekt lik 1. Dermed får vi *i)* $\Leftrightarrow$ *ii)*, mens ekvivalensen *ii)* $\Leftrightarrow$ *iii)* følger fra generalisert Singletonbegrensning. □

2.2 Matroider fra lineære koder

Vi vil nå se nærmere på overgangen mellom lineære koder og matroider. For enhver lineær kode vil vi definere to matroider som er relatert til koden og se hvordan kode- og matroidedualitet korresponderer. Vi vil videre vise den velkjente sammenhengen mellom MDS-koder og uniforme matroider og legge grunnlaget for å definere vekthierarki også for matroider.

La C være en lineær kode, og la G være en generatormatrise for C. Som tidligere bemerket, vil elementære rad- og kolonneoperasjoner på G gi en generatormatrise for en ekvivalent kode.

Vi kan lage $M[G]$, vektormatroiden til G, og de samme operasjonene på G vil gi isomorfe matroider. La så H være en paritetssjekkmatrise for C. Vi kan også lage $M[H]$, vektormatroiden til H, og siden dualkoder til ekvivalente koder også er ekvivalente, som nevnt på side 14, gjelder det samme for elementære rad- og kolonneoperasjoner på H. Vi kan derfor definere følgende, som er entydig, opp til isomorfi, for ekvivalensklassen til koden C:

Definisjon 2.2.1. *La C være en lineær kode, og la G og H være henholdsvis en generatormatrise og en paritetssjekkmatrise for C. **Generatormatroiden** for C er matroiden $M[G]$, mens **paritetssjekkmatroiden** for C er matroiden $M[H]$.*

Proposisjon 2.2.2. *Generatormatroiden og paritetssjekkmatroiden for en lineær kode er duale matroider.*

Bevis. La C være en $[n,k]$-kode, G en generatormatrise for C og $M[G]$ generatormatroiden for C. Vi kan da redusere G til en generatormatrise på standard form, $[I_k \mid A]$, der A er en $k \times (n-k)$-matrise. Teorem 1.4.18 gir oss da at $H = [-A^T \mid I_{n-k}]$ er en paritetssjekkmatrise for C, og teorem 1.3.16 gir oss at paritetssjekkmatroiden $M[H]$ for C er den duale matroiden til $M[G]$. Siden $(M^*)^* = M$ for alle matroider, følger resultatet. □

Siden generatormatrise for en kode C er en paritetssjekkmatrise for $C^\perp$, og motsatt, får vi at dualitet for matroider og koder korresponderer:

$$\begin{aligned} M[G]^* &= M[G^\perp], \text{ og} \\ M[H]^* &= M[H^\perp], \end{aligned}$$

der $G^\perp$ og $H^\perp$ er henholdsvis en generatormatrise og paritetssjekkmatrise for $C^\perp$. Generatormatroiden for $C^\perp$ er altså lik paritetssjekkmatroiden for C, og paritetssjekkmatroiden for $C^\perp$ er lik generatormatroiden for C.

Vi vil nå vise den nære sammenhengen mellom MDS-koder og uniforme matroider, en sammenheng vi også senere vil generalisere til et rent matroideresultat (teorem 2.5.16).

Teorem 2.2.3. *La C være en $[n,k]$-kode med generatormatroide $M[G]$ og paritetssjekkmatroide $M[H]$. Da er følgende ekvivalent:*

i) C er MDS.

ii) $C^\perp$ er MDS.

iii) $M[G]$ er uniform.

iv) $M[H]$ er uniform.

Bevis. Vi har *i)* $\Leftrightarrow$ *ii)* fra proposisjon 2.1.8.

Korollar 2.1.2 gir oss at *i)* er ekvivalent med at alle valg av $n-k$ kolonner i en paritetssjekkmatrise H for C er lineært uavhengige, og vi har alltid at alle valg av $n-k+1$ kolonner i H er lineært avhengige, siden $dim(H) = n-k$. Men dette er det samme som at alle mengder av kardinalitet $n-k$ i $M[H]$ er baser, altså er $M[H] \cong U_{n-k,n}$, den uniforme matroiden av rang $n-k$, og vi har *i)* $\Leftrightarrow$ *iv)*.

Til slutt har vi at $U^*_{n-k,n} = U_{k,n}$, fra eksempel 1.3.17, og proposisjon 2.2.2 gir oss at $M[G]$ og $M[H]$ er duale matroider. Til sammen gir dette oss at *iii)* $\Leftrightarrow$ *iv)*. □

Teorem 1.4.24 gir oss at de generaliserte Hammingvektene til en kode C kun er gitt ved å se på uavhengighet mellom kolonner i paritetssjekkmatrisen for C. Denne informasjonen kan vi også få fra paritetssjekkmatroiden for C:

Korollar 2.2.4. *La C være en $[n,k]$-kode med paritetssjekkmatroide $M[H] = (S,r)$, og la $X \subseteq S$. Da har vi:*

$$d_h(C) \quad = \quad \min\{|X| \,|\, |X| - r(X) \geq h\}, \tag{2.1}$$

for $1 \leq h \leq k$.

Bevis. Dette følger direkte fra teorem 1.4.24, siden $r(X)$ er lik rangen til matrisen som utgjøres av kolonnevektorene i paritetssjekkmatrisen for C med indekser i X. □

Legg merke til at vi her, som i teorem 1.4.24, også har likhet i uttrykket (2.1), fordi resonnementet for dette (proposisjon 1.4.25) kun bygger på aksiom (R2′) for rangfunksjonen r. Altså har vi

$$d_h(C) \quad = \quad \min\{|X| \,|\, |X| - r(X) = h\},$$

og dette vil vi snart gjøre bruk av.

2.3 Vekthierarki for matroider

Som korollar 2.2.4 viser, er de generaliserte Hammingvektene til en kode C gitt kun ved egenskaper til paritetssjekkmatroiden for C. Inspirert av dette vil vi definere generaliserte Hammingvekter for en generell matroide, slik det også er gjort i [L]. Vi innfører først parametrene $n = |S|$ og $k = n - r(M)$ for en matroide $M = (S,r)$ og kaller k **kretsrangen** til M, noe vi senere vil se årsaken til.

Definisjon 2.3.1. *La $M = (S,r)$ være en matroide, og la $X \subseteq S$. Den **h-te generaliserte Hammingvekten** til M er*

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

*for $1 \leq h \leq k$. **Vekthierarkiet** til M er mengden $\{d_h(M) \,|\, 1 \leq h \leq k\}$.*

Som vi bemerket i slutten av forrige kapittel, har vi også følgende:

$$d_h(M) \quad = \quad \min\{|X| \,|\, |X| - r(X) \geq h\}.$$

Spesielt gir definisjon 2.3.1 at

$$\begin{aligned} d_1(M) &= \min\{|X| \,|\, X \subseteq S,\, |X| - r(X) = 1\} \\ &= \min\{|X| \,|\, X \subseteq S \text{ er avhengig}\} \\ &= \min\{|X| \,|\, X \subseteq S \text{ er en krets}\}, \end{aligned}$$

altså er $d_1(M)$ vidden til M, og $d_1(M^*)$ er vidden til M^*, som igjen er kovidden til M.

Legg også merke til at isomorfe matroider har samme vekthierarki.

Bemerkning 2.3.2. *Siden vi generaliserer egenskaper til paritetssjekkmatrisen for en kode C, som er generatormatrisen for $C^\perp$, vil denne definisjonen egentlig være en generalisering av de generaliserte Hammingvektene for $C^\perp$, noe som kan føre til forvirrende notasjonsbruk. Hvis C er en kode med generatormatrise G, paritetssjekkmatrise H og paritetssjekkmatroide $M[H]$, har vi følgende sammenhenger:*

Lengden til C, parameteren n, er den samme for C og $C^\perp$, og dermed også for G og H. Altså vil lengden n tilsvare $|S|$, der S er grunnmengden til den tilsvarende matroiden, noe som er naturlig ut fra definisjonen av vektormatroide.

Redundansen r til C tilsvarer antall rader i H, altså dimensjonen til $C^\perp$. Siden radene i H utgjør en basis for $C^\perp$, og følgelig er lineært uavhengige, har vi

$$r \;=\; \dim(C^\perp) \;=\; \dim(\mathrm{col}(H)) \;=\; \mathrm{rg}(H) \;=\; r(M[H]).$$

Altså vil rangen $r(M)$ til en matroide tilsvare redundansen r til en kode, selv om det naturlige kanskje ville vært å tilknytte rangen til parameteren k, dimensjonen til koden.

Til slutt definerer vi kretsrangen k til å være $n - r(M)$, altså vil den tilsvare dimensjonen k til koden.

Vi har likevel valgt å gi definisjonen slik, blant annet fordi den er noe mer umiddelbar å forstå, i tillegg til at det, spesielt for grafer, er enklere å bestemme vekthierarkiet slik det nå er definert.

Sammenhengen mellom kode- og matroideteori er altså, for en kode C med generatormatroide $M[G]$ og paritetssjekkmatroide $M[H]$,

$$\begin{aligned}\{d_h(C) \,|\, 1 \le h \le k\} &= \{d_h(M[H]) \,|\, 1 \le h \le k\}, \text{ og} \\ \{d_h(C^\perp) \,|\, 1 \le h \le n-k\} &= \{d_h(M[G]) \,|\, 1 \le h \le n-k\}.\end{aligned}$$

Teorem 1.4.22, korollar 1.4.23 og teorem 1.4.26 gjelder også på matroidenivå:

Proposisjon 2.3.3. *For en matroide M har vi*

$$1 \;\le\; d_1(M) \;<\; d_2(M) \;<\; \cdots \;<\; d_k(M) \;\le\; n.$$

Bevis. La $M = (S, r)$ være en matroide. Fra definisjonen av generaliserte Hammingvekter for matroider, er det trivielt at $1 \le d_1(M) \le d_2(M) \le \cdots \le d_k(M) \le n$. Vi må derfor kun vise at ulikhetene er strenge. Anta, for å oppnå en selvmotsigelse, at $d_h = d_{h+1}$ for én $1 \le h \le k-1$. Anta at $X, Y \subseteq S$ er av minst kardinalitet slik at $|X| - r(X) = h$ og $|Y| - r(Y) = h + 1$. Da har vi $|X| = d_h = d_{h+1} = |Y|$, og dette gir oss også at $r(X) - 1 = r(Y)$. Mengdene X og Y er ikke-tomme, siden $d_i > 0$ for alle $1 \le i \le k$. For én $y \in Y$, la $Y_y = Y \setminus \{y\}$. Altså har vi $|Y_y| = |Y| - 1 = |X| - 1$. Egenskap (R2′) fra teorem 1.3.11 gir oss at

$$r(Y_y) \;\le\; r(Y_y \cup \{y\}) \;=\; r(Y).$$

Siden $r(Y) = r(X) - 1$, har vi $r(Y_y) \le r(X) - 1$. Dermed har vi følgende:

$$|Y_y| - r(Y_y) \;\ge\; (|X| - 1) - (r(X) - 1) \;=\; |X| - r(X) \;=\; h.$$

Som bemerket etter definisjon 2.3.1 har vi $d_h(M) = \min\{|X| \,|\, |X| - r(X) \ge h\}$, altså får vi $|Y_y| < |X| = d_h \le |Y_y|$, som er en selvmotsigelse. Resultatet følger. □

Generalisert Singletonbegrensning følger også her direkte fra forrige proposisjon, som det gjorde for koder:

Korollar 2.3.4. *For en matroide M har vi*

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

□

Proposisjon 2.3.5. *La M være en matroide. Da har vi*

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

Bevis. Se proposisjon 5.18 i [L]. □

Proposisjon 2.3.5 gir umiddelbart følgende sammenheng mellom kovidden og vekthierarkiet til en matroide M, siden kovidden til M er lik $d_1(M^*)$:

Korollar 2.3.6. *Følgende er ekvivalent, for en matroide M:*

i) Kovidden til M er a.

ii) $\{n + 2 - a, n + 3 - a, \ldots, n\} \subseteq \{d_h(M) \,|\, 1 \leq h \leq k\}$ *og* $n + 1 - a \notin \{d_h(M) \,|\, 1 \leq h \leq k\}$.

□

2.4 Vekthierarki for grafer

Siden matroider er en generalisering av grafer, kan vi også oversette begrepet om generaliserte Hammingvekter til grafer, noe vi vil gjøre nå. Videre oversetter vi resultatene i kapittel 2.3 til grafer, før vi beregner vekthierarkiet for de komplette og komplette bipartite grafene i et eget kapittel til slutt.

2.4.1 Definisjon og noen eksempler og resultater

For en graf $G = (V(G), E(G))$, innfører vi parametrene $n = n(G) = |E(G)|$, $r = r(G) = |E(T_G)|$ og $k = k(G) = n - r$, der T_G er en utspennende skog for G. Parameteren r kaller vi **rangen** til grafen. Legg merke til at dersom G er en graf med i komponenter, har vi $r = |V(T_G)| - i = |V(G)| - i$, altså har vi $r = |V(G)| - 1$ dersom G er sammenhengende. Vi ser også at parameteren k er kretsrangen til grafen, som vi definerte på side 3. Nå kan vi definere følgende:

Definisjon 2.4.1. *La $G = (V(G), E(G))$ være en graf og $X \subseteq E(G)$. Den **h-te generaliserte Hammingvekten** til G er*

$$d_h(G) \quad = \quad \min\{|X| \,|\, |X| - r(G|_X) = h\}$$

*for $1 \leq h \leq k$, der $G|_X$ er restriksjonen av G til X. Mengden $\{d_h(G) \,|\, 1 \leq h \leq k\}$ kalles **vekthierarkiet** til G.*

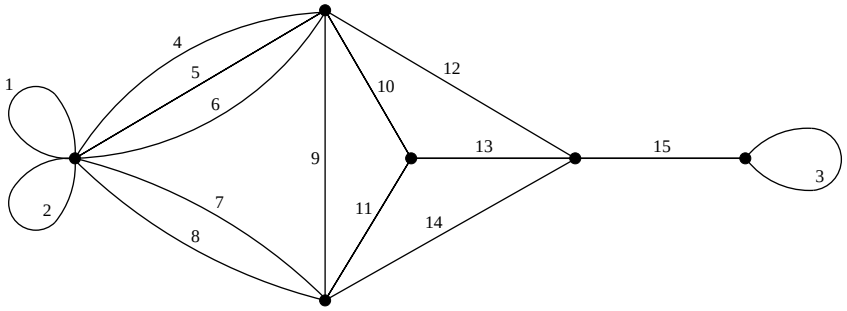
Som for matroider, har vi

$$d_1 \quad = \quad \min\{|X| \,|\, X \text{ er en krets}\},$$

altså er d_1 lik vidden til grafen, og for en planar graf G er $d_1(G^*)$ lik kovidden til G, der G^* er en geometrisk dual til G.

Legg merke til at isomorfe grafer har samme vekthierarki.

Dersom G er en planar graf med relativt liten n, er det som oftest lett å bestemme vekthierarkiet til G. Dette kan gjøres ved så å si å "bygge opp" grafen fra bunnen i en logisk rekkefølge og telle én ny vekt for hver ny krets som dannes, fordi rangen til grafen da ikke vil øke. Vi illustrerer dette med et eksempel:



Figur 2.1: Grafen G i eksempel 2.4.2.

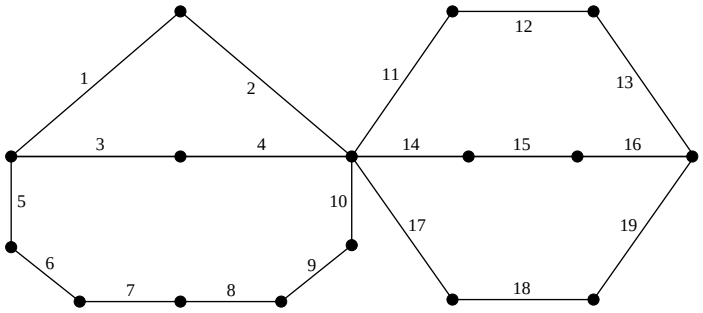
Eksempel 2.4.2. *La G være grafen på figur 2.1. Vi har $n = 15$, $r = |V(G)| - 1 = 5$ og $k = n - r = 10$, altså har G et vekthierarki av kardinalitet 10. Vi ser først at G har tre løkker, nemlig kantene 1−3, altså har vi $d_1 = 1$, $d_2 = 2$ og $d_3 = 3$. Videre er kantene 4−6 parallelle, og danner to nye kretser, derfor har vi $d_4 = 5$ og $d_5 = 6$. Kantene 7−8 er også parallelle, men siden de er færre enn kantene 4−6, teller vi dem etter disse. De danner én ny krets, og vi får $d_6 = 8$. Nå vil kant 9 danne en ny krets, altså får vi $d_7 = 9$. (Merk at kantene 7−9 kan legges i vilkårlig rekkefølge.) Nå vil neste kant øke rangen uansett hvilken vi velger, men legger vi først til kant 10 og så kant 11, vil kant 11 danne en krets, og vi får $d_8 = 11$. Til slutt legger vi til kantene 12−14 i vilkårlig rekkefølge, vi får $d_9 = 13$ og $d_{10} = 14$, og er ferdige. (Vi kunne også valgt en annen rekkefølge på kantene 10−14.) Kant 15 legges til til slutt, men får ingen betydning for vekthierarkiet, fordi ingen ny krets dannes.*

Totalt får vi altså at vekthierarkiet til G er $\{1, 2, 3, 5, 6, 8, 9, 11, 13, 14\}$.

Denne metoden vil likevel ikke alltid fungere, noe neste eksempel viser:

Eksempel 2.4.3. *La H være grafen på figur 2.2. Vi har $n = 19$, $r = |V(G)| - 1 = 15$ og $k = n - r = 4$, altså har G et vekthierarki av kardinalitet 4. Vi må ha $d_1 = 4$, siden kantene 1−4 danner en krets av lengde 4, og ingen andre kretser er mindre. Hvis vi "bygger videre" på kantene 1−4, må vi legge til minimum 6 kanter for å få en ny krets, altså totalt 10 kanter for å få to kretser. Likevel er $d_2 = 9$, ikke 10, siden de ni kantene 11−19 danner to kretser. Ellers ser vi lett at $d_3 = 13$ (kantene 1−4 og 11−19) og $d_4 = n = 19$, siden alle kantene er med i minst én krets. Vi får vekthierarkiet $\{4, 9, 13, 19\}$.*

Tidligere har vi vist at dersom $M(G)$ er kretsmatroiden til en graf G, har vi at $r(X) = r(G_X)$ for $X \subseteq E(G)$, siden $r(G|_X)$ er definert som antall kanter i en utspennende skog for



Figur 2.2: Grafen H i eksempel 2.4.3.

$G|_X$. Altså er definisjon 2.4.1 en direkte oversettelse av definisjon 2.3.1 til grafnivå, og vi får resultatet:

Korollar 2.4.4. *La $M(G)$ være kretsmatroiden til en graf G. Da har vi*

$$\{d_h(M(G)) \,|\, 1 \leq h \leq k\} \;=\; \{d_h(G) \,|\, 1 \leq h \leq k\}.$$

□

Fra dette kan vi overføre teorem 1.4.22, korollar 1.4.23 og teorem 1.4.26 også til grafer:

Korollar 2.4.5. *For en graf G har vi*

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

Bevis. La G være en graf, og la $M(G)$ være kretsmatroiden til G. Korollar 2.4.4 gir oss at

$$\{d_h(G) \,|\, 1 \leq h \leq k\} \;=\; \{d_h(M(G)) \,|\, 1 \leq h \leq k\},$$

og siden vi har

$$1 \;\leq\; d_1(M(G)) \;<\; d_2(M(G)) \;<\; \cdots \;<\; d_k(M(G)) \;\leq\; n$$

fra proposisjon 2.3.3, må vi derfor også ha

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

□

Nok en gang følger generalisert Singletonbegrensning direkte, som det gjorde for koder og matroider:

Korollar 2.4.6. *For en graf G har vi*

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

□

Korollar 2.4.7. *La G være en planar graf, og la G^* være en geometrisk dual til G. Da har vi*

$$\{d_h(G) \mid 1 \leq h \leq k\} \quad = \quad \{1, 2, \ldots, n\} \setminus \{n + 1 - d_h(G^*) \mid 1 \leq h \leq n - k\}.$$

Bevis. La G være en planar graf, og la G^* være en geometrisk dual til G. La videre $M(G)$ og $M^*(G)$ være henholdsvis kretsmatroiden og kokretsmatroiden til G. Proposisjon 1.3.14 gir oss at $M(G^*) \cong M^*(G)$, altså har vi

$$\{d_h(M(G^*)) \mid 1 \leq h \leq n - k\} \quad = \quad \{d_h(M^*(G)) \mid 1 \leq h \leq n - k\}.$$

Ved å kombinere dette med proposisjon 2.3.5 og korollar 2.4.4, får vi følgende likheter:

$$\begin{aligned} \{d_h(G) \mid 1 \leq h \leq k\} &= \{d_h(M(G)) \mid 1 \leq h \leq k\} \\ &= \{1, 2, \ldots, n\} \setminus \{n + 1 - d_h(M^*(G)) \mid 1 \leq h \leq n - k\} \\ &= \{1, 2, \ldots, n\} \setminus \{n + 1 - d_h(M(G^*)) \mid 1 \leq h \leq n - k\} \\ &= \{1, 2, \ldots, n\} \setminus \{n + 1 - d_h(G^*) \mid 1 \leq h \leq n - k\}. \end{aligned}$$

Resultatet følger. □

Legg merke til at vi for en vilkårlig, ikke nødvendigvis planar graf G, har

$$\{d_h(G) \mid 1 \leq h \leq k\} \quad = \quad \{1, 2, \ldots, n\} \setminus \{n + 1 - d_h(M^*(G)) \mid 1 \leq h \leq n - k\},$$

fra det forrige beviset.

Merk også at vekthierarkiet til en vilkårlig geometrisk dual til en planar graf G er entydig bestemt fra vekthierarkiet til G. Vi får derfor umiddelbart følgende resultat:

Korollar 2.4.8. *La G være en planar graf, og la G_1^* og G_2^* være geometriske dualer til G. Da har vi*

$$\{d_h(G_1^*) \mid 1 \leq h \leq n - k\} \quad = \quad \{d_h(G_2^*) \mid 1 \leq h \leq n - k\}.$$

□

Vi kan videre oversette korollar 2.3.6 til å gjelde også for grafer:

Korollar 2.4.9. *Følgende er ekvivalent, for en graf G:*

i) Kovidden til G er a.

ii) $\{n + 2 - a, n + 3 - a, \ldots, n\} \subseteq \{d_h(G) \mid 1 \leq h \leq k\}$ *og* $n + 1 - a \notin \{d_h(G) \mid 1 \leq h \leq k\}$.

Bevis. Som tidligere bemerket (etter proposisjon 1.3.15), er $i)$ ekvivalent med at kovidden til $M(G)$ er a, som ved korollar 2.3.6 igjen er ekvivalent med at $ii)$ gjelder for $M(G)$. Men fra korollar 2.4.4 har vi at $M(G)$ og G har samme vekthierarki, og resultatet følger. □

2.4.2 Vekthierarkiet for komplette og komplette bipartite grafer

De neste resultatene gir vekthierarkiet for generelle komplette og komplette bipartite grafer:

Proposisjon 2.4.10. *For $m \in \mathbb{N}$ har vi følgende:*

$$\{d_h(K_m) \,|\, 1 \leq h \leq k\} \;=\; \bigcup_{i=3}^{m} \left\{ \binom{i-1}{2} + 2, \binom{i-1}{2} + 3, \ldots, \binom{i}{2} \right\},$$

der $k = \binom{m-1}{2}$.

Proposisjon 2.4.11. *La $l, m \in \mathbb{N}$ slik at $l \geq m$. Da har vi*

$$\begin{aligned} \{d_h(K_{l,m}) \,|\, 1 \leq h \leq k\} \;=\; & \bigcup_{i=4}^{2m} \left\{ \left\lfloor \frac{(i-1)^2}{4} \right\rfloor + 2, \left\lfloor \frac{(i-1)^2}{4} \right\rfloor + 3, \ldots, \left\lfloor \frac{i^2}{4} \right\rfloor \right\} \\ & \cup \bigcup_{i=1}^{l-m} \{m^2 + (i-1)m + 2, m^2 + (i-1)m + 3, \ldots, m^2 + im\}, \end{aligned}$$

der $k = (l-1)(m-1)$.

Før vi kan gi bevis for disse to proposisjonene, trenger vi noen delresultater:

Lemma 2.4.12. *For en komplett eller komplett bipartit graf, må enhver delgraf som gir d_i for én $1 \leq i \leq k$ være sammenhengende.*

Bevis. Anta, for å oppnå en selvmotsigelse, at G er en delgraf av K_m som gir $d_i(K_m)$ for én $1 \leq i \leq k$, og G har j komponenter, for $j \geq 2$. Vi lar G ha parametrene n_G, r_G og $k_G\,(= i)$, og vi får $r_G = |V(G)| - j$. Vi velger så én vilkårlig kant fra hver komponent av G og identifiserer disse med hverandre. Vi kaller den nye grafen G' med nye parametre $n_{G'}$, $r_{G'}$ og $k_{G'}$. Da er G' sammenhengende, og vi har $r_{G'} = |V(G')| - 1$. Vi får $|V(G')| < |V(G)| \leq |V(K_m)|$ og $d_1(G') \geq 3$ (siden $d_1 \geq 3$ for hver komponent av G), altså er G' også en delgraf av K_m. I tillegg er det lett å se at vi får $n_{G'} = n_G - (j-1)$ og $|V(G')| = |V(G)| - 2(j-1)$. Totalt gir dette:

$$\begin{aligned} k_{G'} &= n_{G'} - r_{G'} \\ &= n_{G'} - |V(G')| + 1 \\ &= n_G - (j-1) - (|V(G)| - 2(j-1)) + 1 \\ &= n_G - |V(G)| + j \\ &= n_G - r_G \\ &= k_G \\ &= i. \end{aligned}$$

Dermed får vi $d_i(G') = n_{G'} < n_G = d_i(G) = d_i(K_m)$, som er en selvmotsigelse, og resultatet er bevist for K_m.

Et tilsvarende argument holder for $K_{l,m}$:

Anta, for nok en gang å oppnå en selvmotsigelse, at G er en delgraf av $K_{l,m}$ som gir $d_i(K_{l,m})$ for én $1 \leq i \leq k$, og G har j komponenter, for $j \geq 2$. Siden $K_{l,m}$ er bipartit, kan hjørnemengden deles i to deler, $V_1(K_{l,m})$ og $V_2(K_{l,m})$, slik at hver kant i $K_{l,m}$ forbinder et

hjørne i $V_1(K_{l,m})$ med et hjørne i $V_2(K_{l,m})$. Grafen G er en delgraf av $K_{l,m}$, altså kan også hjørnemengden til G deles i to deler, $V_1(G)$ og $V_2(G)$, og vi kan velge disse slik at vi har $V_1(G) \subseteq V_1(K_{l,m})$ og $V_2(G) \subseteq V_2(K_{l,m})$. Vi lar G ha parametrene n_G, r_G og $k_G\,(= i)$, og vi får $r_G = |V(G)| - j$. Også i dette tilfellet velger vi én vilkårlig kant fra hver komponent av G og identifiserer disse med hverandre, men slik at hjørner i $V_1(G)$ identifiseres med hverandre, og tilsvarende for hjørner i $V_2(G)$. Vi kaller den nye grafen G', med nye parametre $n_{G'}$, $r_{G'}$, $k_{G'}$, $V_1(G')$ og $V_2(G')$. Da er G' bipartit, med $V_1(G') \subset V_1(G) \subseteq V_1(K_{l,m})$ og $V_2(G') \subset V_2(G) \subseteq V_2(K_{l,m})$, altså er G' også en delgraf av $K_{l,m}$. Vi får de samme uttrykkene for $r_{G'}$, $n_{G'}$ og $|V(G')|$ som i første del av beviset, dermed får vi også samme selvmotsigelse. □

Vi merker oss at forrige lemma ikke gjelder for vilkårlige grafer; for eksempel er d_3 i grafen på figur 2.1 gitt ved restriksjonen av denne til kantene 1−3, som ikke er sammenhengende.

Lemma 2.4.13. *For $l, m \in \mathbb{N}$ med $l \geq m$ har vi:*

i) Kovidden til K_m er $m - 1$.

ii) Kovidden til $K_{l,m}$ er m.

Bevis. i) La A_x være en kokrets i K_m som deler $V(K_m)$ i to deler av kardinalitet henholdsvis x og $m - x$ for $x \in \mathbb{N}$ slik at $1 \leq x \leq m - 1$. Da er mengden av alle isomorfiklasser av kokretser i K_m inneholdt i mengden $\{A_x \,|\, 1 \leq x \leq m - 1\}$. Vi definerer $f(x) = x(m - x)$, altså har vi $f(x) = |A_x|$ for alle $1 \leq x \leq m - 1$ slik at $x \in \mathbb{N}$, og det er derfor nok å vise at minimumsverdien til f er $m - 1$ (se bemerkning 2.4.14).

Vi har $f'(x) = -2x + m$, og $f'(x) = 0$ gir eneste stasjonære punkt $x_0 = \frac{m}{2}$. Men siden $f''(x_0) = -2 < 0$, er x_0 et maksimumspunkt, og siden f ikke har singulære punkt, vil derfor minimumsverdien til f være i (et av) endepunktene i intervallet, altså $x \in \{1, m - 1\} \subseteq \mathbb{N}$. Vi har $f(1) = f(m - 1) = m - 1$, og resultatet følger.

ii) Som vanlig deler vi hjørnemengden til $K_{l,m}$ i to deler, V_1 og V_2, med $|V_1| = l$ og $|V_2| = m$. La $A_{x,y}$ være en kokrets i $K_{l,m}$ som deler V_1 i to deler av kardinalitet henholdsvis x og $l - x$ for $0 \leq x \leq l$, og som deler V_2 i to deler av kardinalitet henholdsvis y og $m - y$ for $0 \leq y \leq m$ (slik at $K_{l,m} \setminus A \cong K_{x,y} \cup K_{l-x,m-y}$). Da er mengden av alle isomorfiklasser av kokretser i $K_{l,m}$ inneholdt i mengden $\{A_{x,y} \,|\, 0 \leq x \leq l,\, 0 \leq y \leq m\}$. Vi definerer $f(x, y) = x(m-y)+y(l-x)$, altså har vi $f(x, y) = |A_{x,y}|$ for alle par (x, y) som gir at $A_{x,y}$ er en kokrets.

Anta først at vi har $x \in \{0, l\}$ og/eller $y \in \{0, m\}$. Da er det kun fire par (x, y) som gir kokretser, nemlig $(x, y) \in \{(1, 0), (0, 1), (l-1, m), (l, m-1)\}$. Vi har $f(1, 0) = f(l-1, m) = m$ og $f(0, 1) = f(l, m - 1) = l \geq m$.

La så $M = \{(x, y) \,|\, 1 \leq x \leq l - 1,\, 1 \leq y \leq m - 1\} \subseteq \mathbb{R}^2$ (vi må ha $l, m \geq 2$, for ellers får vi $M = \emptyset$). Det er nå nok å vise at vi for alle $(x, y) \in M$ har $f(x, y) \geq m$ (se bemerkning 2.4.14 igjen).

Vi har $\frac{\delta f}{\delta x} = m - 2y$ og $\frac{\delta f}{\delta y} = l - 2x$, og $\frac{\delta f}{\delta x} = \frac{\delta f}{\delta y} = 0$ gir eneste stasjonære punkt $(x_0, y_0) = (\frac{l}{2}, \frac{m}{2})$. Men $\frac{\delta^2 f}{\delta x^2} = \frac{\delta^2 f}{\delta y^2} = 0$ og $\frac{\delta^2 f}{\delta x \delta y} = -2$ gir at $\frac{\delta^2 f}{\delta x^2}(x_0, y_0) \cdot \frac{\delta^2 f}{\delta y^2}(x_0, y_0) - \big(\frac{\delta^2 f}{\delta x \delta y}(x_0, y_0)\big)^2 = -4 < 0$, altså er (x_0, y_0) et sadelpunkt. Siden f ikke har singulære punkt, vil derfor minimumsverdien til f være langs randen av området M, altså i punkter i M på formen $(x, y) \in \{(x, 1), (l - 1, y), (1, y), (x, m - 1)\}$. Innsatt i funksjonen f gir dette følgende:

$$f(x, 1) \;=\; x(m - 1) + (l - x) \;=\; l + (m - 2)x \;\geq\; l + m - 2,$$

$$f(l - 1, y) \;=\; (l - 1)(m - y) + y \;=\; lm - m - (l - 2)y \;\geq\; l + m - 2,$$

$$f(1,y) \;=\; (m-y)+y(l-1) \;=\; m+(l-2)y \;\geq\; l+m-2, \text{ og}$$
$$f(x,m-1) \;=\; x+(m-1)(l-x) \;=\; lm-l-(m-2)x \;\geq\; l+m-2.$$

Minimumsverdien $f(x,y) = l+m-2$ oppnås i punktene $(x,y) \in \{(1,1),(l-1,m-1)\} \subseteq \mathbb{N}^2$, og vi har $l+m-2 \geq m$ for alle $l \geq m \geq 2$, altså følger resultatet. □

Bemerkning 2.4.14. *I forrige bevis behandler vi funksjonene $f(x)$ og $f(x,y)$ som funksjoner over $\mathbb{R}$, selv om de kun er definert over $\mathbb{N}$. Dette er likevel ikke problematisk, siden vi i begge tilfeller finner at x- og y-verdiene som gir funksjonenes minimumsverdier er heltall.*

Nå er vi klare til å vise proposisjon 2.4.10:

Bevis. Vi har $n = \sum_{i=1}^{m-1} i = \binom{m}{2}$ og $r = |V(K_m)| - 1 = m-1$, altså får vi $k = n-r = \sum_{i=1}^{m-1} i - (m-1) = \sum_{i=1}^{m-2} i = \binom{m-1}{2}$.

Vi vil først gi en fremgangsmåte som gir vekthierarkiet vi ønsker vise, for deretter å vise at det ikke er mulig å oppnå et "bedre" resultat enn dette.

Gitt grafen K_m, starter vi med en vilkårlig K_2-delgraf, og legger til ett og ett hjørne sammen med alle kanter (i vilkårlig rekkefølge) som forbinder det nye hjørnet med et hjørne som allerede er lagt til. For hvert nytt hjørne vil kun den første kanten som legges til, øke rangen til grafen, altså er det bare denne som ikke gir en ny vekt. For $3 \leq i \leq m$, vil da kantene som legges til sammen med hjørne i, gi vektene $\left\{\binom{i-1}{2}+2, \binom{i-1}{2}+3, \ldots, \binom{i}{2}\right\}$, siden vi for K_i har $n = \binom{i}{2}$. Totalt gir dette vekthierarkiet

$$\{d_h' \mid 1 \leq h \leq k\} \;=\; \bigcup_{i=3}^{m} \left\{ \binom{i-1}{2}+2, \binom{i-1}{2}+3, \ldots, \binom{i}{2} \right\},$$

der $k = \binom{m-1}{2}$, altså det ønskede resultatet. Fra dette får vi derfor følgende ulikhet for $1 \leq h \leq k$:

$$d_h(K_m) \;\leq\; d_h'. \tag{2.2}$$

I det følgende viser vi motsatte ulikhet, noe som vil fullføre beviset.

Først merker vi oss at vi for $3 \leq i \leq m$ har

$$\left\{ {d_{\binom{i-2}{2}+1}}', {d_{\binom{i-2}{2}+2}}', \ldots, {d_{\binom{i-1}{2}}}' \right\} \;=\; \left\{ \binom{i-1}{2}+2, \binom{i-1}{2}+3, \ldots, \binom{i}{2} \right\},$$

dersom vi definerer $\binom{1}{2} = 0$. Ved korollar 2.4.5 er det derfor nok å vise følgende ulikhet for $3 \leq i \leq m$:

$$d_{\binom{i-2}{2}+1}(K_m) \;\geq\; {d_{\binom{i-2}{2}+1}}'. \tag{2.3}$$

Dette viser vi ved hjelp av induksjon på m:

Trivielt holder det for $m = 3$, siden vekthierarkiet til K_3 er $\{3\}$.

Anta så at uttrykket (2.3) er riktig for alle $3 \leq j \leq m-1$, altså at vi for disse verdiene av j har

$$d_{\binom{i-2}{2}+1}(K_j) \;\geq\; {d_{\binom{i-2}{2}+1}}'$$

for $3 \leq i \leq j$. Vi vil vise at dette medfører at uttrykket (2.3) også gjelder for $j = m$:

La derfor $j = m$. Først viser vi at uttrykket (2.3) gjelder for $3 \leq i \leq j-1$. La G_i være delgrafen (eller én av delgrafene) som gir $d_{\binom{i-2}{2}+1}(K_j)$, for $3 \leq i \leq j-1$. For hver G_i har vi derfor $k = \binom{i-2}{2} + 1$, og uttrykket (2.2) gir $n \leq \binom{i-1}{2} + 2$. I tillegg gir lemma 2.4.12 at G_i er sammenhengende for hver i, altså får vi $|V(G_i)| = r + 1$. Totalt får vi

$$|V(G_i)| \;=\; r+1 \;=\; n-k+1 \;\leq\; \left(\binom{i-1}{2}+2\right) - \left(\binom{i-2}{2}+1\right)+1 \;=\; i.$$

Men siden G_i er en delgraf av K_j med maksimalt i hjørner, er også G_i en delgraf av K_i. Fra induksjonshypotesen får vi derfor

$$d_{\binom{i-2}{2}+1}(K_j) \;=\; d_{\binom{i-2}{2}+1}(G_i) \;\geq\; d_{\binom{i-2}{2}+1}(K_i) \;\geq\; d_{\binom{i-2}{2}+1}{}',$$

for $3 \leq i \leq j-1$.

Da gjenstår det bare å vise at vi har $d_{\binom{j-2}{2}+1}(K_j) \geq d_{\binom{j-2}{2}+1}{}'$. Men fra lemma 2.4.13 har vi at kovidden til K_j er lik $j-1$, som fra korollar 2.4.9 er det samme som at de $j-2$ siste vektene til K_j er $\{\binom{j-1}{2}+2, \binom{j-1}{2}+3, \ldots \binom{j}{2}\}$. Og den $(j-2)$-te siste vekten i vekthierarkiet til K_j er $d_{\binom{j-2}{2}+1}$, derfor får vi:

$$d_{\binom{j-2}{2}+1}(K_j) \;=\; \binom{j-1}{2}+2 \;=\; d_{\binom{j-2}{2}+1}{}'.$$

Dette fullfører beviset. □

Før vi gir beviset for proposisjon 2.4.11, tar vi med et rent summeringsresultat som vi får bruk for, både i dette beviset og senere i oppgaven:

Lemma 2.4.15.

$$\sum_{i=1}^{n} \left\lfloor \frac{i}{2} \right\rfloor \;=\; \left\lfloor \frac{n^2}{4} \right\rfloor.$$

Bevis. Vi viser dette ved induksjon på n:

Vi har trivielt $\sum_{i=1}^{1} \lfloor \frac{i}{2} \rfloor = 0 = \lfloor \frac{1^2}{4} \rfloor$ og $\sum_{i=1}^{2} \lfloor \frac{i}{2} \rfloor = 0 + 1 = \lfloor \frac{2^2}{4} \rfloor$, altså gjelder resultatet for $n = 1$ og $n = 2$.

Anta så at resultatet holder for $j = n$. Vi vil vise at dette medfører at resultatet også holder for $j + 2$, og vi ser at venstresiden av uttrykket da vil øke med

$$\left\lfloor \tfrac{j+1}{2} \right\rfloor + \left\lfloor \tfrac{j+2}{2} \right\rfloor \;=\; \tfrac{j+1}{2} + \tfrac{j+2}{2} - \tfrac{1}{2} \;=\; j+1.$$

På høyresiden får vi

$$\left\lfloor \tfrac{(j+2)^2}{4} \right\rfloor - \left\lfloor \tfrac{j^2}{4} \right\rfloor \;=\; \left\lfloor \tfrac{j^2}{4} + \tfrac{4j}{4} + \tfrac{4}{4} \right\rfloor - \left\lfloor \tfrac{j^2}{4} \right\rfloor \;=\; j+1,$$

altså øker begge sider like mye, og resultatet er vist. □

Bemerkning 2.4.16. *Ved direkte utregning er det lett å sjekke at vi for n odde får*

$$\sum_{i=1}^{n} \left\lfloor \frac{i}{2} \right\rfloor \;=\; \frac{n^2}{4} - \frac{1}{4},$$

mens vi for n jevn får

$$\sum_{i=1}^{n} \left\lfloor \frac{i}{2} \right\rfloor \;=\; \frac{n^2}{4}.$$

Da har vi alt vi trenger for å vise proposisjon 2.4.11:

Bevis. Vi har $n = lm$ og $r = |V(K_{l,m})| - 1 = l + m - 1$, dermed får vi $k = n - r = lm - (l + m - 1) = (l - 1)(m - 1)$.

Beviset følger omtrent samme metode som i beviset for proposisjon 2.4.10, og også her vil vi først gi en fremgangsmåte som gir vekthierarkiet vi ønsker vise, for deretter å vise at det ikke er mulig å oppnå "bedre" resultat enn dette.

Gitt grafen $K_{l,m}$, med $l \geq m$ og hjørnemengder V_1 og V_2, der vi lar $|V_1| = l$ og $|V_2| = m$. Vi starter med en vilkårlig $K_{1,1}$-delgraf og legger til ett og ett hjørne sammen med alle kanter (i vilkårlig rekkefølge) som forbinder det nye hjørnet med et hjørne som allerede er lagt til, og vi velger hjørnene annenhver gang fra V_1 og V_2. Når det ikke er flere hjørner å legge til fra V_2, fortsetter vi med hjørner i V_1 i vilkårlig rekkefølge til vi ender opp med $K_{l,m}$. For hvert nytt hjørne vil kun den første kanten som legges til øke rangen til grafen, altså er det bare denne som ikke gir en ny vekt. I tillegg er antall kanter som legges til for hvert hjørne i én hjørnemengde, lik antall hjørner som allerede er lagt til i den motsatte hjørnemengden. For $4 \leq i \leq 2m$, vil da kantene som legges til sammen med hjørne i, gi vektene $\{\sum_{j=1}^{i-1} \lfloor \frac{j}{2} \rfloor + 2, \sum_{j=1}^{i-1} \lfloor \frac{j}{2} \rfloor + 3, \ldots, \sum_{j=1}^{i} \lfloor \frac{j}{2} \rfloor\}$, siden vi med hjørne i ender opp med delgrafen $K_{\lceil \frac{i}{2} \rceil, \lfloor \frac{i}{2} \rfloor}$, med $\lfloor \frac{i}{2} \rfloor$ nye kanter. Fra lemma 2.4.15 er dette igjen lik $\{\lfloor \frac{(i-1)^2}{4} \rfloor + 2, \lfloor \frac{(i-1)^2}{4} \rfloor + 3, \ldots, \lfloor \frac{i^2}{4} \rfloor\}$. I tillegg får vi, for $1 \leq i \leq l - m$, vektene $\{m^2 + 2 + m(i-1), m^2 + 3 + m(i-1), \ldots, m^2 + mi\}$ når vi legger til hjørne $2m + i$. Totalt gir dette det ønskede vekthierarkiet for $K_{l,m}$.

Altså får vi igjen, som i beviset for proposisjon 2.4.10, følgende ulikhet for $1 \leq h \leq k$:

$$d_h(K_{l,m}) \quad \leq \quad {d_h}'. \tag{2.4}$$

Vi vil derfor i det følgende vise motsatte ulikhet, som vil fullføre beviset.

Først merker vi oss at vi for $4 \leq i \leq 2m$ har

$$\left\{ {d_{\lfloor \frac{(i-3)^2}{4} \rfloor + 1}}', {d_{\lfloor \frac{(i-3)^2}{4} \rfloor + 2}}', \ldots, {d_{\lfloor \frac{(i-2)^2}{4} \rfloor}}' \right\} \quad = \quad \left\{ \left\lfloor \frac{(i-1)^2}{4} \right\rfloor + 2, \left\lfloor \frac{(i-1)^2}{4} \right\rfloor + 3, \ldots, \left\lfloor \frac{i^2}{4} \right\rfloor \right\},$$

og for $1 \leq i \leq l - m$ har vi

$$\left\{ {d_{(m-1)^2 + (i-1)(m-1) + 1}}', {d_{(m-1)^2 + (i-1)(m-1) + 2}}', \ldots, {d_{(m-1)^2 + i(m-1)}}' \right\}$$

$$= \quad \{m^2 + (i-1)m + 2, m^2 + (i-1)m + 3, \ldots, m^2 + im\}.$$

Ved korollar 2.4.5 er det derfor nok å vise følgende ulikheter:

$$d_{\lfloor \frac{(i-3)^2}{4} \rfloor + 1}(K_{l,m}) \quad \geq \quad {d_{\lfloor \frac{(i-3)^2}{4} \rfloor + 1}}' \tag{2.5}$$

for $4 \leq i \leq 2m$ og

$$d_{(m-1)^2 + (i-1)(m-1) + 1}(K_{l,m}) \quad \geq \quad {d_{(m-1)^2 + (i-1)(m-1) + 1}}' \tag{2.6}$$

for $1 \leq i \leq l - m$. Av notasjonsmessige hensyn vil vi istedenfor uttrykket (2.6) heller vise følgende uttrykk, som er det samme uttrykket dersom vi lar i variere mellom $2m + 1$ og $l + m$ i stedet:

$$d_{(m-1)^2 + (i-2m-1)(m-1) + 1}(K_{l,m}) \quad \geq \quad {d_{(m-1)^2 + (i-2m-1)(m-1) + 1}}'. \tag{2.7}$$

(Vi har $d_{(m-1)^2+(i-2m-1)(m-1)+1}{}' = (i-1)m - m^2 + 2$.)

Dette viser vi ved hjelp av induksjon på $l+m$:

Trivielt holder det for $l+m=4$, siden vekthierarkiet til $K_{3,1}$ er $\emptyset$, og vekthierarkiet til $K_{2,2}$ er $\{4\}$.

Anta så at uttrykkene (2.5) og (2.7) er riktig for alle l' og m' der $j = l'+m'$ og $4 \leq j \leq l+m-1$, altså at (2.5) gjelder for alle $4 \leq j \leq \min\{2m, l+m-1\}$ og (2.7) gjelder for alle $4 \leq j \leq l+m-1$. Vi vil vise at dette medfører at uttrykkene også gjelder for $j = l+m$:

La derfor $j = l+m$. Først viser vi at uttrykkene gjelder for $4 \leq i \leq j-1$. La G_i være delgrafen (eller én av delgrafene) som gir $d_{\lfloor\frac{(i-3)^2}{4}\rfloor+1}(K_{l,m})$ for $4 \leq i \leq \min\{2m, l+m-1\}$ og $d_{(m-1)^2+(i-2m-1)(m-1)+1}(K_{l,m})$ for $2m+1 \leq i \leq l+m-1$.

For hver G_i med $4 \leq i \leq \min\{2m, l+m-1\}$ har vi da $k = \lfloor\frac{(i-3)^2}{4}\rfloor + 1$, og uttrykket (2.4) gir $n \leq \lfloor\frac{(i-1)^2}{4}\rfloor + 2$. Fra lemma 2.4.15 får vi derfor $k = \sum_{i'=1}^{i-3} \lfloor\frac{i'}{2}\rfloor + 1$ og $n \leq \sum_{i'=1}^{i-1} \lfloor\frac{i'}{2}\rfloor + 2$. I tillegg gir lemma 2.4.12 at G_i er sammenhengende for hver i, altså får vi $|V(G_i)| = r+1$. Totalt får vi

$$\begin{aligned}
|V(G_i)| &= r+1 \\
&= n-k+1 \\
&\leq \left(\sum_{i'=1}^{i-1} \left\lfloor\frac{i'}{2}\right\rfloor + 2\right) - \left(\sum_{i'=1}^{i-3} \left\lfloor\frac{i'}{2}\right\rfloor + 1\right) + 1 \\
&= \left\lfloor\frac{i-2}{2}\right\rfloor + \left\lfloor\frac{i-1}{2}\right\rfloor + 2 \\
&= i.
\end{aligned}$$

La så $2m+1 \leq i \leq l+m-1$. For hver G_i har vi da $k = (m-1)^2 + (i-2m-1)(m-1) + 1$, og uttrykket (2.4) gir $n \leq (i-1)m - m^2 + 2$. Lemma 2.4.12 gjelder også nå, altså er G_i sammenhengende, og vi har $|V(G_i)| = r+1$ også her. Totalt gir dette

$$\begin{aligned}
|V(G_i)| &= r+1 \\
&= n-k+1 \\
&\leq \big((i-1)m - m^2 + 2\big) - \big((m-1)^2 + (i-2m-1)(m-1) + 1\big) + 1 \\
&= i.
\end{aligned}$$

Altså har vi i begge tilfeller at $|V(G_i)| \leq i \leq l+m-1$, altså er hver G_i delgraf av $K_{l-1,m}$ eller $K_{l,m-1}$, og vi kan bruke induksjonshypotesen. Vi merker oss først at siden $l \geq m$, har vi

$$d_h(K_{l-1,m}) \leq d_h(K_{l,m-1}),$$

for alle $1 \leq h \leq k(K_{l,m-1})$ (Her bruker vi $k(K_{l,m-1})$, fordi $k(K_{l-1,m}) \geq k(K_{l,m-1})$ når $l \geq m$). Dette, kombinert med induksjonshypotesen, gir

$$\begin{aligned}
d_{\lfloor\frac{(i-3)^2}{4}\rfloor+1}(K_{l,m}) &= d_{\lfloor\frac{(i-3)^2}{4}\rfloor+1}(G_i) \\
&\geq d_{\lfloor\frac{(i-3)^2}{4}\rfloor+1}(K_{l-1,m}) \\
&\geq d_{\lfloor\frac{(i-3)^2}{4}\rfloor+1}{}' \qquad (2.8)
\end{aligned}$$

for $4 \leq i \leq \min\{2m, l+m-1\}$, og

$$\begin{aligned} d_{(m-1)^2+(i-2m-1)(m-1)+1}(K_{l,m}) &= d_{(m-1)^2+(i-2m-1)(m-1)+1}(G_i) \\ &\geq d_{(m-1)^2+(i-2m-1)(m-1)+1}(K_{l-1,m}) \\ &\geq d_{(m-1)^2+(i-2m-1)(m-1)+1}{}' \end{aligned} \tag{2.9}$$

for $2m+1 \leq i \leq l+m-1$.

Uttrykkene (2.8) og (2.9) gir oss det vi ønsket for alle $1 \leq i \leq j-1$, så nå gjenstår bare tilfellet $i = j$, altså å vise $d_{(l-2)(m-1)+1}(K_{l,m}) \geq d_{(l-2)(m-1)+1}{}'$. (Uttrykket $(l-2)(m-1)+1$ er $(m-1)^2+(i-2m-1)(m-1)+1$, innsatt $i = l-m$. Dersom $l = m$, er det egentlig uttrykket $\lfloor \frac{(i-3)^2}{4} \rfloor + 1$, innsatt $i = 2m$, vi skal vise dette for, men når $l = m$ er det lett å sjekke at disse uttrykkene er like.)

Fra lemma 2.4.13 har vi at kovidden til $K_{l,m}$ er lik m, som fra korollar 2.4.9 er det samme som at de $m-1$ siste vektene til $K_{l,m}$ er $\{(l-1)m+2, (l-1)m+3, \ldots lm\}$. Og den m-te siste vekten i vekthierarkiet til $K_{l,m}$ er $d_{(l-2)(m-1)+1}$, derfor får vi:

$$d_{(l-2)(m-1)+1}(K_j) = (l-1)m+2 = d_{(l-2)(m-1)+1}{}'.$$

Dette fullfører beviset. □

Eksempel 2.4.17. *Vekthierarkiene til grafene K_5 og $K_{3,3}$ (se figur 1.1) er*

$$\begin{aligned} \{d_h(K_5) | 1 \leq h \leq 6\} &= \{3,5,6,8,9,10\}, \text{ og} \\ \{d_h(K_{3,3}) | 1 \leq h \leq 4\} &= \{4,6,8,9\}. \end{aligned}$$

2.5 MDS-egenskaper for matroider og grafer

I kapitlene 2.3 og 2.4 definerte vi parametrene n og k, samt vekthierarkiet, både for matroider og grafer. Siden MDS-egenskapene for koder kun avhenger av disse, er det naturlig å overføre definisjonene og resultatene i kapittel 2.1 til matroider og grafer, noe vi vil gjøre i kapittel 2.5.1. Videre klassifiserer vi MDS-matroidene og de sammenhengende MDS-, nær-MDS-, nesten-MDS- og 2-MDS-grafene henholdsvis i kapitlene 2.5.2 og 2.5.3, før vi i kapittel 2.5.4 bruker resultatene fra kapittel 2.5.3 til å si noe om hvor mange slike grafer som eksisterer for en gitt n.

2.5.1 Definisjoner og noen resultater

Definisjon 2.5.1. ***Singletondefekten*** *til en matroide M er $S(M) = n-k+1-d_1$.*

Definisjon 2.5.2.

i) En matroide er ***MDS*** *dersom $d_1 = n-k+1$.*
ii) En matroide M er ***nesten-MDS*** *dersom $S(M) = 1$.*
iii) En matroide M er ***nær-MDS*** *dersom $S(M) = S(M^*) = 1$.*
iv) En matroide er ***t-MDS*** *dersom t er det minste tallet slik at $d_t = n-k+t$.*

Definisjon 2.5.3. *En graf G er* ***MDS*** *(henholdsvis* ***nesten-MDS***, ***nær-MDS*** *eller* ***t-MDS****) dersom $M(G)$ er MDS (henholdsvis nesten-MDS, nær-MDS eller t-MDS).*

Årsaken til å definere MDS-egenskapene til en graf ved hjelp av kretsmatroiden og ikke direkte, slik som i definisjon 2.5.2, er at dualitetsbegrepet for grafer kun gjelder for planare grafer. Dermed ville definisjonen av en nær-MDS-graf ikke gjelde for vilkårlige grafer. (Vi skal senere se, i korollar 2.5.27, at det ikke eksisterer ikke-planare nær-MDS-grafer.)

Definisjonene 2.5.1 og 2.5.2 *i*), *ii*) og *iv*) kan likevel benyttes også for grafer, siden G og $M(G)$ har samme parametre n og k og samme vekthierarki. I tillegg kan vi bruke definisjon 2.5.2 *iii*) for planare grafer, siden matroide- og grafdualitet korresponderer, og alle geometriske dualer til en planar graf har samme vekthierarki (korollar 2.4.8). Vi oppsummerer dette i følgende korollar:

Korollar 2.5.4. ***Singletondefekten*** *til en graf G er $S(G) = n - k + 1 - d_1$, og vi har*

$$\begin{aligned} G \text{ er MDS} &\Leftrightarrow d_1 = n - k + 1, \\ G \text{ er nesten-MDS} &\Leftrightarrow S(G) = 1, \text{ og} \\ G \text{ er } t\text{-MDS} &\Leftrightarrow t \text{ er det minste tallet slik at } d_t = n - k + t. \end{aligned}$$

Dersom G i tillegg er planar, har vi

$$G \text{ er nær-MDS} \Leftrightarrow S(G) = S(G^*) = 1,$$

der G^* er en geometrisk dual til G.

□

Som for koder, bruker vi følgende konvensjoner: Frie matroider og grafer som er skoger er MDS, mens matroider og grafer med $d_k < n$ er t-MDS dersom $t = k + 1$.

Merk at vi for en sammenhengende graf G har $|V(G)| = r + 1 = n - k + 1$, altså har vi at Singletondefekten i dette tilfellet er $S(G) = |V(G)| - d_1(G)$.

Fra korollar 2.3.6 og 2.4.9 får vi umiddelbart følgende sammenhenger mellom begrepene t-MDS og kovidde:

Korollar 2.5.5. *Vi har følgende for en matroide M og graf G:*

$$\begin{aligned} \text{Kovidden til } M \text{ er } k - t + 2 &\Leftrightarrow M \text{ er } t\text{-MDS, og} \\ \text{Kovidden til } G \text{ er } k - t + 2 &\Leftrightarrow G \text{ er } t\text{-MDS.} \end{aligned}$$

□

Eksempel 2.5.6. *Fra lemma 2.4.13 er kovidden til K_m lik $m-1$, mens kovidden til $K_{l,m}$ er m når $l \geq m$. Dermed gir korollar 2.5.5 oss at K_m er t_1-MDS og $K_{l,m}$ er t_2-MDS for*

$$\begin{aligned} t_1 &= k(K_m) - m + 3 \\ &= \left(\sum_{i=1}^{m-2} i \right) - m + 3 \\ &= \left(\sum_{i=1}^{m-3} i \right) + 1 \\ &= \binom{m-2}{2} + 1, \text{ og} \\ t_2 &= k(K_{l,m}) - m + 2 \\ &= (l-1)(m-1) - m + 2 \\ &= lm - l - 2m + 3. \end{aligned}$$

I tillegg har vi, for $m \geq 3$, $d_1(K_m) = 3$ *og, for* $l \geq m \geq 2$, $d_1(K_{l,m}) = 4$. *Dette gir*

$$\begin{aligned} S(K_m) &= n(K_m) - k(K_m) + 1 - d_1(K_m) \\ &= |V(K_m)| - d_1(K_m) \\ &= m - 3, \text{ og} \\ S(K_{l,m}) &= n(K_{l,m}) - k(K_{l,m}) + 1 - d_1(K_{l,m}) \\ &= |V(K_{l,m})| - d_1(K_{l,m}) \\ &= l + m - 4, \end{aligned}$$

siden K_m *og* $K_{l,m}$ *er sammenhengende.*

Spesielt har vi at K_5 *er* 4*-MDS,* $K_{3,3}$ *er* 3*-MDS,* $S(K_5) = 2$ *og* $S(K_{3,3}) = 2$ *(se figur* 1.1*), noe som stemmer bra med vekthierarkiene gitt i eksempel* 2.4.17.

Vi har følgende sammenheng mellom MDS-begrepene for matroider og grafer:

Korollar 2.5.7. *Følgende er ekvivalent:*

i) M *er en grafisk MDS-matroide.*

ii) $M \cong M(G)$ *for en sammenhengende MDS-graf* G.

iii) $M = M(G)$ *for en sammenhengende MDS-graf* G.

Videre har M *og* G *samme vekthierarki i dette tilfellet.*

Bevis. Definisjonen av grafisk matroide, kombinert med proposisjon 1.3.19, gir oss at

$$M \text{ er en grafisk matroide} \quad \Leftrightarrow \quad M \cong M(G) \text{ for en sammenhengende graf } G,$$

og som nevnt like etter proposisjon 1.3.19 kan vi også kan erstatte isomorfien her med likhet. Dermed følger resultatet fra definisjonene av MDS-matroider og -grafer. □

Vi merker oss at korollar 2.5.7 også gjelder for alle andre MDS-egenskaper vi har definert.

Siden beviset for teorem 2.1.12 kun bygger på teoremene 1.4.22 og 1.4.26, og disse også gjelder for matroider og planare grafer (proposisjonene 2.3.3 og 2.3.5 og korollarene 2.4.5 og 2.4.7), kan samme argument brukes til å bevise teorem 2.1.12 for disse. For helhetens skyld gir vi resultatene, med påfølgende korollar, som tilsvarer proposisjon 2.1.8 og korollarene 2.1.13 og 2.1.14:

Korollar 2.5.8. *For en matroide* M *har vi:*

$$\textit{Singletondefekten } S(M) = t - 1 \quad \Leftrightarrow \quad M^* \textit{ er } t\textit{-MDS.}$$

□

Korollar 2.5.9. *La* G *være en planar graf, og la* G^* *være en geometrisk dual til* G. *Da har vi:*

$$\textit{Singletondefekten } S(G) = t - 1 \quad \Leftrightarrow \quad G^* \textit{ er } t\textit{-MDS.}$$

□

Vi har $(M^*)^* = M$, og fra korollar 2.4.7 følger det at $(G^*)^*$ og G har samme vekthierarki. På samme måte som for koder, gjelder derfor også de motsatte resultatene:

$$\begin{aligned} M \text{ er } t\text{-MDS} &\Leftrightarrow S(M^*) = t-1, \\ G \text{ er } t\text{-MDS} &\Leftrightarrow S(G^*) = t-1. \end{aligned}$$

Korollar 2.5.10. *For en matroide M har vi:*

$$M \text{ er MDS} \Leftrightarrow M^* \text{ er MDS.}$$

□

Korollar 2.5.11. *For en matroide M gjelder følgende:*

$$\begin{aligned} M \text{ er nesten-MDS} &\Leftrightarrow M^* \text{ er 2-MDS,} \\ M \text{ er 2-MDS} &\Leftrightarrow M^* \text{ er nesten-MDS.} \end{aligned}$$

□

Korollar 2.5.12. *Følgende er ekvivalent, for en matroide M:*

i) M *er nær-MDS.*

ii) M *og* M^* *er nesten-MDS.*

iii) M *og* M^* *er 2-MDS.*

iv) M *er både nesten-MDS og 2-MDS.*

v) M^* *er både nesten-MDS og 2-MDS.*

□

Korollar 2.5.13. *For en planar graf G, der G^* er en geometrisk dual til G, har vi:*

$$G \text{ er MDS} \Leftrightarrow G^* \text{ er MDS.}$$

□

Korollar 2.5.14. *For en planar graf G, der G^* er en geometrisk dual til G, gjelder følgende:*

$$\begin{aligned} G \text{ er nesten-MDS} &\Leftrightarrow G^* \text{ er 2-MDS,} \\ G \text{ er 2-MDS} &\Leftrightarrow G^* \text{ er nesten-MDS.} \end{aligned}$$

□

Korollar 2.5.15. *La G være en planar graf, og la G^* være en geometrisk dual til G. Da er følgende ekvivalent:*

i) G *er nær-MDS.*

ii) G *og* G^* *er nesten-MDS.*

iii) *G og G^* er 2-MDS.*

iv) *G er både nesten-MDS og 2-MDS.*

v) *G^* er både nesten-MDS og 2-MDS.*

□

Vi merker oss at ekvivalensen *i*) $\Leftrightarrow$ *iv*) holder for en vilkårlig graf, siden den holder for kretsmatroiden til en vilkårlig graf. Dermed kan del *iv*) brukes som en alternativ definisjon av en nær-MDS-graf, uten å måtte gå via kretsmatroiden.

2.5.2 MDS-matroider

Følgende resultat viser oss hvordan MDS-matroider ser ut, og det er kanskje ikke så overraskende, sett i lys av teorem 2.2.3:

Teorem 2.5.16. *For en matroide M gjelder følgende:*

$$M \text{ er MDS} \quad \Leftrightarrow \quad M \text{ er uniform.}$$

Bevis. La $M = (S, r)$ være en matroide. Vi legger merke til at M er den uniforme matroiden $U_{n-k,n} = U_{r(M),n}$ hvis og bare hvis vi har følgende ekvivalens for $X \subseteq S$:

$$X \text{ er uavhengig} \quad \Leftrightarrow \quad |X| < r(M) + 1. \tag{2.10}$$

Vi vil vise at dette igjen er ekvivalent med at M er MDS.

Anta først at M er MDS. Fra definisjonene av MDS-matroide og generaliserte Hamming-vekter for en matroide har vi

$$M \text{ er MDS} \quad \Leftrightarrow \quad n - k + 1 \;=\; r(M) + 1 \;=\; d_1 \;=\; \min\{|Y| \,|\, |Y| - r(Y) = 1\},$$

for én $Y \subseteq S$. Anta $|X| < r(M) + 1$. Da medfører $r(M) + 1 = \min\{|Y| \,|\, |Y| - r(Y) = 1\}$ at vi må ha $|X| - r(X) = 0$, altså $|X| = r(X)$. Men fra del (1.1) i proposisjon 1.3.10 er dette det samme som at X er uavhengig. Anta så at X er uavhengig, altså at vi har $|X| = r(X)$. Da er $|X| = r(X) \leq r(M) < r(M) + 1$. Totalt gir dette at vi har ekvivalensen (2.10).

Anta så at (2.10) gjelder. Da har vi

$$X \text{ er avhengig} \quad \Leftrightarrow \quad |X| \geq r(M) + 1,$$

som igjen gir

$$d_1 \;=\; \min\{|X| \,|\, |X| - r(X) = 1\} \;=\; \min\{|X| \,|\, X \text{ er avhengig}\} \;=\; r(M) + 1.$$

Men dette er det samme som at M er MDS, og beviset er ferdig. □

Merk at vi fra dette også har følgende ekvivalens (fra eksempel 1.3.17 eller korollar 2.5.10):

$$M \text{ er MDS} \quad \Leftrightarrow \quad M \text{ er uniform} \quad \Leftrightarrow \quad M^* \text{ er MDS} \quad \Leftrightarrow \quad M^* \text{ er uniform.}$$

2.5.3 Klassifisering av grafer med gitte MDS-egenskaper

Vi vil i resten av kapittel 2 begrense oss til *sammenhengende* grafer, en ikke unaturlig begrensning sett ut fra korollar 2.5.7, i tillegg til den påfølgende bemerkning om at dette resultatet også gjelder for grafer med andre MDS-egenskaper.

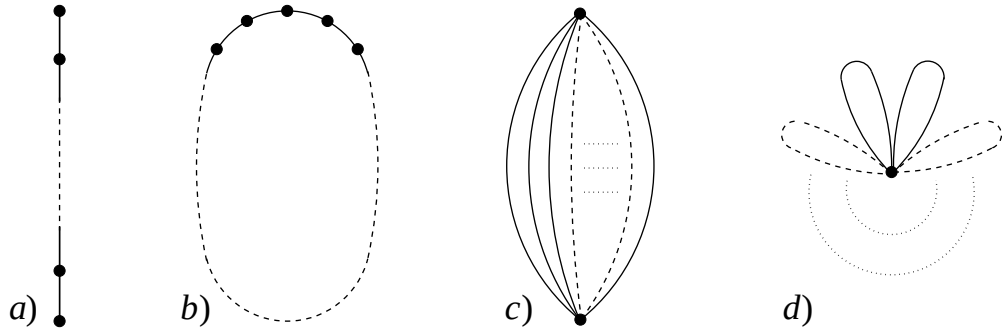
Definisjon 2.5.17. *La G være en graf. Dersom G er MDS eller nær-MDS, kalles den* ***triviell*** *hvis $k \leq 1$ eller $k \geq n-1$.*

Det er lett å se at lemma 2.1.7 og korollar 2.1.15 også gjelder for grafer. Dermed får vi at en triviell MDS-graf har vekthierarki lik $\emptyset$, $\{n\}$, $\{2,3,\ldots,n\}$ eller $\{1,2,\ldots,n\}$, mens for en triviell nær-MDS-graf vil det være $\{n-1\}$ eller $\{1,3,4,\ldots,n\}$.

Definisjon 2.5.18. *La G være en graf som ikke er nær-MDS. Hvis G er nesten-MDS, kalles den* ***triviell*** *dersom $k \geq n-1$, mens hvis G er 2-MDS kalles den* ***triviell*** *dersom $k \leq 1$.*

En triviell nesten-MDS-graf som ikke er nær-MDS vil altså ha vekthierarki på formen $\{d_h \mid 1 \leq h \leq n-1\} = \{1,2,\ldots,i-1,i+1,\ldots,n\}$, for én $3 \leq i \leq n$, mens for en triviell 2-MDS-graf som ikke er nær-MDS har vi vekthierarkiet $\{d_1\} = \{i\}$, for én $1 \leq i \leq n-2$. Spesielt er en triviell nær-MDS-graf også triviell nesten- og 2-MDS.

Legg merke til at enhver graf med $k = 0$ eller $k = n$ er MDS, og dermed ikke nær-, nesten- eller 2-MDS, altså kan vi også sette likhetstegn i definisjonene av trivielle nær-MDS-, nesten-MDS- og 2-MDS-grafer. For at definisjonene skal gi mening, må vi også ha $n \geq 2$ i nær-MDS-tilfellet i definisjon 2.5.17 og $n \geq 3$ i begge tilfeller i definisjon 2.5.18.



Figur 2.3: Trivielle MDS-grafer med k lik henholdsvis 0, 1, $n-1$ og n.

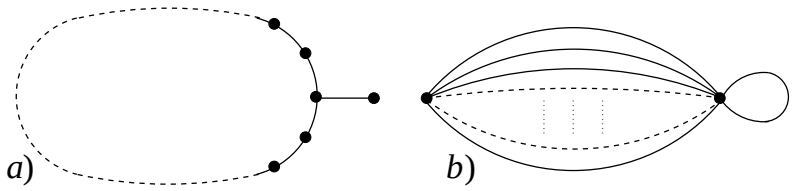
Den neste proposisjonen gir en god grunn for de foregående definisjonene:

Proposisjon 2.5.19. *For alle mulige $n \in \mathbb{N} \cup \{0\}$, eksisterer trivielle MDS-, nær-MDS-, nesten-MDS- og 2-MDS-grafer, og for alle mulige valg av k.*

Bevis. La G være en graf, med $|E(G)| = n$.

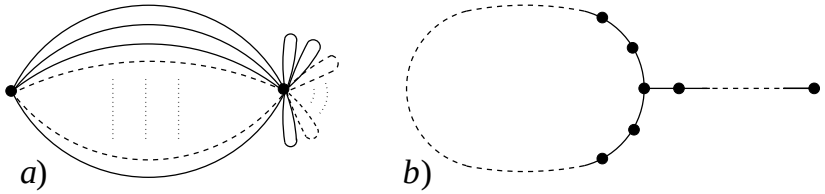
Dersom G er en sti av lengde n (se figur 2.3*a*), er $k = 0$, og G er MDS (alternativt; G er et vilkårlig tre). Dersom G er en krets av lengde n (se figur 2.3*b*), har G vekthierarkiet $\{d_1\} = \{n\}$, og G er MDS, med $k = 1$. Vi ser lett at alle stier og kretser av lengde n er planare, altså har de geometriske dualer, og korollar 2.5.13 gir oss at dualene er MDS. Siden disse dualene har k lik henholdsvis n og $n-1$, er proposisjonen vist for de trivielle MDS-tilfellene. (Dualene er for øvrig på denne formen: Dualen til en sti (eventuelt et tre)

av lengde n er grafen bestående av ett hjørne og n løkker (se figur 2.3d) og har vekthierarki $\{d_h \mid 1 \leq h \leq n\} = \{1, 2, \ldots, n\}$. Dualen til en krets av lengde n består av to hjørner med n kanter mellom (se figur 2.3c). Vekthierarkiet er $\{d_h \mid 1 \leq h \leq n-1\} = \{2, 3, \ldots, n\}$.)



Figur 2.4: Trivielle nær-MDS-grafer med k lik henholdsvis 1 og $n-1$.

La så G være en $(n-1)$-krets sammen med en bro til ett hjørne (se figur 2.4a). Da har vi $k = 1$, og vekthierarkiet er $\{d_1\} = \{n-1\}$, altså er G en triviell nær-MDS-graf. Dersom vi i stedet lar G bestå av to hjørner med $n-1$ kanter mellom og én løkke (se figur 2.4b), er G en triviell nær-MDS-graf med $k = n-1$ og vekthierarki $\{d_h \mid 1 \leq h \leq n-1\} = \{1, 3, 4, \ldots, n\}$. Dette gir oss resultatet for nær-MDS-grafer.



Figur 2.5: Trivielle nesten-MDS- og 2-MDS-grafer.

Dersom G er en graf med to hjørner, $i-1$ løkker og $n-i+1$ kanter mellom de to hjørnene, for én $3 \leq i \leq n$ (se figur 2.5a), får G vekthierarkiet $\{d_h \mid 1 \leq h \leq n-1\} = \{1, 2, \ldots, i-1, i+1, \ldots, n\}$ og er triviell nesten-MDS. Dersom G består av én i-krets og $n-i$ broer, for én $1 \leq i \leq n-2$ (se figur 2.5b), blir vekthierarkiet lik $\{d_1\} = \{i\}$. Dermed er G triviell 2-MDS, og alle tilfellene er vist. □

Legg merke til at grafene på figur 2.3b, 2.3c, 2.3d, 2.4a og 2.4b er de eneste, opp til isomorfi, som gir de aktuelle vekthierarkiene.

Vi vil nå gå over til å se på hvilke ikke-trivielle tilfeller som finnes. For MDS-grafer er resultatet kanskje noe nedslående:

Teorem 2.5.20. *Det eksisterer ikke ikke-trivielle MDS-grafer.*

Vi vil gi to forskjellige bevis for dette, ett rent grafresonnement og ett som bygger på et sterkt resultat for MDS-koder, nemlig Hovedformodningen for MDS-koder:

Formodning 2.5.21. *La C være en $[n,k]$-MDS-kode over $\mathbb{F}_q$, med $1 < k < n$. Da har vi:*

$$n \leq \begin{cases} q+2 & \text{hvis } q \text{ er jevn og } k = 3 \text{ eller } k = q-1, \\ q+1 & \text{ellers.} \end{cases}$$

Bevis. Hovedformodningen er bevist for koder med $k \leq 5$ eller $q \leq 11$, se for eksempel [MacWS]. □

Fra dette kan vi ganske umiddelbart bevise teorem 2.5.20:

Bevis. Anta, for å oppnå en selvmotsigelse, at G er en ikke-triviell MDS-graf. Da er $M(G)$ en MDS-matroide, med $2 \leq k \leq n-2$. Proposisjon 1.3.23 gir at $M(G)$ er representabel over enhver kropp, spesielt over $\mathbb{F}_2$. Altså er $M(G)$ isomorf til vektormatroiden til en matrise H over $\mathbb{F}_2$, der H er paritetssjekkmatrise for en $[n,k]$-MDS-kode C over $\mathbb{F}_2$, med $2 \leq k \leq n-2$. Men dette er en selvmotsigelse, siden hovedformodningen for MDS-koder, innsatt $q=2$, gir at en $[n,k]$-MDS-kode C over $\mathbb{F}_2$ med $1 < k < n$ må ha $n \leq 4$ når $k \in \{1,3\}$, og $n \leq 3$ ellers. Altså eksisterer ikke ikke-trivielle MDS-grafer. □

Som sagt vil vi også gi et annet, rent grafteoretisk bevis for teorem 2.5.20, og dette er mer direkte, uten bruk av andre resultater:

Bevis. La G være en MDS-graf. Anta d_1 eksisterer og $d_1 < n$. Da er det nok å vise at vi har $d_1 \leq 2$. La A være en krets i G av lengde d_1. Siden G er MDS, og $d_1 < n$, må det eksistere $d_2 = d_1 + 1$, altså må det eksistere en kant $e \in E(G)$ slik at $e \notin E(A)$. Videre har vi $r(G) = d_1 - 1 = r(A)$, altså kan ikke e øke rangen til G. Det vil igjen si at endepunktene til e må være hjørner i A, og e må danne en ny krets. Dermed får vi ulikheten:

$$d_1 \quad \leq \quad \text{antall kanter i ny krets} \quad \leq \quad |\{e\}| + \left\lfloor \tfrac{|E(A)|}{2} \right\rfloor \quad = \quad 1 + \left\lfloor \tfrac{d_1}{2} \right\rfloor.$$

Men dette medfører at vi må ha $d_1 \leq 2$, og resultatet følger. □

Siden vi allerede har vist at MDS-matroider er uniforme i teorem 2.5.16, kan vi bruke teorem 2.5.20 til å si hvilke uniforme matroider som er grafiske:

Korollar 2.5.22. *Den uniforme matroiden $U_{r,n}$ er grafisk hvis og bare hvis $r \leq 1$ eller $r \geq n-1$.*

Bevis. (Vi benytter oss av den ekvivalente definisjonen av grafisk matroide som er antydet etter proposisjon 1.3.19.)

La $r, n \in \mathbb{N} \cup \{0\}$ med $0 \leq r \leq n$.

Anta først at matroiden $U_{r,n}$ er grafisk. Fra definisjonen av grafisk matroide er da $U_{r,n} = M(G)$ for en graf G, og da gir korollar 2.4.4 at $U_{r,n}$ og G har samme vekthierarki, med $r = r(U_{r,n}) = n - k(U_{r,n}) = n - k(G)$. Siden $U_{r,n}$ er MDS (teorem 2.5.16), er dermed også G MDS, og teorem 2.5.20 gir at G er triviell. Altså har vi $k(G) \leq 1$ eller $k(G) \geq n-1$, og siden $r = n - k(G)$ er $r \leq 1$ eller $r \geq n-1$.

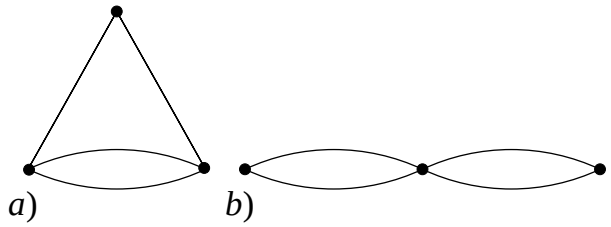
Motsatt, anta at $r \leq 1$ eller $r \geq n-1$. Da gir proposisjon 2.5.19 at det eksisterer en MDS-graf G med parametre n og $k(G) = n - r$, og korollar 2.4.4 gir igjen at $M(G)$ er MDS. Altså er $M(G) = U_{r,n}$, og $U_{r,n}$ er grafisk. (Det følger direkte fra definisjonen at $U_{r,n}$ er unik, opp til isomorfi.) □

Vi klassifiserer så nær-MDS-grafene:

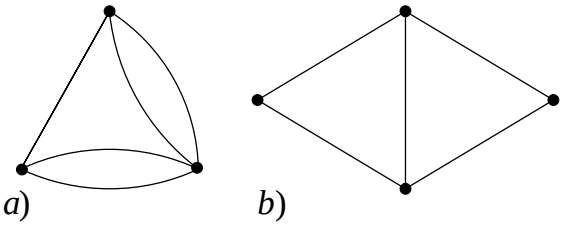
Teorem 2.5.23. *Vi har følgende:*

i) Det eksisterer nær-MDS-grafer som gir alle mulige vekthierarki for $n \leq 6$.

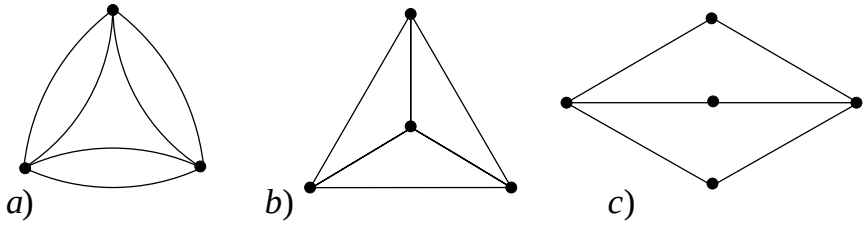
ii) Det eksisterer ikke ikke-trivielle nær-MDS-grafer for $n > 6$.



Figur 2.6: Nær-MDS-grafer med $n = 4$ og vekthierarki $\{2, 4\}$.



Figur 2.7: Nær-MDS-grafer med $n = 5$ og vekthierarkiene $\{2, 4, 5\}$ og $\{3, 5\}$.



Figur 2.8: Nær-MDS-grafer med $n = 6$ og vekthierarkiene $\{2, 4, 5, 6\}$, $\{3, 5, 6\}$ og $\{4, 6\}$.

Bevis. *i*) Foruten de trivielle tilfellene, som allerede er vist, er det bare 6 ulike vekthierarki som er mulige: For $n \leq 3$ er alle mulige nær-MDS-grafer trivielle, og for $n = 4$ er vekthierarkiet $\{2, 4\}$ det eneste ikke-trivielle. For $n = 5$ har vi vekthierarkiene $\{2, 4, 5\}$ og $\{3, 5\}$, mens for $n = 6$ har vi $\{2, 4, 5, 6\}$, $\{3, 5, 6\}$ og $\{4, 6\}$. Figurene 2.6−2.8 viser grafer med alle disse vekthierarkiene, og del *i*) er vist. (Disse grafene er for øvrig også de eneste, opp til isomorfi, som har disse vekthierarkiene.)

ii) Vi vil vise følgende to påstander, som til sammen gir resultatet:

iia) En ikke-triviell nær-MDS-graf med $d_1 \leq 4$ må ha $n \leq 6$.

iib) Det eksisterer ikke ikke-trivielle nær-MDS-grafer med $d_1 \geq 5$.

iia) La G være en ikke-triviell nær-MDS-graf. Da må vi ha $d_1 \geq 2$, for hvis ikke, har vi $k = n - 1$, og G er triviell. Vi må også ha $r = n - k = d_1$, siden Singletondefekten $S(G) = 1$, og siden G er ikke-triviell, må det eksistere d_2, og vi må ha $d_2 = d_1 + 2$.

Anta først at $d_1 = 2$. Da har G ingen løkker, og siden vi har $d_2 = d_1 + 2 = 4$ er det maksimalt to kanter mellom hvert hjørnepar. Men vi har $|V(G)| = r + 1 = d_1 + 1 = 3$, som gir nøyaktig $\binom{3}{2} = 3$ ulike uordnede hjørnepar, og med maksimalt to kanter mellom hvert hjørnepar får vi maksimalt $3 \cdot 2 = 6$ kanter. Vi får altså $n \leq 6$.

Anta så at $d_1 = 3$. Da kan G verken ha løkker eller parallelle kanter. Vi har $|V(G)| = r + 1 = d_1 + 1 = 4$, som gir nøyaktig $\binom{4}{2} = 6$ ulike uordnede hjørnepar. Med maksimalt én kant mellom hvert hjørnepar er maksimalt antall kanter lik $6 \cdot 1 = 6$. Altså får vi $n \leq 6$.

Anta til slutt at $d_1 = 4$. Vi har $d_2 = 6$ og $|V(G)| = r + 1 = d_1 + 1 = 5$. La $V(G) = \{v_1, v_2, v_3, v_4, v_5\}$, og la $A = v_1e_2v_2e_3v_3e_4v_4e_1v_1$ være en krets i G, for $\{e_1, e_2, e_3, e_4\} \subseteq E(G)$. Kretsen A har altså ett hjørne mindre enn G, og delgrafen B av G med $|E(B)| = 6$ som gir to kretser (det kan være flere slike), må derfor inneholde A som en delgraf. Vi kan anta, uten tap av generalitet, at kanten $e_5 = \{v_1, v_5\} \in E(B) \subseteq E(G)$, og vi kaller den siste kanten i B for e_6. Den eneste muligheten er $e_6 = \{v_5, v_3\}$, for alle andre valg vil gi $d_1 < 4$. Dette betyr også at vi ikke kan ha flere kanter i G, og vi får $n = |E(B)| = 6$. Dette fullfører beviset for påstand *iia*.

iib) La G være en nær-MDS-graf med vekthierarki $\{d_1, d_2\} = \{n-2, n\}$. Vi viser først at vi da må ha $n \leq 6$:

La A være en krets i G av lengde $n-2$. La $e_1, e_2 \in E(G)$ være de to kantene i G som ikke er i $E(A)$. Begge må henge sammen med kanter i A, for hvis ikke, får vi ingen nye kretser, siden G er sammenhengende. Ingen av dem kan ha begge endepunkter i A, siden vi da ville få $d_2 = |E(A)| + 1 = d_1 + 1$. Altså må begge ha nøyaktig ett endepunkt i A og ett endepunkt ikke i A. Men da må dette endepunktet være felles for e_1 og e_2, for hvis ikke, har G kun én krets. Vi får ulikheten:

$$n-2 \;=\; d_1 \;\leq\; \text{antall kanter i ny krets} \;\leq\; |\{e_1, e_2\}| + \left\lfloor \tfrac{n-2}{2} \right\rfloor \;=\; 2 + \left\lfloor \tfrac{n-2}{2} \right\rfloor.$$

Dette gir $n \leq 6$.

Anta så, for å oppnå en selvmotsigelse, at det eksisterer en graf G med vekthierarki $\{i-2, i, i+1, i+2, \ldots, n\}$ for én $7 \leq i \leq n$, altså at $d_1 \geq 5$. La så A være restriksjonen av G til kantene som gir d_1 og d_2 i G. (Hvis det er flere slike, velger vi én av disse kantmengdene.) Da er A en graf med vekthierarki $\{i-2, i\}$ for én $i > 6$, som er en selvmotsigelse. Altså eksisterer ikke ikke-trivielle nær-MDS-grafer med $d_1 \geq 5$, og påstand *iib* er også bevist. □

Legg merke til at graf a og b i figur 2.6 og graf a i figur 2.7 alle kan fås ved å fjerne kanter fra graf a i figur 2.8, og graf b i figur 2.7 kan fås ved å fjerne en kant fra graf b i figur 2.8. Grunnen til at det går et skille ved $n = 6$ i teorem 2.5.23 er derfor "komplettheten" ved grafene i figur 2.8: Graf a har nøyaktig to kanter mellom hvert hjørnepar, graf b er K_4 og graf c er $K_{3,2}$.

Når vi nå går over til å studere nesten-MDS- og 2-MDS-grafene, får vi naturlig nok et noe større antall mulige grafer:

Teorem 2.5.24. *For en ikke-triviell nesten-MDS-graf G som ikke er nær-MDS, må vi ha $k = n-2$ og $d_{i-1} = i$ for alle $2 \leq i \leq \lceil \frac{n}{3} \rceil$. Videre eksisterer nesten-MDS-grafer med $k = n-2$ for alle vekthierarki som oppfyller dette kravet.*

Bevis. La G være en ikke-triviell nesten-MDS-graf som ikke er nær-MDS. At G er nesten-MDS gir oss $d_1 = n - k$, og siden G ikke er nær-MDS må vi ha $d_2 = n - k + 1$. Vi viser først at vi må ha $k = n-2$, og dermed også $d_1 = 2$ og $r = 2$:

La A være en krets i G av lengde d_1. Vi har $d_2 = d_1 + 1$, og vi kan anta, uten tap av generalitet, at kantmengden i G av kardinalitet d_2 som gir to kretser, inneholder $E(A)$. Altså eksisterer en kant $e \in E(G)$ med $e \notin E(A)$ som har to hjørner i A som endepunkter. Vi får ulikheten:

$$d_1 \;\leq\; \text{antall kanter i ny krets dannet ved } e \;\leq\; |\{e\}| + \left\lfloor \tfrac{d_1}{2} \right\rfloor \;=\; 1 + \left\lfloor \tfrac{d_1}{2} \right\rfloor.$$

Som i det grafteoretiske beviset for teorem 2.5.20, gir dette at $d_1 \leq 2$, som igjen gir $k \geq n-2$, siden $d_1 = n - k$. Men siden G er ikke-triviell, får vi $k = n - 2$.

La så $a = \lceil \frac{n}{3} \rceil$. For å vise at vi må ha $d_{i-1} = i$ for alle $2 \leq i \leq a$, er det nok å vise at vi må ha $d_{a-1} \leq a$, fra korollar 2.4.5 kombinert med at $d_1 = 2$.

Anta, for å oppnå en selvmotsigelse, at G er en ikke-triviell nesten-MDS-graf som ikke er nær-MDS, med $d_{a-1} > a$. Vi har $|V(G)| = r + 1 = 3$, og vi lar $V(G) = \{v_1, v_2, v_3\}$, mens $E_{i,j}$ er kantene mellom hjørnene v_i og v_j, for $i, j \in \{1, 2, 3\}$. Siden $d_1 \neq 1$, har vi $|E_{i,i}| = 0$ for alle i, og $d_{a-1} > a$ gir $|E_{i,j}| \leq a - 1$ for alle i, j, siden vi ellers ville fått $d_{a-1} \leq a$. Til sammen gir dette ulikheten

$$n \;=\; |E_{1,2}| + |E_{1,3}| + |E_{2,3}| \;\leq\; 3(a-1) \;=\; 3\big(\lceil \tfrac{n}{3} \rceil - 1\big) \;<\; n,$$

som er en selvmotsigelse. Altså har vi $d_{a-1} \leq a$.

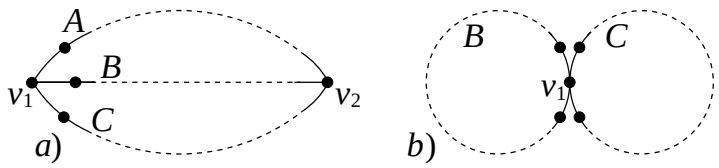
Til slutt viser vi at det eksisterer grafer som har alle slike vekthierarki: La G være grafen med 3 hjørner, n kanter, ingen løkker og i kanter mellom to av hjørnene for én $\lceil \frac{n}{3} \rceil \leq i \leq n-1$. La så $j = \lceil \frac{n-i}{2} \rceil$ og $k = \lfloor \frac{n-i}{2} \rfloor$ være antall kanter mellom de andre hjørneparene. Da får vi $j, k \leq i$ og $i + j + k = n$, og vekthierarkiet til G er $\{2, 3, \ldots, i, i+2, i+3, \ldots, n\}$ for én $\lceil \frac{n}{3} \rceil \leq i \leq n - 1$. Dermed er teoremet bevist. □

Ikke uventet har vi et lignende resultat for ikke-trivielle 2-MDS-grafer:

Teorem 2.5.25. *For en ikke-triviell 2-MDS-graf G som ikke er nær-MDS må vi ha $k = 2$, $d_1 \leq n - \lceil \frac{n}{3} \rceil$ og $d_2 = n$. Videre eksisterer 2-MDS-grafer med $k = 2$ for alle vekthierarki som oppfyller dette kravet.*

Før vi viser dette, gir vi et resultat som vi trenger i beviset:

Lemma 2.5.26. *La G være en graf med $k \geq 2$. Da har vi $d_1 + \lceil \frac{d_1}{2} \rceil \leq d_2$.*



Figur 2.9: To muligheter for en delgraf bestående av to kretser.

Bevis. La G være en graf med $k \geq 2$, og la H være delgrafen (eventuelt én av delgrafene) til G med $E(H) = d_2$ slik at H har to kretser. Vi kan da dele H i tre stier A, B og C med felles endehjørner (kalt v_1 og v_2 på figur 2.9*a*), og vi antar for enkelhets skyld at $|E(A)| \leq |E(B)| \leq |E(C)|$. (Som vist på figur 2.9*b*, kan vi ha $|E(A)| = 0$, og i så fall er ikke B og C stier, men kretser med ett felles hjørne, kalt v_1 på figuren.) Da har vi $d_1 \leq |E(A)| + |E(B)| \leq 2 \cdot |E(C)|$, som igjen gir $\lceil \frac{d_1}{2} \rceil \leq |E(C)|$. Vi får ulikheten

$$\begin{aligned} d_1 + \lceil \tfrac{d_1}{2} \rceil &\leq |E(A)| + |E(B)| + \lceil \tfrac{d_1}{2} \rceil \\ &\leq |E(A)| + |E(B)| + |E(C)| \\ &= |E(H)| \\ &= d_2. \end{aligned}$$

□

Siden d_1 og d_2 er heltall, har vi følgende:

$$\left\lceil \tfrac{3d_1}{2} \right\rceil \leq d_2 \quad \Leftrightarrow \quad \tfrac{3d_1}{2} \leq d_2 \quad \Leftrightarrow \quad d_1 \leq \tfrac{2d_2}{3} \quad \Leftrightarrow \quad d_1 \leq \left\lfloor \tfrac{2d_2}{3} \right\rfloor.$$

Men vi har også $\left\lceil \frac{3d_1}{2} \right\rceil = \left\lceil d_1 + \frac{d_1}{2} \right\rceil = d_1 + \left\lceil \frac{d_1}{2} \right\rceil$ og $\left\lfloor \frac{2d_2}{3} \right\rfloor = \left\lfloor d_2 - \frac{d_2}{3} \right\rfloor = d_2 - \left\lceil \frac{d_2}{3} \right\rceil$, altså får vi:

$$d_1 + \left\lceil \tfrac{d_1}{2} \right\rceil \leq d_2 \quad \Leftrightarrow \quad d_1 \leq d_2 - \left\lceil \tfrac{d_2}{3} \right\rceil. \tag{2.11}$$

Nå er vi klare til å gi beviset for teorem 2.5.25:

Bevis. Anta, for å oppnå en selvmotsigelse, at G er en ikke-triviell 2-MDS-graf som ikke er nær-MDS, med $k \geq 3$. Vi har da $d_1 + 3 \leq d_2$. Siden G er 2-MDS, har vi $d_2 = n - k + 2 = r + 2$, altså $r = d_2 - 2$, som gir $V(G) = r + 1 = d_2 - 1$.

La H være delgrafen som er restriksjonen av G til kantmengden (eventuelt en av kantmengdene) av kardinalitet d_2 som gir 2 kretser. På samme måte som i beviset for lemma 2.5.26, deler vi H i tre stier, A, B og C, med felles endehjørner (se figur 2.9*a*), og vi antar at $|E(A)| \leq |E(B)| \leq |E(C)|$. (Vi kan også her ha at $|E(A)| = 0$ og B og C er kretser istedenfor stier, noe som igjen gir en situasjon som på figur 2.9*b*.) Siden alle stier S har $V(S) = E(S) + 1$ og stiene A, B og C har nøyaktig to hjørner felles, får vi $|V(H)| = (|E(A)|+1) + (|E(B)|+1-2) + (|E(C)|+1-2) = |E(A)| + |E(B)| + |E(C)| - 1 = |E(H)| - 1 = d_2 - 1 = |V(G)|$. Altså har vi $V(G) = V(H)$, som betyr at $d_1 = |E(A)| + |E(B)|$ og $|E(C)| = d_2 - d_1 \geq 3$. Siden G har $k \geq 3$, må vi ha $|E(G)| > |E(H)|$, og kanten(e) i G som ikke er i H må forbinde hjørner i H. La e være en slik kant. Vi har tre muligheter for endepunktene v_1 og v_2 til e:

i) $v_1, v_2 \in V(A) \cup V(B)$,
ii) $v_1, v_2 \in V(C)$,
iii) $v_1 \in V(A) \cup V(B)$ og $v_2 \in V(C)$.

Alternativ *i*) gir $d_2 \leq |E(A)| + |E(B)| + |\{e\}| = d_1 + 1 \leq d_2 - 2$, som er en selvmotsigelse.

Anta alternativ *ii*), og la $E(C')$ være kantene i $E(C)$ som er mellom v_1 og v_2. Vi må ha $1 \leq |E(C')| \leq |\{e\}| = 1$, for ellers danner $(E(A) \cup E(B) \cup E(C) \cup \{e\}) \cap E(C')$ en kantmengde til to kretser med mindre kardinalitet enn d_2. Altså består $E(C')$ av én kant, som betyr at $E(C') \cup \{e\}$ er kantmengden til en krets i G. Men dette er en selvmotsigelse, siden vi da vil få $d_2 \leq d_1 + 2$.

Anta til slutt alternativ *iii*. Hjørne v_2 deler da $E(C)$ i to deler, si $E(C_1)$ og $E(C_2)$. Siden e ikke er i kantmengden som gir d_2, får vi ulikheten:

$$3 \quad \leq \quad d_2 - d_1 \quad = \quad |E(C)| \quad \leq \quad |\{e\}| + \min\{|E(C_1)|, |E(C_2)|\} \quad \leq \quad 1 + \left\lfloor \tfrac{|E(C)|}{2} \right\rfloor.$$

Men dette gir $|E(C)| \leq 2$, som er en selvmotsigelse.

Altså kan ingen slik kant e eksistere, og vi får $k = 2$.

Siden $k = 2$ og G er 2-MDS, får vi $d_2 = n - k + 2 = n$. Lemma 2.5.26 gir oss $d_1 + \left\lceil \frac{d_1}{2} \right\rceil \leq d_2$, som fra ekvivalensen (2.11) ovenfor er det samme som $d_1 \leq d_2 - \left\lceil \frac{d_2}{3} \right\rceil$, altså får vi $d_1 \leq n - \left\lceil \frac{n}{3} \right\rceil$.

Til slutt gir vi et eksempel på en graf med slike parametre: La G' være grafen bestående av tre stier A, B og C, med felles endepunkter, slik at $|E(A)| = \left\lfloor \frac{d_1}{2} \right\rfloor$, $|E(B)| = \left\lceil \frac{d_1}{2} \right\rceil$ og $|E(C)| \geq \left\lceil \frac{d_1}{2} \right\rceil$. Da har vi $d_1 + \left\lceil \frac{d_1}{2} \right\rceil \leq |E(A)| + |E(B)| + |E(C)| = d_2 = n$, som ved ekvivalensen (2.11) ovenfor gir en slik graf. Dermed er resultatet bevist. □

Det følgende korollaret skulle være temmelig umiddelbart ut fra de foregående resultater, men vi vil også gi et stringent bevis for dette, som for øvrig er ganske kort:

Korollar 2.5.27. *Alle MDS-, nær-MDS-, nesten-MDS- og 2-MDS-grafer er planare.*

Bevis. Merk at vi fra definisjonen av grafkonfigurasjon på side 3 har følgende: La G være en vilkårlig graf, og la G' være en G-konfigurasjon. Da har vi $|E(G)| - |V(G)| = |E(G')| - |V(G')| =$ konstant, fordi antall kanter og antall hjørner begge øker med nøyaktig én hver gang det legges til et hjørne langs en kant i grafen. Men siden vi har $k = n-r = |E(G)|-|V(G)|+i$, der i er antall komponenter av G (og G'), har altså G og G' samme kretsrang k. Kombinert med teorem 1.2.1 gir dette oss at en graf med $k < 4$ er planar, siden vi fra eksempel 2.4.17 har $k(K_5) = 6 \geq 4$ og $k(K_{3,3}) = 4$. Dette gir oss resultatet for alle 2-MDS-grafer og halvparten av tilfellene for de trivielle MDS- og nær-MDS-grafene, siden disse har $k \leq 2$ (Definisjoner 2.5.17 og 2.5.18, og teorem 2.5.25).

Siden alle de resterende trivielle tilfellene har ett eller to hjørner (Definisjoner 2.5.17 og 2.5.18 igjen), gir korollar 1.2.2 oss at også disse er planare.

Teorem 2.5.20 gir at det ikke er mer å vise for MDS-grafer, og teorem 2.5.23 begrenser tilfellet for ikke-trivielle nær-MDS-grafer til grafer med $n \leq 6$. Men korollar 1.2.2 gir oss at alle grafer med $n < 9$ er planare.

Fra teorem 2.5.24 har vi at alle ikke-trivielle nesten-MDS-grafer som ikke er nær-MDS har 3 hjørner, og dermed er også disse planare, fra korollar 1.2.2 igjen. Da er alle tilfeller vist. □

2.5.4 Noen telleresultater

I dette kapittelet vil vi bruke resultatene vi fant i kapittel 2.5.3 til å se på hvor mange ulike vekthierarki og ikke-isomorfe (sammenhengende) grafer vi kan finne med gitte MDS-egenskaper for vilkårlig n.

Vi vil i det følgende bruke notasjonen $W_{n,i}$ og $N_{n,i}$ for henholdsvis antall mulige ulike vekthierarki og antall ikke-isomorfe grafer, der $i = 1$ gir MDS, $i = 2$ nær-MDS, $i = 3$ nesten-MDS og $i = 4$ 2-MDS, og n som vanlig er antall kanter. Generelt er $N_{n,i}$ mest komplisert å finne, og vi har selvsagt også $W_{n,i} \leq N_{n,i}$ for alle mulige valg av i og n.

Vi begynner med MDS- og nær-MDS-grafene, resultater som følger ganske umiddelbart fra forrige kapittel:

Proposisjon 2.5.28. *La antall ikke-isomorfe trær med n kanter være gitt ved t_n. Da har vi:*

$$W_{n,1} = \begin{cases} n+1 & \textit{for } n \leq 2, \\ 4 & \textit{ellers.} \end{cases} \qquad N_{n,1} = \begin{cases} W_{n,1} & \textit{for } n \leq 2, \\ t_n + 3 & \textit{ellers.} \end{cases}$$

$$W_{n,2} = \begin{cases} n-1 & \textit{for } n \leq 6, \\ 2 & \textit{ellers.} \end{cases} \qquad N_{n,2} = \begin{cases} 4 & \textit{for } n = 4, \\ W_{n,2} & \textit{ellers.} \end{cases}$$

Bevis. La oss begynne med $W_{n,1}$. Teorem 2.5.20 gir at ikke-trivielle grafer ikke eksisterer. Som tidligere nevnt er de 4 mulige ulike vekthierarkiene for de trivielle tilfellene $A = \emptyset$, $B = \{n\}$, $C = \{2, 3, \ldots, n\}$ og $D = \{1, 2, \ldots, n\}$. Imidlertid er alle disse identiske for $n = 0$, mens for $n = 1$ er $A = C$ og $B = D$ og for $n = 2$ er $B = C$. For $n \geq 3$ er A, B, C, D alle ulike, dermed følger resultatet for $W_{n,1}$.

Når det gjelder $N_{n,1}$, er de trivielle tilfellene beskrevet i beviset for proposisjon 2.5.19 og gitt ved grafiske representasjoner på figur 2.3. Som tidligere nevnt (og som også er lett å sjekke) er figurene 2.3*b*–*d* de eneste, opp til isomorfi, som har de aktuelle vekthierarkiene, altså er antall ikke-isomorfe grafer identisk med antall mulige ulike vekthierarki, for disse

valgene av parametrene n og k. Når det gjelder figur 2.3a, eller nærmere bestemt grafer med $k = 0$, følger det umiddelbart fra definisjonen av generaliserte Hammingvekter for grafer at for en (sammenhengende) graf G har vi:

$$G \text{ er et tre} \quad \Leftrightarrow \quad k = 0.$$

Altså er antall ikke-isomorfe grafer med n kanter og $k = 0$ (som igjen, fra definisjonen av MDS-graf, er antall ikke-isomorfe MDS-grafer med n kanter og $k = 0$) lik t_n, og siden $t_n = 1$ for $n \leq 2$, følger resultatet for $N_{n,1}$.

For $W_{n,2}$ er det meste sagt tidligere. Vi har at de eneste trivielle nær-MDS-vekthierarkiene er $\{n-1\}$ og $\{1, 3, 4, \ldots, n\}$, og for $n = 2$ er disse sammenfallende. Teorem 2.5.23 gir ett ikke-trivielt vekthierarki for $n = 4$, to for $n = 5$ og tre for $n = 6$, mens det for øvrige n ikke eksisterer noen. Totalt gir dette resultatet.

Til slutt har vi $N_{n,2}$, som følger direkte av at vi merker oss at grafene på figurene 2.4 og 2.6−2.8 er de eneste, opp til isomorfi, som har de aktuelle vekthierarkiene. Det er også lett å sjekke, og vi lar det være opp til leseren å gjøre dette. □

For tilfellene nesten-MDS og 2-MDS er resultatene mer kompliserte, og vi vil derfor dele resultatene opp, for så å oppsummere til slutt. Vi begynner med det enkleste:

Proposisjon 2.5.29. *For trivielle nesten-MDS-grafer med n kanter ($n \geq 3$) har vi følgende:*

i) Antall mulige ulike vekthierarki er lik n.

ii) Antall ikke-isomorfe grafer er lik $\left\lfloor \frac{(n+1)^2}{4} \right\rfloor$.

For $n = 2$ er antallet 1 i begge tilfeller.

Bevis. i) Direkte fra definisjonen av triviell nesten-MDS-graf har vi (som tidligere nevnt) at dersom grafen ikke er nær-MDS, må vekthierarkiet være på formen $\{1, 2, \ldots, i-1, i+1, \ldots, n\}$, for én $3 \leq i \leq n$. Dette gir $n - 2$ ulike vekthierarki, som sammen med de 2 nær-MDS-vekthierarkiene vi fant i beviset for 2.5.28 (1 for $n = 2$) gir resultatet.

ii) Vi har, som vi har sett tidligere, at en graf bestående av to hjørner, $i-1$ løkker og $n-i+1$ kanter mellom de to hjørnene for én $3 \leq i \leq n$, vil ha vekthierarkiet $\{1, 2, \ldots, i-1, i+1, \ldots, n\}$. Det er også lett å se at ingen andre grafer kan ha dette vekthierarkiet, så det eneste som kan variere for en slik graf, er hvor løkkene er plassert. For hver i, har vi $i - 1$ løkker, fordelt på to hjørner. På grunn av symmetri, vil antall ikke-isomorfe grafer da være $\left\lfloor \frac{i-1}{2} \right\rfloor + 1 = \left\lfloor \frac{i+1}{2} \right\rfloor$. (Vi velger et av hjørnene, og lar j løkker være plassert på dette hjørnet, for $j \geq 0$. På grunn av symmetri, vil vi få ikke-isomorfe grafer for $0 \geq j \leq \left\lfloor \frac{i-1}{2} \right\rfloor$, mens for $j > \left\lfloor \frac{i-1}{2} \right\rfloor$ får vi kun grafer som er isomorfe til grafer med lavere verdi for j.) Hvis vi til slutt summerer over alle mulige verdier for i, får vi

$$\sum_{i=3}^{n} \left\lfloor \tfrac{i+1}{2} \right\rfloor \;=\; \sum_{i=4}^{n+1} \left\lfloor \tfrac{i}{2} \right\rfloor \;=\; \left\lfloor \tfrac{(n+1)^2}{4} \right\rfloor - \sum_{i=1}^{3} \left\lfloor \tfrac{i}{2} \right\rfloor \;=\; \left\lfloor \tfrac{(n+1)^2}{4} \right\rfloor - 2,$$

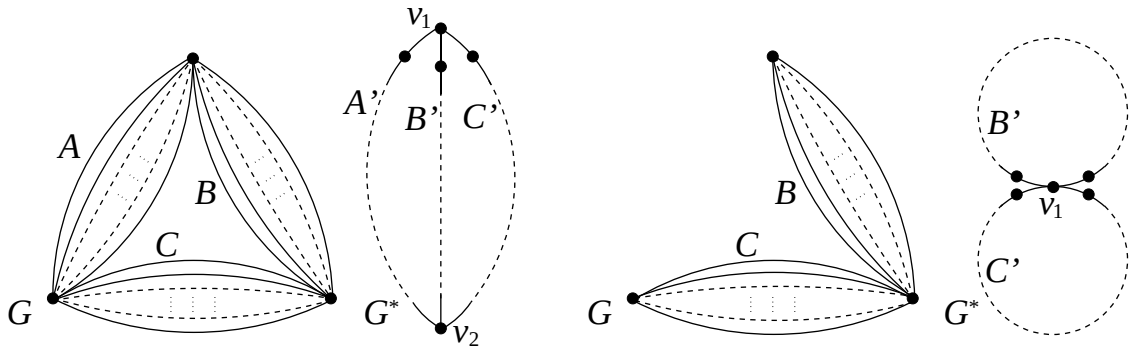
ved bruk av lemma 2.4.15. Inkludert én nær-MDS-graf for $n = 2$ og to for $n \geq 3$, gir dette resultatet. □

Mens de trivielle nesten-MDS-grafene er relativt lette å få oversikt over, er de trivielle 2-MDS-grafene temmelig uoversiktlige, og som vi etter hvert skal se øker antallet raskt når n blir stor. Tidligere har vi sett at vekthierarkiet $\{i\}$ for én $1 \leq i \leq n - 2$ (ikke nær-MDS), og

fra dette følger det umiddelbart at de eneste grafene som har dette vekthierarkiet, består av én i-krets og $n-i$ broer. Men for å kunne telle antall mulige plasseringer av broene, må vi ta hensyn både til fordelingen av kantene på hjørnene i i-kretsen, symmetrien til i-kretsen og antall ikke-isomorfe, rotede trær som kan dannes av kantene som er plassert på hvert hjørne i i-kretsen (der hjørnet i i-kretsen er roten til treet). Det vil føre for langt å regne ut dette i denne oppgaven, derfor nøyer vi oss med å telle antall mulige ulike vekthierarki i dette tilfellet:

Proposisjon 2.5.30. *For trivielle 2-MDS-grafer med n kanter, er antall mulige ulike vekthierarki lik 1 for $n = 2$ og n for $n \geq 3$.*

Bevis. Som sagt er vekthierarkiet til en triviell 2-MDS-graf som ikke er nær-MDS, på formen $\{i\}$ for én $1 \leq i \leq n-2$, noe som gir $n-2$ ulike vekthierarki. Legger vi til én nær-MDS-graf for $n = 2$ og to for $n \geq 3$, følger resultatet. □



Figur 2.10: Ikke-trivielle nesten-MDS- og 2-MDS-grafer, med spesialtilfellet at $|A| = |A'| = 0$.

Før vi gir antall vekthierarki og ikke-isomorfe grafer for de ikke-trivielle nesten-MDS- og 2-MDS-tilfellene, tar vi med et resultat som vi trenger på veien. Resultatet, og kanskje spesielt konstruksjonen gitt i beviset og på figur 2.10, er interessant nok i seg selv, og gir en sammenheng mellom nesten-MDS- og 2-MDS-grafer som vi kanskje kunne forvente ut fra teoremene 2.5.24 og 2.5.25.

Lemma 2.5.31. *Dersom G er en ikke-triviell nesten-MDS- eller 2-MDS-graf, så har G én unik (sammenhengende) geometrisk dual, opp til isomorfi.*

Bevis. Anta først at G er en ikke-triviell nesten-MDS-graf som ikke er nær-MDS. Da er $k = n-2$, fra teorem 2.5.24. Fra korollar 2.5.27 er G planar og har dermed minst én geometrisk dual, og korollar 2.5.14 gir at dersom G^* er en geometrisk dual til G, så er G^* 2-MDS (men ikke nær-MDS). Korollar 2.4.7 gir at G^* har $k = n - k(G) = 2$, altså er G^* også ikke-triviell. Fra teorem 2.5.24 har vi at G er en graf med nøyaktig 3 hjørner, ingen looper og kanter mellom minst 2 av hjørneparene. Som vist på figur 2.10, lar vi A, B og C være mengdene av kanter mellom de tre hjørneparene, slik at $|A| \leq |B| \leq |C|$. Vi lar også G^* være som vist på figur 2.10, der A', B' og C' er kantmengdene til de tre stiene mellom hjørnene v_1 og v_2, og $|A'| = |A|$, $|B'| = |B|$ og $|C'| = |C|$. (Som tidligere bemerket, og som vist på figur 2.10, kan vi ha $|A| = |A'| = 0$, og da er B' og C' kantmengdene til kretser, ikke stier.) Ved symmetribetraktninger på G og G^* er det lett å se at G^* er (opp til isomorfi) den unike

geometriske dualen til G, og motsatt. Siden alle ikke-trivielle 2-MDS-grafer som ikke er nær-MDS også er planare, er det ikke mer å sjekke.

Dersom G i tillegg er nær-MDS, gir teorem 2.5.23 at vi har $n \leq 6$, og vi har tidligere bemerket at alle mulige slike grafer er gitt på figurene 2.6−2.8. Foruten figur 2.8*b* er alle disse spesialtilfeller av enten G eller G^* tidligere i beviset, altså gjelder dette også for disse. Videre er det lett å se at figur 2.8*b* er selvdual, dermed er alle tilfeller vist. □

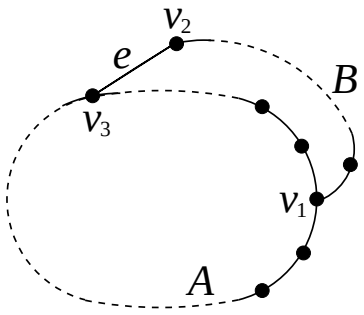
Nå er vi klare til å vise telleresultatene for ikke-trivielle nesten-MDS- og 2-MDS-grafer, og vi starter med tilfellet 2-MDS:

Proposisjon 2.5.32. *For ikke-trivielle 2-MDS-grafer med n kanter ($n > 6$), har vi følgende:*

i) Antall mulige ulike vekthierarki er lik $n - \lceil \frac{n}{3} \rceil$.

ii) La $a = \lceil \frac{n}{3} \rceil$ og $b = \lfloor \frac{n}{2} \rfloor$. Da er antall ikke-isomorfe grafer gitt ved

$$\sum_{i=1}^{n-a} \left(\left\lfloor \frac{i}{2} \right\rfloor + 1 \right) - \sum_{i=b+1}^{n-a} (2i - n) \quad = \quad \left\lfloor \frac{(n-a)^2}{4} \right\rfloor + b + (n - a - b)(a - b).$$



Figur 2.11: Grafen G i beviset for proposisjon 2.5.32.

Bevis. Vi merker oss at vi kan se bort fra nær-MDS-grafer, siden $n > 6$.

i) Dette følger umiddelbart fra teorem 2.5.25.

ii) Fra teorem 2.5.25 må vekthierarkiene være på formen $\{i, n\}$, for $1 \leq i \leq n - \lceil \frac{n}{3} \rceil$, og alle disse vil forekomme og gi 2-MDS-grafer, siden $n \geq 4$. La G være en graf med et slikt vekthierarki, og la A være kretsen (eventuelt en av kretsene) som har lengde i. Siden $d_2 = n$, og på grunn av symmetri, kan vi anta at G inneholder en sti B av lengde $n - i - 1$ med nøyaktig ett hjørne v_1 i A, og ingen kanter i A (se figur 2.11). Da er v_1 et endehjørne i B. La v_2 være det andre endehjørnet i B, og la e være den kanten som verken er i A eller B. Da må e forbinde v_2 med et hjørne v_3 i A, for hvis ikke, er $d_2 < n$. I tillegg må den nye kretsen som dannes, ha lengde $\geq d_1 = i$.

Anta først at $2i \leq n$, altså at $i \leq \lfloor \frac{n}{2} \rfloor$. Da kan v_3 velges fritt blant alle hjørnene i A, og på grunn av symmetri får vi at antall hjørner som gir ikke-isomorfe grafer er $\lfloor \frac{i}{2} \rfloor + 1$.

Anta så at $2i = n + j$ for én $j \geq 1$, altså at $d_1 = i = (n - i) + j$. For at vi ikke skal få en krets av lengde $\leq d_1 = i$, må det være minst j kanter (i A) mellom hjørnene v_1 og v_3. Antall slike hjørner som gir ikke-isomorfe grafer er $\lfloor \frac{i}{2} \rfloor + 1 - j = \lfloor \frac{i}{2} \rfloor + 1 - (2i - n)$.

Antall grafer med vekthierarki $\{i, n\}$ der $2 \leq 2i \leq n$, altså $1 \leq i \leq \lfloor \frac{n}{2} \rfloor$, er dermed

$$\sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \left(\left\lfloor \frac{i}{2} \right\rfloor + 1 \right),$$

mens antall grafer der $\lfloor \frac{n}{2} \rfloor + 1 \leq i \leq n - \lceil \frac{n}{3} \rceil$ er

$$\sum_{i=\lfloor \frac{n}{2} \rfloor + 1}^{n - \lceil \frac{n}{3} \rceil} \left(\left\lfloor \frac{i}{2} \right\rfloor + 1 - (2i - n) \right).$$

Totalt gir dette

$$\sum_{i=1}^{n - \lceil \frac{n}{3} \rceil} \left(\left\lfloor \frac{i}{2} \right\rfloor + 1 \right) - \sum_{i=\lfloor \frac{n}{2} \rfloor + 1}^{n - \lceil \frac{n}{3} \rceil} (2i - n),$$

og resultatet følger.

Til slutt vil vi vise at vi har

$$\sum_{i=1}^{n-a} \left(\left\lfloor \frac{i}{2} \right\rfloor + 1 \right) - \sum_{i=b+1}^{n-a} (2i - n) \quad = \quad \left\lfloor \frac{(n-a)^2}{4} \right\rfloor + b + (n - a - b)(a - b).$$

Vi har for det første at

$$\sum_{i=1}^{n-a} \left(\left\lfloor \frac{i}{2} \right\rfloor + 1 \right) - \sum_{i=b+1}^{n-a} (2i - n)$$

$$= \sum_{i=1}^{n-a} \left\lfloor \frac{i}{2} \right\rfloor + \sum_{i=1}^{n-a} 1 - 2 \sum_{i=1}^{n-a-b} i - 2b \sum_{i=1}^{n-a-b} 1 + n \sum_{i=1}^{n-a-b} 1,$$

og for det andre gir lemma 2.4.15

$$\sum_{i=1}^{n-a} \left\lfloor \frac{i}{2} \right\rfloor \quad = \quad \left\lfloor \frac{(n-a)^2}{4} \right\rfloor.$$

Dermed får vi

$$\sum_{i=1}^{n-a} \left(\left\lfloor \frac{i}{2} \right\rfloor + 1 \right) - \sum_{i=b+1}^{n-a} (2i - n)$$

$$\begin{aligned}
&= \sum_{i=1}^{n-a} \left\lfloor \frac{i}{2} \right\rfloor + \sum_{i=1}^{n-a} 1 - 2 \sum_{i=1}^{n-a-b} i - 2b \sum_{i=1}^{n-a-b} 1 + n \sum_{i=1}^{n-a-b} 1 \\
&= \left\lfloor \frac{(n-a)^2}{4} \right\rfloor + (n - a) - b + b - (n - a - b)(n - a - b + 1) \\
&\quad - 2b(n - a - b) + n(n - a - b) \\
&= \left\lfloor \frac{(n-a)^2}{4} \right\rfloor + b + (n - a - b)(1 - n + a + b - 1 - 2b + n) \\
&= \left\lfloor \frac{(n-a)^2}{4} \right\rfloor + b + (n - a - b)(a - b),
\end{aligned}$$

som var det vi skulle vise. □

Den eneste forutsetningen som ikke holder for $n \leq 6$, er at vekthierarkiet er på formen $\{i, n\}$. Men de eneste 2-MDS-grafene der dette ikke holder, er grafene på figurene 2.7*a*, 2.8*a* og 2.8*b*, altså får vi følgende:

For $n \leq 3$ er alle tilfeller trivielle.

For $n = 4$ gjelder teorem 2.5.32, altså får vi antall mulige ulike vekthierarki lik $4 - \lceil \frac{4}{3} \rceil = 2$, og antall ikke-isomorfe grafer lik $\lfloor \frac{(4-2)^2}{4} \rfloor + 2 + (4-2-2)(2-2) = 3$.

For $n = 5$ får vi et tillegg på én (figur 2.7*a*) både i del *i*) og *ii*) i teorem 2.5.32, altså får vi antall mulige ulike vekthierarki lik $5 - \lceil \frac{5}{3} \rceil + 1 = 4$, og antall ikke-isomorfe grafer lik $\lfloor \frac{(5-2)^2}{4} \rfloor + 2 + (5-2-2)(2-2) + 1 = 5$.

For $n = 6$ får vi et tillegg på to (figurene 2.8*a* og *b*) både i del *i*) og *ii*) i teorem 2.5.32. Altså får vi antall mulige ulike vekthierarki lik $6 - \lceil \frac{6}{3} \rceil + 2 = 6$, og antall ikke-isomorfe grafer lik $\lfloor \frac{(6-2)^2}{4} \rfloor + 3 + (6-2-3)(2-3) + 2 = 8$.

Vi kan bruke lemma 2.5.31 til å vise at det samme også gjelder for ikke-trivielle nesten-MDS-grafer, som det gjorde i 2-MDS-tilfellet:

Korollar 2.5.33. *For ikke-trivielle nesten-MDS-grafer med n kanter ($n > 6$) har vi følgende:*

i) Antall mulige ulike vekthierarki er lik $n - \lceil \frac{n}{3} \rceil$.

ii) La $a = \lceil \frac{n}{3} \rceil$ *og* $b = \lfloor \frac{n}{2} \rfloor$. *Da er antall ikke-isomorfe grafer gitt ved*

$$\sum_{i=1}^{n-a} \left(\left\lfloor \frac{i}{2} \right\rfloor + 1 \right) - \sum_{i=b+1}^{n-a} (2i - n) \quad = \quad \left\lfloor \frac{(n-a)^2}{4} \right\rfloor + b + (n-a-b)(a-b).$$

Bevis. Vi merker oss at resultatet vil følge direkte fra proposisjon 2.5.32 dersom det eksisterer en bijeksjon f : {isomorfiklasser av ikke-trivielle nesten-MDS-grafer} $\leftrightarrow$ {isomorfiklasser av ikke-trivielle 2-MDS-grafer}.

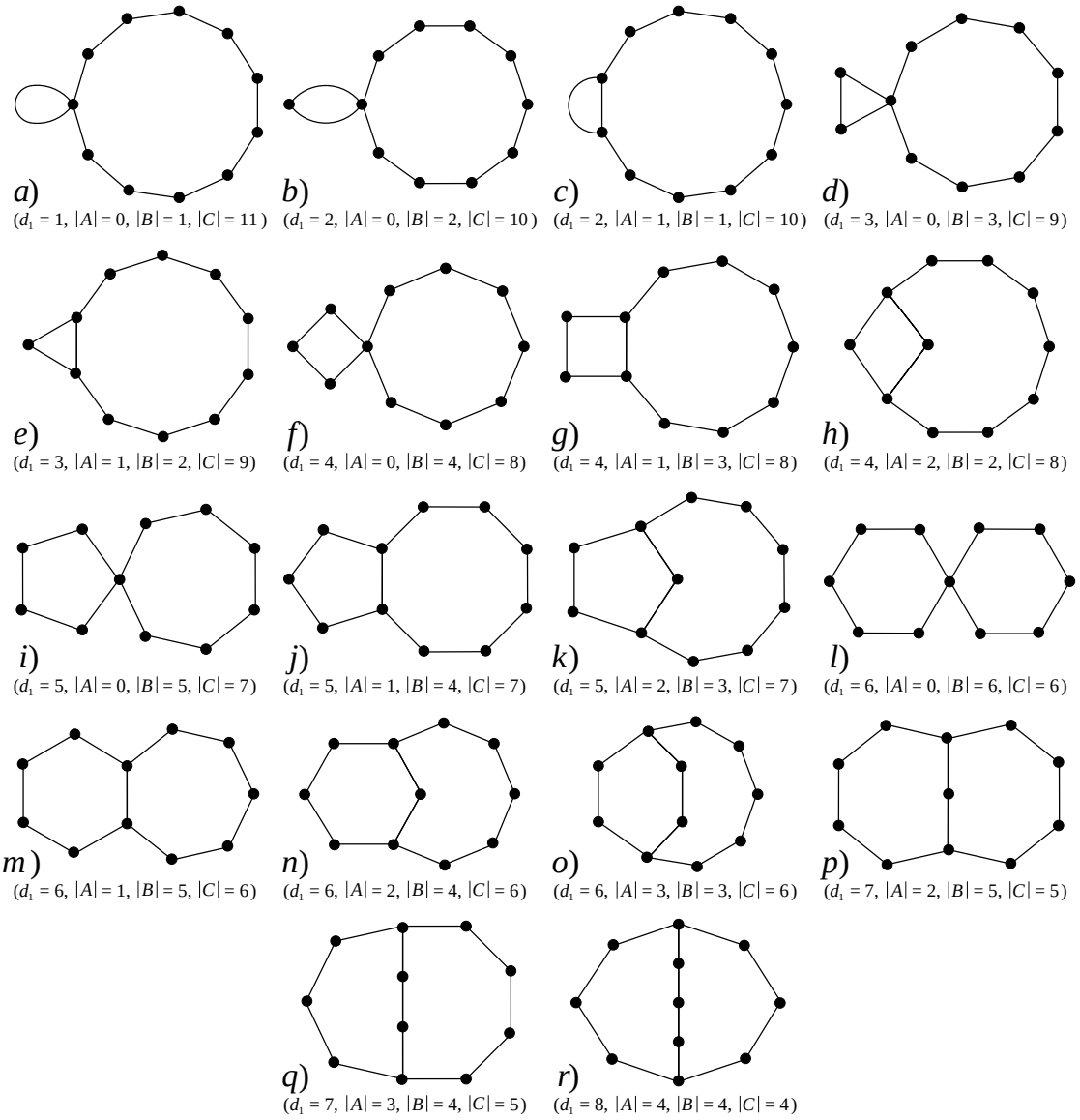
Anta at G er en ikke-triviell nesten-MDS-graf. Fra lemma 2.5.31 har G én unik geometrisk dual (opp til isomorfi) som er ikke-triviell 2-MDS. Fra samme korollar har vi også det motsatte: Anta at G er en ikke-triviell 2-MDS-graf. Også da har G én unik geometrisk dual (opp til isomorfi) som er ikke-triviell nesten-MDS. Altså har vi en bijeksjon f som sender en ikke-triviell nesten-MDS-graf til sin unike geometriske dual som er ikke-triviell 2-MDS, og resultatet følger. □

Bijeksjonen i beviset gjelder også for $n \leq 6$, altså gjelder utregningene vi gjorde før korollar 2.5.33 av antall ikke-trivielle 2-MDS-grafer med $n \leq 6$ også for ikke-trivielle nesten-MDS-grafer.

Vi ser at dersom n i proposisjon 2.5.32 og korollar 2.5.33 er delelig med 6, får vi mye mer kompakte uttrykk. Vi vil derfor kort illustrere dette for 2-MDS-tilfellet, og vi merker oss at det samme også gjelder for ikke-trivielle nesten-MDS-grafer.

Eksempel 2.5.34. *La* $n = 6m$, *for* $m \in \mathbb{N}$ *slik at* $m \geq 2$. *Da er antall mulige ulike vekthierarki for ikke-trivielle 2-MDS-grafer med* $6m$ *kanter gitt ved*

$$6m - \lceil \tfrac{6m}{3} \rceil \quad = \quad 6m - 2m \quad = \quad 4m.$$



Figur 2.12: De 18 ikke-isomorfe, ikke-trivielle 2-MDS-grafene med $n = 12$ kanter.

I tillegg får vi $a = \lceil \frac{6m}{3} \rceil = 2m$ *og* $b = \lfloor \frac{6m}{2} \rfloor = 3m$*, som gir at antall ikke-isomorfe, ikke-trivielle* 2*-MDS-grafer med* $6m$ *kanter er gitt ved*

$$\begin{aligned}\sum_{i=1}^{4m}\left(\left\lfloor\frac{i}{2}\right\rfloor+1\right)-\sum_{i=3m+1}^{4m}(2i-6m) &= \left\lfloor\frac{(4m)^2}{4}\right\rfloor+3m+(6m-2m-3m)(2m-3m)\\ &= 4m^2+3m+m(-m)\\ &= 3m(m+1).\end{aligned}$$

Alternativt får vi rekursjonsformelen

$$a_{m+1} = a_m + 6(m+1), \quad a_2 = 18,$$

der a_m er antall ikke-isomorfe, ikke-trivielle 2-MDS-grafer med $6m$ kanter. Altså vil antall grafer øke med $6(m+1)$ når m øker med én.

På mange måter er også tilfellet i eksempel 2.5.34 det mest interessante. Hvis vi studerer uttrykket

$$\sum_{i=1}^{n-a}\left(\left\lfloor\frac{i}{2}\right\rfloor+1\right)-\sum_{i=b+1}^{n-a}(2i-n)$$

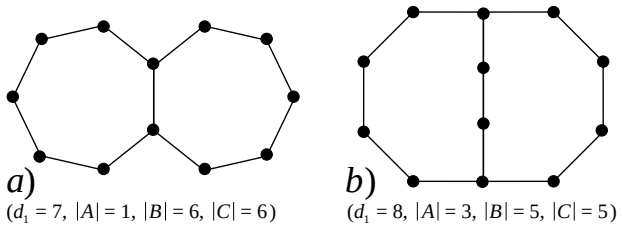
fra proposisjon 2.5.32 og korollar 2.5.33, der $a=\lceil\frac{n}{3}\rceil$ og $b=\lfloor\frac{n}{2}\rfloor$, ser vi at når n øker fra $6m-1$ til $6m$, vil ikke a øke. Altså øker uttrykket $n-a$, den øvre summegrensen, og vi vil få ekstra mange nye grafer i første delen av uttrykket. Samtidig øker b med én, altså øker den nedre summegrensen i den andre delen av uttrykket, som igjen betyr at vi trekker fra færre grafer enn før.

La oss ta et konkret eksempel, for $n=12$:

Eksempel 2.5.35. *Figur 2.12 viser de 18 ikke-isomorfe, ikke-trivielle 2-MDS-grafene med $n=12$ kanter, samt verdien til d_1 og kardinaliteten til kantmengdene A, B og C, slik disse er definert (som henholdsvis A', B' og C') i beviset for lemma 2.5.31.*

Grafene for $n=11$ er gitt ved å beholde parametrene $|A|$ og $|B|$ (og dermed også d_1) og la $|C|$ minke med én i alle grafene gitt på figur 2.12, med unntak av de tilfellene der dette vil medføre $|C|<|B|$, altså i grafene på figur 2.12 med $|B|=|C|$. Dette gjelder grafene l, p og r, som vil bli isomorfe til henholdsvis graf i, n og q. Vi får at antall grafer øker med 3 når n øker fra 11 til 12.

Dersom vi i stedet øker $|C|$ med én, vil vi få 18 ikke-isomorfe, ikke-trivielle 2-MDS-grafer med $n=13$ kanter. I tillegg får vi grafene på figur 2.13. (Dersom vi i disse grafene lar $|C|$ minke med én, vil grafene 2.13a og 2.13b være isomorfe til henholdsvis 2.12m og 2.12q.) Totalt vil antall grafer øke med kun 2 når n øker fra 12 til 13, mot en økning på 3 når n øker fra 11 til 12.



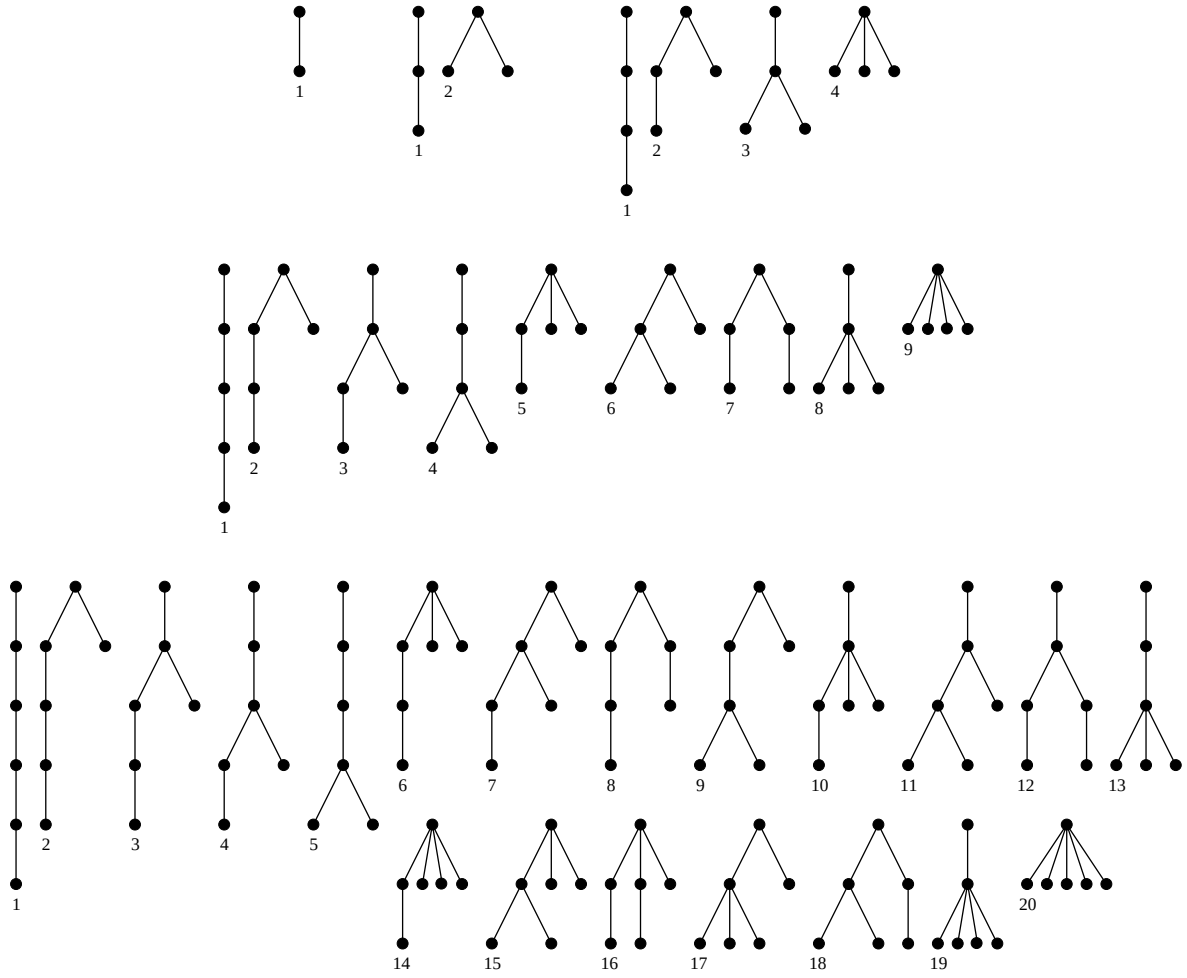
Figur 2.13: Nye ikke-isomorfe, ikke-trivielle 2-MDS-grafer når $n=13$ kanter.

Legg merke til at vi fra figur 2.12 lett kan gi representasjoner også av alle de 18 ikke-isomorfe, ikke-trivielle nesten-MDS-grafene med $n=12$ kanter ved å bruke bijeksjonen i lemma 2.5.31, siden denne kun er avhengig av parametrene $|A|$, $|B|$ og $|C|$.

Til slutt i dette kapittelet vil vi oppsummere telleresultatene for nesten-MDS og 2-MDS-grafer. Følgende tabell gir disse resultatene, med notasjonen $W_{n,i}$ og $N_{n,i}$ introdusert i begynnelsen av kapittelet, og der $T_{n,4}$ angir antall trivielle, ikke-isomorfe 2-MDS-grafer, mens $a=\lceil\frac{n}{3}\rceil$ og $b=\lfloor\frac{n}{2}\rfloor$.

n	2	3	4	5	6	≥ 7
$W_{n,3}$	1	3	6	9	12	$2n-a$
$N_{n,3}$	1	4	9	14	20	$\lfloor \frac{(n+1)^2}{4} \rfloor + \lfloor \frac{(n-a)^2}{4} \rfloor + b + (n-a-b)(a-b)$
$W_{n,4}$	1	3	6	9	12	$2n-a$
$N_{n,4}$	$T_{2,4}$	$T_{3,4}$	$T_{4,4}+3$	$T_{5,4}+5$	$T_{6,4}+8$	$T_{n,4} + \lfloor \frac{(n-a)^2}{4} \rfloor + b + (n-a-b)(a-b)$

Parameteren $T_{n,4}$ i tabellen over er relativt lett å regne ut for små n, men som vi tidligere har nevnt og snart skal se, vil tallet raskt bli stort. Vi vil nå finne antallet for $n \leq 6$, slik at siste rad i tabellen over blir mer komplett.



Figur 2.14: Alle ikke-isomorfe, rotede trær for $1 \leq n \leq 5$, der roten er øverste hjørne i hver graf og retningen nedover for alle kantene.

Dersom vi lar R_i være antall ikke-isomorfe, rotede trær og lar $\Sigma_i = \sum_{j=1}^{R_i} j$, er det relativt lett å se, ved symmetribetraktninger på i-kretser for $1 \leq i \leq n-1$, at vi får følgende uttrykk

for $T_{n,4}$:

$$\begin{aligned}
T_{2,4} &= (R_1),\\
T_{3,4} &= (R_2)+(R_1),\\
T_{4,4} &= (R_3)+(R_2+\Sigma_1)+(R_1),\\
T_{5,4} &= (R_4)+(R_3+R_2R_1)+(R_2+\Sigma_1)+(R_1),\\
T_{6,4} &= (R_5)+(R_4+R_3R_1+\Sigma_2)+\left(R_3+R_2R_1+\left(R_1^2+\tbinom{R_1}{3}\right)\right)\\
&\quad +(R_2+2\Sigma_1)+(R_1).
\end{aligned}$$

(Parentesene er her ordnet slik at parentes nummer i svarer til antall trivielle, ikke-isomorfe 2-MDS-grafer med en i-krets, altså med vekthierarki lik $\{i\}$. Uttrykket $\left(R_1^2+\binom{R_1}{3}\right)$ gir antall ikke-isomorfe grafer vi får ved å "feste" nøyaktig ett rotet tre med $n=1$ til hvert hjørne i en 3-krets. I og med at vi åpenbart har $R_1=1$, er det i vårt tilfelle lett å se at vi kun kan få én slik graf.) Alle ikke-isomorfe, rotede trær med $n\leq 5$ er gitt på figur 2.14, altså har vi $R_1=1$, $R_2=2$, $R_3=4$, $R_4=9$ og $R_5=20$. Totalt kan dette summeres opp i følgende tabell:

n	2	3	4	5	6	≥ 7
$T_{n,4}$	1	3	8	19	48	–
$N_{n,4}$	1	3	11	24	56	$T_{n,4}+\left\lfloor\frac{(n-a)^2}{4}\right\rfloor+b+(n-a-b)(a-b)$

Som vi ser, begynner antall grafer å bli temmelig stort allerede for $n=6$.

2.6 Mulige veier videre

I lys av Kuratowskis teorem (teorem 1.2.1) kunne det være interessant å studere eventuelle begrensninger for MDS-egenskapene til en G-konfigurasjon, gitt MDS-egenskapene til grafen G. Anta at grafen G er h_G-MDS og at H er en G-konfigurasjon som er h_H-MDS. En ikke unaturlig formodning er at vi da har $h_H\geq h_G$ og $S(H)\geq S(G)$. Dersom dette er riktig, ville proposisjon 2.5.27 fulgt direkte fra Kuratowskis teorem, siden K_5 er 4-MDS, $K_{3,3}$ er 3-MDS og $S(K_5)=S(K_{3,3})=2$. Videre er det da naturlig å anta at vi heller ikke kan ha $h_H=h_G$ eller $S(H)=S(G)$ dersom G er K_5 eller $K_{3,3}$ og $H\ncong G$, ut fra "komplettheten" og symmetrien til disse grafene. I så fall ville vi få at K_5 og $K_{3,3}$ er de eneste ikke-planare grafene med Singletondefekt 2, mens $K_{3,3}$ er den eneste ikke-planare 3-MDS-grafen.

Videre kan vi se om telleresultatene i kapittel 2.5.4 lar seg direkte overføre til å gi antall ikke-isomorfe grafiske matroider med korresponderende MDS-egenskaper, eller eventuelt om vi kan bruke disse resultatene til å finne dette. Det er lett å se at isomorfe grafer har isomorfe kretsmatroider, men det motsatte gjelder ikke generelt. Vi vet derfor at grafresultatene gir en øvre grense for det korresponderende antallet grafiske matroider. Et sentralt resultat i denne sammenhengen vil antagelig være Whitneys 2-isomorfisme-teorem, gitt som teorem 5.3.1 i [O].

Kapittel 3

Trelliser fra lineære koder

I dette kapittelet vil vi definere trelliser, som er et spesialtilfelle av en kantvektet digraf, og vi ser på hvordan vi konstruerer trelliser fra koder. Særlig vil vi studere den minimale trellisen til en kode. Denne eksisterer for vilkårlige blokk-koder (se [M]), men vi begrenser oss, som vi har gjort tidligere i oppgaven, til lineære koder. Vi vil vise en relativt enkel konstruksjon av den minimale trellisen til en lineær kode, og fra dette vise at mye informasjon om den minimale trellisen er gitt ved generator- eller paritetssjekkmatroiden for koden, noe som for en del også er gjort i [C]. Minimale trelliser er ikke entydige, opp til kodeekvivalens, derfor vil vi studere hvordan ulike koordinatpermutasjoner gir minimale trelliser av ulik størrelse. Vi vil også se på begrensninger for størrelsen til trelliser fra MDS- og nær-MDS-koder. Til slutt tar vi med en begrunnelse for hvorfor det i praksis kan være interessant å minimere størrelsen til trelliser fra koder, ved å se på den såkalte Viterbi-algoritmen og hvordan denne fungerer bedre jo mindre trellisen er.

3.1 Den minimale trellisen til en kode

Før vi definerer trelliser, vil vi innføre begrepene første og siste base, både for matroider og koder. Proposisjon 3.1.1 og påfølgende algoritmiske bevis gir oss både eksistensen av disse og framgangsmåten for å finne dem:

Proposisjon 3.1.1. *La $M = (S, \mathcal{I})$ være en matroide, og la S være totalt ordnet. Da har vi følgende:*

i) Det eksisterer en base $A = \{a_1, a_2, \ldots, a_r\}$ for M med $a_1 < a_2 < \cdots < a_r$ slik at vi for enhver base $X = \{x_1, x_2, \ldots, x_r\}$ for M med $x_1 < x_2 < \cdots < x_r$, har $a_i \leq x_i$ for alle $1 \leq i \leq r$.

ii) Det eksisterer en base $B = \{b_1, b_2, \ldots, b_r\}$ for M med $b_1 < b_2 < \cdots < b_r$ slik at vi for enhver base $X = \{x_1, x_2, \ldots, x_r\}$ for M med $x_1 < x_2 < \cdots < x_r$, har $x_i \leq b_i$ for alle $1 \leq i \leq r$.

Bevis. Vi vil vise at vi får basene A og B fra følgende enkle grådig-algoritme:

For $1 \leq i \leq r$, la a_i være det minste elementet i S slik at $\{a_1, a_2, \ldots, a_i\} \in \mathcal{I}$, og la b_{r-i+1} være det største elementet i S slik at $\{b_{r-i+1}, b_{r-i+2}, \ldots, b_r\} \in \mathcal{I}$.

I det følgende benytter vi oss av matroideegenskapene (I1)−(I3), slik de er gitt i definisjon 1.3.1.

i) La $A = \{a_1, a_2, \ldots, a_r\}$ være gitt ved denne algoritmen, og anta, for å oppnå en selvmotsigelse, at $X = \{x_1, x_2, \ldots, x_r\}$ er en annen base med $x_1 < x_2 < \cdots < x_r$, og slik at $x_i < a_i$ for én $1 \leq i \leq r$. La så $A_{i-1} = \{a_1, a_2, \ldots, a_{i-1}\} \subseteq A \in \mathcal{I}$ og $X_i = \{x_1, x_2, \ldots, x_i\} \subseteq X \in \mathcal{I}$. Da gir (I2) (eller eventuelt (I2) *og* (I1) dersom $i = 1$) at $A_{i-1}, X_i \in \mathcal{I}$, og vi har $|A_{i-1}| < |X_i|$. Men ifølge (I3) eksisterer det da et element $x \in X_i \setminus A_{i-1}$ slik at $A_{i-1} \cup \{x\} \in \mathcal{I}$. Men dette motsier grådig-algoritmen, siden vi har $x \leq x_i < a_i$.

ii) La $B = \{b_1, b_2, \ldots, b_r\}$ være gitt ved denne algoritmen, og anta, for igjen å oppnå en selvmotsigelse, at $X = \{x_1, x_2, \ldots, x_r\}$ er en annen base med $x_1 < x_2 < \cdots < x_r$, og slik at $b_i < x_i$ for én $1 \leq i \leq r$. Ved å la $B_{i+1} = \{b_{i+1}, b_{i+2}, \ldots, b_r\} \subseteq B \in \mathcal{I}$ og $X_i = \{x_i, x_{i+1}, \ldots, x_r\} \subseteq X \in \mathcal{I}$ oppnår vi da en lignende selvmotsigelse som i beviset for *i*). □

Som antydet, vil vi kalle basene A og B fra forrige proposisjon for henholdsvis **første base** og **siste base** for matroiden M.

Merk at isomorfe matroider kan ha ulike baser A og B, siden en bijeksjon på grunnmengdene kan endre ordningen av elementene.

Vi får umiddelbart følgende resultat:

Korollar 3.1.2. *La $M = (S, \mathcal{B})$ være en matroide med første base A og siste base B. Da er første og siste base for M^* gitt ved henholdsvis $A^* = S \setminus B$ og $B^* = S \setminus A$.*

□

Vi kan også definere første og siste base for en lineær kode:

Definisjon 3.1.3. ***Første base*** *og* ***siste base*** *for en lineær kode C med generatormatrise G er henholdsvis første og siste base for generatormatroiden $M[G]$ for C, der den totale ordningen på grunnmengden til $M[G]$ er gitt ved indekseringen til kolonnene i G.*

Når vi snakker om første og siste base for lineære koder, vil vi derfor bruke parameteren k, dimensjonen til koden, som kardinaliteten til basene.

Som bemerket etter proposisjon 2.2.2 korresponderer dualitetsbegrepene for matroider og koder. Dermed gir korollar 3.1.2 også første og siste base for dualkoder.

Dersom vi rekkereduserer generatormatrisen G på vanlig måte, får vi at første base for koden er gitt ved indeksene til pivotkolonnene til G. Dersom vi i stedet rekkereduserer fra høyre mot venstre, får vi at siste base for koden er gitt ved indeksene til disse pivotkolonnene.

Legg merke til at siden isomorfe matroider kan ha ulike baser A og B, vil altså ekvivalente koder også kunne ha ulike baser A og B.

La oss nå definere en trellis:

Definisjon 3.1.4. *En* ***trellis*** *T er en kantvektet digraf der hjørnene og kantene kommer i* ***lag****, $V_0, V_1, \ldots, V_n$ og $E_{0,1}, E_{1,2}, \ldots, E_{n-1,n}$, for én $n \in \mathbb{N}$, og kanter i $E_{i-1,i}$ har starthjørne i V_{i-1} og slutthjørne i V_i for alle $1 \leq i \leq n$. Videre er $|V_0| = |V_n| = 1$, og hjørnet v_a i V_0 kalles* ***kilden****, mens hjørnet v_z i V_n kalles* ***målet****.*

Vi skriver $w(e)$ for vekten til kanten $e \in E(T)$.

Merk at når vi i det følgende framstiller trelliser grafisk, vil vi la hjørnelagene gå i stigende rekkefølge fra venstre mot høyre. Altså vil alle kantene være rettet fra venstre mot høyre, og vi vil derfor unnlate å gi kantretningene på figurene.

En rettet sti fra kilden til målet i en trellis kaller vi en ***a-z*-sti**. Enhver a-z-sti har dermed lengde n, og kantvektene gir et **ord** av lengde n. Vi sier at en trellis er **én-til-én** dersom ulike a-z-stier gir ulike ord.

Vi innfører notasjonen $\delta_{ut}(v)$ for antall kanter som har starthjørne v i en trellis og tilsvarende $\delta_{inn}(v)$ for antall kanter som har slutthjørne v. Vi sier at det er $\delta_{ut}(v)-1$ **forgreininger** og $\delta_{inn}(v)-1$ **sammenføyninger** i v, med konvensjonen at vi lar antall sammenføyninger i kilden og antall forgreininger i målet være lik 0, ikke -1. (Merk at vi forutsetter at $\delta_{ut}(v), \delta_{inn}(v) \geq 1$ for alle $v \in V(T) \setminus \{v_a, v_z\}$.) En viktig parameter for en trellis T er **forgreiningsindeksen** $\varepsilon(T)$, som gir det totale antall forgreininger i T. Vi får

$$\begin{aligned}
\varepsilon(T) &= \sum_{i=0}^{n-1} \sum_{v \in V_i} (\delta_{ut}(v) - 1) \\
&= \left(\sum_{i=0}^{n-1} \sum_{v \in V_i} \delta_{ut}(v) \right) - (|V(T)| - 1) \\
&= |E(T)| - |V(T)| + 1.
\end{aligned}$$

Det er lett å se at forgreiningsindeksen også gir det totale antall sammenføyninger i T, og siden enhver trellis er sammenhengende, er altså forgreiningsindeksen også lik kretsrangen k til den underliggende grafen til trellisen.

To trelliser T og T' er **isomorfe** dersom det eksisterer en én-til-én-korrespondanse $f : V(T) \to V(T')$ slik at $f(V_i) = V_i'$, og $e = (v_i, v_j)$ er en kant med vekt w i T hvis og bare hvis $e' = (f(v_i), f(v_j))$ er en kant med vekt w i T'.

Overgangen mellom trelliser og koder er ganske enkelt følgende:

Definisjon 3.1.5. *La T være en én-til-én trellis, og la C være mengden av alle ord som kommer fra a-z-stier i T. Da kaller vi C **koden representert av T**.*

Dersom trellisen T representerer koden C, vil altså kodens alfabet være den samme (endelige) mengden som gir kantvektene i trellisen. Som vi ser, omfatter definisjon 3.1.5 enhver blokk-kode, men vi vil i det følgende begrense oss til å se på trelliser som representerer lineære koder.

Legg merke til at enhver kode C er representert av minst én én-til-én trellis, bare ved å la trellisen bestå av $|C|$ kant-disjunkte a-z-stier med kun kilden og målet som felles hjørner, der hver sti representerer et kodeord. I praksis er det imidlertid oftest best å finne en minst mulig trellis som representerer koden, som vi skal se i kapittel 3.6. Det neste teoremet, formulert av Muder, viser at det eksisterer en trellis som er uniformt minst i antall hjørner, og vi skal senere se at denne også har andre gode egenskaper:

Teorem 3.1.6. *La C være en $[n, k]$-kode. Da eksisterer det en trellis T (med hjørnelag $V_0, V_1, \ldots, V_n$) som representerer C, slik at for enhver annen trellis T' (med hjørnelag $V_0', V_1', \ldots, V_n'$) som representerer C, har vi $|V_i| \leq |V_i'|$ for $0 \leq i \leq n$. Videre er T og T' isomorfe dersom vi har likhet for alle i.*

Bevis. Se teorem 1 i [M]. □

Vi kaller trellisen i forrige teorem for **den minimale trellisen** til en kode, som altså er entydig opp til trellisisomorfi. Videre vil vi presentere en konstruksjon som gir denne, for en

vilkårlig lineær kode. Konstruksjonen ble først introdusert av Forney i tillegg A i [F] og er som følger:

La C være en $[n,k]$-kode. Vi definerer **den i-te venstre delkoden** til C som

$$L_i \;=\; \{\underline{c}=(c_1,c_2,\ldots,c_n)\in C \,|\, c_j=0 \text{ for alle } j>i\}$$

og **den i-te høyre delkoden** til C som

$$R_i \;=\; \{\underline{c}=(c_1,c_2,\ldots,c_n)\in C \,|\, c_j=0 \text{ for alle } j\le i\}$$

for $0\le i\le n$, med konvensjonen $L_n=R_0=C$. Vi lar så hjørnene i det i-te laget i trellisen T være elementene i kvotientrommet

$$V_i \;=\; \frac{C}{L_i\oplus R_i},$$

altså elementene i restklassene til $L_i\oplus R_i$ i C. For hvert kodeord $\underline{c}\in C$ lar vi det gå en kant med vekt c_i fra restklassen $(L_{i-1}\oplus R_{i-1})+\underline{c}\in V_{i-1}$ til restklassen $(L_i\oplus R_i)+\underline{c}\in V_i$ og identifiserer med hverandre kanter med samme vekt som har samme start- og slutthjørner.

Da får vi følgende:

Proposisjon 3.1.7. *Trellisen i konstruksjonen ovenfor er den minimale trellisen til koden C.*

Bevis. Siden vi har $L_i\cap R_i=\{\underline{0}\}$ for $0\le i\le n$, får vi $|L_i\oplus R_i|=|L_i|\cdot|R_i|$. Dette gir at vi for trellisen i konstruksjonen ovenfor har

$$|V_i| \;=\; \left|\tfrac{C}{L_i\oplus R_i}\right| \;=\; \tfrac{|C|}{|L_i\oplus R_i|} \;=\; \tfrac{|C|}{|L_i|\cdot|R_i|} \;=\; q^{k-\dim L_i-\dim R_i}.$$

Vi vil vise at vi for enhver annen trellis som representerer C må ha $|V_i|\ge q^{k-\dim L_i-\dim R_i}$.

La så T, med hjørnelag V_i for $0\le i\le n$, være en vilkårlig trellis som representerer C. For én i, og for $v\in V_i$, lar vi l_v være antall ulike stier fra kilden i T til v, og r_v være antall ulike stier fra v til målet i T. Da får vi

$$\sum_{v\in V_i} l_v r_v \;=\; q^k. \tag{3.1}$$

Anta så, for å oppnå en selvmotsigelse, at $|V_i|<q^{k-\dim L_i-\dim R_i}$. Da må vi ha $l_{v_0}>q^{\dim L_i}$ eller $r_{v_0}>q^{\dim R_i}$ for én $v_0\in V_i$, for hvis ikke, får vi

$$\textstyle\sum_{v\in V_i} l_v r_v \;\le\; |V_i|\cdot q^{\dim L_i}\cdot q^{\dim R_i} \;<\; q^k,$$

som motsier uttrykket (3.1). Ved symmetri kan vi anta at vi har $l_{v_0}>q^{\dim L_i}$. La så C' være mengden av ord som er sammensatt av stier fra kilden i T til v_0 og én fiksert sti videre fra v_0 til målet i T. Dermed har vi $C'\subseteq C$ og $|C'|>q^{\dim L_i}$, og for hvert par av kodeord $c_1,c_2\in C'$, har vi $c_1-c_2\in L_i$, altså er $c_1\equiv c_2(\mathrm{mod}\ L_i)$. Men da har vi en restklasse relativt til L_i som har flere elementer enn L_i, altså en selvmotsigelse, ved Lagranges teorem for undergrupper. □

La oss gi et eksempel på en minimal trellis til en kode:

Eksempel 3.1.8. *Den binære Hammingkoden* $C = Ham(3,2)$ *(se for eksempel kapittel* 8 *i* [H] *for definisjon) er gitt ved paritetssjekkmatrisen*

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

Ved bemerkningen etter teorem 1.4.18 *har* C *generatormatrise*

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

som igjen gir

$$C = \left\{ \begin{array}{cccc} \underline{c}_0 = (0000000), & \underline{c}_1 = (1000011), & \underline{c}_2 = (0100101), & \underline{c}_3 = (0010110) \\ \underline{c}_4 = (0001111), & \underline{c}_5 = (1100110), & \underline{c}_6 = (1010101), & \underline{c}_7 = (1001100) \\ \underline{c}_8 = (0110011), & \underline{c}_9 = (0101010), & \underline{c}_{10} = (0011001), & \underline{c}_{11} = (1110000) \\ \underline{c}_{12} = (1101001), & \underline{c}_{13} = (1011010), & \underline{c}_{14} = (0111100), & \underline{c}_{15} = (1111111) \end{array} \right\}.$$

Vi får derfor følgende venstre og høyre delkoder:

$$\begin{array}{lcl@{\qquad}lcl} L_0 &=& \{\underline{c}_0\}, & R_0 &=& C, \\ L_1 &=& \{\underline{c}_0\}, & R_1 &=& \{\underline{c}_0, \underline{c}_2, \underline{c}_3, \underline{c}_4, \underline{c}_8, \underline{c}_9, \underline{c}_{10}, \underline{c}_{14}\}, \\ L_2 &=& \{\underline{c}_0\}, & R_2 &=& \{\underline{c}_0, \underline{c}_3, \underline{c}_4, \underline{c}_{10}\}, \\ L_3 &=& \{\underline{c}_0, \underline{c}_{11}\}, & R_3 &=& \{\underline{c}_0, \underline{c}_4\}, \\ L_4 &=& \{\underline{c}_0, \underline{c}_{11}\}, & R_4 &=& \{\underline{c}_0\}, \\ L_5 &=& \{\underline{c}_0, \underline{c}_7, \underline{c}_{11}, \underline{c}_{14}\}, & R_5 &=& \{\underline{c}_0\}, \\ L_6 &=& \{\underline{c}_0, \underline{c}_3, \underline{c}_5, \underline{c}_7, \underline{c}_9, \underline{c}_{11}, \underline{c}_{13}, \underline{c}_{14}\}, & R_6 &=& \{\underline{c}_0\}, \\ L_7 &=& C. & R_7 &=& \{\underline{c}_0\}. \end{array}$$

Siden vi har $L_0 = L_1 = L_2 = R_4 = R_5 = R_6 = R_7 = \{\underline{c}_0\} = \{\underline{0}\}$*, får vi* $L_i \oplus R_i = R_i$ *for* $i = 0, 1, 2$ *og* $L_i \oplus R_i = L_i$ *for* $i = 4, 5, 6, 7$*. I tillegg har vi*

$$L_3 \oplus R_3 = \{\underline{c}_0 + \underline{c}_0, \underline{c}_0 + \underline{c}_4, \underline{c}_{11} + \underline{c}_0, \underline{c}_{11} + \underline{c}_4\} = \{\underline{c}_0, \underline{c}_4, \underline{c}_{11}, \underline{c}_{15}\}.$$

Totalt gir dette altså:

$$\begin{aligned} L_0 \oplus R_0 &= C, \\ L_1 \oplus R_1 &= \{\underline{c}_0, \underline{c}_2, \underline{c}_3, \underline{c}_4, \underline{c}_8, \underline{c}_9, \underline{c}_{10}, \underline{c}_{14}\}, \\ L_2 \oplus R_2 &= \{\underline{c}_0, \underline{c}_3, \underline{c}_4, \underline{c}_{10}\}, \\ L_3 \oplus R_3 &= \{\underline{c}_0, \underline{c}_4, \underline{c}_{11}, \underline{c}_{15}\}, \\ L_4 \oplus R_4 &= \{\underline{c}_0, \underline{c}_{11}\}, \\ L_5 \oplus R_5 &= \{\underline{c}_0, \underline{c}_7, \underline{c}_{11}, \underline{c}_{14}\}, \\ L_6 \oplus R_6 &= \{\underline{c}_0, \underline{c}_3, \underline{c}_5, \underline{c}_7, \underline{c}_9, \underline{c}_{11}, \underline{c}_{13}, \underline{c}_{14}\}, \\ L_7 \oplus R_7 &= C. \end{aligned}$$

I tillegg finner vi følgende restklasser:

$$K_{1,1} = (L_1 \oplus R_1) + \underline{c}_1 = C \setminus (L_1 \oplus R_1).$$

$$\begin{aligned} K_{2,1} &= (L_2 \oplus R_2) + \underline{c}_1 = \{\underline{c}_1, \underline{c}_6, \underline{c}_7, \underline{c}_{13}\}, \\ K_{2,2} &= (L_2 \oplus R_2) + \underline{c}_2 = \{\underline{c}_2, \underline{c}_8, \underline{c}_9, \underline{c}_{14}\}, \\ K_{2,3} &= (L_2 \oplus R_2) + \underline{c}_5 = \{\underline{c}_5, \underline{c}_{11}, \underline{c}_{12}, \underline{c}_{15}\}. \end{aligned}$$

$$\begin{aligned} K_{3,1} &= (L_3 \oplus R_3) + \underline{c}_1 = \{\underline{c}_1, \underline{c}_7, \underline{c}_8, \underline{c}_{14}\}, \\ K_{3,2} &= (L_3 \oplus R_3) + \underline{c}_2 = \{\underline{c}_2, \underline{c}_6, \underline{c}_9, \underline{c}_{13}\}, \\ K_{3,3} &= (L_3 \oplus R_3) + \underline{c}_3 = \{\underline{c}_3, \underline{c}_5, \underline{c}_{10}, \underline{c}_{12}\}. \end{aligned}$$

$$\begin{aligned} K_{4,1} &= (L_4 \oplus R_4) + \underline{c}_1 = \{\underline{c}_1, \underline{c}_8\}, \\ K_{4,2} &= (L_4 \oplus R_4) + \underline{c}_2 = \{\underline{c}_2, \underline{c}_6\}, \\ K_{4,3} &= (L_4 \oplus R_4) + \underline{c}_3 = \{\underline{c}_3, \underline{c}_5\}, \\ K_{4,4} &= (L_4 \oplus R_4) + \underline{c}_4 = \{\underline{c}_4, \underline{c}_{15}\}, \\ K_{4,5} &= (L_4 \oplus R_4) + \underline{c}_7 = \{\underline{c}_7, \underline{c}_{14}\}, \\ K_{4,6} &= (L_4 \oplus R_4) + \underline{c}_9 = \{\underline{c}_9, \underline{c}_{13}\}, \\ K_{4,7} &= (L_4 \oplus R_4) + \underline{c}_{10} = \{\underline{c}_{10}, \underline{c}_{12}\}. \end{aligned}$$

$$\begin{aligned} K_{5,1} &= (L_5 \oplus R_5) + \underline{c}_1 = \{\underline{c}_1, \underline{c}_4, \underline{c}_8, \underline{c}_{15}\}, \\ K_{5,2} &= (L_5 \oplus R_5) + \underline{c}_2 = \{\underline{c}_2, \underline{c}_6, \underline{c}_{10}, \underline{c}_{12}\}, \\ K_{5,3} &= (L_5 \oplus R_5) + \underline{c}_3 = \{\underline{c}_3, \underline{c}_5, \underline{c}_9, \underline{c}_{13}\}. \end{aligned}$$

$$K_{6,1} = (L_6 \oplus R_6) + \underline{c}_1 = C \setminus (L_6 \oplus R_6).$$

Nå har vi nok informasjon til å konstruere den minimale trellisen til C, og hvis vi lar hjørne $v_{i,0} = L_i \oplus R_i$ for $0 \leq i \leq 7$ og hjørne $v_{i,j} = K_{i,j}$ for alle $K_{i,j}$ listet opp ovenfor, får vi trellisen på figur 3.1.

Den minimale trellisen viser seg ikke bare å være minimal med hensyn til antall hjørner, men også antall kanter og forgreiningsindeksen blir minimert:

Teorem 3.1.9. *La C være en $[n,k]$-kode. La T (med kantlag $E_{0,1}, E_{1,2}, \ldots, E_{n-1,n}$) være den minimale trellisen til C, og la T' (med kantlag ${E_{0,1}}', {E_{1,2}}', \ldots, {E_{n-1,n}}'$) være en vilkårlig annen trellis som representerer C. Da har vi følgende, for $1 \leq i \leq n$:*

i) $|E_{i-1,i}| \leq |{E_{i-1,i}}'|$.

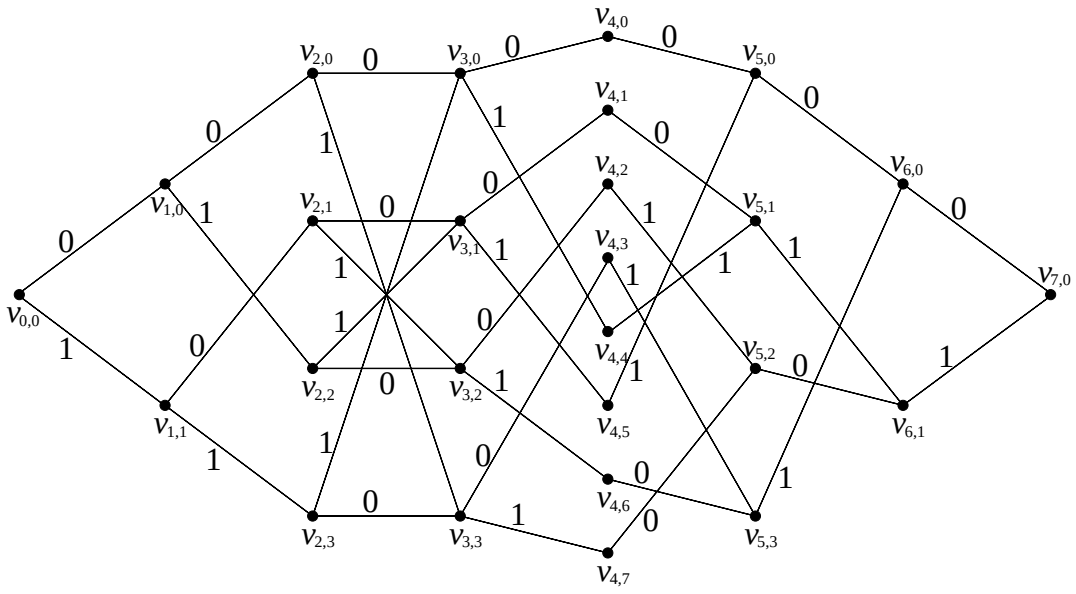
ii) Dersom $|E_{i-1,i}| = |{E_{i-1,i}}'|$ for alle i, er T og T' isomorfe.

Bevis. Se teorem 5.1 i [McE]. (McEliece viser her at både teorem 3.1.6 og 3.1.9 holder for den såkalte BCJR-trellisen for en kode C, altså er BCJR-trellisen til C og den minimale trellisen til C isomorfe, og teorem 3.1.9 holder.) □

Teorem 3.1.10. *La C være en $[n,k]$-kode med minimal trellis T, og la T' være en vilkårlig annen trellis som representerer C. Da har vi*

$$\varepsilon(T) \leq \varepsilon(T').$$

Bevis. Se korollar 7 i [VK]. □



Figur 3.1: Den minimale trellisen til Hammingkoden C i eksempel 3.1.8.

3.2 Matroideegenskaper ved den minimale trellisen

Konstruksjonen av den minimale trellisen gir oss at kardinaliteten til hjørne- og kantlagene i trellisen er gitt ut fra kjennskap til første og siste base for koden, altså informasjon som vi får fra generatormatroiden. Neste resultat, hentet fra [C], viser denne sammenhengen og danner grunnlaget for de fleste resultater videre i kapittel 3:

Proposisjon 3.2.1. *La C være en q-ær $[n,k]$-kode med første base A og siste base B. Da er kardinaliteten til hjørne- og kantlagene i den minimale trellisen til C gitt ved*

$$|V_i| = q^{|A\cap\{1,2,\ldots,i\}|-|B\cap\{1,2,\ldots,i\}|} \quad \textit{for } 0\le i\le n, \tag{3.2}$$

$$|E_{i-1,i}| = q^{|A\cap\{1,2,\ldots,i\}|-|B\cap\{1,2,\ldots,i-1\}|} \quad \textit{for } 1\le i\le n. \tag{3.3}$$

Bevis. La C være gitt ved en generatormatrise G på trappeform. Vi får da at den i-te høyre delkoden R_i er utspent av rekkene i G med ledende enere til høyre for i. Som tidligere bemerket, er første base A gitt ved indeksene til pivotkolonnene i G. Altså er dimensjonen til R_i

$$|A\cap\{i+1,i+2,\ldots,n\}| = k-|A\cap\{1,2,\ldots,i\}|.$$

Motsatt, hvis vi lar G være gitt på trappeform fra høyre mot venstre, er den i-te venstre delkoden L_i utspent av rekkene i G med ledende enere til venstre for $i+1$. Siden siste base B er gitt ved indeksene til de nye pivotkolonnene i G, er dimensjonen til L_i

$$|B\cap\{1,2,\ldots,i\}|.$$

Som vi har sett tidligere, er $|L_i \oplus R_i| = |L_i| \cdot |R_i|$. Vi får derfor

$$\begin{aligned} |V_i| &= \left| \frac{C}{L_i \oplus R_i} \right| \\ &= \frac{|C|}{|L_i \oplus R_i|} \\ &= \frac{|C|}{|L_i| \cdot |R_i|} \\ &= \frac{q^k}{q^{|B \cap \{1,2,\ldots,i\}|} \cdot q^{k-|A \cap \{1,2,\ldots,i\}|}} \\ &= q^{k-|B \cap \{1,2,\ldots,i\}|-(k-|A \cap \{1,2,\ldots,i\}|)} \\ &= q^{|A \cap \{1,2,\ldots,i\}|-|B \cap \{1,2,\ldots,i\}|}. \end{aligned}$$

Det totale antall ulike (rettede) stier fra kilden i den minimale trellisen og fram til hjørnet som tilsvarer $L_i \oplus R_i$ i V_i, er gitt ved det totale antall kodeord $\underline{c} = (c_1, c_2, \ldots, c_n) \in C$ som har $c_j = 0$ for alle $j > i$, altså $|L_i|$, siden den unike stien fra hjørnelag V_i til målet med vekt 0 for hver kant, går fra dette hjørnet. Ved lineariteten til C vil derfor $|L_i|$ også gi det totale antall ulike stier fra kilden og fram til et vilkårlig hjørne i V_i. Tilsvarende vil $|R_i|$ gi det totale antall ulike stier fra et vilkårlig hjørne i V_i og fram til målet i trellisen.

Fra dette får vi

$$|C| = |L_{i-1}| \cdot |E_{i-1,i}| \cdot |R_i|,$$

som igjen gir

$$\begin{aligned} |E_{i-1,i}| &= \frac{|C|}{|L_{i-1}| \cdot |R_i|} \\ &= q^{|A \cap \{1,2,\ldots,i\}|-|B \cap \{1,2,\ldots,i-1\}|}. \end{aligned}$$

□

Legg merke til at vi fra proposisjon 3.2.1 får at ekvivalente koder kan ha minimale trelliser av ulik størrelse, siden, som tidligere bemerket, ekvivalente koder ikke nødvendigvis har samme første og siste baser.

Proposisjon 3.2.1 gir oss følgende sammenhenger mellom første og siste base for en kode og forgreininger og sammenføyninger i den minimale trellisen til koden:

Korollar 3.2.2. *La C være en $[n,k]$-kode med minimal trellis T (med hjørnelag $V_0, V_1, \ldots, V_n$), og la A og B være henholdsvis første og siste base for C. Da har vi:*

i) $\{V_i \,|\, i+1 \in A\} = \{V_i \,|\, \delta_{ut}(v) > 1$ *for alle* $v \in V_i\} = \{V_i \,|\, \delta_{ut}(v) = q$ *for alle* $v \in V_i\}$.

ii) $\{V_i \,|\, i \in B\} = \{V_i \,|\, \delta_{inn}(v) > 1$ *for alle* $v \in V_i\} = \{V_i \,|\, \delta_{inn}(v) = q$ *for alle* $v \in V_i\}$.

iii) $\varepsilon(T) = (q-1)\sum_{i+1 \in A} |V_i| = (q-1)\sum_{i \in B} |V_i|$.

Bevis. i) Ved lineariteten til koden er det nok å se på hjørnet $L_i \oplus R_i \in V_i$ for én $0 \leq i \leq n$. Linearitet gir også at

$$\delta_{ut}(v) > 1 \text{ for alle } v \in V_i \quad \Leftrightarrow \quad \delta_{ut}(v) = q \text{ for alle } v \in V_i,$$

altså er det nok å vise at $i+1 \in A$ er ekvivalent med at $\delta_{ut}(L_i \oplus R_i) > 1$.

Siden $\dim R_i = |A \cap \{i+1, i+2, \ldots, n\}|$ (fra beviset for proposisjon 3.2.1), er $i+1 \in A$ ekvivalent med at $\dim R_i > \dim R_{i+1}$, som igjen er det samme som at det eksisterer en $\underline{c} \in C$ slik at $\underline{c} \in R_i, \underline{c} \notin R_{i+1}$. Siden $\underline{0} \in C$, finnes en kant med starthjørne $L_i \oplus R_i$ som har vekt 0, altså er $\delta_{ut}(L_i \oplus R_i) > 1$ hvis og bare hvis det også eksisterer en kant med starthjørne $L_i \oplus R_i$ som har vekt ulik 0. Men at det eksisterer en $\underline{c} \in C$ slik at $\underline{c} \in R_i$ og $\underline{c} \notin R_{i+1}$ er ekvivalent med at $\underline{c} = (0, 0, \ldots, 0, c_{i+1}, c_{i+2}, \ldots, c_n)$ der $c_{i+1} \neq 0$, som fra konstruksjonen av den minimale trellisen igjen er det samme som at det eksisterer en kant med starthjørne $L_i \oplus R_i$ som har vekt ulik 0.

ii) Beviset er analogt til beviset for del *i*).

iii) Del *i*) gir første likhet direkte, og andre likhet følger av at det totale antall forgreininger i en trellis er lik det totale antall sammenføyninger, kombinert med del *ii*). □

Gitt minimal trellis T for en kode C, kan vi dermed se direkte fra T hva som er første og siste base for C ved å utnytte del *i*) og *ii*) i forrige korollar. Vi finner for eksempel at Hammingkoden i eksempel 3.1.8 har første base $A = \{1, 2, 3, 4\}$ og siste base $B = \{3, 5, 6, 7\}$, direkte fra figur 3.1. Det er lett å sjekke at dette stemmer, ved å studere generatormatrisen G, gitt i samme eksempel.

Vi tar også med en sammenheng mellom en kode og den minimale trellisen til koden, som følger fra proposisjon 3.2.1:

Korollar 3.2.3. *For C, en $[n,k]$-kode med minimal trellis T, gjelder*

$$|C| \;=\; \prod_{i=1}^{n} \frac{|E_{i-1,i}|}{|V_i|}.$$

Bevis. Siden vi har

$$q^{|B\cap\{1,2,\ldots,i\}|-|B\cap\{1,2,\ldots,i-1\}|} \;=\; \begin{cases} q & \text{for } i \in B, \\ 1 & \text{for } i \notin B, \end{cases}$$

gir proposisjon 3.2.1 at vi får

$$\begin{aligned}
\prod_{i=1}^{n} \frac{|E_{i-1,i}|}{|V_i|} &= \prod_{i=1}^{n} \frac{q^{|A\cap\{1,2,\ldots,i\}|-|B\cap\{1,2,\ldots,i-1\}|}}{q^{|A\cap\{1,2,\ldots,i\}|-|B\cap\{1,2,\ldots,i\}|}} \\
&= \prod_{i=1}^{n} q^{|A\cap\{1,2,\ldots,i\}|-|B\cap\{1,2,\ldots,i-1\}|-(|A\cap\{1,2,\ldots,i\}|-|B\cap\{1,2,\ldots,i\}|)} \\
&= \prod_{i=1}^{n} q^{|B\cap\{1,2,\ldots,i\}|-|B\cap\{1,2,\ldots,i-1\}|} \\
&= \prod_{i\in B} q \\
&= q^k \\
&= |C|.
\end{aligned}$$

□

3.3 Trellis-maksimale koder

Fordi første base ikke kan komme tidligere enn $A = \{1, 2, \ldots, k\}$, og siste base ikke kan komme senere enn $B = \{n-k+1, n-k+2, \ldots, n\}$, gir proposisjon 3.2.1 oss en øvre grense for antall hjørner og kanter i den minimale trellisen til en kode:

Proposisjon 3.3.1. *For den minimale trellisen T til en q-ær $[n,k]$-kode, gjelder følgende:*

$$|V(T)| \leq 2\frac{q^{\min\{k,n-k\}}-1}{q-1} + (|n-2k|+1)q^{\min\{k,n-k\}}, \tag{3.4}$$

$$|E(T)| \leq 2q\frac{q^{\min\{k,n-k\}}-1}{q-1} + |n-2k|q^{\min\{k,n-k+1\}}. \tag{3.5}$$

Bevis. Vi vil vise at vi oppnår likhet i disse uttrykkene dersom første og siste base for koden er henholdsvis $A = \{1, 2, \ldots, k\}$ og $B = \{n-k+1, n-k+2, \ldots, n\}$, noe som åpenbart gir en øvre grense, fra proposisjon 3.2.1. Vi antar derfor at koden har disse første og siste basene.

La oss først vise likning (3.4), og vi antar først at vi har $k \leq \frac{n}{2}$. Da gir likning (3.2) i proposisjon 3.2.1 oss at

$$\begin{aligned}
|V(T)| &= |V_0| + |V_1| + \cdots + |V_n| \\
&= q^0 + q^1 + \cdots + q^{k-1} + q^k + q^k + \cdots + q^k + q^{k-1} + q^{k-2} + \cdots + q^0 \\
&= 2\sum_{i=0}^{k-1} q^i + (n-2k+1)q^k \\
&= 2\frac{q^k-1}{q-1} + (n-2k+1)q^k,
\end{aligned}$$

og siden vi har $k \leq \frac{n}{2}$, får vi $k \leq n-k$ og $n-2k \geq 0$, altså gjelder (3.4) i dette tilfellet.

Anta så at $k > \frac{n}{2}$. Da gir likning (3.2) oss at

$$\begin{aligned}
|V(T)| &= |V_0| + |V_1| + \cdots + |V_n| \\
&= q^0 + q^1 + \cdots + q^{n-k-1} + q^{n-k} + q^{n-k} + \cdots + q^{n-k} \\
&\quad + q^{n-k-1} + q^{n-k-2} + \cdots + q^0 \\
&= 2\sum_{i=0}^{n-k-1} q^i + (2k-n+1)q^{n-k} \\
&= 2\frac{q^{n-k}-1}{q-1} + (2k-n+1)q^{n-k},
\end{aligned}$$

og $k > \frac{n}{2}$ gir oss $n-k < k$ og $n-2k < 0$. Dermed gjelder (3.4) også i dette tilfellet.

La oss så vise (3.5), og vi antar igjen først at $k \leq \frac{n}{2}$. Fra likning (3.3) i proposisjon 3.2.1 får vi

$$\begin{aligned}
|E(T)| &= |E_{0,1}| + |E_{1,2}| + \cdots + |E_{n-1,n}| \\
&= q^1 + q^2 + \cdots + q^{k-1} + q^k + q^k + \cdots + q^k + q^{k-1} + q^{k-2} + \cdots + q^1 \\
&= 2q\sum_{i=0}^{k-1} q^i + (n-2k)q^k \\
&= 2q\frac{q^k-1}{q-1} + (n-2k)q^k,
\end{aligned}$$

og vi har $k \leq n-k < n-k+1$ og $n-2k \geq 0$, altså gjelder (3.5) i dette tilfellet.

Dersom $k > \frac{n}{2}$, gir likning (3.3) oss

$$\begin{aligned} |E(T)| &= |E_{0,1}| + |E_{1,2}| + \cdots + |E_{n-1,n}| \\ &= q^1 + q^2 + \cdots + q^{n-k} + q^{n-k+1} + q^{n-k+1} + \cdots + q^{n-k+1} \\ &\quad + q^{n-k} + q^{n-k-1} + \cdots + q^1 \\ &= 2q \sum_{i=0}^{n-k-1} q^i + (2k-n)q^{n-k+1} \\ &= 2q\frac{q^{n-k}-1}{q-1} + (2k-n)q^{n-k+1}, \end{aligned}$$

og vi har $n-k < n-k+1 \leq k$ og $n-2k < 0$, altså gjelder (3.5) også nå. □

Koder som oppfyller likning (3.4) (og dermed også likning (3.5)) med likhet, kaller vi **trellis-maksimale**. Merk at dersom koden C er ekvivalent til en trellis-maksimal kode, trenger ikke C nødvendigvis å være trellis-maksimal. Faktisk er dette bare riktig for MDS-koder, og følgende resultat, formulert av Forney, viser dette:

Teorem 3.3.2. *Følgende er ekvivalent, for en kode C:*

i) C er MDS.

ii) Enhver kode ekvivalent til C er trellis-maksimal.

Bevis. La C være en $[n,k]$-kode. Dersom C er MDS, har vi fra teorem 2.2.3 at generatormatroiden $M[G]$ er den uniforme matroiden $U_{k,n}$, altså vil enhver mengde med k elementer være en base. Dermed er første base $\{1,2,\ldots,k\}$ og siste base $\{n-k+1, n-k+2, \ldots, n\}$, og C er trellis-maksimal.

Motsatt, anta at enhver kode ekvivalent til C er trellis-maksimal, og la $X \subseteq S$ med $|X| = k$, der S er grunnmengden til generatormatroiden $M[G]$. Dersom vi permuterer elementene i S slik at $X = \{1,2,\ldots,k\}$, vil denne matroiden være en generatormatroide for en kode C' ekvivalent til C, og siden C' er trellis-maksimal, er X en base. Siden X er vilkårlig, har vi $M[G] = U_{k,n}$, og teorem 2.2.3 gir igjen at C er MDS. □

3.4 Trellis-optimale koder

Siden ekvivalente koder kan ha minimale trelliser av ulik størrelse, kan vi, gitt en kode C, se på ekvivalensklassen til C og finne koder med minst mulig minimal trellis. Vi har nå ikke lenger noen garanti for at det eksisterer koder som minimerer alle lagene i en trellis, men vi kan likevel definere følgende:

Definisjon 3.4.1. *En lineær kode C med minimal trellis T er **trellis-optimal** dersom vi for enhver ekvivalent kode C' med minimal trellis T' har $|V(T)| \leq |V(T')|$.*

Vi merker oss neste resultat, som følger direkte fra proposisjon 3.2.1 og som gir en ekvivalent definisjon av en trellis-optimal kode:

Korollar 3.4.2. *Følgende er ekvivalent, for en lineær kode C:*

i) C er trellis-optimal.

ii) For enhver ekvivalent kode C' med minimal trellis T', har vi $|E(T)| \leq |E(T')|$.

Bevis. Uttrykkene 3.2 og 3.3 i proposisjon 3.2.1 gir at første og siste base A og B minimerer $|V(T)|$ hvis og bare hvis de også minimerer $|E(T)|$, og siden A og B er entydig gitt for enhver lineær kode, følger resultatet. □

Som vi har sett, er enhver MDS-kode trellis-optimal, men for andre koder er denne definisjonen mer interessant.

Det er generelt noe tidkrevende å finne trellis-optimale koder ut fra det vi hittil har vist, siden man for hver kode i en ekvivalensklasse må rekkeredusere generatormatrisen fra venstre og fra høyre. Med denne metoden går det an å vise at Hammingkoden i eksempel 3.1.8 er trellis-optimal. (For en annen, mer direkte metode, se side 76.) Før vi gir flere eksempler på trellis-optimale koder, introduserer vi derfor et nytt begrep, som for noen koder vil gjøre arbeidet mye mindre tidkrevende:

Definisjon 3.4.3. *La G være en kantmerket graf. En **q-ær lineær kode assosiert til G** er en kode med paritetssjekkmatroide $M(G)$.*

Vi ser at enhver kode med grafisk paritetssjekkmatroide (eventuelt kografisk generatormatroide) er assosiert til en graf, jf. bemerkningen etter proposisjon 1.3.19.

Fra proposisjon 1.3.22 får vi at dersom $A_D{}'$ er hjørne-kant-insidensmatrisen til en retting D av G, redusert modulo q, så vil et maksimalt antall uavhengige rader i $A_D{}'$ danne en paritetssjekkmatrise for en q-ær kode assosiert til G.

Eksempel 3.4.4. *Hjørne-kant-insidensmatrisen A_D til digrafen D på figur 1.3 er gitt i eksempel 1.2.3. Siden rad 1 i A_D er nullvektoren og rad 3 er en lineærkombinasjon av rad 2, 4 og 5, vil en paritetssjekkmatrise H_q for en q-ær lineær kode assosiert til grafen G på samme figur være*

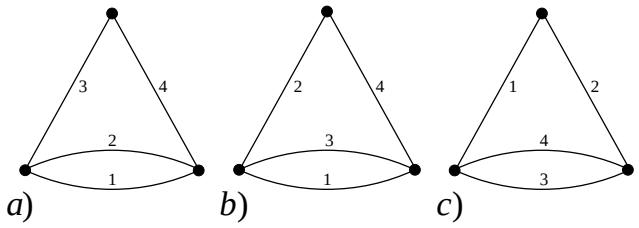
$$H_q = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 \\ 0 & 0 & 1 & 1 & -1 & 0 \end{bmatrix}$$

for $q \geq 3$ og for $q = 2$

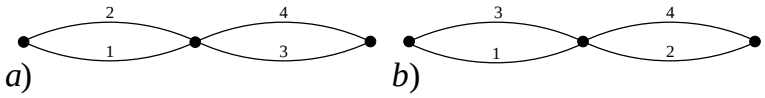
$$H_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Årsaken til at vi gir definisjon 3.4.3 ved paritetssjekkmatroiden og ikke generatormatroiden, er at overgangen fra graf til kode da vil kommutere med definisjonene for parametrene n og k og vekthierarkiet, gitt i kapitlene 1.4 og 2.4.1.

La nå G være en kantmerket graf, og la C være en kode assosiert til G. Vi ser at en permutasjon av koordinater i C vil tilsvare en permutasjon av kantmerkingen til G, mens multiplikasjon av koordinater i C med ikke-null skalarer ikke vil endre paritetssjekkmatroiden, og dermed heller ikke G. Derfor er det, for koder som er assosiert til grafer, nok å studere ulike kantmerkinger av grafen for å finne en ekvivalent, trellis-optimal kode, og generelt er dette enklere enn å studere kodeekvivalensklasser.



Figur 3.2: Ulike merkinger av grafen på figur 2.6*a*.



Figur 3.3: Ulike merkinger av grafen på figur 2.6*b*.

Eksempel 3.4.5. *La oss først finne trellis-optimale koder i ekvivalensklassene til koder assosiert til grafene på figur* 2.6 *(for generell q), altså de to eneste (opp til isomorfi) sammenhengende, ikke-trivielle nær-MDS-grafene med* 4 *kanter. Vi ønsker å finne en eller flere kantmerkinger som gjør at første base for $M(G)$ kommer senest mulig, samtidig som siste base for $M(G)$ kommer tidligst mulig. Oversatt til grafterminologi, vil dette tilsvare kantmerkinger der "første utspennende tre" kommer senest mulig, samtidig som "siste utspennende tre" kommer tidligst mulig, og algoritmen er den samme grådig-algoritmen som i beviset for proposisjon* 3.1.1.

Vi har $k = 2$ for begge grafene, altså består utspennende trær (og dermed baser for $M(G)$) av 2 *kanter.*

La oss starte med grafen på figur 2.6*a. På grunn av symmetri, er det kun $\binom{4}{2} = 6$ mulige ulike merkinger, men kun* 3 *ulike valg for første og siste utspennende tre. Disse er representert på figur* 3.2*. Fra algoritmen får vi første og siste utspennende tre, henholdsvis A og B slik de er gitt i tabellen nedenfor, og disse vil være første og siste base for $M(G)$. Siden $M(G)$ er paritetssjekkmatroiden for kode-ekvivalensklassen vi studerer i dette tilfellet, finner vi samtidig A^* og B^* til de duale matroidene ved hjelp av korollar* 3.1.2*, som dermed vil gi første og siste base for kodene. Totalt får vi:*

$$\begin{array}{lllll} \textit{Figur } 3.2a\text{:} & A = \{1,3\} & B = \{3,4\} & A^* = \{1,2\} & B^* = \{2,4\} \\ \textit{Figur } 3.2b\text{:} & A = \{1,2\} & B = \{3,4\} & A^* = \{1,2\} & B^* = \{3,4\} \\ \textit{Figur } 3.2c\text{:} & A = \{1,2\} & B = \{2,4\} & A^* = \{1,3\} & B^* = \{3,4\} \end{array}$$

Vi får derfor at kodene assosiert til grafene på figur 3.2*a og c er trellis-optimale, og for disse får vi*

$$\begin{array}{rcl} |V(T)| & = & q^0 + q^1 + q^1 + q^1 + q^0 \;=\; 3q + 2, \textit{ og} \\ |E(T)| & = & q^1 + q^1 + q^2 + q^1 \;=\; q(q+3). \end{array}$$

(For 3.2*c er summen av kantlagene, fra venstre mot høyre, lik $q^1+q^2+q^1+q^1$, men det totale antall kanter er selvsagt det samme. Faktisk er disse kodene "speilvendte", det vil si at de fås fra hverandre ved kolonnepermutasjonen $(1,4)(2,3)$, altså vil også de minimale trellisene være "speilvendte", som vi ser på figur* 3.4*.) I tillegg ser vi at koden assosiert til grafen på figur* 3.2*b er trellis-maksimal.*

For grafen på figur 2.6*b, vil tilsvarende argumenter gi kun* 2 *ulike valg for første og siste utspennende trær, og disse er representert på figur* 3.3*. Som for grafen på figur* 2.6*a, kan vi lage følgende tabell:*

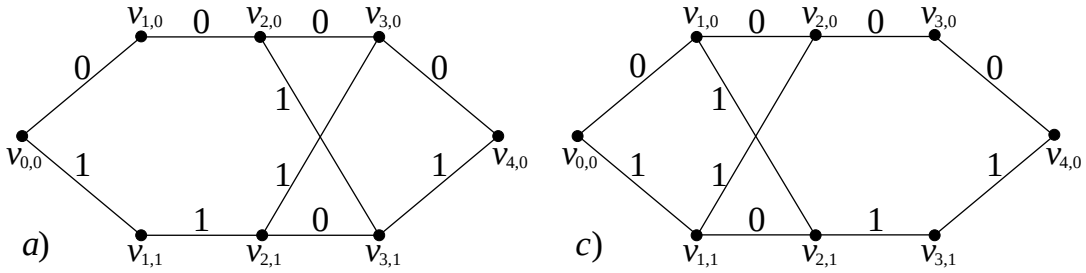
$$\begin{array}{lllll} \textit{Figur } 3.3a\text{:} & A=\{1,3\} & B=\{2,4\} & A^*=\{1,3\} & B^*=\{2,4\} \\ \textit{Figur } 3.3b\text{:} & A=\{1,2\} & B=\{3,4\} & A^*=\{1,2\} & B^*=\{3,4\} \end{array}$$

Altså er koden assosiert til grafen på figur 3.3*a trellis-optimal, og vi får*

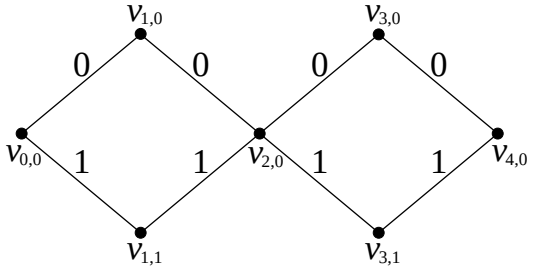
$$\begin{array}{rcrcl} |V(T)| & = & q^0+q^1+q^0+q^1+q^0 & = & 2q+3, \textit{ og} \\ |E(T)| & = & q^1+q^1+q^1+q^1 & = & 4q. \end{array}$$

For helhetens skyld tar vi også med de minimale trellisene til de trellis-optimale kodene, for $q=2$*. Disse er gitt på figurene* 3.4 *og* 3.5*.*

Vi merker oss at dersom man ønsker minst mulig minimal trellis, gitt parametrene $n=4$*,* $k=2$ *og vekthierarkiet* $\{2,4\}$*, gir ekvivalensklassen til kodene assosiert til grafen på figur* 2.6*b bedre resultat enn* 2.6*a. Faktisk skal vi se senere at den minimale trellisen til koden assosiert til grafen på figur* 3.3*a er minst mulig, gitt disse parametrene.*



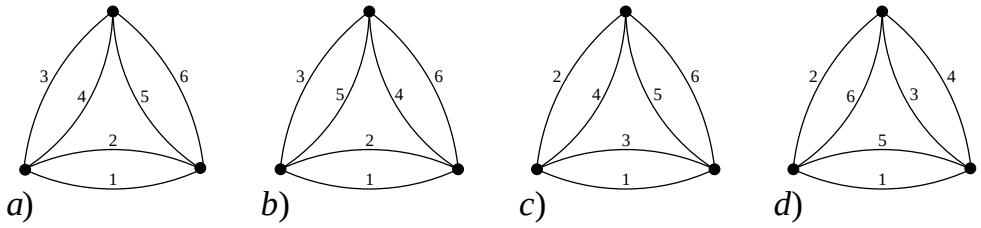
Figur 3.4: De minimale trellisene til kodene assosiert til grafene på figur 3.2*a* og *c*.



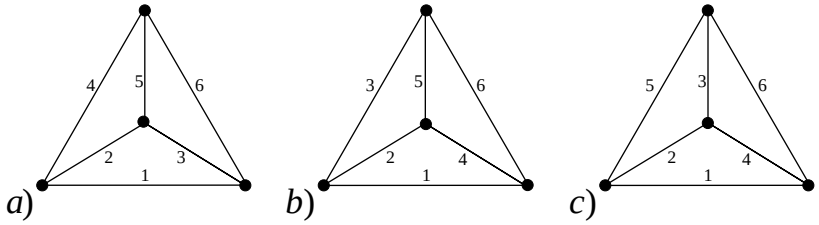
Figur 3.5: Den minimale trellisen til koden assosiert til grafen på figur 3.3*a*.

La oss også studere grafene på figur 2.8:

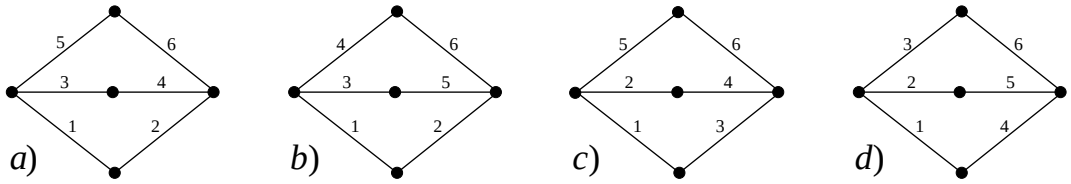
Eksempel 3.4.6. *Det er lett å se at merkingene på figurene* 3.6−3.8 *gir alle mulige valg for første og siste base for grafene på figur* 2.8*. Ved hjelp av grådig-algoritmen beskrevet i beviset for proposisjon* 3.1.1*, finner vi raskt første og siste base* A *og* B *for kretsmatroidene, og ved*



Figur 3.6: Ulike merkinger av grafen på figur 2.8*a*.



Figur 3.7: Ulike merkinger av grafen på figur 2.8*b*.



Figur 3.8: Ulike merkinger av grafen på figur 2.8*c*.

hjelp av korollar 3.1.2 *finner vi også de duale første og siste basene,* A^* *og* B^**, som er de første og siste basene for kodene assosiert til grafene:*

Figur 3.6*a*:	$A = \{1,3\}$	$B = \{4,6\}$	$A^* = \{1,2,3,5\}$	$B^* = \{2,4,5,6\}$
Figur 3.6*b*:	$A = \{1,3\}$	$B = \{5,6\}$	$A^* = \{1,2,3,4\}$	$B^* = \{2,4,5,6\}$
Figur 3.6*c*:	$A = \{1,2\}$	$B = \{4,6\}$	$A^* = \{1,2,3,5\}$	$B^* = \{3,4,5,6\}$
Figur 3.6*d*:	$A = \{1,2\}$	$B = \{5,6\}$	$A^* = \{1,2,3,4\}$	$B^* = \{3,4,5,6\}$

Figur 3.7*a*:	$A = \{1,2,4\}$	$B = \{4,5,6\}$	$A^* = \{1,2,3\}$	$B^* = \{3,5,6\}$
Figur 3.7*b*:	$A = \{1,2,3\}$	$B = \{3,5,6\}$	$A^* = \{1,2,4\}$	$B^* = \{4,5,6\}$
Figur 3.7*c*:	$A = \{1,2,3\}$	$B = \{4,5,6\}$	$A^* = \{1,2,3\}$	$B^* = \{4,5,6\}$

Figur 3.8*a*:	$A = \{1,2,3,5\}$	$B = \{2,4,5,6\}$	$A^* = \{1,3\}$	$B^* = \{4,6\}$
Figur 3.8*b*:	$A = \{1,2,3,4\}$	$B = \{2,4,5,6\}$	$A^* = \{1,3\}$	$B^* = \{5,6\}$
Figur 3.8*c*:	$A = \{1,2,3,5\}$	$B = \{3,4,5,6\}$	$A^* = \{1,2\}$	$B^* = \{4,6\}$
Figur 3.8*d*:	$A = \{1,2,3,4\}$	$B = \{3,4,5,6\}$	$A^* = \{1,2\}$	$B^* = \{5,6\}$

Altså finner vi at kodene assosiert til grafene på figurene 3.6*a,* 3.7*a,* 3.7*b og* 3.8*a er trellis-optimale.*

Det negative med å studere koder som er assosiert til grafer, er selvsagt at koder med grafiske paritetssjekkmatroider er relativt sjeldne. Imidlertid kan vi også finne første og siste base for koder med kografiske paritetssjekkmatroider ved å studere grafer, siden slike koder har grafiske generatormatroider. Vi får da at første og siste base for G er lik henholdsvis første og siste base for C, der G er en graf som korresponderer med generatormatroiden for koden C.

La oss til slutt i dette kapittelet vise hvordan trellis-optimalitet bevares ved dualisering av koden:

Proposisjon 3.4.7. *La C være en q-ær $[n,k]$-kode med minimal trellis T, og la $C^\perp$ ha minimal trellis $T^\perp$. Da gjelder følgende:*

i) $|V_i(T)| = |V_i(T^\perp)|$ *for alle* $1 \leq i \leq n$.

ii) $|V(T)| = |V(T^\perp)|$.

iii) C *er trellis-optimal* $\Leftrightarrow$ $C^\perp$ *er trellis-optimal.*

Bevis. i) For vilkårlige mengder $X_1, X_2 \subseteq S$ har vi

$$(S \setminus X_1) \cap X_2 \;=\; X_2 \setminus (X_1 \cap X_2).$$

Dersom vi kombinerer dette med proposisjon 3.2.1 og korollar 3.1.2 (som tidligere nevnt gjelder korollar 3.1.2 også for duale koder) og lar A, B, $A^\perp$ og $B^\perp$ være henholdsvis første og siste base for C og $C^\perp$, får vi

$$\begin{aligned}
|V_i(T^\perp)| &= q^{|A^\perp \cap \{1,2,\ldots,i\}| - |B^\perp \cap \{1,2,\ldots,i\}|} \\
&= q^{|(\{1,2,\ldots,n\} \setminus B) \cap \{1,2,\ldots,i\}| - |(\{1,2,\ldots,n\} \setminus A) \cap \{1,2,\ldots,i\}|} \\
&= q^{|\{1,2,\ldots,i\} \setminus (B \cap \{1,2,\ldots,i\})| - |\{1,2,\ldots,i\} \setminus (A \cap \{1,2,\ldots,i\})|} \\
&= q^{i - |B \cap \{1,2,\ldots,i\}| - (i - |A \cap \{1,2,\ldots,i\}|)} \\
&= q^{|A \cap \{1,2,\ldots,i\}| - |B \cap \{1,2,\ldots,i\}|} \\
&= |V_i(T)|
\end{aligned}$$

for alle $1 \leq i \leq n$.

ii) Dette følger umiddelbart fra *i)*, siden vi har

$$|V(T)| \;=\; \textstyle\sum_{i=0}^{n} |V_i(T)| \;=\; \sum_{i=0}^{n} |V_i(T^\perp)| \;=\; |V(T^\perp)|.$$

iii) Vi merker oss at siden $(C^\perp)^\perp = C$ for enhver lineær kode C, er det nok å vise én vei i ekvivalensen.

Anta at $C^\perp$ er trellis-optimal, og la C' være en kode ekvivalent til C med minimal trellis T'. Som tidligere nevnt er da $(C')^\perp$ ekvivalent til $C^\perp$, og siden $C^\perp$ er trellis-optimal, har vi $|V(T^\perp)| \leq |V((T')^\perp)|$, der $(T')^\perp$ er den minimale trellisen til $(C')^\perp$. Det følger da fra del *ii)* at vi har $|V(T)| \leq |V(T')|$, altså er C også trellis-optimal. □

For alternativt bevis for del *i)*, se korollaret på side 1185 i [F]. Andre sammenhenger mellom trelliser til duale koder er gitt i kapittel II.A i [KDMEL].

Eksempel 3.4.8. *De merkede grafene på figurene* 3.6*a og* 3.8*a er hverandres geometriske dualer, der kant e_i^* gis merkingen til kant e_i', med notasjonen brukt i konstruksjonen av geometrisk dual til en vilkårlig graf (se side* 4*). Altså er kodene assosiert til grafene hverandres dualer, og som eksempel* 3.4.6 *viser, er begge trellis-optimale.*

3.5 Den minimale trellisen til nær-MDS-koder

Det er lett å sjekke at Hammingkoden i eksempel 3.1.8 er nær-MDS, altså er alle eksemplene vi til nå i dette kapittelet har gitt, av nær-MDS-koder. Vi legger merke til at i alle tilfellene er første base enten $\{1, 2, \ldots, k\}$ eller $\{1, 2, \ldots, k-1, k+1\}$ og siste base enten $\{n-k+1, n-k+2, \ldots, n\}$ eller $\{n-k, n-k+2, n-k+3, \ldots, n\}$. Dette er også de eneste mulige valgene for første og siste base for nær-MDS-koder, noe neste proposisjon viser:

Proposisjon 3.5.1. *La C være en q-ær $[n, k]$-nær-MDS-kode C med første og siste base henholdsvis A og B og minimal trellis T. Da gjelder:*

i) Vi har følgende fire muligheter for A og B:
- *a)* $A = \{1, 2, \ldots, k-1, k+1\}$ *og* $B = \{n-k, n-k+2, n-k+3, \ldots, n\}$.
- *b)* $A = \{1, 2, \ldots, k-1, k+1\}$ *og* $B = \{n-k+1, n-k+2, \ldots, n\}$.
- *c)* $A = \{1, 2, \ldots, k\}$ *og* $B = \{n-k, n-k+2, n-k+3, \ldots, n\}$.
- *d)* $A = \{1, 2, \ldots, k\}$ *og* $B = \{n-k+1, n-k+2, \ldots, n\}$.

ii) Vi har følgende nedre grense for kardinaliteten til hjørne- og kantmengdene til T:

$$|V(T)| \geq \begin{cases} 2\frac{q^k-1}{q-1} + q^{k-2} & \text{for } k = \frac{n}{2}, \\ 2\frac{q^{\min\{k,n-k\}}-1}{q-1} + 2q^{\min\{k,n-k\}-1} & \\ \quad + (|n-2k|-1)q^{\min\{k,n-k\}} & \text{ellers.} \end{cases} \tag{3.6}$$

$$|E(T)| \geq \begin{cases} 2q\frac{q^{k-1}-1}{q-1} + q^{k-2} & \text{for } k = \frac{n+1}{2}, \\ 2q\frac{q^{\min\{k-1,n-k\}}-1}{q-1} + 2q^{\min\{k-1,n-k\}} & \\ \quad + (|n-2k+1|-1)q^{\min\{k,n-k+1\}} & \text{ellers.} \end{cases} \tag{3.7}$$

Videre har vi likhet i begge uttrykk hvis og bare hvis vi har situasjon a) i del i).

iii) Det eksisterer ekvivalensklasser av nær-MDS-koder der:
- *a) Alle fire alternativene i del i) lar seg realisere.*
- *b) Kun alternativene b)−d) i del i) lar seg realisere.*
- *c) Kun alternativene a) og d) i del i) lar seg realisere.*

iv) Dersom alternativ a er mulig i ekvivalensklassen til C, må $\min\{d(C), d(C^\perp)\}$ *være jamn.*

Bevis. i) La G være en generatormatrise for $[n, k]$-nær-MDS-koden C. Vi vil vise at for C vil første base enten være $\{1, 2, \ldots, k\}$ eller $\{1, 2, \ldots, k-1, k+1\}$, og siste base vil enten være $\{n-k+1, n-k+2, \ldots, n\}$ eller $\{n-k, n-k+2, n-k+3, \ldots, n\}$. Dette gjør vi ved å vise følgende to påstander, som til sammen gir resultatet, siden første og siste base finnes ved hjelp av grådig-algoritmen i beviset for proposisjon 3.1.1:

ia) Ethvert valg av $k-1$ kolonner i G er lineært uavhengige.

ib) For ethvert valg av $k-1$ kolonner $\underline{g}_{i_1}, \underline{g}_{i_2}, \ldots, \underline{g}_{i_{k-1}}$ i G, eksisterer maksimalt én annen kolonne $\underline{g}_{i_k}$ i G slik at $\underline{g}_{i_1}, \underline{g}_{i_2}, \ldots, \underline{g}_{i_k}$ er lineært avhengige.

ia) Anta, for å oppnå en selvmotsigelse, at det eksisterer $k-1$ lineært avhengige kolonner i G. Siden G er en paritetssjekkmatrise for $C^\perp$, gir teorem 1.4.19 oss at $d(C^\perp) \leq k-1$. Men vi har også at Singeltondefekten $S(C^\perp) = 1$, som til sammen gir $k-1 \geq d(C^\perp) = n-(n-k)+1-S(C^\perp) = k$, en selvmotsigelse. Altså er påstand *ia*) bevist.

ib) Også her antar vi det motsatte for å oppnå en selvmotsigelse, altså antar vi at det for ett valg av $k-1$ kolonner $\underline{g}_{i_1}, \underline{g}_{i_2}, \ldots, \underline{g}_{i_{k-1}}$ i G eksisterer to ulike kolonner, $\underline{g}_{i_k}$ og $\underline{g}_{i_k}{}'$, slik at både $\underline{g}_{i_1}, \underline{g}_{i_2}, \ldots, \underline{g}_{i_k}$ og $\underline{g}_{i_1}, \underline{g}_{i_2}, \ldots, \underline{g}_{i_{k-1}}, \underline{g}_{i_k}{}'$ er lineært avhengige. Vi lar A være matrisen utspent av de $k-1$ første kolonnene. Da gir *ia*) oss at rangen $\mathrm{rg}(A) = k-1$, og vi har også $\mathrm{rg}([A \,|\, \underline{g}_{i_k} \,|\, \underline{g}_{i_k}{}']) = k-1$. Altså har vi $k+1$ kolonner i G som har rang $k-1$, og siden G er en paritetssjekkmatrise for $C^\perp$, gir teorem 1.4.24 at $d_2(C^\perp) \leq k+1$. Men påstand *ia*) kombinert med teorem 1.4.19 gir $d_1(C^\perp) = k$, og siden $C^\perp$ er nær-MDS, har vi $d_2(C^\perp) = d_1(C^\perp)+2 = k+2$ som er en selvmotsigelse. Dermed er begge påstandene bevist, og del *i*) i proposisjonen følger.

ii) Fra proposisjon 3.2.1 er det klart at blant mulighetene i del *i*) vil *a*) gi ekte mindre verdi både for $|V(T)|$ og $|E(T)|$ enn *b*)−*d*). Del *ii*) vil derfor følge av å vise at vi oppnår likhet i uttrykkene (3.6) og (3.7) dersom vi har alternativ *a*) i del *i*).

La oss begynne med uttrykkene i (3.6), og vi antar at første og siste base for $[n,k]$-nær-MDS-koden C med minimal trellis T er henholdsvis $\{1,2,\ldots,k-1,k+1\}$ og $\{n-k, n-k+1, n-k+2, \ldots, n\}$.

Anta først at $k < \frac{n}{2}$, altså at vi har $k+1 \leq n-k$. Da gir likning (3.2) i proposisjon 3.2.1 følgende:

$$\begin{aligned}
|V(T)| &= |V_0| + |V_1| + \cdots + |V_n| \\
&= q^0 + q^1 + \cdots + q^{k-1} + q^{k-1} + q^k + q^k + \cdots + q^k + q^{k-1} + q^{k-1} + q^{k-2} + \cdots + q^0 \\
&= 2\sum_{i=0}^{k-1} q^i + 2q^{k-1} + (n-2k-1)q^k \\
&= 2\frac{q^k-1}{q-1} + 2q^{k-1} + (n-2k-1)q^k,
\end{aligned}$$

og siden $k < k+1 \leq n-k$ og $n-2k > 0$, gjelder likningen (3.6) i dette tilfellet.

Anta så at $k = \frac{n}{2}$. Likning (3.2) gir da:

$$\begin{aligned}
|V(T)| &= |V_0| + |V_1| + \cdots + |V_n| \\
&= q^0 + q^1 + \cdots + q^{k-1} + q^{k-2} + q^{k-1} + q^{k-2} + \cdots + q^0 \\
&= 2\sum_{i=0}^{k-1} q^i + q^{k-2} \\
&= 2\frac{q^k-1}{q-1} + q^{k-2},
\end{aligned}$$

som stemmer med likning (3.6).

Til slutt antar vi at $k > \frac{n}{2}$, altså at vi har $k-1 \geq n-k$. Da gir likning (3.2):

$$\begin{aligned}
|V(T)| &= |V_0| + |V_1| + \cdots + |V_n| \\
&= q^0 + q^1 + \cdots + q^{n-k-1} + q^{n-k-1} + q^{n-k} + q^{n-k} + \cdots + q^{n-k} \\
&\quad + q^{n-k-1} + q^{n-k-1} + q^{n-k-2} + \cdots + q^0 \\
&= 2\sum_{i=0}^{n-k-1} q^i + 2q^{n-k-1} + (2k-n-1)q^{n-k} \\
&= 2\frac{q^{n-k}-1}{q-1} + 2q^{n-k-1} + (2k-n-1)q^{n-k},
\end{aligned}$$

og siden $k > k-1 \geq n-k$ og $n-2k < 0$, gjelder likningen (3.6) også i dette tilfellet.

Vi viser så uttrykkene i (3.7):

Anta først at $k < \frac{n+1}{2}$, altså at vi har $k \leq n-k$. Da gir likning (3.3) i proposisjon 3.2.1 følgende:

$$\begin{aligned}
|E(T)| &= |E_{0,1}| + |E_{1,2}| + \cdots + |E_{n-1,n}| \\
&= q^1 + q^2 + \cdots + q^{k-1} + q^{k-1} + q^k + q^k + \cdots + q^k + q^{k-1} + q^{k-1} + q^{k-2} + \cdots + q^1 \\
&= 2q\sum_{i=0}^{k-2} q^i + 2q^{k-1} + (n-2k)q^k \\
&= 2q\frac{q^{k-1}-1}{q-1} + 2q^{k-1} + (n-2k)q^k,
\end{aligned}$$

og siden $k-1 < k \leq n-k$ og $n-2k+1 > 0$, stemmer dette med likning (3.7).

Anta så at $k = \frac{n+1}{2}$. Likning (3.3) gir da:

$$\begin{aligned}
|E(T)| &= |E_{0,1}| + |E_{1,2}| + \cdots + |E_{n-1,n}| \\
&= q^1 + q^2 + \cdots + q^{k-1} + q^{k-2} + q^{k-1} + q^{k-2} + \cdots + q^1 \\
&= 2q\sum_{i=0}^{k-2} q^i + q^{k-2} \\
&= 2q\frac{q^{k-1}-1}{q-1} + q^{k-2},
\end{aligned}$$

altså det samme som i likning (3.7).

Til slutt antar vi at $k > \frac{n+1}{2}$, altså at vi har $k-2 \geq n-k$. Da gir likning (3.3):

$$\begin{aligned}
|E(T)| &= |E_{0,1}| + |E_{1,2}| + \cdots + |E_{n-1,n}| \\
&= q^1 + q^2 + \cdots + q^{n-k} + q^{n-k} + q^{n-k+1} + q^{n-k+1} + \cdots + q^{n-k+1} \\
&\quad + q^{n-k} + q^{n-k} + q^{n-k-1} + \cdots + q^1 \\
&= 2q\sum_{i=0}^{n-k-1} q^i + 2q^{n-k} + (2k-n-2)q^{n-k+1} \\
&= 2q\frac{q^{n-k}-1}{q-1} + 2q^{n-k} + (2k-n-2)q^{n-k+1},
\end{aligned}$$

og siden $k-1 > k-2 \geq n-k$ og $n-2k+1 < 0$, gjelder likningen (3.7) også i dette tilfellet. Dermed er beviset for del *ii*) ferdig.

iii) Vi har tidligere gitt eksempler på ekvivalensklasser av nær-MDS-koder som gir alle tre alternativer. Fra eksempel 3.4.6 er alternativ a) er gitt ved ekvivalensklassen til kodene assosiert til grafene på figur 3.6, alternativ b) er gitt ved ekvivalensklassen til kodene assosiert til grafene på figur 3.2 (jf. eksempel 3.4.5), mens alternativ c) er gitt ved ekvivalensklassen til kodene assosiert til grafene på figur 3.3 (også jf. eksempel 3.4.5).

iv) Dette følger av del *ii*) og korollar 1 i [KDMEL]. □

Vi legger for øvrig merke til at alternativ b) i del i) i proposisjon 3.5.1 er mulig innenfor ekvivalensklassen til en kode, hvis og bare hvis også alternativ c) er mulig, ved kolonnepermutasjonen $(1,n)(2,n-1)\cdots\left(\frac{n}{2},\frac{n}{2}+1\right)$ for n jamn og $(1,n)(2,n-1)\cdots\left(\frac{n-1}{2},\frac{n+3}{2}\right)\left(\frac{n+1}{2}\right)$ for n odde, slik vi antydet i eksempel 3.4.5.

Forrige proposisjon, sammen med proposisjon 3.3.1, gir både nedre og øvre grense for det totale antall hjørner og kanter i den minimale trellisen til en nær-MDS-kode. Vi ser at for store kodeparametre q, n og $\min\{k,n-k\}$, vil forskjellene i $|V(T)|$ og $|E(T)|$ mellom ekvivalente koder kunne bli betydelige, selv i nær-MDS-tilfellet, som fra del i) i forrige proposisjon altså har klare begrensninger når det gjelder valgmuligheter for første og siste base. Som vi skal se i eksemplene i kapittel 3.6, kan det i mange tilfeller derfor være effektivt å studere ulike koordinatpermutasjoner av en kode for å finne trellis-optimale koder, eller i det minste for å finne permutasjoner som gir relativt liten minimal trellis.

La oss ellers kort illustrere del *iv*) i forrige proposisjon:

Eksempel 3.5.2. *Det er lett å sjekke at (de underliggende, umerkede) grafene i eksempel* 3.4.5 *(og dermed også kodene assosiert til de ulike merkingene av grafene) er selvduale, og de har vekthierarki* $\{2,4\}$. *Altså har vi* $\min\{d(C),d(C^\perp)\}=2$. *Likevel er det bare i ekvivalensklassen til kodene assosiert til grafene på figur* 3.3 *vi kan oppnå første og siste base* $\{1,3\}$ *og* $\{2,4\}$ *samtidig. Dermed ser vi at det motsatte av del iv*) *i proposisjon* 3.5.1 *ikke gjelder.*

I tillegg er også (den underliggende, umerkede) grafen på figur 3.7 *(og dermed også kodene assosiert til de ulike merkingene av grafen) selvdual(e), med vekthierarki* $\{3,5,6\}$. *Altså får vi* $\min\{d(C),d(C^\perp)\}=3$, *og del iv*) *i proposisjon* 3.5.1 *gir at første og siste baser henholdsvis lik* $\{1,2,4\}$ *og* $\{3,5,6\}$ *ikke kan oppnås samtidig, innenfor ekvivalensklassen til kodene. Dette stemmer også med det vi fant i eksempel* 3.4.6.

Proposisjon 3.5.1 gir en mer direkte måte å finne at Hammingkoden i eksempel 3.1.8 er trellis-optimal, enn å finne første og siste base for alle ekvivalente koder. Vi har tidligere nevnt at denne koden er nær-MDS og har sett at den har første base $A=\{1,2,3,4\}$ og siste base $B=\{3,5,6,7\}$, altså har vi situasjon c) i del i). Fra symmetrien i A og B i likning (3.2) i proposisjon 3.2.1 er det lett å se at vi får samme størrelse på $|V(T)|$ i situasjon b) og c), dermed er det nok å vise at vi ikke kan oppnå situasjon a), innen kodeekvivalensklassen. Men del *iv*) gir resultatet, siden vi har $\min\{d(C),d(C^\perp)\}=3$ (ved å bruke teorem 1.4.19 på generator- og paritetssjekkmatrisen for koden).

3.6 En anvendelse: Viterbi-algoritmen

Vi vil i dette kapittelet se på hvordan trelliser fra koder, og da spesielt den minimale trellisen til en kode, kan brukes. Eksemplene våre omfatter blant annet ulike former for dekoding, og vi henviser til [H] for en grundigere behandling av dette temaet. Varianter av den såkalte

Viterbi-algoritmen er bakgrunnen for alle eksemplene, og vi vil her gi en generell versjon av denne. For en noe mer formell formulering, se [McE], kapittel II.

Viterbi-algoritmen:

La T være en trellis med hjørnelag V_i for $0 \leq i \leq n$, og la, som tidligere, v_a og v_z være henholdsvis kilden og målet i T. For $v \in V(T)$, la $E_{inn}(v) \subseteq E(T)$ være mengden av kanter som har v som slutthjørne. La M være en mengde som er lukket under to binære operasjoner, $*_1$ og $*_2$, der $*_1$ er assosiativ, $*_2$ er assosiativ og kommutativ og $*_2$ distribuerer over $*_1$. La videre $\mu : V(T) \to M$ og $\nu : E(T) \to M$ være funksjoner. Algoritmen er da som følger:

1) (Initialisering.) Tilordne en verdi for $\mu(v_a)$.

2) For $i = 1, 2, \ldots, n$, og for hver $v \in V_i$, la

$$\mu(v) \quad = \quad *_2\{\mu(v_e) *_1 \nu(e) \,|\, e \in E_{inn}(v)\},$$

der v_e er starthjørnet til $e \in E(T)$.

Mengden M, operasjonene $*_1$ og $*_2$ og funksjonen ν kan defineres ulikt fra gang til gang, mens funksjonen μ altså defineres rekursivt i selve algoritmen. Utdata for algoritmen er verdien $\mu(v_z)$.

Merk at i noen tilfeller, for eksempel når algoritmen er brukt til dekoding, består operasjonen $*_2$ i å velge ut én spesiell kant $e \in E_{inn}(v)$, avhengig av verdien til $\mu(v_e) *_1 \nu(e)$. Dermed er $\mu(v_z)$ gitt ved én bestemt a-z-sti i T, og da er som regel også denne stien viktig utdata for algoritmen. (I visse tilfeller, dersom flere kanter i $E_{inn}(v)$ har samme verdi, velger $*_2$ da ut alle disse, og dermed vil alle stiene som velges ut være viktige. Dette kan for eksempel skje dersom flere kodeord er like sannsynlige dekodingsalternativer.)

I en viss forstand kan Viterbi-algoritmen betraktes som en variant av den velkjente Dijkstras korteste sti-algoritme på en generell, kantvektet graf (se for eksempel [T], side 129−131 for definisjon). Men mens Dijkstras algoritme altså er en algoritme på en generell graf, er Viterbi-algoritmen skreddersydd for trelliser: Dijkstras algoritme finner korteste "avstander" fra et bestemt hjørne i grafen (alternativt, trellisen) til alle andre hjørner, mens (én tolkning av) Viterbi-algoritmen kun finner korteste "avstand" mellom kilden og målet i trellisen, og dette er jo også vanligvis det mest interessante i trellis-tilfellet. Viterbi-algoritmen bruker derfor også færre operasjoner enn Dijkstras algoritme, som nevnt på side 1076 i [McE]. De relativt få operasjonene som trengs er også hovedgrunnen til hvorfor Viterbi-algoritmen brukes.

La oss gi et eksempel på dette, som vi også videre vil bruke i senere dekodingseksempler (3.6.4 og 3.6.5):

Eksempel 3.6.1. *La T være en trellis, la operasjonene $*_1$ og $*_2$ i Viterbi-algoritmen på T være henholdsvis + og minimum, og la $\mu(v_a) = 0$. Dersom $\nu(e)$ betegner en avstand mellom start- og slutthjørnet til $e \in E(T)$, vil $\mu(v_z)$ gi korteste avstand fra v_a til v_z i T, og ved å "spore" algoritmen tilbake til v_a, finner vi stien som gir denne.*

Det neste resultatet, som følger lett fra selve Viterbi-algoritmen, viser hvorfor den minimale trellisen til en kode er spesielt interessant ved bruk av denne algoritmen:

Korollar 3.6.2. *La T være en trellis som representerer en kode. Da er antall $*_1$- og $*_2$-operasjoner Viterbi-algoritmen bruker lik henholdsvis $|E(T)|$ og $\varepsilon(T)$.*

Bevis. Direkte fra algoritmen får vi at operasjonen $*_1$ utføres

$$\left(\sum_{i=1}^{n}\sum_{v\in V_i}\delta_{inn}(v)\right) \quad = \quad |E(T)|$$

ganger, og operasjonen $*_2$ utføres

$$\sum_{i=1}^{n}\sum_{v\in V_i}(\delta_{inn}(v)-1)$$

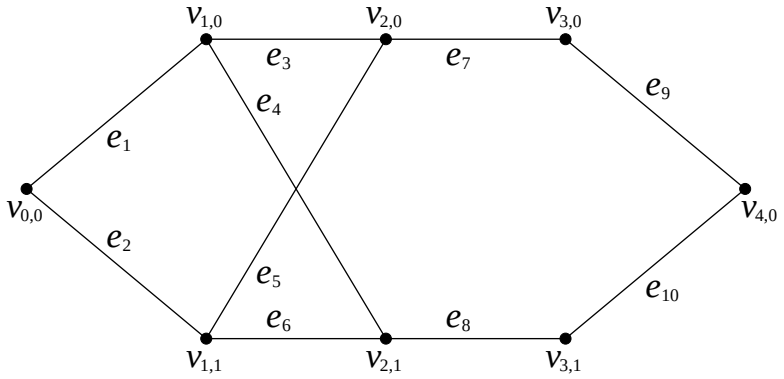
ganger, som er lik $\varepsilon(T)$, siden det totale antall forgreininger i T er lik det totale antall sammenføyninger. □

Vi har tidligere sett at den minimale trellisen til en lineær kode minimerer begge disse parametrene (teoremene 3.1.9 og 3.1.10), altså vil den minimale trellisen gi ekte færre operasjoner for Viterbi-algoritmen enn enhver annen trellis som representerer koden.

I tillegg minimerer den minimale trellisen parameteren $|V(T)|$, som vi så i teorem 3.1.6. Men isolert sett vil færre hjørner medføre større verdi for $\varepsilon(T)$, og dermed også en mindre effektiv Viterbi-algoritme. Muder gir likevel i [M] flere argumenter for at også $|V_i(T)|$, og da spesielt $\max\{|V_i(T)|\,|\,0\leq i\leq n\}$, er naturlige mål for en kodes kompleksitet ved dekoding, som jo er en viktig anvendelse av Viterbi-algoritmen. Vi henviser til hans artikkel for disse resultatene.

Ellers merker vi oss at siden $\varepsilon(T)=|E(T)|-|V(T)|+1$, har vi $0\leq\varepsilon(T)\leq|E(T)|$. Vi konkluderer derfor med at $|E(T)|$ er det viktigste målet på hvor mange operasjoner Viterbi-algoritmen bruker. Dette understrekes ved at antall funksjonsberegninger for ν også er $|E(T)|$.

Siden vi for trellis-optimale koder har minst mulig verdi for $|E(T)|$, innen kodeekvivalensklassen (korollar 3.4.2), kan dermed også trellis-optimalitet være interessant ved bruk av Viterbi-algoritmen, så sant den aktuelle situasjonen tillater bruk av ekvivalente koder. I de kommende eksemplene som omhandler dekoding (3.6.3−3.6.5), er dette i praksis ofte mulig, siden de viktigste kodeparametrene er bevart innen kodeekvivalensklassene. I tillegg har ekvivalente koder samme vektenumerator, så også i eksempel 3.6.6 kan dette være nyttig.



Figur 3.9: Kantmerking av trellisen på figur 3.4*c*.

Videre i dette kapittelet vil vi gi noen eksempler på ulike anvendelser av Viterbi-algoritmen når trellisen representerer en lineær kode. For hver anvendelse vil vi i tillegg vise hva som er

algoritmens utdata, gitt én bestemt trellis T. Til dette benytter vi trellisen på figur 3.4*c*, som representerer koden

$$C \;=\; \{(0000),(1100),(0111),(1011)\}.$$

Vi lar kantmerkingen være som på figur 3.9, altså har vi $w(e_1) = w(e_3) = w(e_6) = w(e_7) = w(e_9) = 0$ og $w(e_2) = w(e_4) = w(e_5) = w(e_8) = w(e_{10}) = 1$. Vi får følgende funksjonsverdier $\mu(v)$ for hjørnene i T:

$$\begin{aligned}
\mu(v_{1,0}) &= \mu(v_{0,0}) *_1 \nu(e_1),\\
\mu(v_{1,1}) &= \mu(v_{0,0}) *_1 \nu(e_2),\\
\mu(v_{2,0}) &= (\mu(v_{1,0}) *_1 \nu(e_3)) *_2 (\mu(v_{1,1}) *_1 \nu(e_5))\\
&= (\mu(v_{0,0}) *_1 \nu(e_1) *_1 \nu(e_3)) *_2 (\mu(v_{0,0}) *_1 \nu(e_2) *_1 \nu(e_5)),\\
\mu(v_{2,1}) &= (\mu(v_{1,0}) *_1 \nu(e_4)) *_2 (\mu(v_{1,1}) *_1 \nu(e_6))\\
&= (\mu(v_{0,0}) *_1 \nu(e_1) *_1 \nu(e_4)) *_2 (\mu(v_{0,0}) *_1 \nu(e_2) *_1 \nu(e_6)),\\
\mu(v_{3,0}) &= \mu(v_{2,0}) *_1 \nu(e_7)\\
&= \big((\mu(v_{0,0}) *_1 \nu(e_1) *_1 \nu(e_3)) *_2 (\mu(v_{0,0}) *_1 \nu(e_2) *_1 \nu(e_5))\big) *_1 \nu(e_7)\\
&= (\mu(v_{0,0}) *_1 \nu(e_1) *_1 \nu(e_3) *_1 \nu(e_7)) *_2 (\mu(v_{0,0}) *_1 \nu(e_2) *_1 \nu(e_5) *_1 \nu(e_7)),\\
\mu(v_{3,1}) &= \mu(v_{2,1}) *_1 \nu(e_8)\\
&= \big((\mu(v_{0,0}) *_1 \nu(e_1) *_1 \nu(e_4)) *_2 (\mu(v_{0,0}) *_1 \nu(e_2) *_1 \nu(e_6))\big) *_1 \nu(e_8)\\
&= (\mu(v_{0,0}) *_1 \nu(e_1) *_1 \nu(e_4) *_1 \nu(e_8)) *_2 (\mu(v_{0,0}) *_1 \nu(e_2) *_1 \nu(e_6) *_1 \nu(e_8)),\\
\mu(v_{4,0}) &= (\mu(v_{3,0}) *_1 \nu(e_9)) *_2 (\mu(v_{3,1}) *_1 \nu(e_{10}))\\
&= \Big(\big((\mu(v_{0,0}) *_1 \nu(e_1) *_1 \nu(e_3) *_1 \nu(e_7))\\
&\quad *_2 (\mu(v_{0,0}) *_1 \nu(e_2) *_1 \nu(e_5) *_1 \nu(e_7))\big) *_1 \nu(e_9)\Big)\\
&\quad *_2 \Big(\big((\mu(v_{0,0}) *_1 \nu(e_1) *_1 \nu(e_4) *_1 \nu(e_8))\\
&\quad *_2 (\mu(v_{0,0}) *_1 \nu(e_2) *_1 \nu(e_6) *_1 \nu(e_8))\big) *_1 \nu(e_{10})\Big)\\
&= (\mu(v_{0,0}) *_1 \nu(e_1) *_1 \nu(e_3) *_1 \nu(e_7) *_1 \nu(e_9))\\
&\quad *_2 (\mu(v_{0,0}) *_1 \nu(e_2) *_1 \nu(e_5) *_1 \nu(e_7) *_1 \nu(e_9))\\
&\quad *_2 (\mu(v_{0,0}) *_1 \nu(e_1) *_1 \nu(e_4) *_1 \nu(e_8) *_1 \nu(e_{10}))\\
&\quad *_2 (\mu(v_{0,0}) *_1 \nu(e_2) *_1 \nu(e_6) *_1 \nu(e_8) *_1 \nu(e_{10})).
\end{aligned}$$

Legg merke til at vi her benytter oss av at $*_2$ distribuerer over $*_1$, fordi vi for enkelthets skyld ønsker et direkte uttrykk for $\mu(v_{4,0})$, som ikke avhenger av tidligere utregninger. Dette vil bety flere operasjoner enn Viterbi-algoritmen bruker (generelt $n \cdot |C|$ operasjoner av type $*_1$ og $|C|-1$ operasjoner av type $*_2$), fordi Viterbi-algoritmen benytter seg av uttrykkene slik de står etter første likhetstegn i hver utregning.

La oss gå over til å gi eksempler på konkrete anvendelser av Viterbi-algoritmen. Våre første, og kanskje viktigste eksempler omhandler dekoding:

Eksempel 3.6.3. *La C være en q-ær lineær kode, og la T være en trellis som representerer C. Anta at $\underline{c} \in C$ sendes gjennom en* ***q-ær symmetrisk kanal****, altså en kanal med følgende egenskaper:*

i) For enhver $x \in \mathbb{F}_q$ er sannsynligheten for feilsending, p $\left(< \frac{1}{2}\right)$, den samme.

ii) Hvis $x \in \mathbb{F}_q$ sendes feil, er alle andre elementer i $\mathbb{F}_q$ like sannsynlige.

Vi har altså at sannsynligheten for å motta $x_2 \in \mathbb{F}_q$, gitt at $x_1 \in \mathbb{F}_q$ er sendt, er

$$\mathrm{P}(x_2 \,|\, x_1) \;=\; \begin{cases} 1-p & \text{hvis } x_2 = x_1, \\ \frac{p}{q-1} & \text{ellers.} \end{cases}$$

Sannsynligheten for å motta $\underline{x} = (x_1, x_2, \ldots, x_n) \in (\mathbb{F}_q)^n$, gitt at $\underline{c} = (c_1, c_2, \ldots, c_n) \in C$ er sendt, blir derfor

$$\mathrm{P}(\underline{x} \,|\, \underline{c}) \;=\; \prod_{i=1}^{n} \mathrm{P}(x_i \,|\, c_i).$$

Gitt mottatt vektor $\underline{x} = (x_1, x_2, \ldots, x_n) \in (\mathbb{F}_q)^n$, ønsker vi å finne det kodeordet som det er mest sannsynlig at er sendt, altså et (eller flere) kodeord $\underline{c}'$ slik at $\mathrm{P}(\underline{x} \,|\, \underline{c}')$ er størst mulig.

Viterbi-algoritmen brukes da på følgende måte:

Vi lar $M = \mathbb{R}$, og lar $\nu(e) = \mathrm{P}(x_i \,|\, w(e))$ dersom $e \in E_{i-1,i}$. Videre lar vi $\mu(v_a) = 1$ og lar $*_1$ og $*_2$ være henholdsvis vanlig multiplikasjon og maksimum. Tallet $0 < \mu(v_z) \leq 1$ vil da gi den største sannsynligheten for et kodeord, og ved å "spore" algoritmen tilbake til v_a, finner vi kodeordet som gir denne.

Anta så at vi i tilfellet med trellisen T på figur 3.4c *mottar vektoren* $(1010) \in (\mathbb{F}_2)^4$. *Viterbi-algoritmen vil da gi*

$$\begin{aligned} \mu(v_{4,0}) &= \max \left\{ \begin{array}{l} 1 \cdot \mathrm{P}(1\,|\,0) \cdot \mathrm{P}(0\,|\,0) \cdot \mathrm{P}(1\,|\,0) \cdot \mathrm{P}(0\,|\,0) \\ 1 \cdot \mathrm{P}(1\,|\,1) \cdot \mathrm{P}(0\,|\,1) \cdot \mathrm{P}(1\,|\,0) \cdot \mathrm{P}(0\,|\,0) \\ 1 \cdot \mathrm{P}(1\,|\,0) \cdot \mathrm{P}(0\,|\,1) \cdot \mathrm{P}(1\,|\,1) \cdot \mathrm{P}(0\,|\,1) \\ 1 \cdot \mathrm{P}(1\,|\,1) \cdot \mathrm{P}(0\,|\,0) \cdot \mathrm{P}(1\,|\,1) \cdot \mathrm{P}(0\,|\,1) \end{array} \right\} \\ &= \max\{(1-p)^2p^2, (1-p)^2p^2, (1-p)^1p^3, (1-p)^3p^1\} \\ &= (1-p)^3p^1, \end{aligned}$$

siden $p < \frac{1}{2}$, og kodeordet som er mest sannsynlig er $\underline{c} = (1011) \in C$.

I [W], kapittel III, finnes et eksempel på hvordan Viterbi-algoritmen kan brukes også i situasjoner med en mer generell sannsynlighetsfordeling.

Eksempel 3.6.4. *Det er lett å se at vi med sannsynlighetsfordeling som i forrige eksempel har følgende ekvivalens:*

$$\mathrm{P}(\underline{x} \,|\, \underline{c}) = (1-p)^{n-i}p^i \quad \Leftrightarrow \quad d(\underline{x}, \underline{c}) = i.$$

Siden $p < \frac{1}{2}$ er uttrykket $(1-p)^{n-i}p^i$ størst mulig når i er minst mulig. Altså vil vi få samme resultat som i forrige eksempel dersom vi finner kodeordet med minst mulig Hammingavstand til den mottatte vektoren.

I dette tilfellet kan Viterbi-algoritmen brukes som i eksempel 3.6.1, *med $M = \mathbb{N} \cup \{0\}$ og $\nu(e)$ lik* 0 *dersom $x_i = w(e)$ og* 1 *ellers, for $e \in E_{i-1,i}$. Heltallet $0 \leq \mu(v_z) \leq n$ vil da gi den minste Hammingavstanden til $\underline{x}$ for et kodeord, og "tilbakesporing" av algoritmen vil altså gi samme kodeord som i eksempel* 3.6.3.

La oss derfor se hva vi får med samme mottatte vektor, $(1010) \in (\mathbb{F}_2)^4$*, og samme kode som i forrige eksempel:*

$$\begin{aligned}\mu(v_{4,0}) &= \min\left\{\begin{array}{l} 0+d(1,0)+d(0,0)+d(1,0)+d(0,0) \\ 0+d(1,1)+d(0,1)+d(1,0)+d(0,0) \\ 0+d(1,0)+d(0,1)+d(1,1)+d(0,1) \\ 0+d(1,1)+d(0,0)+d(1,1)+d(0,1) \end{array}\right\} \\ &= \min\{2,2,3,1\} \\ &= 1,\end{aligned}$$

og kodeordet som gir denne verdien er igjen $\underline{c} = (1011) \in C$*.*

Eksempel 3.6.5. *I enkelte typer (analoge) kanaler vil den mottatte vektoren kunne være et element i* $\mathbb{R}^n$*, og kodeordet som det er mest sannsynlig at er sendt, vil være det kodeordet som har minst mulig* ***Euklidsk avstand*** *til den mottatte vektoren* $\underline{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$*, altså kodeordet* $\underline{c} = (c_1, c_2, \ldots, c_n)$ *slik at* $\sqrt{(x_1-c_1)^2+(x_2-c_2)^2+\cdots+(x_n-c_n)^2}$ *er minst mulig. (Se kapittel* 6 *i* [C]*.)*

Også her kan vi bruke Viterbi-algoritmen som i eksempel 3.6.1*, med* $M = \mathbb{R}$ *og* $\nu(e) = (x_i - w(e))^2$ *for* $e \in E_{i-1,i}$*. Tallet* $\sqrt{\mu(v_z)}$ *vil nå gi den minste Euklidske avstanden til* $\underline{x}$ *for et kodeord, og igjen vil "tilbakesporing" av algoritmen gi kodeordet.*

La oss anta at vi mottar vektoren $\underline{x} = (-0.2, 0.4, 1.3, 0.7) \in \mathbb{R}^4$ *ved bruk av koden gitt ved trellisen* T *på figur* 3.4*c. Vi får da*

$$\begin{aligned}\mu(v_{4,0}) &= \min\left\{\begin{array}{l} 0+(-0.2-0)^2+(0.4-0)^2+(1.3-0)^2+(0.7-0)^2 \\ 0+(-0.2-1)^2+(0.4-1)^2+(1.3-0)^2+(0.7-0)^2 \\ 0+(-0.2-0)^2+(0.4-1)^2+(1.3-1)^2+(0.7-1)^2 \\ 0+(-0.2-1)^2+(0.4-0)^2+(1.3-1)^2+(0.7-1)^2 \end{array}\right\} \\ &= \min\{2.38, 3.98, 0.58, 1.78\} \\ &= 0.58,\end{aligned}$$

altså er $\sqrt{0.58} \approx 0.76$ *minste Euklidske avstand mellom* $\underline{x}$ *og et kodeord, og kodeordet som gir denne verdien er* $\underline{c} = (0111) \in C$*.*

Viterbi-algoritmen er for det meste brukt innen dekoding, men som tidligere nevnt, finnes også andre anvendelser. Blant annet kan man, gitt trellisen T som representerer en kode C, finne vektenumeratoren til C og finne selve koden C, noe vi viser i de neste to eksemplene. Poenget med å bruke Viterbi-algoritmen er som alltid at den bruker få operasjoner for å finne resultatet.

Eksempel 3.6.6. *Følgende spesialiseringer av Viterbi-algoritmen vil gi vektenumeratoren til koden trellisen representerer, ved* $\mu(v_z)$*: La* $M = (\mathbb{N} \cup \{0\})[z]$*, altså mengden av polynomer i* z *med koeffisienter i* $\mathbb{N} \cup \{0\}$*, og la* $\nu(e) = z^{\min\{1,w(e)\}}$ *og* $\mu(v_a) = 1$*. (Dersom koden er binær, kan uttrykket* $z^{\min\{1,w(e)\}}$ *erstattes med* $z^{w(e)}$*.) La videre* $*_1$ *og* $*_2$ *være henholdsvis vanlig multiplikasjon og addisjon.*

Anvendt på trellisen T *på figur* 3.4*c, som altså representerer en binær kode, får vi*

$$\begin{aligned}\mu(v_{4,0}) &= (1\cdot z^0\cdot z^0\cdot z^0\cdot z^0)+(1\cdot z^1\cdot z^1\cdot z^0\cdot z^0) \\ &\quad +(1\cdot z^0\cdot z^1\cdot z^1\cdot z^1)+(1\cdot z^1\cdot z^0\cdot z^1\cdot z^1) \\ &= 1+z^2+2z^3,\end{aligned}$$

som er vektenumeratoren til koden.

Eksempel 3.6.7. *Til slutt vil $\mu(v_z)$ angi hele den q-ære $[n,k]$-koden C dersom vi lar $M = \mathcal{P}(N)$, der $N = \emptyset \cup \big(\bigcup_{i=1}^{n}(\mathbb{F}_q)^i\big)$, $\nu(e) = \{w(e)\}$ og $\mu(v_a) = \emptyset$. Vi definerer $A *_1 B = \{(\underline{a}, \underline{b}) \,|\, \underline{a} \in A, \underline{b} \in B\}$ for $A, B \in M$ og lar $*_2$ være union av mengder.*

Vi lar det være opp til leseren å sjekke dette.

3.7 Mulige veier videre

Del *iv*) av proposisjon 3.5.1 gir oss en nødvendig betingelse for at vi skal kunne finne trellis-optimale koder innenfor ekvivalensklassen til en nær-MDS-kode. Denne betingelsen gir også restriksjoner for parametrene n og k, i tillegg til $d(C)$ og $d(C^\perp)$. Dersom C er en $[n,k]$-nær-MDS-kode, og det eksisterer en trellis-optimal, ekvivalent kode, har vi altså at $\min\{d(C), d(C^\perp)\}$ er jamn. I tillegg er Singletondefekten $S(C) = S(C^\perp) = 1$, og dermed er $d(C) = n-k$ og $d(C^\perp) = k$. Ut fra dette får vi at dersom k er odde, er $d(C^\perp)$ også odde. Dermed må $d(C)$ være jamn og følgelig n odde, i tillegg til at $d(C) < d(C^\perp)$. Altså kan ikke n være jamn, samtidig som at k er odde.

Det kunne videre være interessant å se om det er flere slike generelle restriksjoner for disse parametrene, dersom vi ønsker å kunne finne trellis-optimale nær-MDS-koder.

Videre har vi ut fra resultatene i kapittel 3 ingen garanti for at trellis-optimale koder minimerer antall operasjoner i Viterbi-algoritmen innenfor ekvivalensklassen, siden vi ikke vet om disse minimerer forgreiningsindeksen $\varepsilon(T)$, og antall operasjoner i Viterbi-algoritmen også avhenger av $\varepsilon(T)$. Et naturlig spørsmål er derfor om vi har et lignende resultat til teorem 3.1.10 også for trellis-optimale koder, noe som i så fall ytterligere ville motivere studiet av slike koder.

Kapittel 4

Simplisielle komplekser fra grafer

I dette kapittelet vil vi studere sammenhenger mellom grafer og simplisielle komplekser. Vi konstruerer et Stanley-Reisner-ideal fra de utspennende trærne i en graf og ser på hvilke sammenhenger vi har mellom grafen og det simplisielle komplekset som bestemmes av dette idealet. Videre undersøker vi hvilke kantmengder av grafen som har betydning for den minimale frie resolusjonen av Stanley-Reisner-ringen til dette simplisielle komplekset og gir til slutt flere eksempler på hvordan vi bestemmer hele resolusjonen og dens generatorer direkte fra grafen, uten å gå via det simplisielle komplekset.

Vi forutsetter i dette kapittelet en viss kjennskap til (kombinatorisk) kommutativ algebra og henviser til [MS], kapitlene 1 og 5.1 for en grundigere introduksjon til teorien som gis i kapitlene 4.1 og 4.2.

4.1 Simplisielle komplekser og homologi

For enkelthets skyld lar vi i resten av oppgaven $[n]$ betegne mengden $\{1, 2, \ldots, n\}$, og når ikke annet er oppgitt, antar vi at alle simplisielle komplekser og grafer har henholdsvis hjørne- og kantmengde lik $[n]$.

Definisjon 4.1.1. *Et* ***simplisielt kompleks*** Δ *på hjørnemengden* $[n]$ *er en familie av delmengder av* $[n]$*, kalt* ***fjes****, som oppfyller følgende betingelse:*

(F1) *Hvis* $\sigma_1 \in \Delta$ *og* $\sigma_2 \subseteq \sigma_1$*, så er* $\sigma_2 \in \Delta$*.*

Maksimale fjes kalles ***fasetter****. Et fjes av kardinalitet* $i + 1$ *har* ***dimensjon*** i *og kalles et* ***i-fjes*** i Δ*.*

Som vi ser av (F1), er ethvert simplisielt kompleks Δ entydig bestemt av fasettene til Δ.

Det simplisielle komplekset $\Delta = \{\}$ kalles **det tomme komplekset** og er forskjellig fra $\{\emptyset\}$, **det irrelevante komplekset**.

Vi har to operasjoner på simplisielle komplekser som vil være særlig interessante for oss senere. Vi definerer:

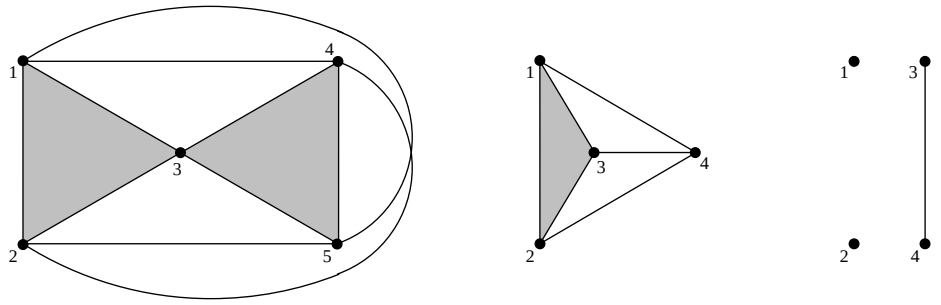
Definisjon 4.1.2. *For et simplisielt kompleks* Δ *er* ***restriksjonen*** *av* Δ *til* $\sigma \subseteq [n]$

$$\Delta|_\sigma \;=\; \{\tau \in \Delta \,|\, \tau \subseteq \sigma\},$$

mens ***lenken*** *til* σ *er*

$$\mathrm{link}_\Delta(\sigma) \quad = \quad \{\tau \in \Delta \,|\, \tau \cup \sigma \in \Delta, \tau \cap \sigma = \emptyset\}.$$

Det er lett å se at både $\Delta|_\sigma$ og $\mathrm{link}_\Delta(\sigma)$ alltid er simplisielle komplekser, og lenken til σ er altså det simplisielle komplekset vi får ved å beholde bare de fjesene i Δ som inneholder σ, for så å restringere til $[n] \setminus \sigma$. Merk at dersom $\sigma \notin \Delta$, så er $\mathrm{link}_\Delta(\sigma) = \{\}$, det tomme komplekset, mens $\mathrm{link}_\Delta(\sigma)$ er det irrelevante komplekset kun dersom σ er en fasett i Δ.



Figur 4.1: Det simplisielle komplekset Δ i eksempel 4.1.3, med restriksjonen $\Delta|_{\{1,2,3,4\}}$ og lenken $\mathrm{link}_\Delta(\{5\})$.

Eksempel 4.1.3. *Figur* 4.1 *viser en grafisk representasjon av det simplisielle komplekset* Δ *på hjørnemengden* $[5]$ *bestående av alle delmengder av* $\{1,2,3\}$, $\{1,4\}$, $\{1,5\}$, $\{2,4\}$, $\{2,5\}$ *og* $\{3,4,5\}$, *i tillegg til de simplisielle kompleksene*

$$\begin{aligned} \Delta|_{\{1,2,3,4\}} &= \big\{\emptyset,\{1\},\{2\},\{3\},\{4\},\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\},\{1,2,3\}\big\} \text{ og} \\ \mathrm{link}_\Delta(\{5\}) &= \big\{\emptyset,\{1\},\{2\},\{3,4\}\big\}. \end{aligned}$$

Når vi etterhvert skal benytte den såkalte Hochsters formel, som vi gir i teorem 4.2.6, trenger vi noen homologiske konstruksjoner fra Δ som oppstår fra det reduserte (ko)kjedekomplekset til Δ over $\mathbb{K}$. Vi definerer:

Definisjon 4.1.4. *La* $F_i(\Delta) = \{\sigma \,|\, \sigma \text{ er et } i\text{-fjes i } \Delta\}$, *og la* $\mathbb{K}^{F_i(\Delta)}$ *være et vektorrom over* $\mathbb{K}$ *med basiselementer* e_σ *som korresponderer med* i*-fjes* $\sigma \in F_i(\Delta)$. ***Det reduserte kjedekomplekset*** *til* Δ *over* $\mathbb{K}$ *er komplekset*

$$\widetilde{\mathcal{C}}_\bullet(\Delta;\mathbb{K}): \quad 0 \longleftarrow \mathbb{K}^{F_{-1}(\Delta)} \xleftarrow{\delta_0} \mathbb{K}^{F_0(\Delta)} \xleftarrow{\delta_1} \mathbb{K}^{F_1(\Delta)} \longleftarrow \cdots \longleftarrow \mathbb{K}^{F_{n-2}(\Delta)} \xleftarrow{\delta_{n-1}} \mathbb{K}^{F_{n-1}(\Delta)} \longleftarrow 0.$$

Randavbildningene δ_i *er definert ved å la* $\mathrm{sign}(j,\sigma) = (-1)^{r-1}$ *hvis* j *er det* r*-te elementet i* $\sigma \subseteq [n]$ *(skrevet i stigende rekkefølge), og*

$$\delta_i(e_\sigma) \quad = \quad \sum_{j \in \sigma} \mathrm{sign}(j,\sigma) e_{\sigma \setminus j}.$$

Som konvensjon lar vi $\mathbb{K}^{F_i(\Delta)} = 0$ *og* $\delta_i = 0$ *dersom* $i < -1$ *eller* $i > n-1$. *Vi kaller* $\mathbb{K}$*-vektorrommet*

$$\widetilde{H}_i(\Delta;\mathbb{K}) \quad = \quad \ker(\delta_i)/\mathrm{im}(\delta_{i+1})$$

den ***i-te reduserte homologien*** *til* Δ *over* $\mathbb{K}$.

Spesielt er $\widetilde{H}_i(\Delta;\mathbb{K}) = 0$ for $i < 0$ og $i > n-1$, så lenge Δ ikke er det irrelevante komplekset $\{\emptyset\}$. Det irrelevante komplekset har homologi bare i $i = -1$, der vi har $\widetilde{H}_{-1}(\Delta;\mathbb{K}) \cong \mathbb{K}$, mens det tomme komplekset $\{\}$ har $\widetilde{H}_i(\Delta;\mathbb{K}) = 0$ for alle i.

Geometrisk kan vi si at $\dim_{\mathbb{K}} \widetilde{H}_i(\Delta;\mathbb{K})$ er gitt ved antall "lineært uavhengige hull" i Δ med i-dimensjonal "rand". Når $i = 0$ vil dette tilsvare antall sammenhengskomponenter av Δ, minus én. For eksempel, dersom $\Delta|_{\{1,2,3,4\}}$ og $\mathrm{link}_\Delta(\{5\})$ er gitt som på figur 4.1, har vi $\dim_{\mathbb{K}} \widetilde{H}_1(\Delta|_{\{1,2,3,4\}};\mathbb{K}) = 2$, ikke 3, siden "hullet" gitt ved trekanten mellom hjørnene 1, 2 og 4 er en "lineærkombinasjon" av hullene gitt ved trekantene mellom hjørnene 1, 3, 4 og 2, 3, 4. Videre er $\dim_{\mathbb{K}} \widetilde{H}_0(\mathrm{link}_\Delta(\{5\});\mathbb{K}) = 2$, siden $\mathrm{link}_\Delta(\{5\})$ har 3 sammenhengskomponenter.

Definisjon 4.1.5. ***Det reduserte kokjedekomplekset*** $\widetilde{\mathcal{C}}^\bullet(\Delta;\mathbb{K})$ *til* Δ *over* $\mathbb{K}$ *er vektorromsdualen til* $\widetilde{\mathcal{C}}_\bullet(\Delta;\mathbb{K})$*, altså* $\mathrm{Hom}_{\mathbb{K}}(\widetilde{\mathcal{C}}_\bullet(\Delta;\mathbb{K}),\mathbb{K})$*, med* ***korandavbildninger*** δ^i *som er vektorromsdualer til* δ_i*. Den* ***i-te reduserte kohomologien*** *til* Δ *over* $\mathbb{K}$ *er*

$$\widetilde{H}^i(\Delta;\mathbb{K}) \quad = \quad \ker(\delta^i)/\mathrm{im}(\delta^{i+1}).$$

I det videre sløyfer vi oftest $\mathbb{K}$ i notasjonen for redusert (ko)homologi.

4.2 Minimale frie resolusjoner av Stanley-Reisner-ringer

I det følgende vil $\mathbb{K}[x_1, x_2, \ldots, x_n]$, polynomringen over kroppen $\mathbb{K}$ i n variabler, spille en sentral rolle. For enkelthets skyld lar vi derfor R betegne denne gjennom resten av oppgaven. Av samme grunn vil vi, i motsetning til tidligere, la $\mathbb{N}$ være de positive heltallene *inkludert* tallet 0, en mengde vi tidligere altså har betegnet $\mathbb{N} \cup \{0\}$.

Definisjon 4.2.1. *Et* ***monom*** *i* R *er et produkt* $x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$ *for* $\underline{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n$*, og vi skriver* $\underline{x}^{\underline{a}}$ *for dette produktet. Dersom i tillegg* $a_i \in \{0, 1\}$ *for alle* $1 \leq i \leq n$*, har vi et* ***kvadratfritt monom****. Et ideal* $I \subseteq R$ *er et* ***monomialideal*** *dersom det er generert av monomer, og et* ***kvadratfritt monomialideal*** *dersom alle generatorene i tillegg er kvadratfrie.*

Vi identifiserer hver delmengde $\sigma \subseteq [n]$ med **den kvadratfrie vektoren** til σ, som har 1 i i-te posisjon hvis $i \in \sigma$ og 0 i alle andre posisjoner. Da får vi en naturlig korrespondanse mellom delmengder av $[n]$ og kvadratfrie monomer i R, ved $\sigma \leftrightarrow \underline{x}^\sigma = \prod_{i\in\sigma} x_i$, og kan definere:

Definisjon 4.2.2. ***Stanley-Reisner-idealet*** *til det simplisielle komplekset* Δ *er det kvadratfrie monomialidealet*

$$I_\Delta \quad = \quad \langle \underline{x}^\sigma \mid \sigma \notin \Delta \rangle,$$

generert av monomer som korresponderer med delmengder av $[n]$ *som ikke er fjes i* Δ*.* ***Stanley-Reisner-ringen*** $\mathbb{K}[\Delta]$ *til* Δ *er kvotientringen* R/I_Δ*.*

Vi merker oss at et simplisielt kompleks Δ og Stanley-Reisner-idealet I_Δ entydig bestemmer hverandre.

Vårt hovedtema i dette kapittelet er å studere den minimale frie resolusjonen av Stanley-Reisner-ringen til simplisielle komplekser, noe vi nå vil definere, for en generell R-modul A. I vårt tilfelle lar vi altså $A = \mathbb{K}[\Delta]$, som er $\mathbb{N}^n$-gradert.

Vi sier at F er en $\mathbb{N}^n$**-gradert fri** R**-modul** dersom

$$F \quad = \quad \bigoplus_{\underline{a}\in\mathbb{N}^n} R(-\underline{a})^{r_{\underline{a}}}, \tag{4.1}$$

der $r_{\underline{a}} \in \mathbb{N}$ og $R(-\underline{a})$ er en $\mathbb{N}^n$-gradert ring slik at $(R(-\underline{a}))_{\underline{b}} = R_{-\underline{a}+\underline{b}}$ for alle $\underline{b} \in \mathbb{N}^n$.

Definisjon 4.2.3. *En* $\mathbb{N}^n$***-gradert fri resolusjon*** *av en R-modul A er et kompleks*

$$\mathcal{F}_\bullet : \quad 0 \longleftarrow F_0 \xleftarrow{\phi_1} F_1 \xleftarrow{\phi_2} F_2 \longleftarrow \cdots \longleftarrow F_{l-1} \xleftarrow{\phi_l} F_l \longleftarrow 0, \tag{4.2}$$

der F_i-ene er frie $\mathbb{N}^n$-graderte R-moduler, og vi har:

i) $A = F_0/\mathrm{im}(\phi_1)$ *og*

ii) $\mathcal{F}_\bullet$ *er eksakt i F_i for $i \geq 1$.*

Lengden *til resolusjonen er det største tallet i slik at $F_i \neq 0$. Som i (4.2), bruker vi parameteren l for dette.*

Siden frie resolusjoner av Stanley-Reisner-ringer alltid er $\mathbb{N}^n$-graderte, vil vi i det følgende la graderingen være underforstått når vi snakker om frie resolusjoner.

Definisjon 4.2.4. *Resolusjonen $\mathcal{F}_\bullet$ fra (4.2) er* ***minimal*** *dersom* $\mathrm{im}(\phi_i) \subseteq \mathfrak{m}F_{i-1}$*, der $\mathfrak{m}$ er idealet $\langle x_1, x_2, \ldots, x_n\rangle$. Resolusjonen er da entydig opp til isomorfi, og alle rangene $r_{\underline{a}}$ (fra uttrykket (4.1)) til modulene F_i er minimert samtidig. I dette tilfellet kaller vi $r_{\underline{a}}$ til F_i det* ***i-te multigraderte Betti-tallet*** *til A i grad $\underline{a}$, betegnet $\beta_{i,\underline{a}}(A)$, og dette tallet er dermed kun avhengig av modulen A. Tallet $\beta_i(A) = \sum_{\underline{a}\in\mathbb{N}^n} \beta_{i,\underline{a}}(A)$ kalles det* ***i-te totale Betti-tallet*** *til A.*

Definisjon 4.2.5. *Resolusjonen $\mathcal{F}_\bullet$ fra (4.2) er* ***lineær*** *dersom hver F_i kan skrives som en direktesum av $\mathbb{N}^n$-graderte ringer på formen $R(-\underline{a})^{r_{\underline{a}}}$, der summen av koordinatene til vektorene $\underline{a} \in \mathbb{N}^n$ for hver F_i er lik $i + d$ for én fiksert $d \in \mathbb{N}$.*

Følgende teorem, kalt Hochsters formel, gir en sammenheng mellom multigraderte Betti-tall og homologi som vi vil få mye bruk for senere i kapittelet.

Teorem 4.2.6. *De multigraderte Betti-tallene til $\mathbb{K}[\Delta]$ som er ulik null ligger bare i kvadratfrie grader σ, og vi har*

$$\beta_{i,\sigma}(\mathbb{K}[\Delta]) \quad = \quad \dim_{\mathbb{K}} \widetilde{H}^{|\sigma|-i-1}(\Delta|_\sigma).$$

Bevis. Dette er korollar 5.12 i [MS]. □

Siden vektorromsdualisering bevarer eksakte sekvenser, er $\widetilde{H}^i(\Delta;\mathbb{K})$ vektorromsdualen til $\widetilde{H}_i(\Delta;\mathbb{K})$, altså har de samme dimensjon. Dermed kan vi erstatte kohomologi med homologi i Hochsters formel, og vi får

$$\beta_{i,\sigma}(\mathbb{K}[\Delta]) \quad = \quad \dim_{\mathbb{K}} \widetilde{H}_{|\sigma|-i-1}(\Delta|_\sigma).$$

I det følgende vil vi konsekvent bruke denne versjonen av Hochsters formel.

4.3 Kant-komplekset til en graf

Vi vil nå innføre en konstruksjon som bestemmer et entydig simplisielt kompleks, gitt en vilkårlig graf. Denne konstruksjonen vil medføre at kantmengden til en graf G er lik hjørnemengden til det tilhørende simplisielle komplekset, og som tidligere nevnt vil vi dermed benytte notasjonen $[n]$ istedenfor $E(G)$. Som i deler av kapittel 2 begrenser vi oss også her til sammenhengende grafer. Dette fordi konstruksjonen som vi nå skal gi kun avhenger av kantmengdene til utspennende trær i en graf. Dersom grafen G er usammenhengende, identifiserer vi derfor ett vilkårlig hjørne fra hver komponent av G med hverandre, og det er lett å se at de utspennende trærne i den nye, sammenhengende grafen og de utspennende skogene i G består av de samme kantene.

Merk at den følgende definisjonen av grafisk ideal er en direkte oversettelse av *matroidalt* ideal, slik dette er definert på side 273 i [ER].

Definisjon 4.3.1. *Idealet $I \subseteq R$ er **grafisk** dersom de minimale generatorene til I er monomer som korresponderer med de utspennende trærne i en graf G (med $E(G) = [n]$), altså at vi har*

$$I \;=\; \langle \underline{x}^{\sigma} \,|\, \sigma \subseteq [n] \text{ er et utspennende tre i } G \rangle.$$

*Vi sier at I **korresponderer med G**. Det simplisielle komplekset Δ på hjørnemengden $[n]$ er **kant-komplekset** til G dersom Stanley-Reisner-idealet I_Δ korresponderer med G, og vi skriver $\Delta(G)$ for dette.*

Vi har tidligere nevnt at Stanley-Reisner-idealet entydig bestemmer det tilhørende simplisielle komplekset, altså er også kant-komplekset til en graf entydig, gitt grafen.

Proposisjon 4.3.2. *La Δ være et simplisielt kompleks. Dersom $\Delta = \Delta(G)$ for en graf G, har $\mathbb{K}[\Delta]$ lineær minimal fri resolusjon, uansett kropp $\mathbb{K}$.*

Bevis. Dette følger av proposisjon 7 i [ER], siden de minimale generatorene til I_Δ er monomer som korresponderer med basene for kretsmatroiden til en graf. □

Merk at forrige resultat gir at vi for enhver $\sigma \subseteq [n]$ har $\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) \neq 0$ for maksimalt én i. Spørsmålet videre er dermed hvilke delmengder av $[n]$ som har $\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) \neq 0$ for én i, for hvilken i dette skjer og hva verdien av dette i-te multigraderte Betti-tallet er, gitt G. Dette vil vi senere gi svar på, og vi vil også gi eksempler på minimale frie resolusjoner av Stanley-Reisner-ringen til kant-komplekset til en graf.

Fra definisjonen 4.3.1 har vi at dersom I_Δ korresponderer med G så svarer det minimale generatorsettet til I_Δ til utspennende trær i G. Dermed har vi at de første multigraderte Betti-tallene $\beta_{1,\sigma}(\mathbb{K}[\Delta]) = 1$ hvis σ er kantmengden til et utspennende tre i G og 0 ellers, og det første totale Betti-tallet $\beta_1(\mathbb{K}[\Delta])$ er lik antall utspennende trær i G.

Dersom σ er kantmengden til et utspennende tre i en graf G, har vi $|\sigma| = r(G)$, rangen til G, slik denne er definert på side 25. Siden den minimale frie resolusjonen av $\mathbb{K}[\Delta(G)]$ er lineær, får vi derfor at alle $\sigma \subseteq [n]$ som har $\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) \neq 0$ må ha $|\sigma| = r(G) + i - 1$. Dette gir en øvre grense for lengden l til den minimale frie resolusjonen, nemlig $l \leq n - r(G) + 1 = k(G) + 1$ (der $k(G)$ er kretsrangen til G), siden $|\sigma| \leq n$.

Neste resultat viser noen sammenhenger mellom en graf og grafens kant-kompleks, og særlig del (4.3) gjør det enkelt å konstruere kant-komplekset direkte fra grafen. (Vi minner om at $G|_\sigma$ betegner restriksjonen av G til σ, som definert på side 2.)

Proposisjon 4.3.3. *La G være en graf og $\sigma \subseteq [n]$. Da har vi:*

$$\sigma \in \Delta(G) \quad \Leftrightarrow \quad r(G|_\sigma) < r(G), \tag{4.3}$$

$$\sigma \in \Delta(G) \quad \Leftrightarrow \quad [n] \setminus \sigma \text{ er en separerende kantmengde i } G, \text{ og} \tag{4.4}$$

$$\sigma \text{ er en fasett i } \Delta(G) \quad \Leftrightarrow \quad [n] \setminus \sigma \text{ er en kokrets i } G. \tag{4.5}$$

Bevis. (4.3) Vi har $I_{\Delta(G)} = \langle \sigma \,|\, \sigma \text{ er et utspennende tre i } G \rangle$. Fra definisjonen av Stanley-Reisner-ideal får vi derfor at utspennende trær i G tilsvarer de minimale delmengdene av $[n]$ som ikke er fjes i $\Delta(G)$. Altså har vi at $\sigma \notin \Delta(G)$ er ekvivalent med at σ inneholder et utspennede tre i G, som igjen er det samme som at $G|_\sigma$ har samme rang som G.

(4.4) En delgraf av G med samme hjørnemengde som G, har mindre rang enn G hvis og bare hvis den har flere komponenter enn G. Dermed følger dette direkte fra del (4.3) og definisjonen av separerende kantmengde på side 3.

(4.5) Dette følger fra del (4.4), siden maksimale fjes i $\Delta(G)$ altså vil svare til minimale separerende kantmengder i G. □

Siden ethvert fjes i et simplisielt kompleks Δ er kontraktibelt, får vi

$$\sigma \in \Delta \quad \Rightarrow \quad \widetilde{H}_i(\Delta|_\sigma) = 0 \text{ for alle } i, \tag{4.6}$$

altså gir Hochsters formel at alle $\sigma \subseteq [n]$ som er fjes i kant-komplekset $\Delta(G)$ til en graf G har $\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) = 0$ for alle i. Vi får dermed følgende resultat direkte fra forrige proposisjon:

Korollar 4.3.4. *For en graf G og $\sigma \subseteq [n]$ har vi*

$$r(G|_\sigma) < r(G) \quad \Rightarrow \quad \beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) = 0 \text{ for alle } i.$$

□

Vi vil senere vise at vi for kant-komplekser til løkkefrie grafer har ekvivalens i (4.6), og dermed også i korollar 4.3.4. Dette gjelder vel å merke ikke for generelle simplisielle komplekser; for eksempel er $\widetilde{H}_i(\Delta|_\sigma) = 0$ for alle i når $\sigma = \{1,2,3\}$ og Δ er gitt ved alle delmengder av $\{1,2\}$ og $\{1,3\}$, på hjørnemengden $[3]$.

Men før vi begynner å arbeide oss fremover mot å vise denne ekvivalensen, vil vi gi to resultater som relaterer kompleks-operasjonene kontraksjon og lenke til grafteoretiske begreper.

Proposisjon 4.3.5. *For en graf G og $\sigma \subseteq [n]$ har vi*

$$r(G|_\sigma) = r(G) \quad \Leftrightarrow \quad \Delta(G|_\sigma) = \Delta(G)|_\sigma.$$

Bevis. Anta først at $r(G|_\sigma) = r(G)$. Vi merker oss at dersom $\tau \in \Delta(G|_\sigma)$ eller $\tau \in \Delta(G)|_\sigma$, så må $\tau \subseteq \sigma$. La derfor $\tau \subseteq \sigma$. Ved gjentatt bruk av (4.3) i proposisjon 4.3.3, er det lett å se at følgende påstander da er ekvivalente:

$$\tau \in \Delta(G|_\sigma) \quad \Leftrightarrow \quad r(G|_\tau) < r(G|_\sigma) \quad \Leftrightarrow \quad r(G|_\tau) < r(G) \quad \Leftrightarrow \quad \tau \in \Delta(G) \quad \Leftrightarrow \quad \tau \in \Delta(G)|_\sigma. \tag{4.7}$$

Anta så at $r(G|_\sigma) < r(G)$. Del (4.3) i proposisjon 4.3.3 gir da at $\sigma \in \Delta(G)$, dermed er $\sigma \in \Delta(G)|_\sigma$. Men $\sigma \notin \Delta(G|_\sigma)$, for ellers har vi, igjen ved (4.3), at $r((G|_\sigma)|_\sigma) < r(G|_\sigma)$, som er en selvmotsigelse. Altså er $\Delta(G|_\sigma) \neq \Delta(G)|_\sigma$. □

Vi merker oss at dersom $r(G|_\sigma) < r(G)$ og $\tau \subseteq \sigma$ er det kun

$$r(G|_\tau) < r(G|_\sigma) \quad \Leftarrow \quad r(G|_\tau) < r(G)$$

i uttrykket (4.7) som ikke er riktig. Vi har dermed $\Delta(G|_\sigma) \subseteq \Delta(G)|_\sigma$ for enhver $\sigma \subseteq [n]$.

Legg også merke til at dersom vi kombinerer forrige proposisjon med Hochsters formel, får vi

$$\beta_{i,\sigma}(\mathbb{K}[\Delta(G|_\sigma)]) \;=\; \beta_{i,\sigma}(\mathbb{K}[\Delta(G)|_\sigma]) \;=\; \dim_{\mathbb{K}} \widetilde{H}_{|\sigma|-i-1}(\Delta(G)|_\sigma) \;=\; \beta_{i,\sigma}(\mathbb{K}[\Delta(G)])$$

dersom $r(G|_\sigma) = r(G)$.

Proposisjon 4.3.6. *For en graf G og $\sigma \subseteq [n]$ har vi*

$$\Delta(G/\sigma) \;=\; \mathrm{link}_{\Delta(G)}(\sigma),$$

der G/σ er kontraksjonen av σ fra G.

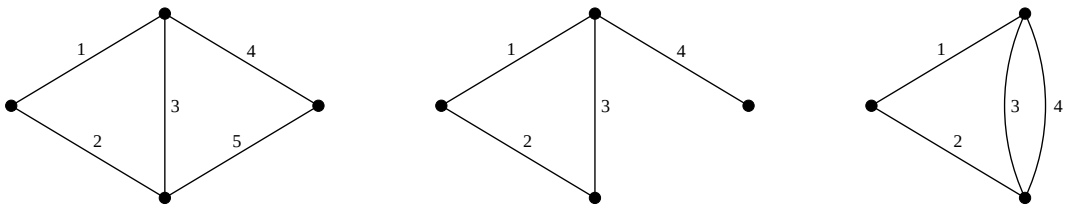
Bevis. Vi merker oss at dersom $\tau \in \Delta(G/\sigma)$ eller $\tau \in \mathrm{link}_{\Delta(G)}(\sigma)$, så må $\tau \cap \sigma = \emptyset$. La derfor $\tau \cap \sigma = \emptyset$. Fra (4.3) i proposisjon 4.3.3 er $\tau \in \Delta(G/\sigma)$ ekvivalent med at $r((G/\sigma)|_\tau) < r(G/\sigma)$, mens $\tau \in \mathrm{link}_{\Delta(G)}(\sigma)$ er ekvivalent med at $r(G|_{\tau\cup\sigma}) < r(G)$ siden vi fra definisjonen av lenke har $\tau \in \mathrm{link}_{\Delta(G)}(\sigma) \Leftrightarrow \tau \cup \sigma \in \Delta(G)$ når $\tau \cap \sigma = \emptyset$. I tillegg er det lett å se at vi har $(G/\sigma)|_\tau = (G|_{\tau\cup\sigma})/\sigma$, fordi både $(G/\sigma)|_\tau$ og $(G|_{\tau\cup\sigma})/\sigma$ har kantmengde τ og hjørnemengde $\{v \in V(G/\sigma) \mid v \text{ er et endepunkt til } e \text{ for én } e \in \tau\}$. Altså er det nok å vise at vi har

$$r((G|_{\tau\cup\sigma})/\sigma) < r(G/\sigma) \quad \Leftrightarrow \quad r(G|_{\tau\cup\sigma}) < r(G). \tag{4.8}$$

Siden σ er inneholdt i kantmengden til både G og $G|_{\tau\cup\sigma}$, vil kontraksjonen av σ fra G og $G|_{\tau\cup\sigma}$ "fjerne" like mange hjørner fra begge grafene, samtidig som at antall komponenter er konstant. Dermed må rangen også minke like mye i begge tilfeller. Fra dette får vi

$$\begin{aligned} r(G|_{\tau\cup\sigma}) < r(G) \quad &\Rightarrow \quad r((G|_{\tau\cup\sigma})/\sigma) < r(G/\sigma), \text{ og} \\ r(G|_{\tau\cup\sigma}) = r(G) \quad &\Rightarrow \quad r((G|_{\tau\cup\sigma})/\sigma) = r(G/\sigma), \end{aligned}$$

som til sammen gir ekvivalensen (4.8), og resultatet er vist. □



Figur 4.2: Grafen G i eksempel 4.3.7, med restriksjonen $G|_{\{1,2,3,4\}}$ og kontraksjonen $G/\{5\}$.

Eksempel 4.3.7. *Figur* 4.2 *viser grafene G, $G|_{\{1,2,3,4\}}$ og $G/\{5\}$. Vi ser at kokretsene i G er mengdene $\{4,5\}$, $\{2,3,5\}$, $\{2,3,4\}$, $\{1,3,5\}$, $\{1,3,4\}$ og $\{1,2\}$. Altså er fasettene i $\Delta(G)$ komplementmengdene $\{1,2,3\}$, $\{1,4\}$, $\{1,5\}$, $\{2,4\}$, $\{2,5\}$ og $\{3,4,5\}$ ved del* (4.5) *i proposisjon* 4.3.3. *Dermed er $\Delta(G)$ det samme simplisielle komplekset som Δ i eksempel* 4.1.3.

I tillegg er $r(G|_{\{1,2,3,4\}}) = r(G)$*, altså er* $\Delta(G|_{\{1,2,3,4\}}) = \Delta(G)|_{\{1,2,3,4\}}$ *ved proposisjon* 4.3.5*, og vi har også* $\Delta(G/\{5\}) = \text{link}_{\Delta(G)}(\{5\})$ *fra proposisjon* 4.3.6*. Fra figur* 4.2 *er det lett å sjekke at fasettene i* $\Delta(G|_{\{1,2,3,4\}})$ *er* $\{1,2,3\}$*,* $\{1,4\}$*,* $\{2,4\}$ *og* $\{3,4\}$*, mens fasettene i* $\Delta(G/\{5\})$ *er* $\{1\}$*,* $\{2\}$ *og* $\{3,4\}$*, noe som samsvarer med* $\Delta|_{\{1,2,3,4\}}$ *og* $\text{link}_{\Delta}(\{5\})$ *i eksempel* 4.1.3.

4.4 Minimale frie resolusjoner fra grafer

Vi er nå klare til å se på hvilke egenskaper ved en graf G som bestemmer den minimale frie resolusjonen av $\mathbb{K}[\Delta(G)]$. Det første resultatet viser at løkker ikke har betydning for resolusjonen:

Proposisjon 4.4.1. *La* G *være en graf, og la* $L = \{e \mid e \text{ er en løkke i } G\}$*. Da har* $\mathbb{K}[\Delta(G)]$ *og* $\mathbb{K}[\Delta(G|_{[n]\setminus L})]$ *samme minimale frie resolusjon, og generatorene er de samme. Altså har vi, for* $\sigma \subseteq [n]$*,*

$$\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) \;=\; \begin{cases} \beta_{i,\sigma}(\mathbb{K}[\Delta(G|_{[n]\setminus L})]) & \textit{hvis } \sigma \cap L = \emptyset, \\ 0 & \textit{ellers.} \end{cases}$$

Bevis. Vi har $r(G|_{[n]\setminus L}) = r(G)$, altså får vi $\Delta(G|_{[n]\setminus L}) = \Delta(G)|_{[n]\setminus L}$, ved proposisjon 4.3.5. For $\sigma \subseteq [n] \setminus L$ får vi derfor

$$\begin{aligned} \beta_{i,\sigma}(\mathbb{K}[\Delta(G|_{[n]\setminus L})]) &= \dim_{\mathbb{K}} \widetilde{H}_{|\sigma|-i-1}(\Delta(G|_{[n]\setminus L})|_\sigma) \\ &= \dim_{\mathbb{K}} \widetilde{H}_{|\sigma|-i-1}((\Delta(G)|_{[n]\setminus L})|_\sigma) \\ &= \dim_{\mathbb{K}} \widetilde{H}_{|\sigma|-i-1}(\Delta(G)|_\sigma) \\ &= \beta_{i,\sigma}(\mathbb{K}[\Delta(G)]), \end{aligned}$$

ved bruk av Hochsters formel.

Motsatt, la $\sigma \subseteq [n]$ slik at $\sigma \cap L \neq \emptyset$, og la $l \in \sigma \cap L$. Da er l en løkke i G og ikke med i noen kokretser i G. Fra del (4.5) i 4.3.3 er dette ekvivalent med at l er med i alle fasetter i $\Delta(G)$. Men da er l med i alle fasetter også i $\Delta(G)|_\sigma$, dermed er $\Delta(G)|_\sigma$ kontraktibelt og $\widetilde{H}_i(\Delta(G)|_\sigma) = 0$ for alle i. Fra Hochsters formel får vi

$$\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) \;=\; \dim_{\mathbb{K}} \widetilde{H}_{|\sigma|-i-1}(\Delta(G)|_\sigma) \;=\; 0.$$

□

Videre i dette kapittelet begrenser vi oss til å studere *løkkefrie* grafer, altså grafer som ikke inneholder noen løkker, en ikke unaturlig begrensning på bakgrunn av forrige proposisjon.

Før vi går over til å se på hvordan parallelle kanter i en graf G gir utslag for den minimale frie resolusjonen av $\mathbb{K}[\Delta(G)]$, trenger vi å innføre et nytt grafbegrep: For en graf G er en **forenkling** av G grafen som fås ved å fjerne alle løkker og beholde nøyaktig én kant i hver mengde av parallelle kanter i G. Kanter som ikke er løkker eller parallelle, beholdes også. Resultatet blir dermed alltid en enkel graf, altså en graf uten løkker og parallelle kanter. Vi merker oss at en kantmerket graf kan ha flere ulike forenklinger, men de underliggende, umerkede grafene er isomorfe. I vårt tilfelle begrenser vi oss altså til løkkefrie grafer, så en forenkling vil da kun ha betydning for eventuelle parallelle kanter.

Proposisjon 4.4.2. *La G være en løkkefri graf, la $\sigma \subseteq [n]$ og la P_σ være mengden av kanter som fjernes ved en forenkling av $G|_\sigma$. Da har vi:*

$$\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) \quad = \quad \beta_{i-|P_\sigma|,\sigma\setminus P_\sigma}(\mathbb{K}[\Delta(G|_{[n]\setminus P_\sigma})]).$$

Før vi går til beviset, vil vi gi en lang eksakt homologisekvens som vi får bruk for, både i dette beviset og senere, i kombinasjon med Hochsters formel.

Lemma 4.4.3. *For et simplisielt kompleks Δ og $e \in [n]$ er følgende sekvens lang eksakt:*

$$\cdots \to \widetilde{H}_{i+1}(\Delta) \to \widetilde{H}_i(\mathit{link}_\Delta(\{e\})) \to \widetilde{H}_i(\Delta|_{[n]\setminus\{e\}}) \to \widetilde{H}_i(\Delta) \to \widetilde{H}_{i-1}(\mathit{link}_\Delta(\{e\})) \to \cdots .$$

Bevis. Dette er en konsekvens av den såkalte Mayer-Vietori-sekvensen:

$$\cdots \to H_{i+1}(X) \to H_i(A) \to H_i(X_1) \oplus H_i(X_2) \to H_i(X) \to H_{i-1}(A) \to \cdots .$$

Denne er lang eksakt når $X = X_1 \cup X_2$ er et topologisk rom, X_1 og X_2 er åpne delmengder av X og $A = X_1 \cap X_2$ (Se kapittel 17 i [GH]).

Vi definerer **stjernen** til $\sigma \in \Delta$, betegnet $\mathrm{star}_\Delta(\sigma)$, som det simplisielle komplekset vi får ved å beholde kun de fjesene i Δ som inneholder σ, i tillegg til delmengder av disse. Dersom vi for $e \in [n]$ lar $X = \Delta$, $X_1 = \Delta|_{[n]\setminus\{e\}}$ og $X_2 = \mathrm{star}_\Delta(\{e\})$ (egentlig en åpen omegn om $\Delta|_{[n]\setminus\{e\}}$ og $\mathrm{star}_\Delta(\{e\})$), er det lett å se at vi har $X = X_1 \cup X_2$ og $A = (\Delta|_{[n]\setminus\{e\}}) \cap (\mathrm{star}_\Delta(\{e\})) = \mathrm{link}_\Delta(\{e\})$. I tillegg er $\mathrm{star}_\Delta(\{e\})$ kontraktibel siden e er inneholdt i alle fasettene, altså er $\widetilde{H}_i(\mathrm{star}_\Delta(\{e\})) = 0$ for alle i, og vi får $\widetilde{H}_i(\Delta|_{[n]\setminus\{e\}}) \oplus \widetilde{H}_i(\mathrm{star}_\Delta(\{e\})) \cong \widetilde{H}_i(\Delta|_{[n]\setminus\{e\}})$ for alle i. Dermed er sekvensen i lemmaet over lik Mayer-Vietori-sekvensen med disse valgene av X, X_1 og X_2 og følgelig lang eksakt. □

Nå kan vi bevise proposisjon 4.4.2:

Bevis. Ved induksjon er det nok å vise at resultatet gjelder for $\sigma \subseteq [n]$ med $|P_\sigma| = 1$, og vi lar $p, q \in \sigma$ være de to parallelle kantene i $G|_\sigma$, med $P_\sigma = \{p\}$. Vi må altså vise at

$$\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) \quad = \quad \beta_{i-1,\sigma\setminus\{p\}}(\mathbb{K}[\Delta(G|_{[n]\setminus\{p\}})]).$$

Siden p og q er parallelle, får vi at $r(G|_{\sigma\setminus\{p\}}) = r(G|_\sigma)$ og $r(G|_{[n]\setminus\{p\}}) = r(G)$. Kombinert med korollar 4.3.4 gir dette at dersom $r(G|_\sigma) < r(G)$, får vi $\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) = 0$ og $\beta_{i,\sigma\setminus\{p\}}(\mathbb{K}[\Delta(G|_{[n]\setminus\{p\}})]) = 0$ for alle i, og resultatet holder.

La oss derfor anta at $r(G|_\sigma) = r(G)$, som altså gir $r(G|_{\sigma\setminus\{p\}}) = r(G|_{[n]\setminus\{p\}})$. Vi har at kokretser i $G|_\sigma$ inneholder p hvis og bare hvis de også inneholder q, som ved del (4.5) i proposisjon 4.3.3 gir at q må være inneholdt i alle fasetter i $\Delta(G|_\sigma)$ som inneholder p. Dermed er q inneholdt i alle fasetter i $\mathrm{link}_{\Delta(G|_\sigma)}(\{p\})$, vi får at $\mathrm{link}_{\Delta(G|_\sigma)}(\{p\})$ er kontraktibel og $\widetilde{H}_i(\mathrm{link}_{\Delta(G|_\sigma)}(\{p\})) = 0$ for alle i. Ved lemma 4.4.3 ovenfor må vi derfor ha $\widetilde{H}_i(\Delta(G|_\sigma)|_{\sigma\setminus\{p\}}) \cong \widetilde{H}_i(\Delta(G|_\sigma))$. Men fordi $r(G|_{\sigma\setminus\{p\}}) = r(G|_\sigma)$ har vi $\Delta(G|_{\sigma\setminus\{p\}}) = \Delta(G|_\sigma)|_{\sigma\setminus\{p\}}$ fra proposisjon 4.3.5, og vi får $\widetilde{H}_i(\Delta(G|_{\sigma\setminus\{p\}})) \cong \widetilde{H}_i(\Delta(G|_\sigma))$. Hochsters formel gir da

$$\begin{aligned}
\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) &= \dim_{\mathbb{K}} \widetilde{H}_{|\sigma|-i-1}(\Delta(G)|_\sigma) \\
&= \dim_{\mathbb{K}} \widetilde{H}_{|\sigma|-i-1}(\Delta(G|_\sigma)) \\
&= \dim_{\mathbb{K}} \widetilde{H}_{|\sigma|-i-1}(\Delta(G|_{\sigma\setminus\{p\}})) \\
&= \dim_{\mathbb{K}} \widetilde{H}_{|\sigma|-i-1}(\Delta(G|_{[n]\setminus\{p\}})|_{\sigma\setminus\{p\}}) \\
&= \beta_{i-1,\sigma\setminus\{p\}}(\mathbb{K}[\Delta(G|_{[n]\setminus\{p\}})]),
\end{aligned}$$

som var det vi skulle vise. (Vi har $\Delta(G|_{\sigma\setminus\{p\}}) = \Delta((G|_{[n]\setminus\{p\}})|_{\sigma\setminus\{p\}}) = \Delta(G|_{[n]\setminus\{p\}})|_{\sigma\setminus\{p\}}$ fra proposisjon 4.3.5, siden $r(G|_{\sigma\setminus\{p\}}) = r(G|_{[n]\setminus\{p\}})$.) □

Som vi senere skal se, gir det neste resultatet (og beviset for dette) oss det vi trenger for å kunne bestemme den minimale frie resolusjonen av $\mathbb{K}[\Delta(G)]$, gitt grafen G:

Teorem 4.4.4. *For en løkkefri graf G har vi $\beta_{k(G)+1,[n]}(\mathbb{K}[\Delta(G)]) \neq 0$, der $k(G)$ er kretsrangen til G.*

Bevis. Fra proposisjon 4.4.2 kan vi begrense oss til tilfellet der G er en enkel graf, altså en graf uten (løkker og) parallelle kanter, siden kretsrangen minker med én for hver parallelle kant som fjernes.

La først G være et tre. Da har vi at $k(G) = 0$, og $\beta_{1,[n]}(\mathbb{K}[\Delta(G)]) = 1 \neq 0$, siden $G = G|_{[n]}$ er et utspennende tre for G.

Anta så at G ikke er et tre. Ved induksjon på n vil vi vise at vi også i dette tilfellet har $\beta_{k(G)+1,[n]}(\mathbb{K}[\Delta(G)]) \neq 0$.

Induksjonen vår starter med $n = 3$, siden det for $n < 3$ ikke eksisterer enkle grafer som ikke er trær, mens det for $n = 3$ eksisterer nøyaktig én, nemlig grafen G bestående av tre kanter som danner en krets. Vi har $k(G) = 1$, og vi vil derfor regne ut $\beta_{2,[n]}(\mathbb{K}[\Delta(G)])$, som ved Hochsters formel er dimensjonen til $\widetilde{H}_{n-2-1}(\Delta(G)) = \widetilde{H}_0(\Delta(G))$. De eneste kantmengdene i G som ikke har full rang, er de som består av nøyaktig én kant, altså har vi $\Delta(G) = \{\emptyset, \{1\}, \{2\}, \{3\}\}$, som har 3 komponenter. Dette gir at $\dim_{\mathbb{K}} \widetilde{H}_0(\Delta(G)) = 2 \neq 0$, altså gjelder resultatet for G.

Anta så at $\beta_{k(G)+1,[j]}(\mathbb{K}[\Delta(G')]) \neq 0$ for alle enkle grafer G' der $E(G') = [j]$ og $j < n$, og la G være en enkel graf som ikke er et tre, med $E(G) = [n]$. Siden G ikke er et tre, er $k(G) > 0$, og det eksisterer dermed en $e \in [n]$ slik at $r(G|_{[n]\setminus\{e\}}) = r(G)$. I tillegg har vi $|E(G|_{[n]\setminus\{e\}})| = n - 1$, og dermed $k(G|_{[n]\setminus\{e\}}) = k(G) - 1$. Altså er $G|_{[n]\setminus\{e\}}$ omfattet av induksjonshypotesen, og vi får

$$\begin{aligned}\beta_{k(G),[n]\setminus\{e\}}(\mathbb{K}[\Delta(G|_{[n]\setminus\{e\}})]) &= \beta_{k(G),[n]\setminus\{e\}}(\mathbb{K}[\Delta(G)|_{[n]\setminus\{e\}}]) \\ &= \dim_{\mathbb{K}} \widetilde{H}_{r(G)-2}(\Delta(G)|_{[n]\setminus\{e\}}) \\ &\neq 0.\end{aligned}$$

Hvis vi i stedet ser på $G/\{e\}$, kontraksjonen av $\{e\}$ fra G, får vi $|E(G/\{e\})| = n - 1$ og $r(G/\{e\}) = r(G) - 1$ (siden $G/\{e\}$ har ett hjørne mindre enn G og like mange sammenhengskomponenter), og dermed $k(G/\{e\}) = k(G)$. Også $G/\{e\}$ er derfor omfattet av induksjonshypotesen, og vi får

$$\begin{aligned}\beta_{k(G)+1,[n]\setminus\{e\}}(\mathbb{K}[\Delta(G/\{e\})]) &= \beta_{k(G)+1,[n]\setminus\{e\}}(\mathbb{K}[\mathrm{link}_{\Delta(G)}(\{e\})]) \\ &= \dim_{\mathbb{K}} \widetilde{H}_{r(G)-3}(\mathrm{link}_{\Delta(G)}(\{e\})) \\ &\neq 0.\end{aligned}$$

Siden resolusjonene av $\mathbb{K}[\Delta(G)|_{[n]\setminus\{e\}}]$ og $\mathbb{K}[\mathrm{link}_{\Delta(G)}(\{e\})]$ er lineære, får vi også at $\beta_{i,[n]\setminus\{e\}}(\mathbb{K}[\Delta(G)|_{[n]\setminus\{e\}}]) = 0$ og $\beta_{i+1,[n]\setminus\{e\}}(\mathbb{K}[\mathrm{link}_{\Delta(G)}(\{e\})]) = 0$ når $i \neq k$, og dermed er $\widetilde{H}_j(\Delta(G)|_{[n]\setminus\{e\}}) = 0$ og $\widetilde{H}_{j-1}(\mathrm{link}_{\Delta(G)}(\{e\})) = 0$ for $j \neq r(G) - 2$. Spesielt er $\widetilde{H}_{r(G)-3}(\Delta(G)|_{[n]\setminus\{e\}}) = 0$ og $\widetilde{H}_{r(G)-2}(\mathrm{link}_{\Delta(G)}(\{e\})) = 0$. Ved lemma 4.4.3 har vi derfor en kort eksakt sekvens

$$0 \;\to\; \widetilde{H}_{r(G)-2}(\Delta(G)|_{[n]\setminus\{e\}}) \;\to\; \widetilde{H}_{r(G)-2}(\Delta(G)) \;\to\; \widetilde{H}_{r(G)-3}(\mathrm{link}_{\Delta(G)}(\{e\})) \;\to\; 0, \tag{4.9}$$

der altså $\widetilde{H}_{r(G)-2}(\Delta(G)|_{[n]\setminus\{e\}})$ og $\widetilde{H}_{r(G)-3}(\text{link}_{\Delta(G)}(\{e\}))$ er ulik 0. Dette betyr at også $\widetilde{H}_{r(G)-2}(\Delta(G))$ er ulik 0, og vi får

$$\dim_{\mathbb{K}} \widetilde{H}_{r(G)-2}(\Delta(G)) \quad = \quad \beta_{k(G)+1,[n]}(\mathbb{K}[\Delta(G)]) \quad \neq \quad 0.$$

□

Lengden l til den minimale frie resolusjonen av $\mathbb{K}[\Delta(G)]$ følger nå ganske direkte:

Korollar 4.4.5. *Lengden l til den minimale frie resolusjonen av $\mathbb{K}[\Delta(G)]$ for en løkkefri graf G er $l = k(G) + 1$.*

Bevis. Tidligere, på side 87, har vi sett at vi må ha $l \leq k(G) + 1$. Men teorem 4.4.4 gir at $\beta_{k(G)+1,[n]}(\mathbb{K}[\Delta(G)]) \neq 0$, dermed er også det $(k(G) + 1)$-te totale Betti-tallet til G ulik 0, og vi får $l \geq k(G) + 1$. □

Ved å kombinere proposisjon 4.4.1 og teorem 4.4.4 får vi at dersom $L \subseteq [n]$ er mengden av løkker i en graf G, så er $\beta_{k(G)+1-|L|,[n]\setminus L}(\mathbb{K}[\Delta(G)]) \neq 0$, mens $\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) = 0$ for alle i dersom σ ekte inneholder $[n] \setminus L$. Dermed får vi, ved lignende argument som i beviset for korollar 4.4.5, at lengden til den minimale frie resolusjonen av $\mathbb{K}[\Delta(G)]$ er $l = k(G) + 1 - |L|$.

Vi merker oss også at det $(k(G) + 1)$-te totale Betti-tallet til G, $\beta_{k(G)+1}(\mathbb{K}[\Delta(G)])$, er lik det multigraderte Betti-tallet $\beta_{k(G)+1,[n]}(\mathbb{K}[\Delta(G)])$, siden den minimale frie resolusjonen av $\mathbb{K}[\Delta(G|_\sigma)]$ er lineær, og ingen andre delmengder av $[n]$ har kardinalitet n.

Teorem 4.4.4 gir oss videre hvilke delmengder av $[n]$ som har $\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) \neq 0$ for én i, og for hvilken i dette skjer:

Korollar 4.4.6. *For en løkkefri graf G, la $\sigma \subseteq [n]$ være slik at $r(G|_\sigma) = r(G)$. Da gjelder følgende:*

$$k(G|_\sigma) = i - 1 \quad \Leftrightarrow \quad \beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) \neq 0.$$

Videre har vi i dette tilfellet at $\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) = \beta_{i,\sigma}(\mathbb{K}[\Delta(G|_\sigma)])$.

Bevis. Siden $r(G|_\sigma) = r(G)$, er

$$\begin{aligned} \beta_{i,\sigma}(\mathbb{K}[\Delta(G|_\sigma)]) &= \dim_{\mathbb{K}} \widetilde{H}_{|\sigma|-i-1}(\Delta(G|_\sigma)) \\ &= \dim_{\mathbb{K}} \widetilde{H}_{|\sigma|-i-1}(\Delta(G)|_\sigma) \\ &= \beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) \end{aligned}$$

for alle i. Teorem 4.4.4 gir at $\beta_{i,\sigma}(\mathbb{K}[\Delta(G|_\sigma)]) \neq 0$ når $i = k(G|_\sigma) + 1$, og siden den minimale frie resolusjonen av $\mathbb{K}[\Delta(G|_\sigma)]$ er lineær, er dette også den eneste verdien for i der dette gjelder. □

Forrige korollar gir dermed at alle $\sigma \subseteq [n]$ med $r(G|_\sigma) = r(G)$ har $\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) \neq 0$ for nøyaktig én i. Dermed får vi det resultatet vi beskrev på side 88, nemlig ekvivalens i uttrykket (4.6) og korollar 4.3.4:

Korollar 4.4.7. *For en løkkefri graf G og $\sigma \subseteq [n]$ er følgende ekvivalent:*

i) $\sigma \in \Delta(G)$.

ii) $r(G|_\sigma) < r(G)$.

iii) $\widetilde{H}_i(\Delta(G)|_\sigma) = 0$ *for alle* i.

iv) $\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) = 0$ *for alle* i.

Bevis. Ekvivalensen *i)* $\Leftrightarrow$ *ii)* er del (4.3) i proposisjon 4.3.3, *iii)* $\Leftrightarrow$ *iv)* følger fra Hochsters formel og *ii)* $\Leftrightarrow$ *iv)* altså fra korollar 4.4.6, kombinert med korollar 4.3.4. □

En siste følge av teorem 4.4.4 som vi tar med, er en nyttig konsekvens av den korte eksakte sekvensen (4.9) i beviset:

Korollar 4.4.8. *La G være en løkkefri graf som ikke er et tre, og la $e \in [n]$ være slik at $r(G|_{[n]\setminus\{e\}}) = r(G)$. Da har vi:*

$$\begin{aligned}\beta_{k(G)+1,[n]}(\mathbb{K}[\Delta(G)]) &= \beta_{k(G),[n]\setminus\{e\}}(\mathbb{K}[\Delta(G)|_{[n]\setminus\{e\}}]) + \beta_{k(G)+1,[n]\setminus\{e\}}(\mathbb{K}[\mathrm{link}_{\Delta(G)}(\{e\})]) \\ &= \beta_{k(G),[n]\setminus\{e\}}(\mathbb{K}[\Delta(G|_{[n]\setminus\{e\}})]) + \beta_{k(G)+1,[n]\setminus\{e\}}(\mathbb{K}[\Delta(G/\{e\})]).\end{aligned}$$

Bevis. Den første likheten følger direkte fra sekvensen (4.9) og Hochsters formel, siden (4.9) gir at

$$\dim_{\mathbb{K}} \widetilde{H}_{r(G)-2}(\Delta(G)) = \dim_{\mathbb{K}} \widetilde{H}_{r(G)-2}(\Delta(G)|_{[n]\setminus\{e\}}) + \dim_{\mathbb{K}} \widetilde{H}_{r(G)-3}(\mathrm{link}_{\Delta(G)}(\{e\})),$$

mens den andre likheten kommer fra proposisjonene 4.3.5 og 4.3.6. □

Legg merke til at vi i forrige korollar kan benytte multigraderte og totale Betti-tall om hverandre, siden vi som tidligere nevnt har $\beta_{k+1}(\mathbb{K}[\Delta(G)]) = \beta_{k+1,[n]}(\mathbb{K}[\Delta(G)])$ for enhver graf G.

Korollar 4.4.8 gir oss altså en enkel metode for å redusere til to enklere tilfeller når vi skal finne Betti-tallene som inngår i den minimale frie resolusjonen av $\mathbb{K}[\Delta(G)]$, for en graf G. Dette vil vi gjøre mye bruk av når vi nå går over til å studere konkrete grafer.

4.5 Noen eksempler

Før vi gir konkrete eksempler på minimale frie resolusjoner, gir vi to resultater til, som vi etter hvert vil bruke i eksemplene. Det første viser at vi kan begrense oss til å finne de multigraderte Betti-tallene til kantmengder uten broer:

Proposisjon 4.5.1. *La G være en graf, og la $B = \{e \mid e$ er en bro i $G\}$. Dersom $B \neq [n]$, har vi*

$$\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) = \beta_{i,\sigma\setminus B}(\mathbb{K}[\Delta(G/B)])$$

for alle $\sigma \subseteq [n]$ med $r(G|_\sigma) = r(G)$.

Bevis. Ved induksjon er det nok å vise at resultatet gjelder når $|B| = 1$, og vi lar $B = \{b\}$. Vi må altså vise at

$$\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) = \beta_{i,\sigma\setminus\{b\}}(\mathbb{K}[\Delta(G/\{b\})])$$

for alle $\sigma \subseteq [n]$ med $r(G|_\sigma) = r(G)$.

Fordi $r(G|_\sigma) = r(G)$, så må $b \in \sigma$. Altså er $\{b\}$ en separerende kantmengde i $G|_\sigma$ og $\sigma \setminus \{b\} \in \Delta(G|_\sigma) = \Delta(G)|_\sigma$. Dermed er $\sigma \setminus \{b\}$ også et fjes i $\Delta(G)|_{\sigma\setminus\{b\}}$, altså er $\Delta(G)|_{\sigma\setminus\{b\}} = \mathcal{P}(\sigma \setminus \{b\})$, potensmengden til $\sigma \setminus \{b\}$, og vi får $\widetilde{H}_i(\Delta(G)|_{\sigma\setminus\{b\}}) = \widetilde{H}_i(\Delta(G|_\sigma)|_{\sigma\setminus\{b\}}) = 0$ for alle i. Fra lemma 4.4.3 har vi derfor $\widetilde{H}_i(\Delta(G|_\sigma)) \cong \widetilde{H}_{i-1}(\mathrm{link}_{\Delta(G|_\sigma)}(\{b\}))$ for alle i. Vi får

$$\begin{aligned}
\beta_{i,\sigma}(\mathbb{K}[\Delta(G)]) &= \dim_{\mathbb{K}} \widetilde{H}_{|\sigma|-i-1}(\Delta(G)|_\sigma) \\
&= \dim_{\mathbb{K}} \widetilde{H}_{|\sigma|-i-1}(\Delta(G|_\sigma)) \\
&= \dim_{\mathbb{K}} \widetilde{H}_{|\sigma|-i-2}(\mathrm{link}_{\Delta(G|_\sigma)}(\{b\})) \\
&= \dim_{\mathbb{K}} \widetilde{H}_{|\sigma|-i-2}(\mathrm{link}_{\Delta(G)}(\{b\})|_{\sigma\setminus\{b\}}) \\
&= \beta_{i,\sigma\setminus\{b\}}(\mathbb{K}[\mathrm{link}_{\Delta(G)}(\{b\})]) \\
&= \beta_{i,\sigma\setminus\{b\}}(\mathbb{K}[\Delta(G/\{b\})]).
\end{aligned}$$

(Vi har $\mathrm{link}_{\Delta(G|_\sigma)}(\{b\}) = \mathrm{link}_{\Delta(G)}(\{b\})|_{\sigma\setminus\{b\}}$, siden begge består av delmengder τ av $\sigma \setminus \{b\}$ slik at $\tau \cup \{b\} \in \Delta(G)$.) □

Dersom $B = [n]$, altså tilfellet der G er et tre, kan vi bruke forrige proposisjon med B lik mengden av $n-1$ vilkårlige kanter i G. Dette er likevel ikke særlig nyttig, siden vi allerede vet hvordan den minimale frie resolusjonen i dette tilfellet ser ut.

Neste resultat er en enkel anvendelse av korollar 4.4.8 og gir alt vi trenger for å finne den minimale frie resolusjonen av $\mathbb{K}[\Delta(G)]$ når G er en n-krets:

Proposisjon 4.5.2. *La G være en n-krets for $n \geq 2$. Da er lengden til den minimale frie resolusjonen av $\mathbb{K}[\Delta(G)]$ lik $l = 2$, og de totale Betti-tallene er $\beta_1(\mathbb{K}[\Delta(G)]) = n$ og $\beta_2(\mathbb{K}[\Delta(G)]) = n-1$.*

Bevis. At $l = 2$ følger direkte av korollar 4.4.5, siden G er løkkefri og $k(G) = 1$. I tillegg er alle delmengder av $[n]$ av kardinalitet $n-1$ kantmengder til utspennende trær i G, altså er $\beta_1(\mathbb{K}[\Delta(G)]) = \binom{n}{n-1} = n$.

At $\beta_2(\mathbb{K}[\Delta(G)]) = n-1$ viser vi ved induksjon på n, men først merker vi oss at $\beta_2(\mathbb{K}[\Delta(G)]) = \beta_{2,[n]}(\mathbb{K}[\Delta(G)])$, det andre multigraderte Betti-tallet til hele grafen.

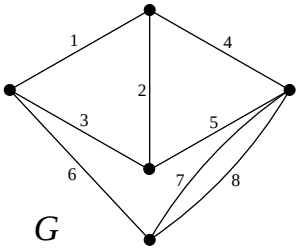
For $n = 2$ benytter vi oss av proposisjon 4.4.2, og får at $\beta_{2,[2]}(\mathbb{K}[\Delta(G)])$ for 2-kretsen er lik $\beta_{1,[1]}(\mathbb{K}[\Delta(G')])$ når G' er grafen som består av nøyaktig én bro. Men dette er lik 1, som var det vi skulle vise.

Anta så at resultatet gjelder for $j = n-1$, og la G være en n-krets. Ved korollar 4.4.8 er $\beta_{2,[n]}(\mathbb{K}[\Delta(G)]) = \beta_{1,[n]\setminus\{e\}}(\mathbb{K}[\Delta(G|_{[n]\setminus\{e\}})]) + \beta_{2,[n]\setminus\{e\}}(\mathbb{K}[\Delta(G/\{e\})])$ for en vilkårlig kant e, siden enhver kant i G gir $r(G|_{[n]\setminus\{e\}}) = r(G)$. Videre er $G|_{[n]\setminus\{e\}}$ en sti med $n-1$ kanter, altså er $\beta_{1,[n]\setminus\{e\}}(\mathbb{K}[\Delta(G|_{[n]\setminus\{e\}})]) = 1$, mens $G/\{e\}$ er en $(n-1)$-krets, som er omfattet av induksjonshypotesen. Vi får derfor at $\beta_2(\mathbb{K}[\Delta(G)]) = n-1$. □

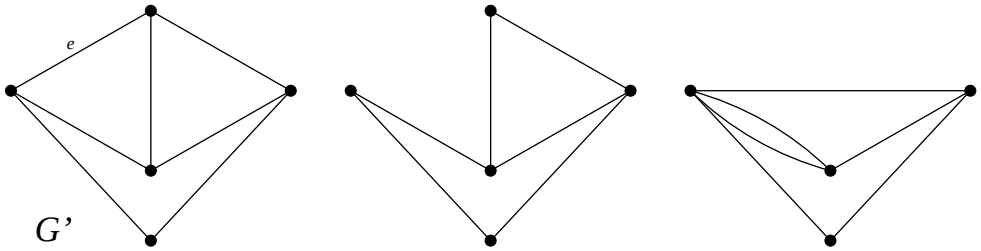
Når vi nå videre vil gi eksempler på minimale frie resolusjoner, vil vi benytte $\mathbb{N}$-graderingen av de frie modulene F_i, gitt ved summen av koordinatene i $\mathbb{N}^n$-graderingen, i framstillingene av disse. Siden vi har kvadratfrie grader (ved teorem 4.2.6), er dette i vårt tilfelle også lik kardinaliteten til den tilhørende delmengden av $[n]$. I tillegg, siden alle resolusjonene i denne oppgaven er lineære, er kardinaliteten til alle generatorer for hver modul den samme, og hver F_i er dermed alltid isomorf til $R(-i-d)^{\beta_i(\mathbb{K}[\Delta(G)])}$ for én fiksert $d \in \mathbb{N}$. Dersom vi for eksempel

har en $\mathbb{N}^4$-gradert fri modul $F \cong R(-(1,0,1,1))^2 \oplus R(-(1,1,0,1)) \oplus R(-(0,1,1,1))^3$, vil $\mathbb{N}$-graderingen altså være $F \cong R(-3)^6$.

Vi gjør denne forenklingen fordi $\mathbb{N}^n$-graderingen vil gi veldig store uttrykk for de frie modulene i resolusjonene når disse har mange generatorer, for eksempel har vi i eksempel 4.5.3 nedenfor 51 ulike generatorer for F_2. Merk at det likevel er lett å gi også de $\mathbb{N}^n$-graderte resolusjone ut fra teksten i eksemplene, siden vi alltid eksplisitt gir generatorene for hver F_i.



Figur 4.3: Grafen G i eksempel 4.5.3.



Figur 4.4: En (umerket) forenkling G' av grafen G på figur 4.3, med restriksjonen og kontraksjonen som brukes i eksempel 4.5.3.

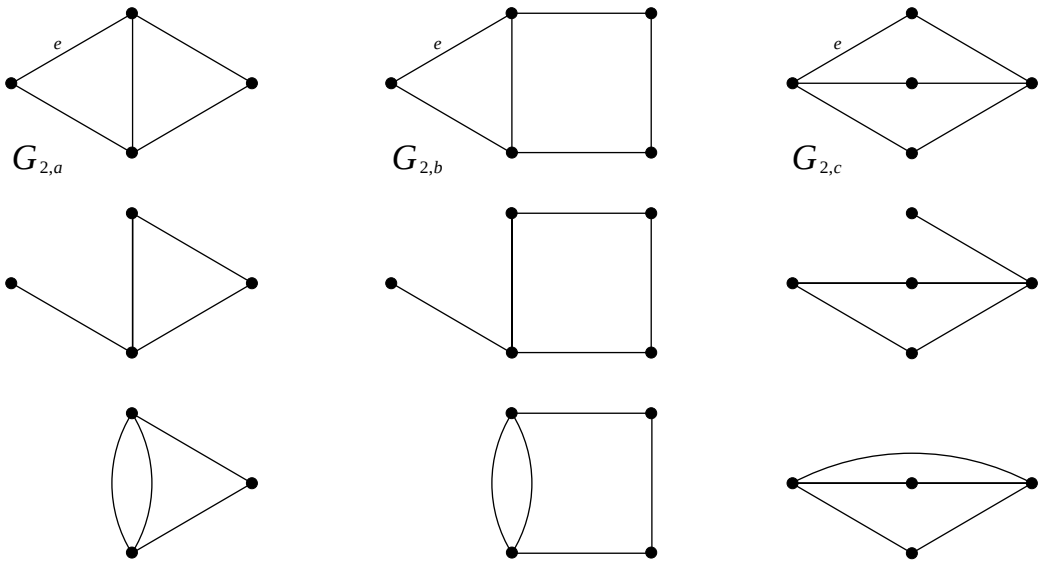
Eksempel 4.5.3. *Vårt første eksempel er grafen G på figur 4.3, og vi vil finne den minimale frie resolusjonen av $\mathbb{K}[\Delta(G)]$.*

Vi merker oss at vi har $n = 8$ og $r = |V(G)| - 1 = 4$, altså får vi $k = 4$ og lengden til resolusjonen $l = k + 1 = 5$. Ved korollar 4.4.6 ønsker vi altså for $1 \leq i \leq 5$ å finne $\beta_{i,\sigma}(\mathbb{K}[\Delta(G)])$ for alle $\sigma \subseteq [8]$ med $r(G|_\sigma) = r(G)$ og $k(G|_\sigma) = i - 1$.

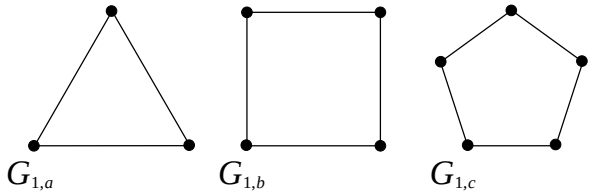
Før vi ser på hvilke $\sigma \subseteq [8]$ dette gjelder, vil vi studere bestemte delgrafer av G, nemlig alle (umerkede) ikke-isomorfe, enkle delgrafer uten broer. Disse er vist på figurene 4.5 (øverste linje) og 4.6, i tillegg til grafen G' på figur 4.4. Vi ønsker å finne det siste totale Betti-tallet til Stanley-Reisner-ringene som kommer fra disse grafene (som vi tidligere har sett at er lik det siste multigraderte Betti-tallet i grad $[n]$), og vi skal senere se hvorfor.

Proposisjon 4.5.2 gir oss dette for grafene på figur 4.6, nemlig $\beta_2(\mathbb{K}[\Delta(G_{1,a})]) = 2$, $\beta_2(\mathbb{K}[\Delta(G_{1,b})]) = 3$ og $\beta_2(\mathbb{K}[\Delta(G_{1,c})]) = 4$.

Når det gjelder grafene $G_{2,a}$, $G_{2,b}$ og $G_{2,c}$ på figur 4.5 og G' på figur 4.4, benytter vi oss av korollar 4.4.8 for å redusere til to enklere grafer, nemlig $G|_{[n]\setminus\{e\}}$ og $G/\{e\}$, for en kant e der $r(G|_{[n]\setminus\{e\}}) = r(G)$. Disse grafene er vist på de tilhørende figurene, og den valgte kanten e er også markert her.



Figur 4.5: Øverst: Delgrafer av grafen G' på figur 4.4 som har kretsrang $k = 2$. Under: Tilhørende restriksjoner og kontraksjoner som brukes i eksempel 4.5.3.



Figur 4.6: Delgrafer av grafen G' på figur 4.4 som har kretsrang $k = 1$.

Vi kan benytte korollar 4.5.1 *og redusere* $(G_{2,a})|_{[n]\setminus\{e\}}$ *til* $G_{1,a}$ *og både* $(G_{2,b})|_{[n]\setminus\{e\}}$ *og* $(G_{2,c})|_{[n]\setminus\{e\}}$ *til* $G_{1,b}$*, mens proposisjon* 4.4.2 *kan brukes til å redusere* $(G_{2,a})/\{e\}$*,* $(G_{2,b})/\{e\}$ *og* $(G')/\{e\}$ *til henholdsvis* $G_{1,a}$*,* $G_{1,b}$ *og* $G_{2,a}$*. Videre er* $(G_{2,c})/\{e\} \cong G_{2,a}$ *og* $(G')|_{[n]\setminus\{e\}} \cong G_{2,b}$*. Dermed får vi:*

$$\begin{aligned}
\beta_3(\mathbb{K}[\Delta(G_{2,a})]) &= \beta_2(\mathbb{K}[\Delta(G_{1,a})]) + \beta_2(\mathbb{K}[\Delta(G_{1,a})]) &&= 4,\\
\beta_3(\mathbb{K}[\Delta(G_{2,b})]) &= \beta_2(\mathbb{K}[\Delta(G_{1,b})]) + \beta_2(\mathbb{K}[\Delta(G_{1,b})]) &&= 6,\\
\beta_3(\mathbb{K}[\Delta(G_{2,c})]) &= \beta_2(\mathbb{K}[\Delta(G_{1,b})]) + \beta_3(\mathbb{K}[\Delta(G_{2,a})]) &&= 7,\\
\beta_4(\mathbb{K}[\Delta(G')]) &= \beta_3(\mathbb{K}[\Delta(G_{2,b})]) + \beta_3(\mathbb{K}[\Delta(G_{2,a})]) &&= 10.
\end{aligned}$$

Vi kan nå gå videre til å studere delmengder av $[n]$ *som genererer de frie modulene* F_i *i den minimale frie resolusjonen av* $\mathbb{K}[\Delta(G)]$*, og som vi skal se, er Betti-tallene vi har funnet til nå, nok til å finne Betti-tallene for alle disse generatorene. Vi begynner med* F_1*, som altså er generert av alle utspennende trær i* G*. Disse har dermed kardinalitet lik* $r(G) = 4$*, og er*

følgende delmengder av [8]*:*

$$\left\{\begin{matrix}\{1,2,4,6\},\{1,2,4,7\},\{1,2,4,8\},\{1,2,5,6\},\{1,2,5,7\},\{1,2,5,8\},\{1,2,6,7\},\{1,2,6,8\},\\ \{1,3,4,6\},\{1,3,4,7\},\{1,3,4,8\},\{1,3,5,6\},\{1,3,5,7\},\{1,3,5,8\},\{1,3,6,7\},\{1,3,6,8\},\\ \{1,4,5,6\},\{1,4,5,7\},\{1,4,5,8\},\{1,5,6,7\},\{1,5,6,8\},\{2,3,4,6\},\{2,3,4,7\},\{2,3,4,8\},\\ \{2,3,5,6\},\{2,3,5,7\},\{2,3,5,8\},\{2,3,6,7\},\{2,3,6,8\},\{2,4,6,7\},\{2,4,6,8\},\{2,5,6,7\},\\ \{2,5,6,8\},\{3,4,5,6\},\{3,4,5,7\},\{3,4,5,8\},\{3,4,6,7\},\{3,4,6,8\},\{4,5,6,7\},\{4,5,6,8\}\end{matrix}\right\}$$

Det er altså 40 *utspennende trær i* G*, og alle har første multigraderte Betti-tall lik* 1*. Dermed er* $F_1 \cong R(-4)^{40}$*.*

Når det gjelder F_2*, er denne generert av delmengder* $\sigma \subseteq [8]$ *med* $r(G|_\sigma) = r(G)$ *og* $k(G|_\sigma) = 1$*, eller alternativt, delmengder av kardinalitet* 5 *som inneholder nøyaktig én krets. Disse er gitt i følgende tabell, der grafen som står til venstre er delgrafen vi får ved å forenkle* $G|_\sigma$*, for deretter å kontrahere alle broer dersom ikke forenklingen er et tre.*

Et tre	$\{1,2,4,7,8\},\{1,2,5,7,8\},\{1,2,6,7,8\},\{1,3,4,7,8\},\{1,3,5,7,8\},\{1,3,6,7,8\},$ $\{1,4,5,7,8\},\{1,5,6,7,8\},\{2,3,4,7,8\},\{2,3,5,7,8\},\{2,3,6,7,8\},\{2,4,6,7,8\},$ $\{2,5,6,7,8\},\{3,4,5,7,8\},\{3,4,6,7,8\},\{4,5,6,7,8\}.$
$G_{1,a}$	$\{1,2,3,4,6\},\{1,2,3,4,7\},\{1,2,3,4,8\},\{1,2,3,5,6\},\{1,2,3,5,7\},\{1,2,3,5,8\},$ $\{1,2,3,6,7\},\{1,2,3,6,8\},\{1,2,4,5,6\},\{1,2,4,5,7\},\{1,2,4,5,8\},\{2,3,4,5,6\},$ $\{2,3,4,5,7\},\{2,3,4,5,8\},\{2,4,5,6,7\},\{2,4,5,6,8\}.$
$G_{1,b}$	$\{1,2,4,6,7\},\{1,2,4,6,8\},\{1,3,4,5,6\},\{1,3,4,5,7\},\{1,3,4,5,8\},\{1,3,4,6,7\},$ $\{1,3,4,6,8\},\{1,3,5,6,7\},\{1,3,5,6,8\},\{1,4,5,6,7\},\{1,4,5,6,8\},\{2,3,5,6,7\},$ $\{2,3,5,6,8\},\{3,4,5,6,7\},\{3,4,5,6,8\}.$
$G_{1,c}$	$\{1,2,5,6,7\},\{1,2,5,6,8\},\{2,3,4,6,7\},\{2,3,4,6,8\}.$

Nå har vi også det vi trenger for å finne det andre multigraderte Betti-tallet til alle generatorene til F_2*. La oss ta et par eksempler:*

Grafen $G|_{\{1,2,4,7,8\}}$ *består av de parallelle kantene* 7 *og* 8*, foruten tre broer. Delmengden* $\{1,2,4,7,8\}$ *har altså kardinalitet* 5 *og inneholder nøyaktig én krets, nemlig kantene* 7 *og* 8*, dermed er* $\beta_{2,\{1,2,4,7,8\}}(\mathbb{K}[\Delta(G)]) \neq 0$*. Videre er grafen* $G|_{\{1,2,4,7\}}$ *en forenkling av* $G|_{\{1,2,4,7,8\}}$*, og proposisjon* 4.4.2 *gir at* $\beta_{2,\{1,2,4,7,8\}}(\mathbb{K}[\Delta(G)]) = \beta_{1,\{1,2,4,7\}}(\mathbb{K}[\Delta(G)])$*. Men* $G|_{\{1,2,4,7\}}$ *er et tre, altså har vi* $\beta_{2,\{1,2,4,7,8\}}(\mathbb{K}[\Delta(G)]) = 1$*. Dette gjelder også alle andre delmengder som er listet opp i første rekke i tabellen ovenfor.*

Grafen $G|_{\{1,2,3,4,6\}}$ *består av* 3*-kretsen* $G|_{\{1,2,3\}}$*, i tillegg til to broer. Delmengden* $\{1,2,3,4,6\}$ *har dermed også kardinalitet* 5 *og inneholder nøyaktig én krets, dermed er også* $\beta_{2,\{1,2,3,4,6\}}(\mathbb{K}[\Delta(G)]) \neq 0$*. Vi benytter proposisjon* 4.5.1 *og får at* $\beta_{2,\{1,2,3,4,6\}}(\mathbb{K}[\Delta(G)]) = \beta_{2,\{1,2,3\}}(\mathbb{K}[\Delta(G/\{4,6\})]) = 2$*, siden* $G/\{4,6\} \cong G_{1,a}$*. Dette gjelder igjen alle delmengder som er listet opp sammen med* $\{1,2,3,4,6\}$ *i tabellen ovenfor.*

Tilsvarende kan vi fjerne eventuelle broer også for restriksjonen av G *til de resterende delmengdene i denne tabellen og benytte proposisjon* 4.5.1 *til å finne det andre multigraderte Betti-tallet i disse gradene, som er lik det andre totale Betti-tallet til grafen som står oppført til venstre for delmengdene i tabellen. Totalt får vi*

$$F_2 \;\cong\; \big(R(-5)^1\big)^{16} \oplus \big(R(-5)^2\big)^{16} \oplus \big(R(-5)^3\big)^{15} \oplus \big(R(-5)^4\big)^4 \;\cong\; R(-5)^{109},$$

siden vi har 16 *grafer som har andre multigraderte Betti-tall lik* 1*,* 16 *som har* 2*,* 15 *som har* 3 *og* 4 *som har* 4*.*

Modulen F_3 er generert av delmengdene som er listet opp i følgende tabell, og på samme måte som for F_2, har restriksjonen av G til disse delmengdene samme tredje multigraderte Betti-tall som det siste totale Betti-tallet til grafene som står til venstre i tabellen, et tall vi tidligere har regnet ut.

$G_{1,a}$	$\{1,2,3,4,7,8\},\{1,2,3,5,7,8\},\{1,2,3,6,7,8\},\{1,2,4,5,7,8\},\{2,3,4,5,7,8\},$ $\{2,4,5,6,7,8\}.$
$G_{1,b}$	$\{1,2,4,6,7,8\},\{1,3,4,5,7,8\},\{1,3,4,6,7,8\},\{1,3,5,6,7,8\},\{1,4,5,6,7,8\},$ $\{2,3,5,6,7,8\},\{3,4,5,6,7,8\}.$
$G_{1,c}$	$\{1,2,5,6,7,8\},\{2,3,4,6,7,8\}.$
$G_{2,a}$	$\{1,2,3,4,5,6\},\{1,2,3,4,5,7\},\{1,2,3,4,5,8\}.$
$G_{2,b}$	$\{1,2,3,4,6,7\},\{1,2,3,4,6,8\},\{1,2,3,5,6,7\},\{1,2,3,5,6,8\},\{1,2,4,5,6,7\},$ $\{1,2,4,5,6,8\},\{2,3,4,5,6,7\},\{2,3,4,5,6,8\}.$
$G_{2,c}$	$\{1,3,4,5,6,7\},\{1,3,4,5,6,8\}.$

Totalt får vi

$$\begin{aligned} F_3 &\cong \big(R(-6)^2\big)^6 \oplus \big(R(-6)^3\big)^7 \oplus \big(R(-6)^4\big)^2 \oplus \big(R(-6)^4\big)^3 \oplus \big(R(-6)^6\big)^8 \oplus \big(R(-6)^7\big)^2 \\ &\cong R(-6)^{115}. \end{aligned}$$

Videre får vi følgende tabell for generatorene til F_4:

$G_{2,a}$	$\{1,2,3,4,5,7,8\}.$
$G_{2,b}$	$\{1,2,3,4,6,7,8\},\{1,2,3,5,6,7,8\},\{1,2,4,5,6,7,8\},\{2,3,4,5,6,7,8\}.$
$G_{2,c}$	$\{1,3,4,5,6,7,8\}.$
G'	$\{1,2,3,4,5,6,7\},\{1,2,3,4,5,6,8\}.$

Dermed får vi totalt

$$F_4 \cong \big(R(-7)^4\big)^1 \oplus \big(R(-7)^6\big)^4 \oplus \big(R(-7)^7\big)^1 \oplus \big(R(-7)^{10}\big)^2 \cong R(-7)^{55}.$$

Til slutt er hele kantmengden $[8]$ *eneste generator for F_5, og ved proposisjon* 4.4.2 *har vi $\beta_5(\mathbb{K}[\Delta(G)]) = \beta_{5,[8]}(\mathbb{K}[\Delta(G)]) = \beta_4(\mathbb{K}[\Delta(G')]) = 10$, siden G' er en forenkling av G. Vi får*

$$F_5 \cong \big(R(-8)^{10}\big)^1 \cong R(-8)^{10}.$$

Den minimale ($\mathbb{N}$-graderte) frie resolusjonen av $\mathbb{K}[\Delta(G)]$ er altså

$$\mathcal{F}_\bullet: \quad 0 \leftarrow R \leftarrow R(-4)^{40} \leftarrow R(-5)^{109} \leftarrow R(-6)^{115} \leftarrow R(-7)^{55} \leftarrow R(-8)^{10} \leftarrow 0.$$

Legg for øvrig merke til at alle $\sigma \subseteq [8]$ med $|\sigma| \geq 6$ i eksempelet ovenfor er generatorer for én F_i. Dette er fordi grafen G har kovidde lik 3, og dermed vil alle delmengder σ av kardinalitet større enn $8-3=5$ ha $r(G|_\sigma) = r(G)$. Videre er for eksempel kantmengden $\{1,2,4\}$ en minste kokrets i G, så $\sigma = [8] \setminus \{1,2,4\}$ er en delmengde av kardinalitet 5 med $r(G|_\sigma) < r(G)$ og altså ikke generator for noen F_i.

Neste eksempel gir de minimale ($\mathbb{N}$-graderte) frie resolusjonene av $\mathbb{K}[\Delta(G)]$ når G er MDS:

Eksempel 4.5.4. *Figur* 2.3 *viser hvordan alle MDS-grafer ser ut, og vi har også sett at disse er entydig gitt opp til isomorfi, med unntak av graf a, som kan være et vilkårlig tre.*

Dersom G er en MDS-graf med kretsrang $k = 0$, er altså G et tre, og $\mathbb{K}[\Delta(G)]$ har minimal fri resolusjon

$$\mathcal{F}_\bullet : \quad 0 \leftarrow R \leftarrow R(-n) \leftarrow 0.$$

Dersom G i stedet har kretsrang $k = 1$, er G en n-krets. Den minimale frie resolusjonen av $\mathbb{K}[\Delta(G)]$ er derfor gitt ved proposisjon 4.5.2*, og er*

$$\mathcal{F}_\bullet : \quad 0 \leftarrow R \leftarrow R(-n+1)^n \leftarrow R(-n)^{n-1} \leftarrow 0.$$

Anta så at G har kretsrang $k = n - 1$. Da er G grafen bestående av to hjørner med n kanter mellom, som vist på figur 2.3*c. Lengden til den minimale frie resolusjonen av $\mathbb{K}[\Delta(G)]$ er derfor $l = k + 1 = n$, og generatorer for F_i er delmengder av $[n]$ av kardinalitet i som inneholder nøyaktig $i - 1$ kretser. Men alle delmengder av $[n]$ av kardinalitet i inneholder akkurat så mange kretser, altså er alle delmengder av $[n]$ av kardinalitet i generatorer for F_i. I tillegg gir proposisjon* 4.4.2 *at ethvert ikke-null multigradert Betti-tall er lik* 1*. Det i-te totale Betti-tallet er derfor lik antall delmengder av $[n]$ av kardinalitet i, og den minimale frie resolusjonen av $\mathbb{K}[\Delta(G)]$ er*

$$\mathcal{F}_\bullet : \quad 0 \leftarrow R \leftarrow R(-1)^{\binom{n}{1}} \leftarrow R(-2)^{\binom{n}{2}} \leftarrow \cdots \leftarrow R(-i)^{\binom{n}{i}} \leftarrow \cdots \leftarrow R(-n)^{\binom{n}{n}} \leftarrow 0.$$

*Merk at denne resolusjonen er det såkalte **Kozul-komplekset** (se definisjon* 1.26 *i* [MS]*). Vi har $I_{\Delta(G)} = \langle x_1, x_2, \ldots, x_n \rangle$, altså er $\mathbb{K}[\Delta(G)] \cong \mathbb{K}$, og proposisjon* 1.28 *i* [MS] *gir at Kozul-komplekset er en minimal fri resolusjon av $\mathbb{K}$.*

Til slutt, dersom G har kretsrang $k = n$, så består G av ett hjørne med n løkker, og ved proposisjon 4.4.1 *har $\mathbb{K}[\Delta(G)]$ samme minimale frie resolusjon som i tilfellet der grafen består av ett hjørne og ingen kanter. I dette tilfellet er $n = 0$, og vi får at Stanley-Reisner-idealet $I_{\Delta(G)} = \langle 1 \rangle = R$. Altså er $\mathbb{K}[\Delta(G)] = 0$, og vi får ingen resolusjon.*

På tilsvarende måte som i forrige eksempel, er det lett å gi de minimale frie resolusjonene av $\mathbb{K}[\Delta(G)]$ også når G er triviell nær-, nesten- og 2-MDS, ut fra beskrivelsene av disse i beviset for proposisjon 2.5.19 og figurene 2.4 og 2.5. I tillegg kan resolusjonene som oppstår fra de ikke-trivielle nær-MDS-grafene på figurene 2.6−2.8 finnes på tilsvarende måte som grafen i eksempel 4.5.3.

Å finne resolusjonene når G er en ikke-triviell nesten- eller 2-MDS-graf er generelt vanskeligere, og uttrykkene blir mye mindre kompakte. La oss illustrere dette med det kanskje enkleste (løkkefrie) tilfellet:

Eksempel 4.5.5. *La G være en ikke-triviell 2-MDS-graf bestående av to kant-disjunkte kretser med kantmengder B og C (der $|B| > 1$ og $|C| > 1$) og ett felles hjørne v_1. (Vi har altså situasjonen som er vist på figur* 2.9*b.) Da er $k = 2$, altså er lengden l til den minimale frie resolusjonen av $\mathbb{K}[\Delta(G)]$ lik* 3*, siden G er løkkefri.*

Ethvert utspennende tre i G er på formen $G|_{[n]\setminus\{b,c\}}$, der $b \in B$ og $c \in C$, altså har vi

$$\beta_1(\mathbb{K}[\Delta(G)]) \quad = \quad |B| \cdot |C|.$$

Videre er generatorer for F_2 på formen $G|_{[n]\setminus\{e\}}$ for en vilkårlig $e \in [n]$. Dersom $e \in B$, gir proposisjon 4.5.1 *at $\beta_{2,[n]\setminus\{e\}}(\mathbb{K}[\Delta(G)])$ er lik det andre totale Betti-tallet til $|C|$-kretsen $G|_C$, som ved proposisjon* 4.5.2 *er lik $|C| - 1$. Tilsvarende er $\beta_{2,[n]\setminus\{e\}}(\mathbb{K}[\Delta(G)]) = |B| - 1$ dersom $e \in C$. Totalt gir dette at*

$$\beta_2(\mathbb{K}[\Delta(G)]) \quad = \quad |B| \cdot (|C| - 1) + |C| \cdot (|B| - 1) \quad = \quad 2 \cdot |B| \cdot |C| - |B| - |C|.$$

Til slutt finner vi $\beta_3(\mathbb{K}[\Delta(G)]) = \beta_{3,[n]}(\mathbb{K}[\Delta(G)])$ *ved å benytte korollar* 4.4.8 $|B|-2$ *(eller* $|C|-2$*) ganger, og vi lar det være opp til leseren å sjekke at vi da får*

$$\beta_3(\mathbb{K}[\Delta(G)]) \;=\; (|B|-1)(|C|-1).$$

Den minimale frie resolusjonen av $\mathbb{K}[\Delta(G)]$ *er derfor*

$$\mathcal{F}_\bullet:\ 0 \leftarrow R \leftarrow R(-n+2)^{|B|\cdot|C|} \leftarrow R(-n+1)^{2\cdot|B|\cdot|C|-|B|-|C|} \leftarrow R(-n)^{(|B|-1)(|C|-1)} \leftarrow 0.$$

Til slutt viser vi hvordan vi ved hjelp av korollar 4.4.8 kan finne enkelte av de totale Betti-tallene til $\mathbb{K}[\Delta(K_m)]$ for generell m, og vi gir dette som en proposisjon:

Proposisjon 4.5.6. *La* l_m *være lengden til den minimale frie resolusjonen av* $\mathbb{K}[\Delta(K_m)]$*. For* $m \in \mathbb{N}$ *med* $m \geq 2$ *har vi da*

i) $\beta_1(\mathbb{K}[\Delta(K_m)]) = m^{m-2}$,

ii) $\beta_{l_m}(\mathbb{K}[\Delta(K_m)]) = (m-1)!$*, og*

iii) $\beta_{l_m-1}(\mathbb{K}[\Delta(K_m)]) = n(m-2)\big((m-2)!\big)$ *(for* $m \geq 3$*)*

for $n = \binom{m}{2}$ *og* $l_m = \binom{m-1}{2} + 1$.

Bevis. Fra proposisjon 2.4.10 er $n = \binom{m}{2}$ og $k = \binom{m-1}{2}$. Dermed er $l_m = k+1 = \binom{m-1}{2}+1$, siden K_m ikke inneholder noen løkker.

i) Cayleys formel, gitt som teorem 2.9 i [BM], gir at antall utspennende trær i K_m er m^{m-2}, altså er $\beta_1(\mathbb{K}[\Delta(K_m)]) = m^{m-2}$.

ii) Vi viser dette ved induksjon på m, og starter altså med $m = 2$. Da har vi et tre, og $\beta_{l_2}(\mathbb{K}[\Delta(K_2)]) = \beta_1(\mathbb{K}[\Delta(K_2)]) = 1 = (2-1)!$.

Anta så at $\beta_{l_j}(\mathbb{K}[\Delta(K_j)]) = (j-1)!$ for $j = m-1 \geq 2$. Vi velger en vilkårlig kant e_1 i K_m og har $r(K_m|_{[n]\setminus\{e_1\}}) = r(K_m)$ siden $m > 2$, altså kan vi benytte korollar 4.4.8. Men grafen $K_m/\{e_1\}$ vil ha minst én kant mellom hvert hjørnepar, og siden $V(K_m/\{e_1\}) = m-1$, er en forenkling av $K_m/\{e_1\}$ lik K_{m-1}. Dermed gir proposisjon 4.4.2 at det siste totale Betti-tallet til $\mathbb{K}[\Delta(K_m/\{e_1\})]$ er lik $\beta_{l_{m-1}}\mathbb{K}[\Delta(K_{m-1})]$, som ved induksjonshypotesen er $(m-2)!$.

For grafen $K_m|_{[n]\setminus\{e_1\}}$ benytter vi korollar 4.4.8 igjen, så sant ikke denne inneholder noen broer, og vi lar den nye kanten vi bruker, e_2, ha ett felles endepunkt v med e_1. Da vil $(K_m|_{[n]\setminus\{e_1\}})/\{e_2\}$ også denne gangen ha minst én kant mellom hvert hjørnepar, altså er også en forenkling av denne lik K_{m-1}.

Dette kan vi gjenta for kanter e_i med samme endepunkt v, så lenge rangen fremdeles er lik $r(G)$, altså $m-2$ ganger. I tillegg vil en forenkling av den aktuelle kontraksjonen hver gang være lik K_{m-1}, siden alle kanter som ikke har endepunkt v fremdeles er med i kantmengden. Når vi ikke lenger kan gjenta dette, betyr det at vi har fjernet alle kanter i G med endepunkt v, unntatt én. La oss kalle denne kanten e_{m-1} og den aktuelle grafen G'. Kanten e_{m-1} er dermed en bro i G', og ved proposisjon 4.5.1 har vi at det siste totale Betti-tallet til $\mathbb{K}[\Delta(G')]$ er lik det siste totale Betti-tallet til $\mathbb{K}[\Delta(G'/\{e_{m-1}\})]$. Men $G'/\{e_{m-1}\} = K_{m-1}$, dermed er $\beta_{l_m}(\mathbb{K}[\Delta(K_m)]) = (m-1)\cdot\beta_{l_{m-1}}(\mathbb{K}[\Delta(K_{m-1})]) = (m-1)\cdot(m-2)! = (m-1)!$, ved induksjonshypotesen.

iii) Siden K_m ikke innholder noen broer når $m \geq 3$, vil alle de n delmengdene av $[n]$ av kardinalitet $n-1$ være generatorer for modulen F_{l_m-1}, og siden alle grafer på formen $K_m|_{[n]\setminus\{e\}}$ for én $e \in [n]$ er isomorfe, er det (l_m-1)-te multigraderte Betti-tallet likt for

alle disse. Dermed får vi at $\beta_{l_m-1}(\mathbb{K}[\Delta(K_m)])$ er lik n ganger det siste totale Betti-tallet til $\mathbb{K}[\Delta(K_m|_{[n]\setminus\{e\}})]$, for en vilkårlig $e \in [n]$. Men dette har vi sett i beviset for del *ii*) at er lik $(m-2)\cdot\beta_{l_{m-1}}(\mathbb{K}[\Delta(K_{m-1})]) = (m-2)\big((m-2)!\big)$. □

Vi illustrerer forrige resultat ved å finne den minimale frie resolusjonen av $\mathbb{K}[\Delta(K_4)]$:

Eksempel 4.5.7. *Grafen K_4 har $n = \binom{4}{2} = 6$, kretsrang $k = \binom{4-1}{2} = 3$ og ingen løkker, altså har resolusjonen lengde $l = 4$. Forrige proposisjon gir oss at $\beta_1(\mathbb{K}[\Delta(K_4)]) = 4^{4-2} = 16$, $\beta_3(\mathbb{K}[\Delta(K_4)]) = 6(4-2)\big((4-2)!\big) = 24$ og $\beta_4(\mathbb{K}[\Delta(K_4)]) = (4-1)! = 6$, og generatorene for F_3 er alle delmengder av $[6]$ av kardinalitet 5, mens F_4 som vanlig er generert av hele kantmengden $[6]$.*

Dermed gjenstår det bare å finne generatorene for F_2 og det andre multigraderte Betti-tallet i disse gradene. Generatorene har kardinalitet 4, altså fås de ved å fjerne to kanter i K_4. I tillegg har K_4 kovidde 3 ved lemma 2.4.13, altså er $r(G|_\sigma) = r(G)$ for alle σ av kardinalitet 4, og alle slike σ genererer følgelig F_2.

For $e_1, e_2 \in [6]$ har vi to muligheter for grafen $K_4|_{[6]\setminus\{e_1,e_2\}}$, avhengig av om e_1 og e_2 har et felles endepunkt. Dersom dette er tilfelle, er $K_4|_{[6]\setminus\{e_1,e_2\}}$ grafen som består av en 3-krets og en bro, altså er $\beta_{2,[6]\setminus\{e_1,e_2\}}(\mathbb{K}[\Delta(K_4)]) = 2$. Dersom e_1 og e_2 ikke har noen felles endepunkt, er derimot $K_4|_{[6]\setminus\{e_1,e_2\}}$ en 4-krets, og vi får $\beta_{2,[6]\setminus\{e_1,e_2\}}(\mathbb{K}[\Delta(K_4)]) = 3$. Det er lett å se at den første situasjonen oppstår $\binom{3}{1} = 3$ ganger for hvert hjørne i K_4, altså 12 ganger, og totalt finnes $\binom{6}{4} = 15$ delmengder av $[6]$ av kardinalitet 4. Dermed må situasjonen som gir en 4-krets oppstå $15 - 12 = 3$ ganger. Vi får $\beta_4(\mathbb{K}[\Delta(K_4)]) = 2\cdot 12 + 3\cdot 3 = 33$, og den minimale frie resolusjonen av $\mathbb{K}[\Delta(K_4)]$ er altså

$$\mathcal{F}_\bullet: \quad 0 \leftarrow R \leftarrow R(-3)^{16} \leftarrow R(-4)^{33} \leftarrow R(-5)^{24} \leftarrow R(-6)^6 \leftarrow 0.$$

Merk at argumentet for å finne generatorene for F_2 i forrige eksempel også holder generelt hvis vi ønsker å finne generatorene for F_{l-2} når grafen er K_m ($m \geq 4$), der l som vanlig er lengden til den minimale frie resolusjonen. Altså trenger vi kun å beregne de $(l-2)$-te multigraderte Betti-tallene i grad $[n]\setminus\{e_1, e_2\}$ for de to tilfellene beskrevet i eksempelet, og som i dette eksempelet vil den første situasjonen oppstå $m\cdot\binom{m-1}{m-3}$ ganger og den andre dermed $\binom{n}{n-2} - m\cdot\binom{m-1}{m-3}$ ganger, av samme grunn som i tilfellet $m = 4$.

4.6 Mulige veier videre

Som vi har sett tidligere i oppgaven, korresponderer utspennende trær i en graf med baser for kretsmatroiden til grafen. Slik det er antydet i forkant av definisjon 4.3.1, kan dermed definisjonen av kantkomplekset til en graf direkte oversettes slik at man kan få et entydig simplisielt kompleks også fra en matroide, ved at de minimale generatorene til Stanley-Reisner-idealet er monomer som korresponderer med basene for matroiden. Dette er gjort tidligere, for eksempel i artikkelen [ER], og proposisjon 4.3.2 i denne oppgaven er da også i utgangspunktet gitt på matroidenivå i [ER].

En naturlig vei videre kan dermed være å undersøke hvilke av resultatene i kapitlene 4.3−4.5 (foruten proposisjon 4.3.2) som kan generaliseres til matroider som ikke nødvendigvis er grafiske. Terminologien i "byggesteinene", proposisjonene 4.3.3, 4.3.5 og 4.3.6, er allerede på plass: Rangfunksjonen og kokretsbegrepet er definert for matroider tidligere i denne oppgaven.

Videre er det lett å se at separerende kantmengder i en graf tilsvarer avhengige mengder i kokretsmatroiden til grafen, og graf-operasjonene restriksjon og kontraksjon har også sine direkte generaliseringer til matroider (se [O], side 22 og 104, og punkt 3.1.2 og proposisjon 3.2.1).

Bibliografi

[BM] J. A. Bondy and U. S. R. Murty, *Graph Theory with Applications*, The MacMillian Press LTD (1976).

[C] P. J. Cameron, *Codes, matroids and trellises*, 15 siders preprint (2000), link tilgjengelig på http://www.maths.qmul.ac.uk/∼pjc/papers.html.

[ER] J. A. Eagon & V. Reiner, Resolutions of Stanley-Reisner rings and Alexander duality, *Journal of Pure and Applied Algebra* 130, s. 265-275 (1998).

[F] G. D. Forney, Jr., Coset Codes - Part II: Binary Lattices and Related Codes, *IEEE Transactions on Information Theory*, Vol. 34, No. 5, s. 1152-1187 (1988).

[GH] M. J. Greenberg & J. R. Harper, *Algebraic Topology: A First Course*, Mathematics Lecture Note Series, Addison-Wesley Publishing Company (1981).

[H] R. Hill, *A First Course in Coding Theory*, Oxford Applied Mathematics and Computing Science Series, Oxford University Press (1986).

[KDMEL] A. B. Kiely, S. J. Dolinar, Jr., R. J. McEliece, L. L. Ekroot and W. Lin, Trellis Decoding Complexity of Linear Block Codes, *IEEE Transactions on Information Theory*, Vol. 42, No. 6, s. 1687-1697 (1996).

[L] A. H. Larsen, *Matroider og lineære koder*, masteroppgave i algebra, Universitetet i Bergen (2005).

[MacWS] F. J. MacWilliams & N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library, volume 16, Elsevier Science Publishers B. V. (1977).

[McE] R. J. McEliece, On the BCJR Trellis for Linear Block Codes, *IEEE Transactions on Information Theory*, Vol. 42, No. 4, s. 1072-1092 (1996).

[MS] E. Miller & B. Sturmfels, *Combinatorial Commutative Algebra*, Graduate Texts in Mathematics 227, Springer Science+Business Media, Inc. (2005).

[M] D. J. Muder, Minimal Trellises for Block Codes, *IEEE Transactions on Information Theory*, Vol. 34, No. 5, s. 1049-1053 (1988).

[O] J. Oxley, *Matroid Theory*, Oxford Graduate Texts in Mathematics 3, Oxford University Press (1992).

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

[T] A. Tucker, *Applied Combinatorics*, fourth edition, John Wiley & Sons, Inc. (2002).

[VK] A. Vardy and F. R. Kschischang, Proof of a Conjecture of McEliece Regarding the Expansion Index of the Minimal Trellis, *IEEE Transactions on Information Theory*, Vol. 42, No. 6, s. 2027-2034 (1996).

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

[Wel] D. J. A. Welsh, *Matroid Theory*, L. M. S. Monographs 8, Academic Press Inc. (1976).

[W] J. K. Wolf, Efficient Maximum Likelihood Decoding of Linear Block Codes Using a Trellis, *IEEE Transactions on Information Theory*, Vol. IT-24, No. 1, s. 76-80 (1978).