Jorn van der Pol
Department of Combinatorics and Optimization
University of Waterloo
jvanderpol@uwaterloo.ca

Onderzoek Stieltjesprijs 2017

Typische eigenschappen van matroïden

Matroïden abstraheren verschillende noties van 'onafhankelijkheid' in uiteenlopende situaties. Er bestaan veel vragen en weinig antwoorden over het typische gedrag van grote matroïden. Voor zijn proefschrift *Large Matroids: Enumeration and Typical Properties*, geschreven onder supervisie van Remco van der Hofstad en Rudi Pendavingh, won Jorn van der Pol de Stieltjesprijs 2017.

Iedere verzameling vectoren in een vectorruimte is *afhankelijk* of *onafhankelijk*. Als je de onderliggende vectorruimte vergeet en alleen kijkt naar de abstracte combinatorische eigenschappen van afhankelijke en onafhankelijke verzamelingen, dan kom je uit bij matroïdentheorie. De term matroide werd geïntroduceerd door Whitney [7], die de volgende definitie gaf.

Definitie. Een *matroïde* is een paar $M = (E, \mathcal{I})$ waar E een eindige verzameling is en $\mathcal{I}$ een verzameling deelverzamelingen van E zodat
1. $\emptyset \in \mathcal{I}$;
2. als $I \subseteq J$ en $J \in \mathcal{I}$, dan is ook $I \in \mathcal{I}$;
3. als $I, J \in \mathcal{I}$ en $|I| < |J|$, dan is er een $e \in J$ zodat $I \cup \{e\} \in \mathcal{I}$.

We noemen E de grondverzameling van M; deelverzamelingen van E noemen we afhankelijk als ze in $\mathcal{I}$ zitten, en anders onafhankelijk. Het verband met lineaire onafhankelijkheid wordt doorgaans op de volgende manier gelegd. Laat A een matrix zijn, en veronderstel dat haar kolommen zijn gelabeld met de elementen van E. De verzameling $\mathcal{I}$ van lineair onafhankelijke verzamelingen kolommen voldoet aan de eigenschappen 1–3 en is dus de verzameling onafhankelijke verzamelingen van een matroïde met grondverzameling E. Matroïden die op deze manier gerealiseerd kunnen worden noemen we lineair of representeerbaar.

Foto: Elsa van Hout

Jorn van der Pol

Matroïden zijn geen perfecte omschrijving van lineaire onafhankelijkheid: hoewel iedere matrix een matroïde definieert, is niet iedere matroïde representeerbaar. Maar in zekere zin zijn matroïden precies de juiste veralgemenisering van lineaire onafhankelijkheid, die ze bruikbaar maakt in uiteenlopende situaties, van lineaire algebra tot grafentheorie en van projectieve meetkunde tot combinatorische optimalisering.

Laat bijvoorbeeld $G = (V, E)$ een graaf zijn met punten V en kanten E. Een bos in G is een deelverzameling $E' \subseteq E$ zodat de deelgraaf (V, E') geen cykels be-

vat. Als we $\mathcal{I}$ de verzameling van alle bossen laten zijn, dan voldoet $\mathcal{I}$ aan de eigenschappen 1–3 en dus is $(E,\mathcal{I})$ een matroïde. Zulke matroïden noemen we grafisch.

Een van de redenen dat we geïnteresseerd zijn in matroïden is hun diepgaande verband met combinatorische optimalisering, in het bijzonder met het *gretige* algoritme. We noemen een algoritme gretig als het een globaal optimum vindt door steeds een lokaal optimale keuze te maken.

Een voorbeeld van zo'n gretig algoritme is het algoritme van Kruskal voor het vinden van een opspannende boom van minimaal gewicht (minimum spanning tree, MST) in een samenhangende graaf waarin alle kanten een gewicht hebben.

Het algoritme van Kruskal vindt een MST door te beginnen met $T=\emptyset$ en steeds een kant van zo klein mogelijk gewicht toe te voegen aan T, waarbij de nieuwe kant wordt gekozen uit de verzameling kanten die kunnen worden toegevoegd aan T zonder een cykel te vormen. Het algoritme stopt als er geen nieuwe kant kan worden toegevoegd aan T.

In matroïdentermen vindt het gretige algoritme een onafhankelijke verzameling van minimaal gewicht in de grafische matroïde behorend bij G. De relatie met matroïden gaat veel verder dan dit: een familie van deelverzamelingen $(E,\mathcal{I})$ die aan eigenschap 1 en 2 voldoet is een matroïde dan en slechts dan als het gretige algoritme een onafhankelijke verzameling van minimaal gewicht geeft voor iedere gewichtsfunctie $w: E \to \mathbb{R}_+$. Matroïden karakteriseren dus die families waarvoor het gretige algoritme werkt.

Typische eigenschappen

Whitney vroeg in zijn artikel al hoe goed matroïden lineaire onafhankelijkheid omschrijven. Er zijn verschillende manieren waarop je deze vraag kunt proberen te beantwoorden, bijvoorbeeld door te kijken of het toevoegen van een extra axioma aan het drietal in de definitie een precieze omschrijving van representeerbare matroïden geeft.

Ik ben geïnteresseerd in een kwantitatieve aanpak van dit soort vragen: hoe groot is het aantal representeerbare matroïden vergeleken met het totaal aantal matroiden op een bepaalde grondverzameling E, in het bijzonder in de limiet als $|E|$ naar oneindig gaat? (Omdat het niet uitmaakt welke elementen in E zitten, mogen we aannemen dat $E=[n]=\{1,2,\ldots,n\}$.)

Ter illustratie bekijken we eerst de matroïden die representeerbaar zijn als een matrix over het lichaam met twee elementen $\mathrm{GF}(2)$, de zogenaamde binaire matroiden. Schrijf $b(n)$ voor het aantal binaire matroïden met grondverzameling $[n]$. Iedere binaire matroïde met grondverzameling $[n]$ kan worden gerepresenteerd door een $n\times n$-matrix met elementen uit $\mathrm{GF}(2)$; er zijn 2^{n^2} van dit soort matrices, dus we vinden onmiddellijk de volgende bovengrens op $b(n)$.

Stelling 1. $b(n)\leq 2^{n^2}$.

In Stelling 4 zullen we zien dat $b(n)$ verwaarloosbaar klein is vergeleken met $m(n)$, het aantal matroïden op grondverzameling $[n]$; dat wil zeggen

$$\lim_{n\to\infty}\frac{b(n)}{m(n)}=0. \qquad (1)$$

We zeggen dat een 'typische' matroïde niet-binair is, of dat 'bijna alle' matroïden niet-binair zijn.

Net zo kunnen we laten zien dat een typische matroïde niet representeerbaar is over het eindige lichaam $\mathrm{GF}(q)$. Het wordt een ander verhaal als we willen laten zien dat een typische matroïde niet-representeerbaar is over een oneindig lichaam (zoals $\mathbb{R}$) of zelfs over een willekeurig lichaam. Peter Nelson [3] bewees onlangs de volgende verrassende stelling, die laat zien dat een typische matroïde niet-representeerbaar is over enig lichaam.

Stelling 2. *Voor alle $n\geq 12$ geldt: het aantal representeerbare matroïden met grondverzameling $[n]$ is hooguit $2^{n^{3/4}}$.*

Random matroïden

Welke eigenschappen heeft een typische matroïde nog meer? Deze vraag kennen we goed uit het gebied van random-grafentheorie. Laat G een random graaf op n punten zijn, dat wil zeggen dat G met gelijke kans elk van de $2^{n(n-1)/2}$ mogelijke grafen op n punten is. We zeggen dat een typische graaf een bepaalde eigenschap heeft, als de kans dat G de eigenschap heeft naar 1 gaat als we n naar oneindig laten gaan (in de random-grafenliteratuur wordt vaak de term 'met grote kans' gebruikt). Zo weten we bijvoorbeeld dat een typische graaf samenhangend is.

Je kunt de random graaf G construeren door voor elk van de $\frac{n(n-1)}{2}$ mogelijke kanten een munt te werpen om te beslissen of je die kant toevoegt aan G of niet (dit wordt het Erdős–Rényi-model genoemd). De random graaf G is dus het resultaat van $\frac{n(n-1)}{2}$ onafhankelijke keuzes. De probabilistische onafhankelijkheid van de verschillende muntworpen speelt een cruciale rol in de analyse van random grafen.

Het slechte nieuws is dat we niet zo'n mooi model hebben voor random matroïden. Als we bijvoorbeeld een random deelverzameling van de machtsverzameling van $[n]$ kiezen, dan voldoet deze met grote kans niet aan de eigenschappen 1–3 en vormt dus niet de onafhankelijke verzamelingen van een matroïde.

We beperken ons daarom tot het vergelijken van telfuncties, zoals in (1). Hiervoor is het belangrijk een goed beeld te hebben van het asymptotische gedrag van $m(n)$, het aantal matroïden met grondverzameling $[n]$.

Veel matroïden

Een verzameling van k elementen heeft 2^k deelverzamelingen. Aangezien de onafhankelijke verzamelingen een deelverzameling van de machtsverzameling van $[n]$ is, volgt direct dat $m(n)\leq 2^{2^n}$.

Met een beetje moeite kunnen we deze triviale bovengrens verbeteren. Op grond van eigenschap 2 kunnen we de onafhankelijke verzamelingen omschrijven door alleen de inclusiegewijs maximale onafhankelijke verzamelingen te geven. Net als in een vectorruimte noemen we zo'n maximale onafhankelijke verzameling een basis, en net als in een vectorruimte hebben alle bases dezelfde kardinaliteit (dit volgt uit eigenschap 3). De gemeenschappelijke kardinaliteit van de bases noemen we de rang van de matroïde. In de rest van dit artikel spelen de bases van een matroïde een belangrijke rol.

De bases van een matroïde van rang r vormen een deelverzameling van de $\binom{n}{r}$ mogelijke deelverzamelingen ter grootte r van $[n]$, en dus volgt onmiddellijk

$$m(n,r)\leq 2^{\binom{n}{r}}$$

waar $m(n,r)$ staat voor het aantal matroiden van rang r met grondverzameling $[n]$. Voor vaste n is $\binom{n}{r}$ maximaal als $r=\lfloor n/2\rfloor$, dus vinden we

$$m(n) = \sum_{r=0}^{n} 2^{\binom{n}{r}} \leq (n+1)\, 2^{\binom{n}{\lfloor n/2 \rfloor}}. \quad (2)$$

Een standaardafschatting van binomiaalcoëfficiënten vertelt ons dat $\binom{n}{\lfloor n/2 \rfloor} \approx \frac{2^n}{\sqrt{n}}$. Door te kijken naar matroïden van vast gekozen rang kunnen we de exponent in de triviale bovengrens dus verbeteren met ongeveer een factor $\sqrt{n}$.

Sparse-paving matroïden

De bovengrens (2) zit niet al te ver van de waarheid. Dit kunnen we laten zien door een grote verzameling van speciale matroiden te construeren.

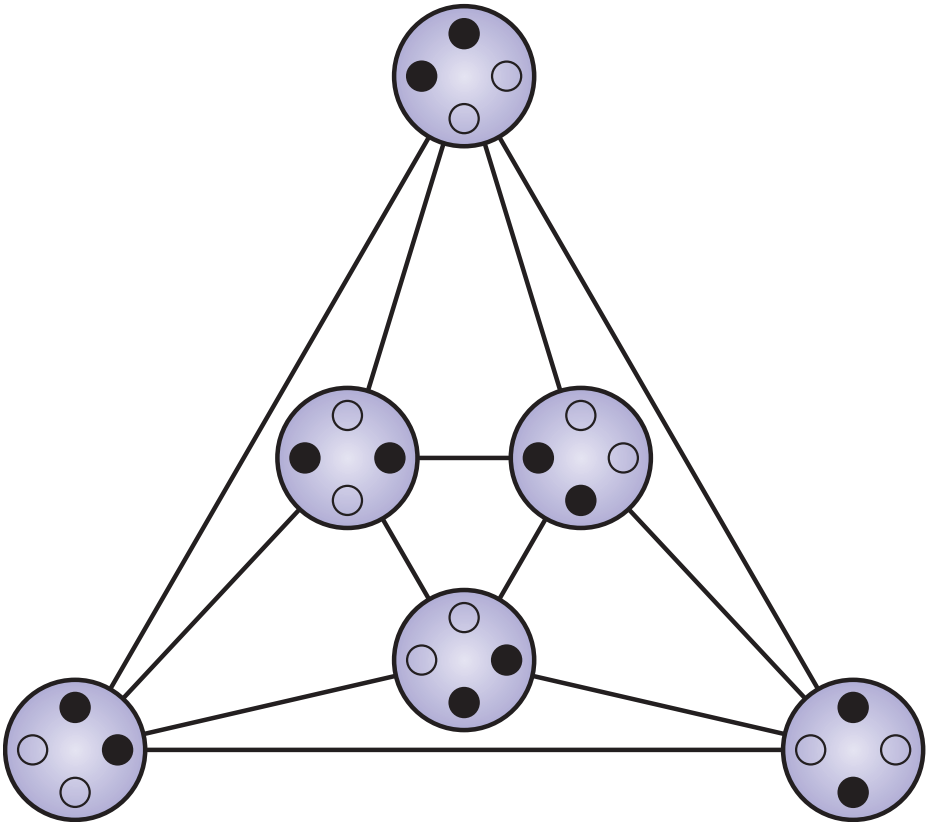
Het is een aardige opgave te laten zien dat een verzameling $\mathcal{B}$ van deelverzamelingen van $[n]$ de verzameling bases van een matroïde van rang r is dan en slechts dan als $\mathcal{B}$ niet-leeg is en voldoet aan de volgende uitwisselingseigenschap:

> voor alle $B, B' \in \mathcal{B}$ en alle $e \in B \backslash B'$
> bestaat er een $f \in B' \backslash B$
> zodat $(B \backslash \{e\}) \cup \{f\}$. (3)

(De definities van matroïden in termen van onafhankelijke verzamelingen en bases zijn equivalent. Er bestaan nog veel meer van zulke 'cryptomorfe' definities, een weerspiegeling van de veelzijdige oorsprong van het vakgebied.)

De bases van een matroïde van rang r met grondverzameling $[n]$ vormen een deelverzameling van de punten van de zogenaamde Johnson-graaf $J(n,r)$. Dit is de graaf met puntenverzameling $\{X \subseteq [n] : |X| = r\}$ waarin twee punten buren zijn dan en slechts dan als ze in precies $r-1$ elementen gemeen hebben, zie Figuur 1.

We noemen een verzameling X van punten in een graaf stabiel als geen twee punten van X buren. Als X een stabiele verzameling van $J(n,r)$ is, dan is $V(J(n,r)) \backslash X$, het complement van X in de punten van $J(n,r)$, niet-leeg en voldoet aan de uitwisselingseigenschap (3); ze vormt dus de verzameling bases van een matroïde. Matroïden die we op deze manier verkrijgen uit een stabiele verzameling van de Johnson-graaf noemen we 'sparse-paving'. Iedere stabiele verzameling van $J(n,r)$ definieert dus zo'n sparse-paving matroïde. Een charmante constructie van Graham en Sloane [2] laat zien dat $J(n,r)$ een grote stabiele verzameling bevat.



Figuur 1 De Johnson-graaf $J(4,2)$. De zes punten zijn de mogelijke deelverzamelingen van een verzameling ter grootte 4, en twee punten zijn verbonden met een kant als ze precies een element gemeenschappelijk hebben.

Stelling 3. *$J(n,r)$ heeft een stabiele verzameling met ten minste $\frac{1}{n}\binom{n}{r}$ punten.*

Bewijs. Kleur de punten van $J(n,r)$ met de getallen $\{0,1,\ldots,n-1\}$, waarbij punt X als kleur de som van zijn elementen modulo n krijgt. Het is niet lastig te zien dat twee buurpunten verschillend worden gekleurd, dus elk van de n kleurklassen vormt een stabiele verzameling. De stelling volgt omdat ten minste een van de kleurklassen minstens $\frac{1}{n}\binom{n}{r}$ punten bevat. □

Een deelverzameling van een stabiele verzameling is opnieuw stabiel, en iedere stabiele verzameling van $J(n,r)$ correspondeert met een sparse-paving matroïde. Uit Stelling 3 volgt onmiddellijk dat

$$m(n,r) \geq 2^{\frac{1}{n}\binom{n}{r}}$$

en dus dat

$$m(n) \geq m(n,\lfloor n/2 \rfloor) \geq 2^{\frac{1}{n}\binom{n}{\lfloor n/2 \rfloor}}.$$

Met Nikhil Bansal en Rudi Pendavingh [1] heb ik bewezen dat deze ondergrens de juiste waarde van $m(n)$ geeft, op misschien een factor 2 in de exponent na.

Stelling 4. *Voor alle $\varepsilon > 0$ geldt voor voldoende grote n:*

$$2^{\frac{1}{n}\binom{n}{\lfloor n/2 \rfloor}} \leq m(n) \leq 2^{\frac{2+\varepsilon}{n}\binom{n}{\lfloor n/2 \rfloor}}.$$

Het bewijs van Stelling 4 is vrij technisch, maar is gebaseerd op de volgende twee ideeën. (Voor het gemak nemen we aan dat we het hier hebben over matroïden van rang $r = \lfloor n/2 \rfloor$.) Eerst begrenzen we het aantal mogelijke stabiele verzamelingen van $J(n,r)$ (en dus het aantal sparse-paving matroïden) door te laten zien dat iedere stabiele verzameling X van $J(n,r)$ een kleine deelverzameling S bevat met de eigenschap dat $X \backslash S \subseteq V(J(n,r)) \backslash (S \cup N(S))$ en $|V(J(n,r)) \backslash (S \cup N(S))| \leq \frac{2}{n}\binom{n}{r}$. Met 'klein' bedoelen we hier: zo klein dat het aantal mogelijke verzamelingen S hooguit $2^{\frac{\varepsilon}{n}\binom{n}{r}}$ is. Dit impliceert onmiddellijk dat $J(n,r)$ hooguit

$$2^{\frac{\varepsilon}{n}\binom{n}{r}} \times 2^{\frac{2}{n}\binom{n}{r}}$$

stabiele verzamelingen heeft. (Deze telmethode is een speciaal geval van een algemene methode die bekend staat als de containermethode, de geïnteresseerde lezer verwijzen we naar het overzichtsartikel [6].)

In de tweede stap breiden we dit argument uit naar algemene matroïden. Omdat in een algemene matroïde de verzameling niet-bases niet noodzakelijk een stabiele verzameling van $J(n,r)$ vormt, hebben we iets meer informatie nodig. Nog steeds geldt dat we voor iedere mogelijke verzameling niet-bases X een kleine verzameling S kunnen vinden als voorheen, maar nu moeten we naast de niet-bases in $V(J(n,r))\setminus(S\cup N(S))$ ook de niet-bases in $N(S)$ omschrijven. Vanwege de matroïdestructuur volstaat een kleine hoeveelheid extra informatie hiervoor, waarbij 'klein' betekent: gegeven S neemt $X\cap N(S)$ hooguit $2^{\frac{\varepsilon}{n}\binom{n}{r}}$ verschillende waarden aan. Omdat ε willekeurig gekozen was, volstaat dit om de bovengrens in Stelling 4 te bewijzen.

Terug naar typische eigenschappen

Het goede nieuws is nu dat we een verzameling technieken hebben ontwikkeld om vragen over typische eigenschappen te beantwoorden. Een van de krachtigste, die ik heb ontwikkeld samen met Rudi Pendavingh [4], is een verfijning van de telmethode die we hebben gebruikt om Stelling 4 te bewijzen. Het gaat te ver om het precieze resultaat hier te vermelden, maar een gevolg ervan is dat het aantal niet-bases van een typische matroïde dicht bij $\frac{1}{n}\binom{n}{r}$ ligt.

Stelling 5. *Er bestaan constanten $C_1,C_2>0$ zodat een typische matroïde ten minste $\frac{C_1}{n}\binom{n}{\lfloor n/2\rfloor}$ en hooguit $\frac{C_2\log^3(n)}{n}\binom{n}{\lfloor n/2\rfloor}$ niet-bases heeft.*

Veel matroïde-eigenschappen laten zich vertalen naar statistieken over niet-bases, wat Stelling 5 nuttig maakt voor de analyse van typische eigenschappen: als matroïden zonder een bepaalde eigenschap te veel of te weinig niet-bases hebben, dan volgt uit Stelling 5 dat de eigenschap typisch is. Ik geef twee voorbeelden van resultaten die Rudi Pendavingh en ik op deze manier hebben bewezen [4, 5].

Samenhang en symmetrie

Net als in grafentheorie speelt het begrip samenhang een belangrijke rol in matroïdentheorie. We noemen een matroïde $(E,\mathcal{B})$, hier gegeven door zijn verzameling bases, *samenhangend* als we E niet kunnen opsplitsen in twee niet-lege verzamelingen X en Y waarvoor $(X,\{B\cap X\colon B\in\mathcal{B}\})$ en $(Y,\{B\cap Y\colon B\in\mathcal{B}\})$ beide matroïden zijn. Het bestaan van zo'n partitie impliceert het bestaan van veel niet-bases, omdat iedere deelverzameling van E die X en Y niet doorsnijdt in het juiste aantal elementen geen basis is.

Stelling 6. *Een typische matroïde is samenhangend.*

(Eigenlijk hebben we bewezen dat een typische matroïde k-samenhangend is voor alle k, waar k-samenhang een sterkere notie van samenhang is.)

Een automorfisme van een matroïde M op grondverzameling E is een permutatie van E zodat bases op bases en niet-bases op niet-bases worden afgebeeld. We zeggen dat een matroïde *asymmetrisch* is als het enige automorfisme de identiteitsfunctie is. Als een matroïde een niet-triviaal automorfisme σ heeft, dan is de verzameling niet-bases gesloten onder toepassing van σ; als σ complex genoeg is, dan beperkt dit de verzamelingen mogelijke niet-bases. Op deze manier kunnen we laten zien dat bijna alle matroïden 'bijna asymmetrisch' zijn.

Stelling 7. *De automorfismegroep van een typische matroïde is triviaal of wordt voortgebracht door een enkele transpositie.*

(Een transpositie is een permutatie die precies twee elementen verwisselt.)

We geloven dat de waarheid is dat een typische matroïde asymmetrisch is. Verrassend genoeg brengt dit vermoeden ons terug bij het afschatten van $m(n)$; het blijkt namelijk dat het enige obstakel voor het bewijs de factor twee verschil tussen de exponent van de onder- en bovengrens is!

Open vragen

Met behulp van de gereedschappen die we hebben ontwikkeld, waaronder Stelling 5, kunnen we een groot aantal vragen over het gedrag van typische matroïden beantwoorden. Maar veel meer vragen staan nog wijd open. Ik sluit af met twee vragen die van centraal belang zijn.

Probleem. Is een typische matroïde sparse-paving?

Veel vragen over typische matroïden zijn makkelijker te beantwoorden voor sparse-paving matroïden. Een positief antwoord op deze vraag zou daarom direct grote gevolgen hebben.

De tweede vraag gaat over het asymptotische gedrag van de functie $m(n)$. De onder- en bovengrens in Stelling 4 verschillen slechts in een factor 2. Het is niet bekend of deze grenzen scherp zijn, en zo niet, hoe ze kunnen worden verbeterd.

Probleem. Wat is het asymptotische gedrag van $m(n)$?

Referenties

1 N. Bansal, R. Pendavingh en J. van der Pol, On the number of matroids, *Combinatorica* 35(1) (2015), 253–277.

2 R. Graham en N. Sloane, Lower bounds for constant weight codes, *IEEE Trans. Inf. Th.* 26(1) (1980), 37–43.

3 P. Nelson, Almost all matroids are non-representable, *Bull. London Math. Soc.* 50 (2018), 245–248.

4 R. Pendavingh en J. van der Pol, On the number of bases of almost all matroids, *Combinatorica* 38(4) (2018), 955–985.

5 R. Pendavingh en J. van der Pol, Asymptotics of symmetry in matroids, *J. Comb. Th. B* 135 (2019), 349–365.

6 W. Samotij, Counting independent sets in graphs, *Eur. J. Comb.* 48 (2015), 15–18.

7 H. Whitney, On the abstract properties of linear dependence, *American J. Math.* 57(3) (1935), 509–533.