Aart Blokhuis
Faculteit Wiskunde en Informatica
Technische Universiteit Eindhoven
a.blokhuis@tue.nl

Dion Gijswijt
Delft Institute of Applied Mathematics
TU Delft
d.c.gijswijt@tudelft.nl

De oplossing

Het Cap Set-probleem

Mei vorig jaar zorgde de Nederlandse wiskundige Dion Gijswijt van de TU Delft samen met Jordan Ellenberg (University of Wisconsin) voor een doorbraak in het Cap Set-probleem. In dit artikel bespreken Aart Blokhuis en Dion Gijswijt het probleem en de gevonden oplossing aan de hand van het kaartspel SET.

Vijftien jaar geleden verscheen er in dit tijdschrift een artikel van N.G. de Bruijn [4] over het nog immer populaire kaartspel SET. Elke kaart in dit spel heeft vier eigenschappen (vorm, kleur, aantal en invulling) en elke eigenschap komt voor in drie varianten. Drie kaarten vormen een SET als ze voor elke eigenschap ofwel alle drie gelijk zijn, ofwel alle drie verschillend. Het doel van het spel is om binnen de kaarten die op tafel liggen zo snel mogelijk een SET te vinden. Wanneer er geen SET is, worden extra kaarten neergelegd.

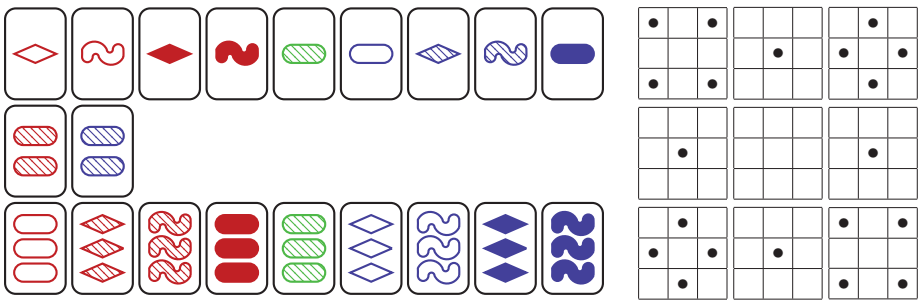
Zoals in het artikel van De Bruijn wordt uitgelegd, kunnen de 81 kaarten worden geïdentificeerd met de punten van $AG(4,3)$, de vierdimensionale (affiene) ruimte over het lichaam $\mathbb{F}_3 = \{0,1,2\}$ met drie elementen en met optelling en vermenigvuldiging modulo 3. Hierbij vormen drie kaarten een SET precies dan wanneer de bijbehorende punten op één lijn liggen (en dus een lijn vormen). Het grootste aantal kaarten zonder SET is dus precies de maximale kardinaliteit van een *cap set* of *cap* in $AG(4,3)$, een verzameling punten met hooguit twee op een lijn. Op affiene transformaties na is er precies één grootste cap: de 'Pellegrino cap' afgebeeld in Figuur 1.

Voor een toegankelijke introductie tot het Cap Set-probleem en de relatie met SET verwijzen we de lezer graag naar het artikel van Davis en Maclagan [7].

Het Cap Set-probleem

Een van de centrale problemen in de eindige meetkunde, de studie van affiene en projectieve ruimten over een eindige lichaam met q elementen, is het bepalen van onder- en bovengrenzen op de kardinaliteit van zulke 'caps' of 'cap sets': een collectie punten met de eigenschap dat er geen drie op één lijn liggen. Voor een projectief vlak van de orde q is hier de bovengrens $q+2$ als q even is, en $q+1$ voor q oneven.

Een van de hoogtepunten in de geschiedenis van de eindige meetkunde is het resultaat uit 1954 van Beniamino Segre [14] dat voor oneven q een cap van de maximale grootte $q+1$ in $PG(2,q)$ (of $AG(2,q)$), het projectieve (affiene) vlak van orde q, altijd een kegelsnede is (en dus voldoet aan een homogene tweedegraadsvergelijking). Voor even q is de classificatie van caps met het maximale aantal van $q+2$ punten, zogenaamde hyperovalen nog een open probleem. Om een idee te krijgen



Figuur 1 De twintig kaarten links zonder SET representeren een cap in $AG(4,3)$ van maximale grootte. Puzzeltje: vind een correspondentie tussen de kaarten links en de vierkantjes met een punt rechts.

van de ontwikkelingen op dit gebied kan men bijvoorbeeld de hyperovaalpagina op de homepage van Bill Cherowitzo [5] raadplegen.

In dimensie 3 is de zaak ook nog redelijk duidelijk. Hier is de grens q^2+1 voor de projectieve ruimte $PG(3,q)$ en q^2 voor de affiene ruimte $AG(3,q)$ (voor $q>2$). Een cap van deze afmeting heet een ovoïde. Voor oneven q is dit noodzakelijk een elliptische kwadriek (in het affiene geval met een raakvlak op oneindig), voor even q is er één andere familie bekend. Het vermoeden is, dat dat alles is. Vanaf dimensie 4 is alles onduidelijk. Het laatste grote overzicht over deze en soortgelijke problemen is te vinden op de homepage van Leo Storme [12] en dateert van 2001. Een meer recent (2012), beperkter, maar voor ons verhaal belangrijker overzicht is te vinden in [2] en op de pagina van Yves Edel [9].

Voor $q=2$ is het bovenstaande probleem niet interessant, hier geldt de triviale bovengrens 2^n in $PG(n,2)$ en $AG(n,2)$, in het laatste geval door simpelweg alle punten te nemen. Ons Cap Set-probleem is het geval $q=3$ en meer speciaal $AG(n,3)$ of $\mathbb{F}_3^n$. We kunnen in dit geval het probleem als volgt herformuleren. Laat $\mathbb{Z}/3\mathbb{Z}$ de groep zijn met drie elementen, dus $\{0,1,2\}$ met optellen modulo 3 (ofwel de optelgroep van het lichaam $\mathbb{F}_3$). Onze cap is nu een deelverzameling $C\subset(\mathbb{Z}/3\mathbb{Z})^n$ met de eigenschap dat $a+b+c=\underline{0}$ geen oplossingen heeft met $a,b,c\in C$, of beter gezegd, de enige oplossingen zijn die met $a=b=c$. Nog een manier om dit te formuleren is dat C geen rekenkundige rij ter lengte 3 bevat. In termen van de n-dimensionaal variant van SET bestuderen we verzamelingen kaarten zonder SET.

Asymptotisch gedrag

Laat c_n het maximale aantal punten van een cap in $AG(n,3)$ zijn. De enige waarden die exact bekend zijn, zijn $c_1=2$, $c_2=4$, $c_3=9$, $c_4=20$, $c_5=45$ en $c_6=112$ (rij A090245 van de OEIS). Naast specifieke waarden zijn we vooral geïnteresseerd in het asymptotisch gedrag van de rij (c_n). Wanneer C_1 een cap is in $AG(n,3)$ en C_2 een cap is in $AG(m,3)$, dan is het product $C_1\times C_2=\{(c_1,c_2)\mid c_1\in C_1, c_2\in C_2\}$ een cap in $AG(n+m,3)$. Uit onze observatie volgt (via Fekete's lemma) dat

$$c=\lim_{n\to\infty}\sqrt[n]{c_n}$$

bestaat en dat $c\geq\sqrt[n]{c_n}$ voor elke n. De cap uit Figuur 1 levert dus op dat $c\geq\sqrt[4]{20}\geq 2{,}11$. De beste ondergrens die bekend is komt van een constructie van een cap in $AG(480,3)$ door Edel [8] en geeft $c\geq 2{,}21739$.

Een overduidelijke bovengrens is $c\leq 3$, want $AG(n,3)$ heeft immers maar 3^n punten. Brown en Buhler [3] gaven in 1982 de eerste niet-triviale bovengrens $c_n=o(3^n)$. Door gebruik te maken van ideeën uit de Fourieranalyse verbeterde Meshulam dit in 1995 tot $c_n=O(3^n/n)$. De beste bovengrens, tot vorig jaar, was een resultaat van Bateman en Katz [1]. Het bewijs is wederom gebaseerd op Fourieranalyse en geeft $c_n=O(3^n/(n^{1+\varepsilon}))$ voor een zekere positieve (maar heel kleine) ε. Voor de constante c geven deze bovengrenzen echter geen verbetering. Het volgende probleem (geformuleerd door Brown en Buhler) bleef dan ook open.

Probleem 1 (Cap Set-probleem)**.** Geldt er dat $c<3$?

De doorbraak

Een doorbraak kwam in mei 2016 toen Ernie Croot, Seva Lev en Péter Pach [6] een verwant probleem oplosten. Zij bewezen dat elke deelverzameling van $(\mathbb{Z}/4\mathbb{Z})^n$ zonder rekenkundige rij van lengte 3 niet meer dan γ^n elementen kan bevatten voor een zeker constante $\gamma\approx 3{,}60$ kleiner dan 4. Binnen een paar weken wisten Jordan Ellenberg en de tweede auteur van dit stuk, onafhankelijk van elkaar, het bewijs van Croot, Lev en Pach aan te passen voor $\mathbb{F}_q^n$, met q een oneven priemmacht. Het geval $q=3$ correspondeert precies met het Cap Set-probleem, waarvoor ze de volgende expliciete grens vonden:

Stelling 2. *Laat $A\subseteq\mathbb{F}_3^n$ een cap set zijn. Dan geldt $|A|\leq 3\cdot 2{,}756^n$ (en dus $c\leq 2{,}756$).*

Het resulterende artikel [10] en het artikel van Croot, Lev en Pach zijn, zij aan zij, verschenen in hetzelfde nummer van *Annals of Mathematics*.

Hypermatrices en slice-rank

Kort na deze oplossing van het Cap Set-probleem gaf Terence Tao in een blogpost [15] een elegante herformulering van het bewijs in termen van de 'slice-rank' van hypermatrices. Hieronder geven we een schets van de ideeën in het bewijs.

Een *hypermatrix* van *orde* $k\geq 2$ is een functie

$$H: J_1\times J_2\times\cdots\times J_k\to\mathbb{F}$$

voor zekere eindige verzamelingen $J_1,\ldots,J_k$ en een lichaam $\mathbb{F}$. In het geval $k=2$ is H een $|J_1|\times|J_2|$-matrix en in het algemeen kunnen we H zien als een k-dimensionale tabel waarbij de 'plakken' in de t-de richting gelabeld zijn met de elementen uit J_t.

We zeggen dat H *simpel* is als in een van de richtingen $t\in\{1,\ldots,k\}$ geldt dat de $|J_t|$ plakken waaruit H bestaat lineaire veelvouden van elkaar zijn. In formules:

$$H(x_1,\ldots,x_k)=f(x_t)\cdot G(x_1,\ldots,x_{t-1},x_{t+1},\ldots,x_k)$$

voor zekere functies $f: J_t\to\mathbb{F}$ en $G: J_1\times\cdots\times J_{t-1}\times J_{t+1}\times\cdots\times J_k\to\mathbb{F}$. In dit verhaal is de *rang* (maar eigenlijk 'slice-rank') van een hypermatrix H het kleinste getal r waarvoor H te schrijven is als de som van r simpele hypermatrices. Voor $k=2$ komt dit overeen met de gebruikelijke matrixrang. Veel eigenschappen van matrixrang gelden ook in het algemene geval. Analoog aan het geval van diagonaal matrices geldt het volgende belangrijke lemma (waarvan het bewijs een leuke oefening is).

Lemma 3. *Laat $H: J\times\cdots\times J\to\mathbb{F}$ een hypermatrix van orde k zijn met $H(x_1,\ldots,x_k)\neq 0$ dan en slechts dan als $x_1=x_2=\cdots=x_k$. Dan geldt* rang $H=|J|$.

Verboden deelstructuren

Zoals veel andere problemen uit de extremale combinatoriek kan het Cap Set-probleem worden geformuleerd als het bepalen van de maximale grootte van een verzameling waarin een gegeven structuur ontbreekt. Preciezer gezegd: laat V een eindige verzameling zijn en $E\subseteq V^k$ een verzameling 'verboden' k-tallen. We zijn geïnteresseerd in de maximale kardinaliteit $\alpha(V,E)$ van een deelverzameling $S\subseteq V$ zonder verboden k-tal (dat wil zeggen waarvoor geldt: $S^k\cap E=\emptyset$). In het Cap Set-probleem is $V=\mathbb{F}_3^n$, bestaat E uit alle drietallen collineaire punten en is $c_n=\alpha(V,E)$.

We zeggen dat een hypermatrix $H: V^k\to\mathbb{F}$ *past* bij (V,E) als alle diagonaalelementen $H(a,\ldots,a)$ ongelijk aan nul zijn en de elementen $H(a_1,\ldots,a_k)$ buiten de diagonaal alleen ongelijk nul kunnen zijn voor $(a_1,\ldots,a_k)\in E$. De volgende stelling geeft een bovengrens voor $\alpha(V,E)$ die analoog is aan de Haemers-grens [11].

Stelling 4. *Laat H een hypermatrix zijn die past bij (V,E). Dan geldt $\alpha(V,E) \leq \operatorname{rang} H$.*

Het bewijs volgt direct uit Lemma 3 en het feit dat de rang van H niet kleiner is dan die van zijn beperking tot S^k wanneer $S \subseteq V$ een deelverzameling is zonder verboden k-tal.

Het bewijs

We schetsen nu het bewijs van Stelling 2. Laat H de volgende hypermatrix zijn:

$$H : \mathbb{F}_3^n \times \mathbb{F}_3^n \times \mathbb{F}_3^n \to \mathbb{F}_3,$$
$$H(a,b,c) := \begin{cases} 1 & \text{als } a+b+c=0, \\ 0 & \text{anders.} \end{cases} \quad (1)$$

Wegens Stelling 4 is het nu voldoende om een goede bovengrens te vinden voor de rang van H. Hiertoe schrijven we H als een polynoom in de $3n$ variabelen $x=(x_1,\ldots,x_n)$, $y=(y_1,\ldots,y_n)$ en $z=(z_1,\ldots,z_n)$:

$$H(x,y,z) = \prod_{i=1}^{n} [1-(x_i+y_i+z_i)^2]. \quad (2)$$

Hier gebruiken we dat $1^2 = 2^2 = 1$ in $\mathbb{F}_3$ en dus $H(x,y,z)=0$ zodra $x_i+y_i+z_i \neq 0$ voor zekere i.

Voor elk monoom

$$x^\alpha y^\beta z^\gamma = x_1^{\alpha_1}\cdots x_n^{\alpha_n} \cdot y_1^{\beta_1}\cdots y_n^{\beta_n} \cdot z_1^{\gamma_1}\cdots z_n^{\gamma_n}$$

in de expansie van H geldt dat elke variabele exponent ten hoogste 2 heeft, en de totale graad ten hoogste $2n$ is. Dit impliceert dat H geschreven kan worden als

$$\begin{aligned} H(x,y,z) = &\sum_\alpha x^\alpha F_\alpha(y,z) \\ &+ \sum_\beta y^\beta G_\beta(x,z) \\ &+ \sum_\gamma z^\gamma H_\gamma(x,y) \end{aligned} \quad (3)$$

voor zekere functies F_α, G_β, H_γ, waarbij α, β, γ in de som lopen over de verzameling $T = \{t \in \{0,1,2\}^n \mid t_1+\cdots+t_n \leq \frac{2n}{3}\}$. Aangezien elke term in (3) een simpele hypermatrix is, volgt dat H rang ten hoogste $3|T|$ heeft. Met behulp van de ongelijkheid van Chernoff kan $|T|$ worden afgeschat als $|T| \leq 2{,}756^n$. We vinden dus dat de maximale kardinaliteit van een cap set in dimensie n niet meer is dan $3 \cdot 2{,}756^n$. □

Referenties

1 M. Bateman en N. Katz, New bounds on cap sets, *Journal of the American Mathematical Society* 25(2) (2012), 585–613.

2 J. Bierbrauer en Y. Edel, Large caps in projective Galois spaces, in Jan de Beule en Leo Storme, eds., *Current Research Topics in Galois Geometry*, Nova Science Publishers (2012), 87–104.

3 T.C. Brown en J. P. Buhler, A density version of a geometric Ramsey theorem, *Journal of Combinatorial Theory, Series A* 32(1) (1982), 20–34.

4 N.G. de Bruijn, Set!, *Nieuw Archief voor Wiskunde* 5/3(4) (2002), 320–325.

5 B. Cherowitzo, Bill Cherowitzo's hyperoval page (2004), http://math.ucdenver.edu/~wcherowi/research/hyperoval/hypero.html.

6 E. Croot, V.F. Lev en P.P. Pach, Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small, *Annals of Mathematics* 185(1) (2017), 331–337.

7 B.L. Davis en D. Maclagan, The card game SET, *The Mathematical Intelligencer* 25(3) (2003), 33–40.

8 Y. Edel, Extensions of generalized product caps, *Designs, Codes and Cryptography* 31(1) (2004), 5–14.

9 Y. Edel, Caps (2010), www.mathi.uni-heidelberg.de/~yves/Matritzen/CAPs/CAPMatIndex.html.

10 J.S. Ellenberg en D. Gijswijt, On large subsets of $\mathbb{F}_n^q$ with no three-term arithmetic progression, *Annals of Mathematics* 185(1) (2017), 339–343.

11 W. Haemers, An upper bound for the Shannon capacity of a graph, *Colloq. Math. Soc. Janos Bolyai*, 1978, pp. 267–272.

12 J.W.P. Hirschfeld en L. Storme, *The Packing Problem in Statistics, Coding Theory and Finite Projective Spaces: Update 2001*, Developments in Mathematics, Vol. 3, Eds. A. Blokhuis, J.W.P. Hirschfeld, D. Jungnickel en J.A. Thas, eds., *Finite Geometries, Proceedings of the Fourth Isle of Thorns Conference*, Kluwer, 2001, pp. 201–246.

13 R. Meshulam, On subsets of finite abelian groups with no 3-term arithmetic progressions, *Journal of Combinatorial Theory, Series A* 71(1) (1995), 168–172.

14 B. Segre, Sulle ovali nei piani lineari finiti, *Atti Accad. Naz. Lincei Rend.* 17(1-2) (1954).

15 T. Tao, A symmetric formulation of the Croot–Lev–Pach–Ellenberg–Gijswijt capset bound (2016), http://terrytao.wordpress.com/2016/05/18/a.