

CIRKELS

Op het college hebben we het gehad over Cirkels. Dat zijn deelverzamelingen van $\mathbb{P}^1\mathbb{C} = \mathbb{C} \cup \{\infty\}$ die ofwel van de vorm $\{z \in \mathbb{C} \mid |z - m| = r\}$ zijn met m een complex getal en r een positief reëel getal (cirkels), ofwel van de vorm $\{z_0 + tv \mid t \in \mathbb{R}\} \cup \{\infty\}$ met $z_0 \in \mathbb{C}$ en $v \in \mathbb{C} \setminus \{0\}$ (lijnen).

Er is een mooiere definitie, en die vind je door de vergelijkingen in homogene coördinaten uit te drukken. Bijvoorbeeld ligt $(z_0 : z_1) \in \mathbb{P}^1\mathbb{C}$ op bovenstaande cirkel als en alleen als $z_1 \neq 0$ is en

$$\begin{aligned} & \left(\frac{\bar{z}_0}{\bar{z}_1} - \bar{m}\right)\left(\frac{z_0}{z_1} - m\right) = r^2 \\ \Leftrightarrow & (\bar{z}_0 - \bar{m}\bar{z}_1)(z_0 - mz_1) = r^2 z_1 \bar{z}_1 \\ \Leftrightarrow & \bar{z}_0 z_0 - m \bar{z}_0 z_1 - \bar{m} \bar{z}_1 z_0 + (|m|^2 - r^2) \bar{z}_1 z_1 = 0 \\ \Leftrightarrow & \begin{bmatrix} \bar{z}_0 & \bar{z}_1 \end{bmatrix} \begin{bmatrix} 1 & -m \\ -\bar{m} & (|m|^2 - r^2) \end{bmatrix} \begin{bmatrix} z_0 \\ z_1 \end{bmatrix} = 0. \end{aligned}$$

De matrix A in het midden voldoet aan $A^* = A$, waarbij $*$ de geconjugeerde getransponeerde van A is, en aan $\det A < 0$, en aan $A_{11} \neq 0$. Omgekeerd is elke matrix A' die aan deze eisen voldoet een reëel veelvoud van een matrix van de vorm $\begin{bmatrix} 1 & -m \\ -\bar{m} & (|m|^2 - r^2) \end{bmatrix}$, en de verzameling punten $(z_0 : z_1)$ die voldoet aan $\underline{z}^* A \underline{z} = 0$,

waar $\underline{z} = \begin{bmatrix} z_0 \\ z_1 \end{bmatrix}$ is dus een cirkel. Cirkels corresponderen dus een op een met zulke matrices, behalve dat reële veelvouden van A dezelfde cirkel definiëren. Als je A_{11} nul maakt maar aan de overige eisen vasthoudt krijg je de vergelijking voor een reële lijn in $\mathbb{C}$. Dus lijnen zijn gedegenerende cirkels. Conclusie: Cirkels zijn precies alle verzamelingen van de vorm

$$\{(z_0 : z_1) \mid \begin{bmatrix} \bar{z}_0 & \bar{z}_1 \end{bmatrix} A \begin{bmatrix} z_0 \\ z_1 \end{bmatrix} = 0\}$$

waarbij A een Hermitische matrix is (d.w.z. $A^* = A$) met negatieve determinant.

Met deze interpretatie is het duidelijk dat een complexe inverteerbare 2×2 -matrix g een Cirkel C_1 afbeeldt op een Cirkel. Immers, als A de Cirkel C_1 definieert, dan bestaat het beeld uit alle punten $(z_0 : z_1)$ waarvoor geldt $(g^{-1}\underline{z})^* A g^{-1}\underline{z} = \underline{z}^* (g^{-1})^* A g^{-1} \underline{z} = 0$, en de matrix $(g^{-1})^* A g^{-1}$ is weer Hermitisch met negatieve determinant.

Hieruit volgt ook dat elke Cirkel C van de vorm $g\mathbb{P}^1\mathbb{R}$ is voor zekere $g \in \text{GL}_2(\mathbb{C})$. Op college hebben we daarom, voor algemene lichaamsuitbreidingen $K \subseteq L$, “Cirkels” gedefinieerd als alle verzamelingen van de vorm $g\mathbb{P}^1K$ met $g \in \text{GL}_2(L)$. Deze vormen een 3-design: door 3 verschillende punten gaat een unieke “Cirkel”.

1. ERDŐS-KO-RADO

De stelling van Erdős-Ko-Rado zegt dat als n, k natuurlijke getallen zijn met $n \geq 2k$, en als F een collectie k -deelverzamelingen van $\{1, \dots, n\}$ is met de eigenschap dat $A \cap B$ niet leeg is voor alle $A, B \in F$, dan $|F| \leq \binom{n-1}{k-1}$.

Het bewijs van Gyula Katona gaat als volgt: tel het aantal paren (A, C) , waarbij $A \in F$ en C een cyclische ordening van $1, \dots, n$ is, waarvoor geldt dat A in C een “interval” is, dat wil zeggen uit k in de cyclische ordening opeenvolgende elementen

bestaat. Aan de ene kant is dit aantal gelijk aan $|F|k!(n-k)!$: immers, als je A kiest ($|F|$ mogelijkheden), dan zijn er $k!(n-k)!$ cyclische ordeningen waarin A een interval is, want je kunt eerst de elementen van A op een willekeurige volgorde zetten ($k!$ manieren) en die laten volgen door een willekeurige volgorde van de rest. Aan de andere kant is het aantal paren hooguit gelijk aan $(n-1)!k$: immers, er zijn $(n-1)!$ verschillende cyclische ordeningen, en in elke cyclische ordening zijn hooguit k elementen van F een interval, want als je meer dan k intervallen hebt, dan zijn er twee die elkaar niet snijden (ga na!). Dus $|F|k!(n-k)! \leq k(n-1)!$, dus $|F| \leq \binom{n-1}{k-1}$.

De Frankl-Wilson stelling is het analogon van deze stelling voor vectorruimten over $\mathbb{F}_q$: voor dezelfde n en k , als F een collectie van k -dimensionale vectordeelruimten van $\mathbb{F}_q^n$ is zo dat voor alle $A, B \in F$ geldt $A \cap B \neq \{0\}$, dan is $|F| \leq \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q$.

Een bewijs voor het geval dat $k|n$ gaat als volgt: “partitioneer” $\mathbb{F}_q^n$ in k -dimensionale deelruimten. D.w.z. kies een collectie S van k -dimensionale deelruimten van $\mathbb{F}_q^n$ wier vereniging de hele ruimte $\mathbb{F}_q^n$ is en waarvoor geldt: voor alle $A, B \in S$ is $A \cap B = \{0\}$. Zo’n collectie bestaat, en wel uit $(q^n - 1)/(q^k - 1)$ deelruimten. Tel nu paren (A, g) , waarbij $A \in F$ is en $g \in \text{GL}_n(\mathbb{F}_q)$, zo dat gA in S voorkomt. Als je A vast kiest, en het element van S waar A naartoe moet worden afgebeeld, dan zijn er $|\text{GL}_k(\mathbb{F}_q)||\text{GL}_{n-k}(\mathbb{F}_q)|q^{k(n-k)}$ mogelijkheden voor g (denk aan een bovendriehoeks-blokmatrix). Dus het aantal paren is

$$|F| \frac{q^n - 1}{q^k - 1} (q^k - 1) \cdots (q^k - q^{k-1}) (q^{n-k} - 1) \cdots (q^{n-k} - q^{n-k-1}) q^{k(n-k)}.$$

Aan de andere kant, als je eerst g kiest, dan kan g hooguit één $A \in F$ op een element van S afbeelden. Immers, de elementen van F snijden elkaar paarsgewijs in minstens 1 dimensie, en g verandert daar niets aan, maar de elementen van S snijden elkaar paarsgewijs alleen in 0. Dus het aantal paren is hooguit $|\text{GL}_n(\mathbb{F}_q)| = (q^n - 1) \cdots (q^n - q^{n-1})$. Dit geeft de gewenste bovengrens op $|F|$.