Matroider

Majbritt Felleki

Den amerikanske matematiker Hassler Whitney fandt i 1935 sammenhænge mellem sætninger i grafteori og sætninger i lineær algebra. Dette førte til definitionen af *matroider*, matematiske objekter som afspejler disse fælles egenskaber. Jeg stødte ind i matroider på Victoria University of Wellington, New Zealand, hvor jeg var takket være Rejselegat for matematikere. Teorien for matroider starter i den lette ende, også hvis man aldrig har studeret grafteori. Sidenhen skal man ikke lade sig narre, der kommer rigeligt at fundere over. Det er min intention at alle som har læst lineær algebra modsvarende Mat1GA skal kunne forstå denne sammenfatning.

Der findes en hel del ekvivalente definitioner af matroider. Den som følger her angiver en matroid ud fra de *uafhængige mængder*.

Definition 1 En matroid M er et par $(E, \mathcal{I})$ bestående af en endelig mængde E og en samling $\mathcal{I}$ af delmængder af E som opfylder betingelserne

(I1) $\emptyset \in \mathcal{I}$.

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

(I3) Hvis I_1 og I_2 er i $\mathcal{I}$, og $|I_1| < |I_2|$, så findes et element e i $I_2 - I_1$ så $I_1 \cup \{e\} \in \mathcal{I}$.

Mængderne i $\mathcal{I}$ kaldes uafhængige mængder.

Her betyder $I_2 - I_1$ mængden af elementer som tilhører I_2 men som ikke tilhører I_1. Dette skrives iblandt $I_2 \setminus I_1$, men ikke her.

Matroider er som sagt inspirerede af vektorrum. Det er derfor oplagt at se om definitionen stemmer overens med definitionen af lineært uafhængige vektorer.

Sætning 2 *Lad $V = (m, \mathbb{F})$ være det m-dimensionelle vektorrum over legemet $\mathbb{F}$. Lad E være en endelig mængde af vektorer fra V. Lad $\mathcal{I}$ bestå af de mængder I af vektorer fra E som er lineært uafhængige. Så er $(E, \mathcal{I})$ en matroid.*

Inden beviset for sætningen er det tid for et eksempel. Lad vektorrummet bestå af par $m = 2$ over de reelle tal $\mathbb{F} = \mathbb{R}$, altså $\mathbb{R}^2$, og lad E være vektorerne

$$E = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}.$$

Dette skrives lettere som $E = \{1, 2, 3, 4\}$ hvor tallene korresponderer til søjlerne i matricen

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

Med disse symboler for elementerne i E er mængderne af lineært uafhængige vektorer

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

Det er hurtigt klaret at tjekke (I1), (I2) og (I3) og overbevise sig om at $(E, \mathcal{I})$ er en matroid.

Bevis for sætningen. Det skal tjekkes at $\mathcal{I}$ opfylder (I1), (I2) og (I3), hvor (I1) og (I2) følger direkte. Tilbage er at se at $\mathcal{I}$ opfylder (I3). Lad I_1 og I_2 være to lineært uafhængige delmængder af E og antag at $|I_1| < |I_2|$. Lad W være underrummet udspændt af $I_1 \cup I_2$. Så er dimensionen af W mindst $|I_2|$. Hvis $I_1 \cup \{e\}$ er lineært afhængig for alle e i $I_2 - I_1$, er W indeholdt i underrummet udspændt af I_1, og så er

$$|I_2| \leq \dim W \leq |I_1| < |I_2|,$$

hvilket er en modstrid. Altså findes et e i $I_2 - I_1$ så $I_1 \cup \{e\}$ er lineært uafhængig. $\square$

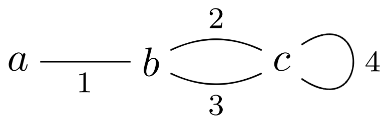
I grafteori findes ligesom i lineær algebra en form for uafhængighed. Denne uafhængighed beskrives her.

Definition 3 En *graf* G er et par (V, E) bestående af en ikke tom mængde V af knuder og en mængde E af kanter fra $\{\, \{u, v\} \mid u, v \in V\,\}$.

Et eksempel på en graf er

$$V = \{a, b, c\} \text{ og } E = \{\{a, b\}, \{b, c\}, \{b, c\}, \{c, c\}\}.$$

Den er illustreret herunder med elementerne i E nummererede $\{1, 2, 3, 4\}$.



En *kreds* i en graf er en vej som starter og ender i samme knude og ikke passerer den samme knude to gange. I grafen oven findes altså to kredse. Nu defineres en *uafhængig del* til at være en del af en graf som ikke indeholder nogen kreds. Termen uafhængig del er det som på engelsk hedder *forest*. Jeg modtager gerne en mail med den korrekte danske oversættelse. Oversættelsen kan retfærdiggøres med at når der ikke findes nogen kreds, så er der højst en mulighed for at gå fra en knude til en anden.

Grafen i eksemplet omfatter de uafhængige dele

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

Det er ikke et tilfælde at denne samling har fået navnet $\mathcal{I}$, der er nemlig tale om en matroid $(E, \mathcal{I})$, og det er præcis den samme som i vektorrumseksemplet.

Sætning 4 *Lad $G = (V, E)$ være en graf. Lad $\mathcal{I}$ bestå af de delmængder I af E som er en uafhængig del i G. Så er $(E, \mathcal{I})$ en matroid.*

Beviset overspringes.

Grafer og mængder af vektorer giver ifølge sætningerne altid anledning til en matroid. Dette gælder ikke den anden vej rundt, det er let at finde en matroid som ikke kan illustreres som en graf på den måde det er beskrevet i sætningen.

Matroiden $M = (\{1, 2, 3, 4\}, \mathcal{I})$, hvor

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

er et eksempel på en sådan. To kanter skal danne en uafhængig del, men tre kanter skal danne en kreds. Derfor bliver den fjerde kant umulig at placere.

Hvis en matroid kan fås ud fra en mængde af vektorer over et givet legeme, siges det at den er *repræsenteret* over legemet. Det er muligt at finde en matroid som ikke kan fås ud fra en mængde af vektorer over noget som helst legeme, men også matroider som kun kan fås over visse legemer. Oftest ser man dog på det fra den anden side. Man forsøger at vise hvad som kræves for eksistensen af en repræsentation over et legeme. Blandt andet findes en sætning som siger at enhver matroid givet ved en graf kan repræsenteres over samtlige legemer, men den sætning er ikke specielt svær at vise. Derimod er der en del åbne problemer forbundet med netop repræsentationer over legemer, her iblandt Rota's formodning som vil blive beskrevet senere.

Først endnu to beskrivelser af matroider hvoraf den ene knytter sig til vektorrum mens den anden hænger stærkest sammen med grafer.

Definition 5 En *basis* for en matroid $(E, \mathcal{I})$ er en maksimal uafhængig delmængde af E. Samlingen af baser betegnes $\mathcal{B}$.

Definition 6 En *kreds* for en matroid $(E, \mathcal{I})$ er en minimal ikke-uafhængig delmængde af E. Samlingen af kredse betegnes $\mathcal{C}$.

I matroiden i eksemplerne er baserne $\mathcal{B} = \{\{1,2\},\{1,3\}\}$ og kredsene er $\mathcal{C} = \{\{2,3\},\{4\}\}$. Det ses at kredsene for matroiden modsvarer kredsene i grafen, og baserne korresponderer til vektorparrene

$$\left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix}\right\},\left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix}\right\}$$

som er baser for $\mathbb{R}^2$.

Sætning 7 *En samling $\mathcal{B}$ er en samling af baser for en matroid hvis og kun hvis $\mathcal{B}$ opfylder*

(B1) *$\mathcal{B}$ er ikke tom.*

(B2) *Hvis B_1 og B_2 er i $\mathcal{B}$, og $x \in B_1 - B_2$, så findes et element $y \in B_2 - B_1$ så $(B_1 - \{x\}) \cup \{y\} \in \mathcal{B}$.*

Hvis $\mathcal{B}$ er en samling af baser, er $\mathcal{I}$ givet ved at $\mathcal{I}$ indeholder alle delmængder af mængder i $\mathcal{B}$.

Sætning 8 *En samling $\mathcal{C}$ er en samling af kredse for en matroid hvis og kun hvis $\mathcal{C}$ opfylder*

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

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

(C3) *Hvis C_1 og C_2 er to forskellige mængder i $\mathcal{C}$, og $e \in C_1 \cup C_2$, så findes C_3 i $\mathcal{C}$ så $C_3 \subseteq (C_1 \cup C_2) - \{e\}$.*

Hvis $\mathcal{C}$ er en samling af kredse, er $\mathcal{I}$ givet ved at $\mathcal{I}$ indeholder alle delmængder af E som ikke indeholder en mængde fra $\mathcal{C}$.

Beviserne overspringes.

Sætningerne er alternative definitioner af matroider, og der findes endnu flere definitioner. Disse er samlede på internetadressen `http://planetmath.org/encyclopedia/Matroid.html`. Det tager lidt tid men det er ikke en uoverskuelig opgave at vise at de alle er ækvivalente.

Tre operationer som kan udføres på matroider er dual-dannelse, kontrahering og sletning af et element. Alle tre er inspirerede af de tilsvarende operationer på grafer. En *plan graf* er en graf som kan tegnes uden at nogle kanter krydser hinanden. Den duale til en plan graf dannes ved at man sætter en knude på samtlige flader samt en udenfor grafen. Derefter tegnes linjer som krydser de oprindelige kanter og forbinder de nye knuder, en linje for hver kant. Dual-dannelse for grafer har nogle brister. En dual eksisterer ikke når grafen ikke kan tegnes plant, og desuden afhænger dualen af den givne tegning af grafen.

For matroider eksisterer den duale altid og den er givet som følger

Definition 9 Lad $\mathcal{B}$ være en samling af baser for en matroid $M = (E, \mathcal{I})$. Den duale matroid M^* er givet ved samlingen af baser

$$\mathcal{B}^* = \{\, E - B \mid B \in \mathcal{B} \,\}.$$

Det er ikke oplagt at $\mathcal{B}^*$ opfylder (B2), men det gør den. Trods bristerne i grafers dual-dannelse gælder sætningen

Sætning 10 *Hvis G^* er dualen af en plan graf G er*

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

Her betyder $M(G)$ matroiden genereret af G, og $M^*(G)$ betyder $(M(G))^*$. Lighedstegnet er i virkelighed en isomorfi, men isomorfier i matroide-verdenen betyder blot at bytte symboler på elementer.

Når et element e slettes fra en matroid $M = (E, \mathcal{I})$ fås matroiden $M \backslash e = (E - \{e\}, \mathcal{I}(M \backslash e))$, hvor

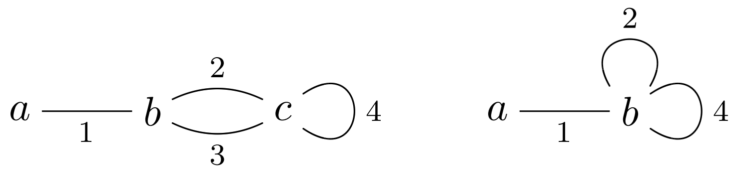
$$\mathcal{I}(M \backslash e) = \{\, I \subseteq (E - \{e\}) \mid I \in \mathcal{I}\,\}.$$

Operationen kontrahering med hensyn til et element e, som ikke er en kreds, er givet ved matroiden $M/e = (E - \{e\}, \mathcal{I}(M/e))$, hvor

$$\mathcal{I}(M/e) = \{\, I \subseteq (E - \{e\}) \mid I \cup \{e\} \in \mathcal{I}\,\}.$$

Kontrahering med hensyn til en kreds e er givet ved $M/e = M \backslash e$.

Det er ikke svært at vise at de to operationer at slette et element og kontrahering opfylder at $M \backslash x \backslash y = M \backslash y \backslash x$, $M/x/y = M/y/x$ og $M \backslash x/y = M/y \backslash x$, og således giver det mening at tale om $M \backslash X/Y$ når X og Y er to disjunkte delmængder af E. En *minor* af M er en matroid på denne form, hvor X og Y er to disjunkte og eventuelt tomme delmængder af E. En klasse af matroider kaldes *minor-afsluttet* hvis alle minor af matroider i klassen også ligger i klassen. Dette gælder for klassen af matroider som kan illustreres som en graf. I en graf er operationen at slette et element givet ved at den korresponderende kant slettes, og kontrahering er givet ved at grafen trækkes sammen som illustreret herunder hvor grafen til venstre bliver til grafen til højre efter kontrahering med hensyn til 3.



Der gælder at $M(G) \backslash e = M(G \backslash e)$ og at $M(G)/e = M(G/e)$, og det følger at hvis en matroid kan illustreres som en graf, så kan alle dens minor også illustreres som en graf. Matroider som kan illustreres som en graf kaldes *grafiske*. Klassen af grafiske matroider er altså minor-afsluttet.

Matroider som kan fås ud fra en mængde af vektorer over et givet legeme $\mathbb{F}$ kaldes $\mathbb{F}$-*repræsentable*.

Sætning 11 *Lad $\mathbb{F}$ være et legeme. Klassen af $\mathbb{F}$-repræsentable matroider er minor-afsluttet.*

Del af et bevis. Hvis $M = (E, \mathcal{I})$ er $\mathbb{F}$-repræsentabel findes en matrix A med søjler nummererede ved E, så mængder af lineært uafhængige søjler korresponderer med mængder i $\mathcal{I}$. Hvis $x \in E$ slettes fra M, er $M \backslash x$ repræsenteret af matricen A hvor søjlen x er slettet. Derfor er $M \backslash x$ $\mathbb{F}$-repræsentabel.

At M/x også er $\mathbb{F}$-repræsentabel bygger på to sætninger om dualer.

- Hvis M er $\mathbb{F}$-repræsentabel er også M^* $\mathbb{F}$-repræsentabel.
- $M^* \backslash x = (M/x)^*$.

Ifølge første sætning og ovenstående er $(M^* \backslash x)^*$ $\mathbb{F}$-repræsentabel, og ifølge anden sætning er $M/x = M^{**}/x = (M^* \backslash x)^*$. □

Det er nu påstået at hvis en matroid er grafisk, så er alle dens minor også grafiske, og hvis en matroid er $\mathbb{F}$-repræsentabel, så er alle dens minor også $\mathbb{F}$-repræsentable.

Det er et stort område indefor matroide-teori at gå den anden vej. Ud fra en matroids minor kan det afgøres om den er grafisk, og i nogle tilfælde om den er repræsentabel over et givet legeme. Rettere kan det vises hvilke minor en matroid ikke kan have hvis den til eksempel er grafisk. Matroiden bliver altså karakteriseret af de minor som den ikke har. Et eksempel på en sådan sætning er følgende med efterfølgende forklaringer.

Sætning 12 *En matroid er $GF(2)$-repræsentabel hvis og kun hvis den ikke har $U_{2,4}$ som en minor.*

Her er $GF(2)$ legemet med to elementer. For de som ikke er kommet til endelige legemer endnu og for os som har glemt det, findes et legeme $GF(q)$ med q elementer hvis og kun hvis q er en primtalspotens, $q = p^n$, og dette legeme er entydigt.

Matroiden $U_{2,4}$ er en matroid som er så populær at den har fået sit eget symbol. Den er givet ved $U_{2,4} = (\{1,2,3,4\}, \{I \subseteq \{1,2,3,4\} \mid |I| \leq 2\})$. Generelt er $U_{k,n}$, $0 \leq k \leq n$ givet ved $U_{k,n} = (\{1,\ldots,n\}, \{I \subseteq \{1,\ldots,n\} \mid |I| \leq k\})$, og sådanne matroider kaldes uniforme. På side 21 blev $U_{2,4}$ brugt som et eksempel på en matroid som ikke er grafisk.

Når en minor-afsluttet klasse kan karakteriseres ved at en matroid findes i klassen netop når den ikke har en eller flere bestemte minor, kaldes disse for *udelukkede minor* for klassen. Matroiden $U_{2,4}$ er altså en udelukket minor for klassen af $GF(2)$-repræsentable matroider.

I tabel 1 ses udelukkede minor for forskellige minor-afsluttede klasser. Der er en hel del matroider med eget symbol, og konstruktionen af dem er en anelse omfattende. De symboler som optræder i tabellen er ikke det som er vigtigst, formålet er at se på klasserne og antallet af udelukkede minor.

Det ses at for de endelige legemer $GF(2)$, $GF(3)$ og $GF(4)$ findes kun endeligt mange udelukkede minor for repræsentabilitet over disse. I 1970 kom Rota med følgende formodning som er det mest berømte problem indenfor matroide-teori.

Rotas formodning Lad $GF(q)$ være et endeligt legeme. Der findes endeligt mange udelukkede minor for $GF(q)$-repræsentabilitet.

Klasse af matroider	Antal udelukkede minor	Hvilke minor er udelukkede	Årstal
Grafiske	5	$U_{2,4}, F_7, F_7^*, M^*(K_{3,3}), M^*(K_5)$	1958
Repræsentable over alle legemer	3	$U_{2,4}, F_7, F_7^*$	1958
Repræsentable over uendelige legemer	∞		1958
Repræsentable over $GF(2)$	1	$U_{2,4}$	1958
Repræsentable over $GF(3)$	4	$U_{2,5}, U_{3,5}, F_7, F_7^*$	1979
Repræsentable over $GF(4)$	7	$U_{2,6}, U_{4,6}, F_7^-, (F_7^-)^*, P_6, P_8, P_8''$	2000

Tabel 1 Udelukkede minor for forskellige minor-afsluttede klasser.

Eftersom der findes uendeligt mange udelukkede minor for klassen af matroider som kan repræsenteres over uendelige legemer, kan formodningen ikke udvides til alle legemer.

Årstallene i tabellen illustrerer hvor mange år det har taget at vise formodningen for legemerne med 2, 3 og 4 elementer. For endelige legemer med 5 eller flere elementer er problemet uløst.

Det her er selvfølgelig kun en kort og meget ufuldstændig introduktion til matroider. For videre læsning kan det anbefales at besøge James Oxleys hjemmeside `http://www.math.lsu.edu/~oxley/`. Der findes flere artikler at downloade som er overkommelige at forstå, blandt andet [4], [5] og [3]. En kortfattet historisk oversigt over vejen til bevis for Rotas formodning så langt er kapitel 5 i [1].

Litteratur

[1] Kristensen, Kasper Kabell. *Extremal Matroid Theory and the Erdös-Pósa Theorem*, 2005, `http://www.imf.au.dk/publications/phd/2006/imf-phd-2006-kkk.pdf`.

[2] Oxley, James. *Matroid Theory*, Oxford University Press, New York, 1992.

[3] Oxley, James. *On the interplay between graphs and matroids*, London Math. Soc. Lecture Notes 288, Cambridge Univ. Press, 2001, p.199–239, `http://www.math.lsu.edu/~oxley/jobcc.pdf`.

[4] Oxley, James. *What is a matroid?*, Cubo 5, 2003, p.179–218, `http://www.math.lsu.edu/~oxley/survey4.pdf`.

[5] Hobbs, Arthur M., Oxley, James. *William T. Tutte, 1917–2002*, Notices Amer. Math. Soc. 51, 2004, p. 320–330, `http://www.math.lsu.edu/~oxley/ahjo.pdf`.

[6] Whittle, Geoff. Lecture notes, Victoria University of Wellington.