Algebraic Methods in Combinatorics*

Dr. Christian Reiher
(GeTEXt von Xiangxiang Michael Zheng)

Wintersemester 2022 - 2023

Inhaltsverzeichnis

*Trotz des englischen Titels wird die Vorlesung (von Dr. Christian Reiher) auf Deutsch gehalten.

Dieser Kurs wird sich in drei Schwierigkeitsstufen aufteilen:

1. Gewisse kombinatorische Probleme lassen sich elegant lösen „nur“ mit linearer Algebra.
2. Andere Probleme lassen sich nicht lösen mit nur linearer Algebra, Tricks und Fakten über Polynomringe werden dann beispielsweise notwendig.
3. Methoden der kommutativen Algebra werden benötigt.

1 Einführung

Als Geschmacksprobe für den Kurs werden wir zuerst die folgenden Probleme behandeln:

Probleme[1]

1. Gegeben ist eine endliche Menge X. $\mathcal{C} \subseteq \mathcal{P}(X)$ erfülle:
   (a) Für alle $A \in \mathcal{C}$ ist $|A|$ gerade.
   (b) Für alle $A, B \in \mathcal{C}$ ist $|A \cap B|$ gerade.
   Wie groß ist $\mathcal{C}$ höchstens?[2]
2. Gegeben ist eine endliche Menge X. $\mathcal{C} \subseteq \mathcal{P}(X)$ erfülle:
   (a) Für alle $A \in \mathcal{C}$ ist $|A|$ ungerade.
   (b) Für alle $A, B \in \mathcal{C}$ ist $|A \cap B|$ gerade.
   Gleiche Frage: Wie groß ist $\mathcal{C}$ höchstens?[3]
3. Sei $X \subseteq \mathbb{R}^n$ eine Menge von Punkten derart, dass je zwei gleichen Abstand haben. Wie groß ist X höchstens?
4. Sei $X \subseteq \mathbb{R}^n$ eine Menge von Punkten, bei der nun zwei Abstände auftreten. Wie groß ist X höchstens?
5. Kann man ein sogenanntes Tetraeder in endlich viele Polyeder zerlegen und diese zu einem Würfel zusammensetzen?[4]
6. Es seien 13 Gewichte gegeben mit der Eigenschaft, dass wenn man ein beliebiges auf die Seite legt, die übrigen in 2 Mengen von 6 Gewichten mit gleichem Gesamtgewicht aufteilen kann. Müssen die 13 Gewichte gleich schwer sein?
7. Was kann man über $\{C_3, C_4\}$-freie r-reguläre Graphen mit möglichst wenigen Ecken sagen?

Zu den meisten Problemen kann man auf simple Konstruktionen kommen.

[1] Zum Teil ungelöst.
[2] Dieses Problem ist bekannt als das „Eventown Problem“.
[3] Dieses Problem ist bekannt als das „Oddtown Problem“.
[4] Das ist Hilberts drittes Problem.

1. Paare die Elemente von X auf ($\rightsquigarrow \lfloor |X|/2 \rfloor$ Paare) und bilde alle möglichen Teilmengen dieser Paare ($\rightsquigarrow 2^{\lfloor |X|/2 \rfloor}$).
2. Nehme als Club $\mathcal{C}$ die Menge aller ein-elementigen Teilmengen von X ($\rightsquigarrow |\mathcal{C}| = |X|$).
3. Für $n = 1, 2, 3$ erhält man mit einer Linie, einem gleichseitigen Dreieck und einem Tetraeder eine Konstruktion mit $n + 1$ Punkten.
4. Für $n = 2$ erhält man etwas besseres als in 3., beispielsweise kann eine Konfiguration mit vier Punkten konstruiert werden, indem man den Mittelpunkt in das gleichseitige Dreieck hinzufügt. Man kriegt sogar mit den Ecken eines regelmäßigen Fünfecks sogar fünf Punkte hin.[5]

Wir werden nun nacheinander zeigen, dass diese Konstruktionen optimal sind.[6]

Satz 1.1. Seien $A_1, \ldots, A_m \subseteq X$, wobei

- $|A_i|$ ungerade ist für $i = 1, \ldots, m$,
- $|A_i \cap A_j|$ gerade ist für $i \neq j$.

Dann ist $m \leq |X|$.

Beweis. O.B.d.A. sei $X = [n] (= \{1, \ldots, n\})$. Betrachte den n-dimensionalen Vektorraum mit Basis $e_1, \ldots, e_n$. Jeder Menge $A \subseteq [n]$ werde der Vektor

$$v_A = \sum_{j \in A} e_j$$

zugeordnet. Das Standardskalarprodukt $\langle x, y \rangle$ ist durch $\langle e_i, e_j \rangle = \delta_{i,j}$ gegeben. Für $A, B \subseteq [n]$ ist $\langle v_A, v_B \rangle = |A \cap B|$. Insbesondere gilt

$$\left\langle v_{A_i}, v_{A_j} \right\rangle = \begin{cases} \text{ungerade}, & i = j \\ \text{gerade}, & \text{sonst.} \end{cases}$$

Noch haben wir den Körper nicht spezifiziert, und werden nun bequemlichkeitshalber den Körper $\mathbb{F}_2$ wählen. Dann vereinfacht sich die Gleichung zu $\left\langle v_{A_i}, v_{A_j} \right\rangle = \delta_{i,j}$. Die Vektoren $v_{A_1,}, \ldots, v_{A_m}$ sind somit linear unabhängig, denn haben wir eine Linearkombination

$$\sum_{i=1}^{m} \alpha_i v_{A_i} = 0,$$

wobei $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_2$, so ist

$$0 = \left\langle \sum_{i=1}^{m} \alpha_i v_{A_i}, v_{A_j} \right\rangle = \alpha_j$$

für alle $j = 1, \ldots, m$. Damit folgt $m \leq n$. □

[5] Dies ist optimal.

[6] Diese Konstruktionen sind **nicht** im Allgemeinen eindeutig. Für $n = 7$ zu der 1. Frage bildet $\mathcal{C}$ mit $\emptyset$ und den Komplementen der Geraden der Fano-Ebene eine optimale Konfiguration der Größe 2^3.

Ein Standard-kombinatorischer Beweis ist auf MathOverflow zu finden.

Bemerkung 1.2. Für alle $A, B \in [n]$ ist

$$v_A + v_B = v_{A \Delta B},$$

wobei $A \Delta B$ die *symmetrische Differenz* von A und B ist. Dies zeigt, dass $\mathcal{P}(X)$ mit Δ als Addition ein $\mathbb{F}_2$-Vektorraum ist. Weiter ist

$$\langle A, B \rangle = \text{Parität von } |A \cap B|.$$

Satz 1.3. Sei $\mathcal{C} \subseteq \mathcal{P}(X)$ eine Menge derart, dass $|A \cap B|$ gerade für alle $A, B \in \mathcal{C}$ ist. Dann ist

$$|\mathcal{C}| \leq 2^{\left\lfloor \frac{|X|}{2} \right\rfloor}.$$

Beweis. Sei $n = |X|$. Für alle $A, B \in \mathcal{C}$ ist $\langle A, B \rangle = 0$. Sei $U \subseteq \mathcal{P}(X)$ der von $\mathcal{C}$ erzeugte Untervektorraum. Dann folgt $\langle A, B \rangle = 0$ für alle $A, B \in U$. Somit ist $U^\perp \supseteq U$ und

$$n = \dim U^\perp + \dim U \geq 2 \dim U.$$

Also ist $\dim U \leq \lfloor n/2 \rfloor$ und $|\mathcal{C}| \leq |U| = 2^{\dim U} \leq 2^{\lfloor n/2 \rfloor}$. □

Als nächstes zeigen wir, dass die Antwort auf die 6. Frage „Nein." lautet.

Proposition 1.4. Es seien $a_1, \ldots, a_{2n+1} \in \mathbb{R}$. Wenn es für jedes $i \in [2n+1]$ eine Partition $[2n+1] \setminus \{i\} = X_i \cup Y_i$ mit $|X_i| = |Y_i| = n$ und

$$\sum_{j \in X_i} a_j = \sum_{j \in Y_i} a_j$$

gibt, dann ist $a_1 = \cdots = a_{2n+1}$.

Beweis.

Beobachtung 1.5. Wenn $a_1, \ldots, a_{2n+1}$ diese Eigenschaft haben, dann auch

$$\lambda a_1 + \mu, \ldots, \lambda a_{2n+1} + \mu \ (\lambda, \mu \in \mathbb{R}).$$

Wir werden zuerst zeigen, dass die Aussage für $\mathbb{N}_0$ gilt, dann für $\mathbb{Z}$, $\mathbb{Q}$, und zuletzt $\mathbb{R}$: Angenommen es gäbe ein Gegenbeispiel mit $a_1, \ldots, a_{2n+1} \in \mathbb{N}_0$. Wähle ein solches mit $\max\{a_1, \ldots, a_{2n+1}\}$ minimal. Nun muss $0 \in \{a_1, \ldots, a_{2n+1}\}$ gelten, da man zu gegebenen Gegenbeispiel durch geeignete Translation das minimale Element 0 machen kann. Wegen

$$a_i \equiv a_i + \sum_{j \in X_i} a_j + \sum_{j \in Y_i} a_j \equiv \sum_{j=1}^{2n+1} a_j \pmod 2$$

haben $a_1, \ldots, a_{2n+1}$ gleiche Parität, das heißt alle sind gerade. Dann ist aber

$$\frac{a_1}{2}, \ldots, \frac{a_{2n+1}}{2}$$

ein kleineres Gegenbeispiel. ↯
Somit stimmt auch die Behauptung für $a_1, \dots, a_{2n+1} \in \mathbb{Z}$ (wegen der Translationsinvarianz) und für $a_1, \dots, a_{2n+1} \in \mathbb{Q}$ (wegen der Skalierungsinvarianz). Angenommen $a_1, \dots, a_{2n+1}$ wäre ein reelles Gegenbeispiel und $a_r \neq a_s$. Für alle $i \in [2n+1]$ schreiben wir die i-te Gleichung in der Form $\langle c_i, a \rangle = 0$, wobei c_i in der i-ten Koordinate 0, in n Koordinaten $+1$ und in n Koordinaten -1 ist. Außerdem ist $\langle a, e_r - e_s \rangle \neq 0$.
Andererseits wissen wir: Wenn $b \in \mathbb{Q}^{2n+1}$, $\langle c_i, b \rangle = 0$ für $i = 1, \dots, 2n+1$, dann

$$\langle b, e_r - e_s \rangle = 0.$$

Sei $U \subseteq \mathbb{Q}^{2n+1}$ der von $c_1, \dots, c_{2n+1}$ erzeugte Untervektorraum. Für alle $b \in U^\perp$ ist $\langle b, e_r - e_s \rangle = 0$. Daher ist $e_r - e_s \in (U^\perp)^\perp = U$. Es gibt also $\lambda_1, \dots, \lambda_{2n+1} \in \mathbb{Q}$ mit

$$e_r - e_s = \sum_{i=1}^{2n+1} \lambda_i c_i.$$

Folglich ist

$$\langle a, e_r - e_s \rangle = \sum_{i=1}^{2n+1} \lambda_i \langle a, c_i \rangle = 0. \; ↯ \qquad \square$$

Wir betrachten nun die 3. Frage.

Fakt 1.6. Haben $x_1, \dots, x_m \in \mathbb{R}^n$ paarweise Abstand 1, dann ist $m \leq n+1$.

Beweis. Durch Verschiebung erreicht man

$$x_1 + \dots + x_m = 0.$$

Für alle $i \in [m]$ ist

$$\begin{aligned} m - 1 &= \sum_{j=1}^{m} \|x_i - x_j\|^2 \\ &= m \|x_i\|^2 + \sum_{j=1}^{m} \|x_j\|^2 - 2 \left\langle x_i, \underbrace{x_1 + \dots + x_n}_{=0} \right\rangle \\ &= m \|x_i\|^2 + \sum_{j=1}^{m} \|x_j\|^2 , \end{aligned}$$

also $\|x_i\|^2 = (m-1)/(2m)$ für alle $i \in [m]$. Für $i \neq j$ ist

$$1 = \|x_i - x_j\|^2 = \|x_i\|^2 - 2 \langle x_i, x_j \rangle + \|x_j\|^2 ,$$

also $\langle x_i, x_j \rangle = -1/(2m)$. Betrachte die Vektoren

$$y_i = \begin{pmatrix} \frac{1}{\sqrt{2m}} & x_i \end{pmatrix} \in \mathbb{R} \times \mathbb{R}^n.$$

Da $y_1, \dots, y_m$ paarweise senkrecht sind, ist $m \leq n+1$. $\square$

Diese Schranke ist auch optimal: Die Vektoren

$$\frac{1}{\sqrt{2}}e_1, \ldots, \frac{1}{\sqrt{2}}e_{n+1} \in \mathbb{R}^{n+1}$$

haben paarweise Abstand 1. sind paarweise senkrecht, und befinden sich in einem n-dimensionalen, affinen Unterraum von $\mathbb{R}^{n+1}$.
Nun sei $f(n)$ die größtmögliche Anzahl von Punkten in $\mathbb{R}^n$, bei denen es nur zwei Abstände gibt. Die Vektoren $e_i + e_j \in \mathbb{R}^{n+1}$ $(1 \leq i < j \leq n+1)$ haben nun die Abstände 2 und $\sqrt{2}$ und befinden sich in einem n-dimensionalen, affinen Unterraum von $\mathbb{R}^{n+1}$.
Dies zeigt

$$f(n) \geq \binom{n+1}{2}.$$

Wir zeigen im folgenden, dass dies asymptotisch optimal ist.

Satz 1.7. Für alle $n \in \mathbb{N}$ ist

$$f(n) \leq \frac{(n+1)(n+4)}{2}.$$

Beweis. Bei $a_1, \ldots, a_m \in \mathbb{R}^n$ mögen nun die Abstände $r, s \in \mathbb{R}_{>0}$ auftreten. Betrachte das Polynom

$$F(x,y) = \left(\|x-y\|^2 - r^2\right)\left(\|x-y\|^2 - s^2\right).$$

Es gilt

$$F(a_i, a_j) = \begin{cases} 0, & i \neq j \\ (rs)^2, & i = j. \end{cases}$$

Für $i \in [m]$ betrachte

$$f_i(x) = F(x, a_i).$$

Nun sind $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$ linear unabhängig, denn: Seien $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$ so, dass $\alpha_1 f_1 + \cdots + \alpha_m f_m = 0$. Durch Einsetzen von a_j erhält man $\alpha_j (rs)^2 = 0$, also $\alpha_j = 0$.
Beachte, dass

$$f_i(x) = \left(\|x\|^2 - 2\langle a_i, x\rangle + \|a_i\|^2 - r^2\right)\left(\|x\|^2 - 2\langle a_i, x\rangle + \|a_i\|^2 - s^2\right).$$

Durch Ausmultiplizieren sieht man, dass jedes der $f_i(x)$ im von

$$\left(\|x\|^2\right)^2, x_j \|x\|^2 \ (1 \leq j \leq n), x_j x_k \ (1 \leq j \leq k \leq n), x_j \ (1 \leq j \leq n), 1$$

erzeugten $\mathbb{R}$-Untervektorraum von $\mathbb{R}[x_1, \ldots, x_n]$ ist. Somit gilt

$$f(n) \leq 1 + n + \binom{n+1}{2} + n + 1 = \frac{(n+1)(n+4)}{2}.$$

Damit wäre der Beweis vollbracht. □

Als nächstes wenden wir uns der 5. Frage zu. Hierfür brauchen wir ein kleines Hilfsresultat.

Fakt 1.8. Die Zahl $1/\pi \cdot \arccos(1/3)$ ist irrational.

Beweis. Für jeden Winkel α ist nach dem Satz von de Moivre

$$\cos(n\alpha) + \mathrm{i}\sin(n\alpha) = (\cos(\alpha) + \mathrm{i}\sin(\alpha))^n,$$

also erhält man durch Vergleich des Realteils

$$\begin{aligned}\cos(n\alpha) &= (\cos(\alpha))^n - \binom{n}{2}(\cos(\alpha))^{n-2}(\sin(\alpha))^2 + \binom{n}{4}(\cos(\alpha))^{n-4}(\sin(\alpha))^4 - \dots \\ &= (\cos(\alpha))^n - \binom{n}{2}(\cos(\alpha))^{n-2}\left(1-(\cos(\alpha))^2\right) + \binom{n}{4}(\cos(\alpha))^{n-4}\left(1-(\cos(\alpha))^2\right)^2 - \dots \\ &= a_0(\cos(\alpha))^n + a_1(\cos(\alpha))^{n-2} + a_2(\cos(\alpha))^{n-4} + \dots,\end{aligned}$$

wobei $a_0, a_1, \dots \in \mathbb{Z}$. Durch den binomischen Lehrsatz sieht man

$$a_0 = 1 + \binom{n}{2} + \binom{n}{4} + \dots = \frac{1}{2}\left((1+1)^n + (1-1)^n\right) = 2^{n-1}.$$

Setze nun $\alpha = \arccos(1/3)$. Angenommen $\alpha/(2\pi) = m/n$ mit $m, n \in \mathbb{N}$. Nun gilt

$$1 = \cos(2m\pi) = \cos(n\alpha) = \frac{a_0}{3^n} + \frac{a_1}{3^{n-2}} + \frac{a_2}{3^{n-4}} + \dots,$$

also

$$2^{n-1} = a_0 = 3^n\left(1 - \frac{a_1}{3^{n-2}} - \frac{a_2}{3^{n-4}} - \dots\right) = 9 \cdot (3^{n-2} - a_1 - 9a_2 - \dots).$$

Somit ist 2^{n-1} durch 9 teilbar. ↯ □

Satz 1.9 (Dehn)**.** Es seien $P \subseteq \mathbb{R}^3$ ein reguläres Tetraeder und $Q \subseteq \mathbb{R}^3$ ein volumengleicher Würfel. Es ist nicht möglich, P in (endlich viele) Polyeder zu zerschneiden und diese zu Q zusammenzusetzen.

Beweis (Skizze). Zwei Flächen des Tetraeders schließen den Winkel $\varphi = \arccos(1/3)$ ein.[7] Angenommen, man kann P, Q derart in Polyedern $P_1, \dots, P_n$ bzw. $Q_1, \dots, Q_n$ zerlegen, dass $P_i \cong Q_i$ für alle $i \in [n]$. Es sei M die Menge der Flächenwinkel dieser Polyeder und $V \subseteq \mathbb{R}$ der von $M \cup \{\pi\}$ erzeugte $\mathbb{Q}$-Untervektorraum von $\mathbb{R}$. Da $\varphi/\pi \notin \mathbb{Q}$, existiert eine Linearform $f\colon V \to \mathbb{Q}$ mit $f(\pi) = 0, f(\varphi) \neq 0$. Für jedes betrachtete Polyeder setze

$$D(R) = \sum_{e \text{ Kante von } R} |e|\, f(\alpha_e),$$

wobei $|e|$ die Länge von e und α_e der zugehörige Flächenwinkel ist.

[7] Dies lässt sich relativ elementar zeigen.

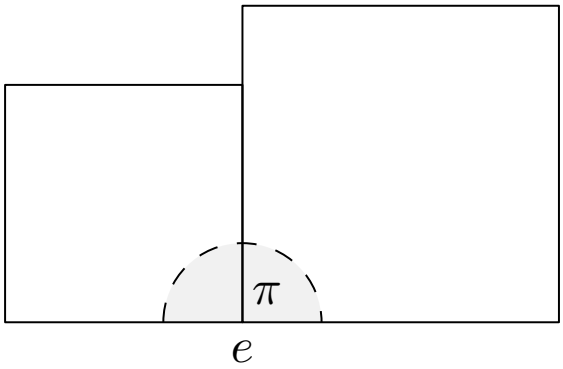


Abbildung 1: e ist eine eingeschlossene Kante des Polyeders, welches durch die Vereinigung der zwei Quader (gleicher Tiefe) einen Winkel von π erhält.

Man kann zeigen (oder sich erschließen), dass die *Dehn-Invariante* D bewegungsinvariant und additiv ist. Zerschneiden wir nämlich einen Polyeder P in Polyeder P_1, P_2, so ist für die in P „eingeschlossenen“ Kanten der Flächenwinkel dann π, womit diese dann in der Summe verschwinden würden. Nun ist

$$0 = D(Q) = \sum_{i=1}^{n} D(Q_i) = \sum_{i=1}^{n} D(P_i) = D(P).$$

Also gilt doch $f(\varphi) = 0$, Widerspruch. □

Dehn ist tatsächlich auch so in der Art vorgegangen, auch wenn er es nicht unbedingt so formuliert hat...
Wir wenden uns schließlich der 7. Frage zu:

Beobachtung 1.10. Jeder r-reguläre $\{C_3, C_4\}$-freie Graph hat mindestens r^2+1 Ecken.

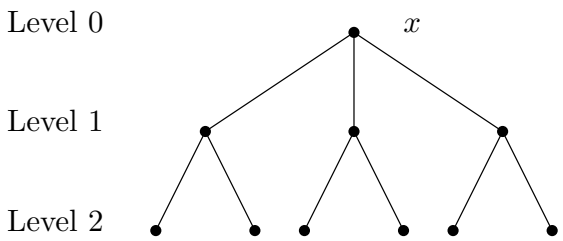


Abbildung 2: Bild zu Beobachtung 1.10 mit $r = 3$

Beweis. Sei $x \in V(G)$ beliebig. x hat r Nachbarn, diese haben je $r-1$ weitere Nachbarn. Insgesamt haben wir damit

$$1 + r + r(r-1) = r^2 + 1$$

Ecken. Diese sind verschieden, da G sonst einen C_3 oder C_4 enthielte. □

Für welche r gäbe es denn solche Graphen mit genau $r^2 + 1$ Knoten?

- $r = 1$: Bei $r^2 + 1 = 2$ kommt man schnell auf den Graph mit 2 Knoten und einer Kante.
- $r = 2$: Hier kämen nur Graphen, die die Vereinigung von unabhängigen Kreisen größerer Länge sind, mit $r^2 + 1 = 5$ Knoten in Frage. Also ist C_5 / ein „Pentagon“ das einzige solche Exemplar.
- $r = 3$: Hier gäbe es den Petersen Graph G, welcher definiert ist durch

$$V(G) \coloneqq [5]^{(2)}$$
$$E(G) \coloneqq \{A, B \in V(G) \mid A \cap B = \emptyset\}.$$

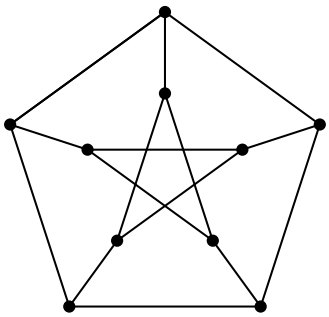


Abbildung 3: Der Petersen Graph

- $4 \leq r \leq 6$: Existiert nicht.[8]
- $r = 7$: Hier gibt es auch so ein Exemplar, ein recht großes, siehe Abbildung 4.

Es stellt sich heraus, dass (bis auf eine Ausnahme) wir damit alle solche r mit entsprechenden Graphen betrachtet haben:

Satz 1.11 (Hoffman, Singleton)**.** Wenn ein r-regulärer Graph auf $r^2 + 1$ Ecken ohne C_3, C_4 existiert, dann $r \in \{1, 2, 3, 7, 57\}$.

Beweis. Es sei G mit $V(G) = [r^2 + 1]$ so ein Graph.
Die Adjazenzmatrix $A = (a_{i,j})_{1 \leq i,j \leq r^2+1}$ von G ist durch

$$a_{i,j} = \begin{cases} 1, & ij \in E(G) \\ 0, & \text{sonst} \end{cases}$$

für $1 \leq i, j \leq r^2 + 1$ definiert. Der (i, j)-te Eintrag von A^2 zählt die gemeinsamen Nachbarn von i, j. Dies ist

[8] Wir werden auch gleich sehen wieso.

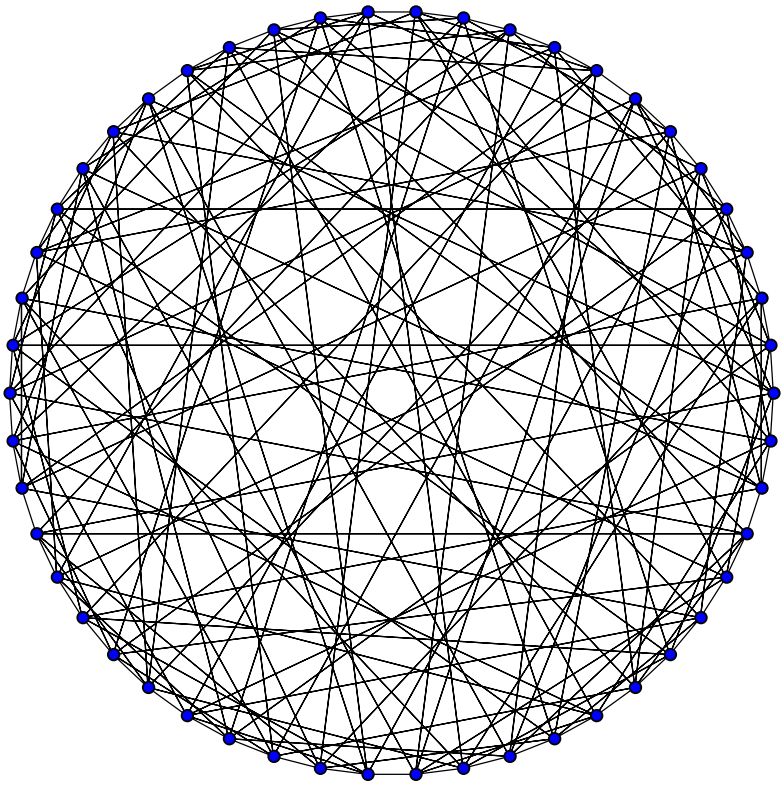


Abbildung 4: Der Hoffman-Singleton Graph (Quelle: Wikipedia)

- r wenn $i = j$ gilt,
- 0 wenn $ij \in E(G)$, und
- 1 wenn $i \neq j, ij \notin E(G)$.

Beachte, dass wenn wir den Beweis von Beobachtung 1.10 startend bei i anwenden für $i \neq j, ij \notin E(G)$, j dann auf „Level 2“ wäre, i und j also tatsächlich genau einen gemeinsamen Nachbarn haben. Somit ist

$$A^2 + A = (r-1) \cdot I + J, \tag{$*$}$$

wobei I die Einheitsmatrix und J die Matrix ist, bei der alle Elemente 1 sind.
Der Vektor $b = (1, \ldots, 1)^\top$ ist Eigenvektor von A zum Eigenwert r. Sei v ein nicht zu b proportionaler Eigenvektor von A mit Eigenwert λ. Dann gilt

$$Av = \lambda v, A^2 v = A\lambda v = \lambda^2 v,$$

also durch Einsetzen in $(*)$ $[\lambda^2 + \lambda - (r-1)] \cdot v = \langle b, v \rangle \cdot b$. Somit ist $\lambda^2 + \lambda - (r-1) = 0$, das heißt

$$\lambda_{1,2} = -\frac{1}{2} \pm \frac{1}{2}\sqrt{4r-3}. \tag{$**$}$$

Es seien m_1, m_2 die Vielfachheiten der Eigenwerte λ_1, λ_2. Dann ist

$$m_1 + m_2 + 1 = r^2 + 1,$$
$$\lambda_1 m_1 + \lambda_2 m_2 + r = \mathrm{Tr}(A) = 0.$$

Ersteres gilt, da A als reelle symmetrische Matrix nach dem Spektralsatz diagonalisierbar ist, insbesondere die geometrische Vielfachheit mit der algebraischen übereinstimmt. Letzteres gilt, da die Spur einer (reellen oder komplexen) Matrix gerade die Summe ihrer Eigenwerte ist. Setzen wir nun $(**)$ in die zweite Gleichung ein und nutzen dann die erste Gleichung aus, erhalten wir

$$\underbrace{-(m_1 + m_2)}_{=-r^2} + \sqrt{4r-3} \cdot (m_1 - m_2) = -2r.$$

Also gilt

$$\sqrt{4r-3} \cdot (m_1 - m_2) = r^2 - 2r,$$

wobei $m_1 - m_2 \in \mathbb{Z}$.
Wenn $r \neq 2$, folgt aus $\sqrt{4r-3} = (r^2 - 2r)/(m_1 - m_2)$, dass $s = \sqrt{4r-3}$ ganz ist.[9] Außerdem gilt $s \mid (r^2 - 2r)$. Da $r = (s^2+3)/4$ folgt $s \mid ((s^2+3)^2 - 8(s^2+3))$. Somit folgt $s \mid (9 - 24)$, also $s \mid 15$, das heißt $s \in \{1, 3, 5, 15\}$ und $r \in \{1, 3, 7, 57\}$. □

Tatsächlich ist es unbekannt, ob es so einen Graphen auch für $r = 57$ gibt.

2 Eingeschränkte Schnitte

Als nächstes wollen wir uns konkretere Klassen an Problemen anschauen, beginnend mit Resultaten über gewisse Mengenfamilien auf einer endlichen Grundmenge.

Satz 2.1 (Erdős, Ko, Rado)**.** Es sei $n \geq 2k$ und $\mathcal{A} \subseteq [n]^{(k)} = \{A \subseteq [n] \mid |A| = k\}$. Wenn sich je zwei Mengen aus $\mathcal{A}$ schneiden, dann gilt

$$|\mathcal{A}| \leq \binom{n-1}{k-1}.$$

Wenn $n < 2k$ gilt, dann hat $[n]^{(k)}$ diese Eigenschaft. Für $\mathcal{A} = \left\{A \in [n]^{(k)} \;\middle|\; 1 \in A\right\}$ gilt Gleichheit, also ist diese Ungleichung scharf.

Beweis (von Katona). Betrachte alle $n!$ Möglichkeiten, die Zahlen $1, \ldots, n$ an die Ecken eines regulären n-Ecks zu schreiben. Wir zählen nun die Anzahl an Paaren zwischen solchen Anordnungen und Mengen von $\mathcal{A}$, wo die Menge als Intervall in der Anordnung vorkommt.

[9] Aus der Analysis weiß man, dass die Wurzel von $n \in \mathbb{N}$ genau dann rational ist, wenn n ein Quadrat ist.

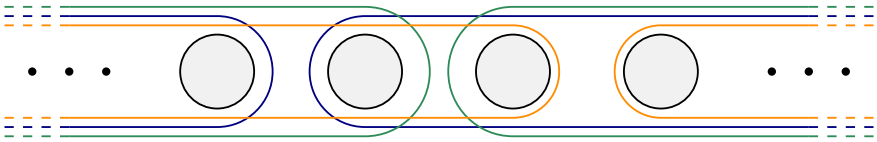


Abbildung 5: Intervall I der Länge k (hier $k = 4$)

Bei jeder der Anordnungen, sind höchstens k Intervalle in $\mathcal{A}$ (siehe Abbildung 5): Angenommen $A \in \mathcal{A}$ ist als Intervall I der Länge k in einer Anordnung zu finden. Da jede andere Menge von $\mathcal{A}$, welches als Intervall in der Anordnung auftritt, zudem I schneiden muss, kommen nur $2 \cdot (k-1)$ weitere Intervalle in Frage für diese Mengen. Da zudem paarweise je zwei Intervalle, die I schneiden, disjunkt sind (angedeutet in Abbildung 5 durch gleiche Farbe), kann pro Paar an disjunkten Intervallen nur eins in $\mathcal{A}$ sein. Damit kann es zusammen mit A insgesamt höchstens $1 + (k-1) = k$ Mengen in $\mathcal{A}$ geben, die in der Anordnung als Intervalle auftreten.
Andererseits ist jede der Mengen in $\mathcal{A}$ in $n \cdot k!(n-k)!$ Anordnungen ein Intervall: Es gibt n Möglichkeiten, ab wo das Intervall für die Menge startet, $k!$ Möglichkeiten, die Menge als Intervall zu ordnen, und $(n-k)!$ Möglichkeiten, wie man die restlichen Zahlen den Ecken zuordnet. Also gilt

$$n \cdot k!(n-k)! \, |\mathcal{A}| \leq n! \cdot k,$$

das heißt

$$|\mathcal{A}| \leq \frac{n!}{k!(n-k)!} \cdot \frac{k}{n} = \frac{k}{n}\binom{n}{k} = \binom{n-1}{k-1}.$$

Damit wäre der Beweis vollbracht. □

Satz 2.2 (alle)**.** Sei $\mathcal{A} \subseteq \mathcal{P}([n])$. Wenn sich je zwei Mengen aus $\mathcal{A}$ schneiden, dann

$$|\mathcal{A}| \leq 2^{n-1}.$$

Gleichheit gilt zum Beispiel, wenn $\mathcal{A} = \{A \subseteq [n] \mid 1 \in A\}$.

Beweis. Teile $\mathcal{P}([n])$ in 2^{n-1} Paare der Form $\{A, [n] \setminus A\}$ auf. Aus jedem Paar enthält $\mathcal{A}$ höchstens eine Menge. □

Satz 2.3 (de Bruijn, Erdős)**.** Sind $C_1, \ldots, C_m \subseteq [n]$ verschieden mit $|C_i \cap C_j| = 1$ für alle $i \neq j$, dann ist $m \leq n$.

Es gibt viele Gleichheitsfälle, zum Beispiel $C_i = \{i, n\}$ für $i \leq n-1$ und $C_n = [n-1]$. Weitere Beispiele sind gegeben durch die projektive Ebenen.

Beweis („Urbeweis“). Der Fall $n = 1$ ist trivial, also sei o.B.d.A. $n \geq 2$. Wenn $C_i = [n]$ für ein $i \in [m]$, sind die anderen C_j einelementig und es gilt $m \leq 2 \leq n$. ✓
Ab jetzt gelte also $C_i \neq [n]$ für alle $i \in [m]$. Für $x \in [n]$ setze

$$d(x) = |\{i \in [m] \mid x \in C_i\}|.$$

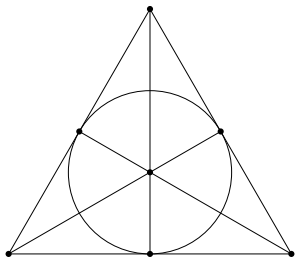


Abbildung 6: Fano-Ebene als Beispiel für eine projektive Ebene

Ist $d(x) = m$ für ein $x \in [n]$, so sind $C_1 \setminus \{x\}, \ldots, C_m \setminus \{x\}$ paarweise verschiedene, paarweise disjunkte Teilmengen von $[n] \setminus \{x\}$ und somit $m \leq n$. Also sei ab sofort $d(x) < m$ für alle $x \in [n]$. Doppeltes Abzählen zeigt

$$\sum_{x=1}^{n} d(x) = \sum_{i=1}^{m} |C_i| \,.$$

Beachte, dass für festes $x \in [n]$ genau $m - d(x)$ der C_i's x nicht enthalten, und für festes $i \in [m]$ genau $n - |C_i|$ der Elemente von $[n]$ nicht in C_i enthalten sind. Somit ist

$$\sum_{x \in [n], i \in [m] \colon x \notin C_i} \frac{d(x)}{m - d(x)} = \sum_{i \in [m], x \in [n] \colon x \notin C_i} \frac{|C_i|}{n - |C_i|}.$$

Es gibt also $x \in [n]$ und $i \in [m]$ mit $x \notin C_i$ und

$$\frac{d(x)}{m - d(x)} \geq \frac{|C_i|}{n - |C_i|} \implies \frac{m - d(x)}{d(x)} \leq \frac{n - |C_i|}{|C_i|}.$$

Also gilt

$$\frac{m}{d(x)} \leq \frac{n}{|C_i|} \implies \frac{m}{n} \leq \frac{d(x)}{|C_i|}.$$

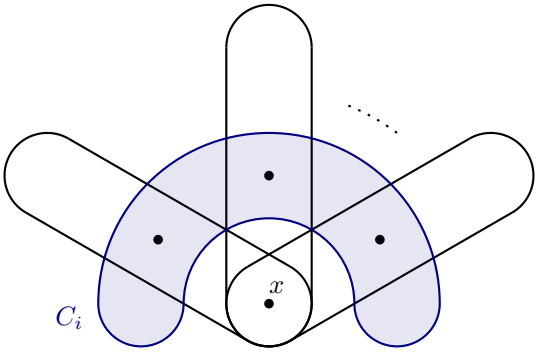


Abbildung 7: Die C_j's, die x enthalten, können sich sonst nicht schneiden. Insbesondere schneidet C_i diese dann in verschiedenen Elementen.

Nun ist $d(x) \leq |C_i|$ (siehe Abbildung 7) und folglich $m/n \leq 1$. □

Satz 2.4 (Bose)**.** Es seien $C_1, \dots, C_m \subseteq [n]$ paarweise verschieden und $1 \leq t < n$. Wenn $|C_i \cap C_j| = t$ für alle $i < j$ gilt, dann ist $m \leq n$.

Der Satz ist auch als *Fisher's Inequality* bekannt. Ein kombinatorischer Beweis wurde von Douglas R. Woodall in *A Note on Fisher's Inequality (1997)* erbracht.

Beweis. Definiere $A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq m} \in \mathbb{R}^{n \times m}$ durch

$$a_{i,j} = \begin{cases} 1, & i \in C_j \\ 0, & \text{sonst.} \end{cases}$$

Fasst man also C_j als ihre Inzidenzvektoren auf, ist also

$$A = \underbrace{\begin{pmatrix} C_1 & C_2 & \dots & C_m \end{pmatrix}}_{m} \Big\} n$$

Annahme. $m > n$.

Wähle Vektor $x \in \mathbb{R}^m$ mit $x \neq 0$ und $Ax = 0$. Nun ist $x^\top A^\top A x = 0$. Der (i,j)-te Eintrag von $A^\top A$ ist $|C_i \cap C_j| = t$. Also gilt $A^\top A = t \cdot J + D$, wobei

- J die $(m \times m)$-Matrix mit allen Einträgen 1 ist, und
- D die Diagonalmatrix mit Einträgen $|C_1| - t, \dots, |C_m| - t$. Diese sind nicht-negativ und, bis auf höchstens eine Ausnahme, positiv.

Schreibe $x = (x_1, \dots, x_m)^\top$. Nun ist

$$x^\top J x = \left(\sum_{i=1}^{m} x_i \right)^2, \qquad x^\top D x = \sum_{i=1}^{m} (|C_i| - t)\, x_i^2$$

und folglich

$$t \cdot \left(\sum_{i=1}^{m} x_i \right)^2 + \sum_{i=1}^{m} \underbrace{(|C_i| - t)}_{\geq 0 \text{ und } > 0 \text{ bis auf höchstens eine Ausnahme}} x_i^2 = 0.$$

Damit die linke Seite Null ist, muss insbesondere die Summe der x_i's Null sein. Da aber $x \neq 0$ gilt, müssen mindestens zwei Komponenten nicht Null sein, wobei das Quadrat von mindestens einen davon im hinteren Term einen positiven Vorfaktor hat.
Also gilt doch $x_1 = \dots = x_m = 0$. ↯ □

Definition 2.5. Es seien $L \subseteq \mathbb{N}_0$ und $\mathcal{A} \subseteq \mathcal{P}(X)$. Wenn $|A \cap B| \in L$ für alle $A \neq B$ aus $\mathcal{A}$ heißt $\mathcal{A}$ *L-schneidend.*

Beachte wie dies die Situation von den bisherigen Sätzen wie dem Satz von Erdős, Ko, Rado verallgemeinert. Dieser behandelt beispielsweise den Fall $L = \mathbb{N}$.

Satz 2.6 (Frankl & Wilson)**.** Sind $L \subseteq \mathbb{N}_0$ eine s-elementige Menge und $\mathcal{A} \subseteq \mathcal{P}([n])$ ein L-schneidendes Mengensystem, so gilt

$$|\mathcal{A}| \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{0}.$$

Gleichheit gilt zum Beispiel wenn $L = \{0, 1, \ldots, s-1\}$ und $\mathcal{A} = \{A \subseteq [n] \mid |A| \leq s\}$.

Beweis. Es sei V der von allen $\prod_{i \in A} x_i$ mit $A \subseteq [n], |A| \leq s$ erzeugte $\mathbb{R}$-Untervektorraum von $\mathbb{R}[x_1, \ldots, x_n]$. Offenbar gilt

$$\dim(V) = \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{0}.$$

Zu jedem Polynom $P \in \mathbb{R}[x_1, \ldots, x_n]$ mit $\operatorname{grad}(P) \leq s$ gibt es ein Polynom $\tilde{P} \in V$ mit

$$P(x_1, \ldots, x_n) = \tilde{P}(x_1, \ldots, x_n)$$

für alle $(x_1, \ldots, x_n) \in \{0,1\}^n$. Man findet $\tilde{P}$, indem man in P jedes Monom $x_{i_1}^{a_1} \cdot \ldots \cdot x_{i_r}^{a_r}$ mit $i_1 < \cdots < i_r$, $a_1, \ldots, a_r > 0$ durch $x_{i_1} \cdot \ldots \cdot x_{i_r}$ ersetzt.
Schreibe nun $\mathcal{A} = \{A_1, \ldots, A_m\}$ mit $|A_1| \leq |A_2| \leq \cdots \leq |A_m|$. Für $i \in [m]$, setze

$$P_i(x) = \prod_{\lambda \in L, \lambda < |A_i|} (\langle x, A_i \rangle - \lambda),$$

wobei wir wieder A_i mit ihrem Inzidenzvektor identifizieren. Für alle $i, j \in [m]$ ist

$$\tilde{P}_i(A_j) = P_i(A_j) = \prod_{\lambda \in L, \lambda < |A_i|} (|A_i \cap A_j| - \lambda).$$

Falls $j < i$, ist $|A_j \cap A_i| < |A_i|$ (da $|A_j| \leq |A_i|$ und $A_i \neq A_j$) und somit $\tilde{P}_i(A_j) = 0$. Außerdem gilt

$$\tilde{P}_i(A_i) = \prod_{\lambda \in L, \lambda < |A_i|} (|A_i| - \lambda) \neq 0.$$

Annahme. $\tilde{P}_1, \ldots, \tilde{P}_m$ sind $\mathbb{R}$-linear abhängig.

Wähle $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$, nicht alle Null, mit

$$\sum_{i=1}^{m} \alpha_i \cdot \tilde{P}_i = 0.$$

Sei $j \in [m]$ minimal mit $\alpha_j \neq 0$. Dann ist

$$\sum_{i<j} \underbrace{\alpha_i}_{=0 \text{ nach Wahl von } j} \tilde{P}_i(A_j) + \underbrace{\alpha_j \tilde{P}_j(A_j)}_{\neq 0} + \sum_{i>j} \alpha_i \underbrace{\tilde{P}_i(A_j)}_{=0} = 0. \; \lightning$$

Somit sind $\tilde{P}_1, \ldots, \tilde{P}_m$ linear unabhängig, also

$$m \leq \dim(V) = \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{0}. \qquad \square$$

Als nächstes werden wir die Abschätzung zu $|\mathcal{A}| \leq \binom{n}{s}$ verbessern, falls $\mathcal{A} \subseteq [n]^{(k)}$ für ein $k \in [s, n]$ gilt. Dies erfordert jedoch umfangreiche Vorbereitungen.

Definition 2.7. Es seien $\mathcal{A} \subseteq \mathcal{P}([n])$ mit $s \leq n$. Man nennt $\mathcal{A}$ *s^*-abhängig*, wenn es reelle Zahlen λ_A ($A \in \mathcal{A}$) mit

$$\sum_{A \in \mathcal{A} \text{ und } X \subseteq A} \lambda_A = 0 \qquad (*)$$

für alle $X \subseteq [n]$ mit $|X| \leq s$ gibt, die nicht alle Null sind.

Intuitiv kann man sich das so erklären: Man betrachte die Matrix M mit $\binom{n}{s} + \cdots + \binom{n}{0}$ Zeilen, indiziert durch $\{X \subseteq [n] \mid |X| \leq s\}$, und $|\mathcal{A}|$ Spalten, indiziert durch $\mathcal{A}$, und setzt

$$M_{X,A} = \begin{cases} 1, & X \subseteq A \\ 0, & \text{sonst.} \end{cases}$$

Dann ist $\mathcal{A}$ genau dann s^*-abhängig, wenn die Spalten von M linear abhängig sind.

Bemerkung 2.8. Für $|\mathcal{A}| > \binom{n}{s} + \cdots + \binom{n}{0}$ hat das lineare Gleichungssystem $(*)$ mehr Variablen als Gleichungen und mithin eine nicht-triviale Lösung, das heißt $\mathcal{A}$ ist s^*-abhängig.

Satz 2.9. Es seien $A_1, \ldots, A_m \subseteq [n]$ paarweise verschieden und $P_1, \ldots, P_m \subseteq \mathbb{R}[x]$ Polynome vom Grad höchstens s. Es gelte

$$P_i(|A_i \cap A_j|) = 0$$

für $j < i$ und

$$P_i(|A_i|) \neq 0$$

für alle $i \in [m]$. Dann ist $\mathcal{A} = \{A_1, \ldots, A_m\}$ s^*-unabhängig.

Beweis. Andernfalls gäbe es $\lambda_1, \ldots, \lambda_m \in \mathbb{R}$ nicht alle Null, mit

$$\sum_{i \in [m] \colon X \subseteq A_i} \lambda_i = 0$$

für alle $X \subseteq [n]$ mit $|X| \leq s$. Für alle r und j mit $0 \leq r \leq s$ und $j \in [m]$ ist

$$\sum_{X \in A_j^{(r)}} \sum_{i \in [m] \colon X \subseteq A_i} \lambda_i = 0.$$

Der Summand λ_i kommt hier $\binom{|A_i \cap A_j|}{r}$ mal vor. Also gilt

$$\sum_{i=1}^{m} \lambda_i \binom{|A_i \cap A_j|}{r} = 0.$$

Nun ist $\binom{x}{0}, \ldots, \binom{x}{s}$[10] eine Basis des $\mathbb{R}$-Vektorraums $\{P(x) \in \mathbb{R}[x] \mid \operatorname{grad}(P) \leq s\}$. Das heißt man kann jedes $P(x) \in \mathbb{R}[x]$ mit $\operatorname{grad}(P) \leq s$ als

$$P(x) = \beta_s \binom{x}{s} + \cdots + \beta_0 \binom{x}{0}$$

für gewisse $\beta_s, \ldots, \beta_0 \in \mathbb{R}$ schreiben. Nun ist

$$\begin{aligned}
\sum_{i=1}^{m} P(|A_i \cap A_j|)\lambda_i &= \sum_{i=1}^{m} \sum_{r=0}^{s} \beta_r \binom{|A_i \cap A_j|}{r} \lambda_i \\
&= \sum_{r=0}^{s} \beta_r \underbrace{\left(\sum_{i=1}^{m} \binom{|A_i \cap A_j|}{r} \lambda_i \right)}_{=0} \\
&= 0.
\end{aligned}$$

Für alle $P \in \mathbb{R}[x]$ mit $\operatorname{grad}(P) \leq s$ und alle $j \in [m]$ ist also

$$\sum_{i=1}^{m} P(|A_i \cap A_j|)\lambda_i = 0.$$

Wählt man aber speziell $j \in [m]$ maximal mit $\lambda_j \neq 0$ und $P = P_j$, so erhält man

$$\sum_{i<j} \underbrace{P_j(|A_i \cap A_j|)}_{=0} \lambda_i + \underbrace{P_j(|A_j|)\lambda_j}_{\neq 0} + \sum_{i>j} P_j(|A_i \cap A_j|) \underbrace{\lambda_i}_{=0} = 0,$$

Widerspruch. □

Folgerung 2.10 (Frankl & Wilson)**.** Es sei $L \subseteq \mathbb{N}_0, |L| = s$. Jedes L-schneidendes Mengensystem $\mathcal{A} \subseteq \mathcal{P}([n])$ ist s^*-unabhängig. Insbesondere gilt

$$|\mathcal{A}| \leq \binom{n}{s} + \cdots + \binom{n}{0}.$$

Beweis. Schreibe $\mathcal{A} = \{A_1, \ldots, A_m\}$ mit $|A_1| \leq |A_2| \leq \cdots \leq |A_m|$. Setze

$$P_i(x) = \prod_{\lambda \in L, \lambda < |A_i|} (x - \lambda).$$

Offenbar ist $\operatorname{grad}(P_i) \leq |L| = s$. Für $j < i$ ist $|A_j \cap A_i| \in L$ und $|A_j \cap A_i| < |A_i|$, also $P_i(|A_i \cap A_j|) = 0$. Außerdem gilt

$$P_i(|A_i|) = \prod_{\lambda \in L, \lambda < |A_i|} (|A_i| - \lambda) \neq 0.$$

Nach Satz 2.9 ist $\mathcal{A}$ somit s^*-unabhängig. Benutze dann Bemerkung 2.8. □

[10] Im Sinne der Definition des Binomialkoeffizienten aus der Analysis.

Definition 2.11. Es sei $\mathcal{A} \subseteq \mathcal{P}([n])$ ein Mengensystem und $s \leq n$. $\mathcal{A}$ heißt *s-abhängig*, wenn es reelle Zahlen μ_A $(A \in \mathcal{A})$ mit

$$\sum_{A \in \mathcal{A} \text{ und } X \subseteq A} \mu_A = 0$$

für alle $X \in [n]^{(s)}$ gibt, die nicht alle Null sind.

Wie in Bemerkung 2.8 zeigt man: Wenn $|\mathcal{A}| > \binom{n}{s}$ gilt, dann ist $\mathcal{A}$ s-abhängig. Klar ist zudem, dass wenn $\mathcal{A}$ s^*-abhängig ist, $\mathcal{A}$ insbesondere s-abhängig ist. Folgendes Lemma liefert, dass auch in besonderen Fällen die Rückrichtung gilt:

Lemma 2.12. Es seien $s \leq k \leq n$ und $\mathcal{A} \subseteq [n]^{(k)}$. Wenn $\mathcal{A}$ s^*-unabhängig ist, dann ist $\mathcal{A}$ auch s-unabhängig.

Beweis. Seien μ_A $(A \in \mathcal{A})$ reelle Zahlen mit

$$\sum_{A \in \mathcal{A} \text{ und } X \subseteq A} \mu_A = 0$$

für alle $X \in [n]^{(s)}$. Für alle $Y \subseteq [n]$ mit $|Y| \leq s$ gilt dann

$$\sum_{X \supseteq Y, |X| = s} \sum_{A \in \mathcal{A} \text{ und } X \subseteq A} \mu_A = 0.$$

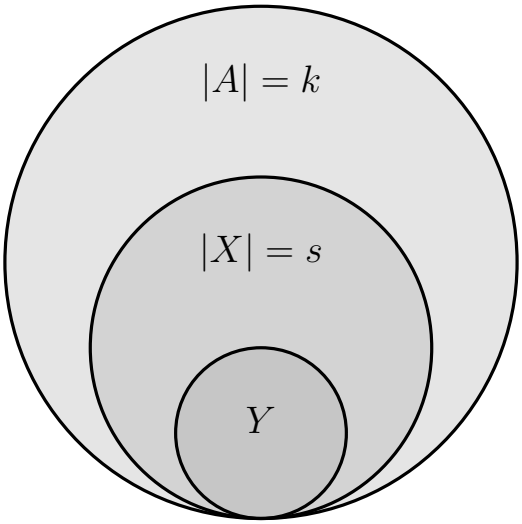


Abbildung 8: Situation im Beweis von Lemma 2.12

Für $Y \not\subseteq A$ kommt μ_A links nicht vor. Für $Y \subseteq A$ kommt μ_A genau $\binom{k-|Y|}{s-|Y|}$ mal vor. Also ist

$$\binom{k-|Y|}{s-|Y|} \sum_{A \in \mathcal{A} \text{ und } Y \subseteq A} \mu_A = 0.$$

Da $k - |Y| \geq s - |Y| \geq 0$, ist $\binom{k-|Y|}{s-|Y|} \neq 0$. Dies zeigt

$$\sum_{A \in \mathcal{A} \text{ und } Y \subseteq A} \mu_A = 0$$

für alle $Y \subseteq [n]$ mit $|Y| \leq s$. Da $\mathcal{A}$ s^*-unabhängig ist, folgt $\mu_A = 0$ für alle $A \in \mathcal{A}$. □

Der nächste Satz ist ein sehr wichtiges Resultat.

Satz 2.13 (Ray-Chaudhuri-Wilson)**.** Es seien $L \subseteq \mathbb{N}_0$, $|L| = s$ und $k \geq s$. Für jedes L-schneidende Mengensystem $\mathcal{A} \subseteq [n]^{(k)}$ gilt $|\mathcal{A}| \leq \binom{n}{s}$.

Beweis. Nach dem Satz von Frankl und Wilson ist $\mathcal{A}$ s^*-unabhängig. Nach Lemma 2.12 ist $\mathcal{A}$ auch s-unabhängig. Folglich ist $|\mathcal{A}| \leq \binom{n}{s}$. □

Beispiel 2.14. Es ist $k \geq s \geq 1$ und $n \geq 4k$. Dann gibt es ein $\{0, 1, \ldots, s-1\}$-schneidendes Mengensystem $\mathcal{A} \subseteq [n]^{(k)}$ mit

$$|\mathcal{A}| > \left(\frac{n}{2k}\right)^s.$$

Die Schranke von Satz 2.13 ist also asymptotisch für feste $k \geq s \geq 1$ optimal.

Beweis. Nach dem Bertrandschen Postulat[11] existiert eine Primzahl p mit

$$\frac{n}{2k} < p \leq \frac{n}{k}.$$

Für jedes Polynom $P \in \mathbb{F}_p[x]$ betrachten wir $A(P) = \{(\xi, P(\xi)) \colon \xi \in [k]\}$.[12]
Dies ist eine k-elementige Teilmenge von $[k] \times \mathbb{F}_p$, wobei $|[k] \times \mathbb{F}_p| = p \cdot k \leq n$.
Für verschiedene $P, Q \in \mathbb{F}_p[x]$ ist

$$|A(P) \cap A(Q)| = |\{\xi \in [k] \mid (P-Q)(\xi) = 0\}| \leq \sum_{\xi \in [k] \colon (P-Q)(\xi)=0} \mu_\xi \leq \operatorname{grad}(P-Q),$$

wobei μ_ξ die Vielfachheit einer Nullstelle ξ von $P - Q$ ist.
Somit ist $\mathcal{A} = \{A(P) \colon P \in \mathbb{F}_p[x], \operatorname{grad}(P) < s\}$ ein $\{0, 1, \ldots, s-1\}$-schneidendes Mengensystem. Außerdem gilt

$$|\mathcal{A}| = p^s > \left(\frac{n}{2k}\right)^s. \qquad \square$$

Lemma 2.15. Seien $k, s \in \mathbb{N}_0, n \geq k + s$ und F ein Körper. Ferner sei $\alpha \colon \mathcal{P}([n]) \to F$ eine Funktion mit

(a) $\alpha(U) = 0$ für $|U| \geq s$,

(b) $\sum_{T \subseteq X} \alpha(T) = 0$ falls $k < |X| \leq k + s$.

Dann gilt $\alpha = 0$.

[11] Ein Beweis ist gegeben in *Das BUCH der Beweise* von Martin Aigner und Günter M. Ziegler.
[12] Mit $P(\xi)$ ist dabei natürlich die Auswertung von P in der Restklasse von ξ gemeint.

Beweis. Betrachte ein Gegenbeispiel mit minimalem k. Seien $X \subseteq Z \subseteq [n]$ Mengen mit $|X| = k, |Z| = k + s$.

Behauptung. Für jede Menge $T \subseteq Z$ ist

$$\sum_{X \cup T \subseteq Y \subseteq Z} (-1)^{|Y \setminus X|} = \begin{cases} (-1)^s, & X \cup T = Z \\ 0, & \text{sonst.} \end{cases} \tag{$*$}$$

Beweis der Behauptung. Setze $S = Z \setminus (X \cup T)$. Jede Menge Y, die auf der linken Seite vorkommt, kann man eindeutig in der Form $(X \cup T) \uplus S'$ mit $S' \subseteq S$ schreiben. Daher ist die linke Seite

$$\begin{aligned} \sum_{X \cup T \subseteq Y \subseteq Z} (-1)^{|Y \setminus X|} &= \sum_{S' \subseteq S} (-1)^{|((X \cup T) \uplus S') \setminus X|} \\ &= (-1)^{|(X \cup T) \setminus X|} \sum_{S' \subseteq S} (-1)^{|S'|} \\ &= (-1)^{|T \setminus X|} \left(\binom{|S|}{0} - \binom{|S|}{1} + \binom{|S|}{2} \dots \right) \\ &= (-1)^{|T \setminus X|} \cdot (1-1)^{|S|} \\ &= \begin{cases} (-1)^s, & X \cup T = Z \\ 0, & \text{sonst.} \end{cases} \end{aligned}$$

□

Nun ergibt das

$$\begin{aligned} \sum_{T \subseteq X} \alpha(T) &\overset{\text{(b)}}{=} \sum_{X \subseteq Y \subseteq Z} (-1)^{|Y \setminus X|} \left(\sum_{T \subseteq Y} \alpha(T) \right) \\ &= \sum_{T \subseteq Z} \left(\sum_{X \cup T \subseteq Y \subseteq Z} (-1)^{|Y \setminus X|} \right) \alpha(T) \\ &\overset{(*)}{=} (-1)^s \sum_{T \subseteq Z, X \cup T = Z} \alpha(T) \\ &\overset{\text{(a)}}{=} 0, \end{aligned}$$

denn aus $X \cup T$ folgt $|T| \geq |Z \setminus X| = s$. Also gilt (b) auch für alle $X \subseteq [n]$ mit $|X| = k$.

Fall 1: $k > 0$. Dann ist $k - 1, s + 1, \alpha$ ein kleineres Gegenbeispiel, was der Minimalität von k widerspricht.

Fall 2: $k = 0$. Dann gilt $\alpha(\emptyset) = 0$. Wähle X mit $\alpha(X) \neq 0$ und $|X|$ minimal. Nach (a) ist $0 < |X| < s$. Nach (b) ist $\sum_{T \subseteq X} \alpha(T) = 0$. Für $T \subset X$ ist zudem $\alpha(T) = 0$ (nach der Minimalität von $|X|$). Also ist $\alpha(X) = 0$. ↯

Damit wäre der Beweis vollbracht. □

Lemma 2.16. Es seien p eine Primzahl und $k, s, n \in \mathbb{N}_0$ mit $p > k, s \geq 0$ und $n \geq k+s$. Setze $\Omega = \{0,1\}^n$. Definiere $f\colon \Omega \to \mathbb{F}_p$ durch $f(x_1, \ldots, x_n) = \sum_{i=1}^{k} x_i - k$. Für $B \subseteq [n]$ setze $x_B = \prod_{i \in B} x_i$. Dann ist

$$\{x_B \cdot f \mid B \subseteq [n] \text{ und } |B| < s\}$$

linear unabhängig in $\mathbb{F}_p^\Omega$.

Beweis. Andernfalls gäbe es ein von Null verschiedenes $\alpha\colon \mathcal{P}([n]) \to \mathbb{F}_p$ mit

(a) $\alpha(B) = 0$ falls $|B| \geq s$, (b) $\sum_{B \subseteq [n]} \alpha(B) \cdot x_B \cdot f = 0$ (in $\mathbb{F}_p^\Omega$).

Sei $K \subseteq [n], k < |K| \leq k+s$. Setze das zu K zugehörige Element in (b) ein. Da $f(K) = |K| - k \neq 0$, zeigt dies

$$\sum_{B \subseteq [n]} \alpha(B) \cdot x_B(K) = 0.$$

Da aber zudem

$$x_B(K) = \begin{cases} 1, & B \subseteq K \\ 0, & \text{sonst} \end{cases}$$

gilt, erhalten wir

$$\sum_{B \subseteq K} \alpha(B) = 0.$$

Nach Lemma 2.15 ist also doch $\alpha = 0$. ↯ □

Als nächstes beweisen wir einen zentralen Satz, welcher – bis auf ein paar Ausnahmen – alles zuvorige verallgemeinert.

Satz 2.17 (Alon-Babai-Suzuki)**.** Es seien p eine Primzahl, $L \subset \mathbb{F}_p, |L| = s$ und k eine natürliche Zahl mit $k \notin L$.[13] Ferner seien $n \geq k+s$ und $\mathcal{A} \subseteq \mathcal{P}([n])$ ein Mengensystem mit:

- Für alle $A \in \mathcal{A}$ ist $|A| \equiv k \pmod{p}$.
- Für alle verschiedenen $A, B \in \mathcal{A}$ ist $|A \cap B| \in L$.

Dann gilt $|\mathcal{A}| \leq \binom{n}{s}$.

Beweis. Seien $\Omega = \{0,1\}^n, f\colon \Omega \to \mathbb{F}_p$ und $x_B = \prod_{i \in B} x_i$ wie in Lemma 2.16. Der von

$$\{x_B \mid B \subseteq [n] \text{ und } |B| \leq s\}$$

erzeugte $\mathbb{F}_p$-Untervektorraum von $\mathbb{F}_p^\Omega$ heiße V. Schreibe $\mathcal{A} = \{A_1, \ldots, A_m\}$ und wähle $P_1, \ldots, P_m \in V$ so, dass für alle $x \in \Omega$

$$P_i(x) = \prod_{\lambda \in L} (\langle x, A_i \rangle - \lambda)$$

gilt, indem du wie im Beweis von Satz 2.6 Exponenten höherer Ordnung ignorierst.

[13] Natürlich in dem Sinne, dass k's Restklasse nicht in L ist.

Behauptung. $\{P_i \mid i \in [m]\} \cup \{x_B \cdot f \mid B \subseteq [n] \text{ und } |B| < s\}$ ist linear unabhängig.

Beweis der Behauptung. Seien $\alpha_1, \ldots, \alpha_m, \beta(B)$ $(B \subseteq [n], |B| < s)$ aus $\mathbb{F}_p$ mit

$$\sum_{i=1}^{m} \alpha_i \cdot P_i + \sum_{B \subseteq [n], |B| < s} \beta(B) \cdot x_B \cdot f = 0.$$

Sei $j \in [m]$. Da $|A_j| \equiv k \pmod{p}$ ist $f(A_j) = 0$ und somit $\alpha_j \cdot P_j(|A_j|) = 0$, das heißt $\alpha_j = 0$. Nach Lemma 2.16 ist auch $\beta(B) = 0$ für alle $B \subseteq [n]$ mit $|B| < s$. □

Somit haben wir

$$m + \binom{n}{s-1} + \cdots + \binom{n}{0} \leq \dim(V) = \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{0},$$

das heißt $m \leq \binom{n}{s}$. □

Beachte, dass die Bedingung $k \notin L$ notwendig ist, wie Satz 1.3 zeigt. Neben Satz 1.1, erhalten wir den folgenden Satz als Konsequenz:

Satz 2.18. Es seien p eine Primzahl und

$$\mathcal{A} \subseteq [4p-1]^{(2p-1)}$$

ein Mengensystem mit $|A \cap B| \neq p-1$ für alle $A, B \in \mathcal{A}$. Dann ist

$$|\mathcal{A}| \leq \binom{4p-1}{p-1}.$$

Mit Hilfe der Stirling'schen Formel kann man $|\mathcal{A}| < 1.8^{4p-1}$ abschätzen. Meistens genügt, dass es $\varepsilon > 0$ mit $|\mathcal{A}| < (2-\varepsilon)^{4p-1}$ gibt.

Beweis. Wende Satz 2.17 mit $L = \{0, 1, \ldots, p-2\}$ und $k = p-1$ an. Für alle verschiedenen $A, B \in \mathcal{A}$ ist $|A \cap B| \in L + p\mathbb{Z}$. □

Ohne Beweis erwähnen wir eine „stärkere“ Version des Satzes 2.18:

Satz 2.19 (Frankl & Rödl)**.** Für alle $0 < \alpha < \beta < 1$ existiert ein $\varepsilon \in (0,1)$ derart, dass jedes Mengensystem $\mathcal{A} \subseteq [n]^{\lfloor \beta n \rfloor}$ mit $|A \cap B| \neq \lfloor \alpha n \rfloor$ für alle $A, B \in \mathcal{A}$ höchstens die Größe

$$|\mathcal{A}| \leq (1-\varepsilon)^n \binom{n}{\lfloor \beta n \rfloor}$$

hat.

Der Beweis ist lang und hat leider wenig mit Algebra zu tun, weswegen wir ihn nicht behandeln werden.

3 Geometrische Anwendungen

Für $n \in \mathbb{N}$ sei $\mathcal{G}_n$ der Graph mit $V(\mathcal{G}_n) = \mathbb{R}^n$ und $E(\mathcal{G}_n) = \{xy\colon \|x - y\| = 1\}$.
Die chromatische Zahl $\chi(\mathcal{G}_n)$ ist die kleinste Zahl $p \in \mathbb{N}_0$ derart, dass man die Punkte des $\mathbb{R}^n$ so mit p Farben färben kann, dass je zwei Punkte x, y mit $\|x - y\| = 1$ verschiedenfarbig sind.

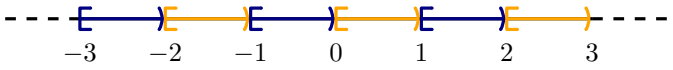


Abbildung 9: Färbung für $\mathcal{G}_1$

Beispiele. Für $n = 1$ können wir eine Färbung angeben, die zeigt, dass $\chi(\mathcal{G}_1) = 2$ gilt.
Für $n = 2$ ist dieses Problem, bekannt als *Hadwiger-Nelson Problem*, bereits ungelöst. Man kann sich aber relativ schnell erschließen, dass $\chi(\mathcal{G}_2) \geq 4$ ist (siehe Abbildung 10):

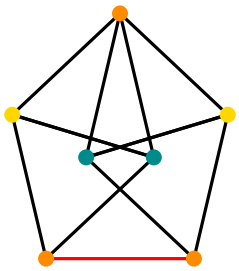


Abbildung 10: Konfiguration für $\chi(\mathcal{G}_2) \geq 4$

Angenommen es gäbe eine 3-Färbung von $\mathcal{G}_2$. Dann müssten in einem gleichseitigem Dreieck mit Seitenlänge 1 die Ecken unterschiedliche Farben besitzen. Betrachtet man also zwei solcher Dreiecke, die eine Seite teilen, so müssen die Ecken mit Abstand $\sqrt{3}$ dieselbe Farbe besitzen. Insgesamt müssen also Punkte mit Abstand $\sqrt{3}$ immer gleichgefärbt sein. Aber dann ist der Punkt, welcher zum einen Punkt Abstand 1 hat und zum anderen Abstand $\sqrt{3}$, nicht färbbar. ↯
Aubrey de Grey zeigte kürzlich sogar $\chi(\mathcal{G}_2) \geq 5$, wobei er hierfür eine Konfiguration mit mehreren 1000 Punkten fand.
Auch bekannt ist, dass $\chi(\mathcal{G}_2) \leq 7$ gilt, indem man die Ebene mit Hexagons geeigneter Größe überdeckt und wie in Abbildung 11 diese dann färbt.
Für $n = 3$ weiß man $6 \leq \chi(\mathcal{G}_3) \leq 15$.

Fakt 3.1. Für alle $n \in \mathbb{N}$ ist $\chi(\mathcal{G}_n) \leq 9^n$.

Beweis. Siehe Blatt 3, Aufgabe 4. □

Lemma 3.2. Für jede Primzahl p ist $\chi(\mathcal{G}_{4p-1}) > (3/2)^p$.

Beweis. Es sei $\varphi\colon \mathbb{R}^{4p-1} \to [t]$ eine Färbung mit $\varphi(x) \neq \varphi(y)$ wann immer $\|x - y\| = 1$.

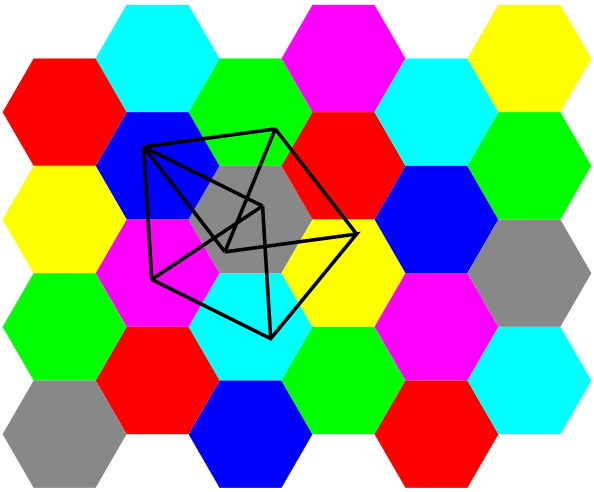


Abbildung 11: 7-Färbung $\mathcal{G}_2$ (Quelle: Wikipedia)

Uns interessieren die $\binom{4p-1}{2p-1}$ Punkte in

$$\mathcal{A} = \left\{ \frac{1}{\sqrt{2p}} \cdot A \,\middle|\, A \in [4p-1]^{(2p-1)} \right\},$$

wobei A mit dem zugehörigen 0-1-Vektor identifiziert wird. Für $\tau \in [t]$ setze

$$\mathcal{A}_\tau = \left\{ A \in [4p-1]^{(2p-1)} \,\middle|\, \varphi\left(\frac{1}{\sqrt{2p}} \cdot A \right) = \tau \right\}.$$

Für $A, B \in \mathcal{A}_\tau$ ist $\|A - B\| \neq \sqrt{2p}$ und folglich

$$2p \neq \|A - B\|^2 = \|A\|^2 - 2\langle A, B\rangle + \|B\|^2 = 2(2p-1) - 2|A \cap B|,$$

das heißt $|A \cap B| \neq p-1$. Nach Satz 2.18 ist also $|\mathcal{A}_\tau| \leq \binom{4p-1}{p-1}$ für alle $\tau \in [t]$. Somit gilt

$$t \geq \frac{\binom{4p-1}{2p-1}}{\binom{4p-1}{p-1}} = \frac{(p-1)!(3p)!}{(2p-1)!(2p)!} = \frac{3p \cdot \ldots \cdot (2p+1)}{(2p-1) \cdot \ldots \cdot p} > \left(\frac{3}{2}\right)^p. \qquad \square$$

Tatsächlich könnte man auch den Satz beweisen mit Satz 2.19 und hätte so direkt eine Aussage für alle Dimensionen.

Folgerung 3.3. Es gibt eine Konstante $c > 1$ mit $\chi(\mathcal{G}_n) > c^n$.

Beweis. Setze $c = \sqrt[8]{3/2}$. Für $n \leq 8$ ist $\chi(\mathbb{R}^n) \geq 2 > c^n$. Sei nun $n > 8$. Nach dem Bertrandschen Postulat existiert eine Primzahl p mit

$$\frac{n}{8} \leq p \leq \frac{n}{4}.$$

Nun haben wir damit nach Lemma 3.2

$$\chi(\mathcal{G}_n) \geq \chi(\mathcal{G}_{4p-1}) > \left(\frac{3}{2}\right)^p = c^{8p} \geq c^n. \qquad \square$$

Dies stimmt sogar für $c = 1.2$.
Als nächstes beschäftigen wir uns mit einem Problem von Borsuk[14]:
Der *Durchmesser* von $\emptyset$ sei Null und für nicht-leere $A \subseteq \mathbb{R}^n$

$$\operatorname{diam}(A) = \sup \{\|x - y\| \mid x, y \in A\}.$$

Borsuk vermutete: Wenn $A \subseteq \mathbb{R}^n$ endlichen Durchmesser hat (also beschränkt ist), dann gibt es eine Partition $A = A_1 \cup \ldots \cup A_{n+1}$ mit $\operatorname{diam}(A_i) < \operatorname{diam}(A)$ für $i = 1, \ldots, n+1$.
Dies ist notwendig, wenn man sich beispielsweise reguläre Tetraeder betrachtet.

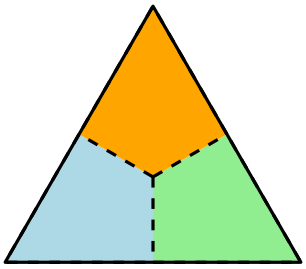


Abbildung 12: Ein gleichseitiges Dreieck lässt sich nicht in zwei Mengen partitionieren mit kleinerem Durchmesser.

Tatsächlich ist aber die Vermutung falsch.

Satz 3.4 (Kahn, Kalai)**.** Es sei $p \geq 13$ eine Primzahl. Dann ist Borsuks Vermutung für $n = \binom{4p-1}{2}$ falsch.

Beweis. Setze $d = 4p-1$ und arbeite mit $\mathbb{R}^{[d]^{(2)}}$ statt $\mathbb{R}^n$. Ordne jeder Menge $A \in [d]^{(2p-1)}$ die Menge

$$\Phi(A) = \left\{ \{x, y\} \in [d]^{(2)} \;\middle|\; x \in A, y \notin A \right\}$$

zu. Man kann sich $\Phi(A)$ als die Kanten des vollständig bipartiten Graphens mit Partitionsklassen A und $[d] \setminus A$ ansehen. Sie entspricht auch einem 0-1-Vektor in $\mathbb{R}^{[d]^{(2)}}$.
Setze

$$\mathcal{A} = \left\{ \Phi(A) \;\middle|\; A \in [d]^{[2p-1]} \right\} \subseteq \mathbb{R}^{[d]^{(2)}}.$$

Beachte, dass wegen $d - (2p-1) = 2p$ wir $\|\Phi(A)\|^2 = |A| \cdot |[d] \setminus A| = (2p-1) \cdot 2p$ für alle $A \in [d]^{(2p-1)}$ haben. Zudem lassen sich für $A, B \in [d]^{(2p-1)}$ die Elemente $\{x, y\} \in \Phi(A) \cap \Phi(B)$ in zwei Kategorien einteilen: Die Elemente, wo $x \in A \cap B$ und $y \in [d] \setminus (A \cup B)$ ist, und die, wo wir $x \in A \setminus B$ und $y \in B \setminus A$ haben.
Damit ist für alle $A, B \in [d]^{(2p-1)}$

$$\begin{aligned} \|\Phi(A) - \Phi(B)\|^2 &= \|\Phi(A)\|^2 - 2\langle \Phi(A), \Phi(B) \rangle + \|\Phi(B)\|^2 \\ &= 2 \cdot (2p-1) \cdot 2p - 2\,|\Phi(A) \cap \Phi(B)| \end{aligned}$$

[14] Der Mathematiker, nach dem der Satz von Borsuk-Ulam unter anderem benannt wurde.

$$= 4p \cdot (2p-1) - 2\left(|A \cap B| \cdot (|A \cap B| + 1) + ((2p-1) - |A \cap B|)^2\right)$$
$$= \frac{1}{4}(4p-1)^2 - 4\left[|A \cap B| - \left(p - \frac{3}{4}\right)\right]^2.$$

Beachte, dass $|[d] \setminus (A \cup B)| = d - |A \cup B| = d - (|A| + |B| - |A \cap B|) = 1 + |A \cap B|$ gilt. Also ist $\|\Phi(A) - \Phi(B)\|$ genau dann maximal, bzw. nimmt den Wert von $\operatorname{diam}(\mathcal{A})$ an, wenn $||A \cap B| - (p - 3/4)|$ minimal ist, das heißt wenn $|A \cap B| = p - 1$.
Ist also $\mathcal{A} = \mathcal{A}_1 \dot\cup \ldots \dot\cup \mathcal{A}_m$ eine Partition mit $\operatorname{diam}(\mathcal{A}_i) < \operatorname{diam}(\mathcal{A})$ für $i = 1, \ldots, m$, so muss dann für alle $A, B \in [d]^{(2p-1)}$ mit $\Phi(A), \Phi(B) \in \mathcal{A}_i$ $|A \cap B| \neq p - 1$ gelten.
Nach Satz 2.18 ist also $|\mathcal{A}_i| \leq \binom{4p-1}{p-1}$ für alle $i \in [m]$. Somit gilt

$$m \geq \frac{\binom{4p-1}{2p-1}}{\binom{4p-1}{p-1}} > \binom{4p-1}{2} + 1 = n + 1$$

für $p \geq 13$. Daher widerspricht $\mathcal{A}$ Borsuks Vermutung. □

Insbesondere ist Borsuks Vermutung für $n = \binom{51}{2} = 51 \cdot 25 = 1275$ falsch. Der Weltrekord im Widerlegen der Vermutung liegt bei $n = 64$.[15] Also könnte *theoretisch* Borsuks Vermutung für Dimensionen kleiner gleich 63 richtig sein.[16]
Es sei $f(n)$ die kleinste Zahl, sodass jede beschränkte Menge $A \subseteq \mathbb{R}^n$ eine Partition $A = A_1 \dot\cup \ldots \dot\cup A_{f(n)}$ mit $\operatorname{diam}(A_i) < \operatorname{diam}(A)$ für alle $i \in [f(n)]$ besitzt. Obiger Beweis zeigt: Es gibt $c > 1$ mit $f(n) > c^{\sqrt{n}}$. Man weiß auch, dass es eine Konstante $c' > 1$ mit $f(n) < (c')^n$ gibt. Ob tatsächlich $\sqrt{n}$ oder n im Exponent optimal ist, ist bis heute offen.

4 Der Satz von Helly

Eine Menge $K \subseteq \mathbb{R}^n$ heißt *konvex*, wenn für alle $p, q \in K$ auch $\overline{pq} \subseteq K$ gilt, wobei

$$\overline{pq} = \{\lambda p + (1-\lambda)q \mid \lambda \in [0,1]\}.$$

Die *konvexe Hülle* von $A \subseteq \mathbb{R}^n$ ist

$$H(A) = \bigcap_{K \subseteq \mathbb{R}^n :\, K \text{ konvex } \&\; A \subseteq K} K.$$

Der Schnitt ist nicht leer, da $K = \mathbb{R}^n$ stets konvex ist und A enthält. Offenbar ist $H(A)$ konvex, genauer die kleinste konvexe Menge, die A enthält.

Lemma 4.1. Sei $A \subseteq \mathbb{R}^n$ nicht leer. Dann ist $H(A)$ die Menge aller $\sum_{i=1}^m \lambda_i a_i$, wobei $\lambda_1, \ldots, \lambda_m \in [0,1], \sum_{i=1}^m \lambda_i = 1$ und $a_i, \ldots, a_m \in A$.

Beweis. Wir zeigen zuerst durch Induktion nach m, dass die angegebenen Punkte zu $H(A)$ gehören.

[15] Siehe *A 64-dimensional two-distance counterexample to Borsuk's conjecture (2013)*, Thomas Jenrich.
[16] Sehr unwahrscheinlich.

$m = 1$: Trivial.

$m - 1 \rightsquigarrow m$: O.B.d.A. sei $\lambda_m \neq 1$. Nun ist

$$b = \frac{\lambda_1 a_1 + \cdots + \lambda_{m-1} a_{m-1}}{\lambda_1 + \cdots + \lambda_{m-1}}$$

nach Induktionsannahme in $H(A)$ und

$$\lambda_1 a_1 + \cdots + \lambda_m a_m = (1 - \lambda_m) b + \lambda_m a_m$$

liegt auf der Strecke $\overline{ba_m}$, gehört also auch zu $H(A)$.

Nun zeigen wir umgekehrt, dass die Menge der genannten Punkte konvex ist. Hierfür betrachten wir die Punkte $p = \lambda_1 a_1 + \cdots + \lambda_m a_m$ und $q = \mu_1 b_1 + \cdots + \mu_k b_k$, wobei $\lambda_1, \ldots, \lambda_m, \mu_1, \ldots, \mu_k \geq 0, \sum_{i=1}^{m} \lambda_i = \sum_{j=1}^{k} \mu_j = 1$ und $a_1, \ldots, a_m, b_1, \ldots, b_k \in A$. Jeden Punkt $z \in \overline{pq}$ kann man in der Form $z = (1 - \nu)p + \nu q$ mit $\nu \in [0, 1]$ schreiben.
Es gilt dann

$$z = \sum_{i=1}^{m} (1 - \nu)\lambda_i a_i + \sum_{j=1}^{k} \nu \mu_j b_j$$

und wegen

$$\sum_{i=1}^{m} (1 - \nu)\lambda_i + \sum_{j=1}^{k} \nu \mu_j = (1 - \nu) + \nu = 1$$

hat auch z die gewünschte Form. □

Satz 4.2 (Carathéodory[17])**.** Es sei $A \subseteq \mathbb{R}^n$ nicht leer. Für jeden Punkt $z \in H(A)$ gibt es $\lambda_1, \ldots, \lambda_{n+1} \in [0, 1]$ und $a_1, \ldots, a_{n+1} \in A$ und $\sum_{i=1}^{n+1} \lambda_i = 1, \sum_{i=1}^{n+1} \lambda_i a_i = z$.

Der Unterschied zu Lemma 4.1 besteht also darin, dass m gleichmäßig durch $n + 1$ beschränkt wird.

Beweis. Sei $k \in \mathbb{N}$ minimal derart, dass es $\lambda_1, \ldots, \lambda_k \in [0, 1]$ und $a_1, \ldots, a_k \in A$ mit $\sum_{i=1}^{k} \lambda_i = 1$ und $\sum_{i=1}^{k} \lambda_i a_i = z$ gibt. Wegen der Minimalität gilt $\lambda_1, \ldots, \lambda_k > 0$.
Angenommen $k > n + 1$. O.B.d.A. sei $k = n + 2$, sonst führe das untere Widerspruchsargument durch für $\lambda_1/s, \ldots, \lambda_{n+2}/s \in [0, 1], a_1, \ldots, a_{n+2} \in A$ und

$$z' = \frac{1}{s} \sum_{i=1}^{n+2} \lambda_i a_i,$$

wobei $s = \sum_{i=1}^{n+2} \lambda_i$. Da $a_1 - a_{n+2}, \ldots, a_{n+1} - a_{n+2}$ linear abhängig sind, gibt es $\mu_1, \ldots, \mu_{n+1} \in \mathbb{R}$, die nicht alle Null sind, mit

$$\sum_{i=1}^{n+1} \mu_i (a_i - a_{n+2}) = 0.$$

[17] Hat nichts mit dem Satz von Carathéodory aus der Maßtheorie zu tun, ist aber dieselbe Person.

Setze $\mu_{n+2} = -\sum_{i=1}^{n+1} \mu_i$. Dann sind

$$\sum_{i=1}^{n+2} \mu_i = 0, \qquad \sum_{i=1}^{n+2} \mu_i a_i = 0.$$

Setze $T = \{\tau \in \mathbb{R} \mid \forall\, i \in [n+2] \colon \lambda_i + \tau\mu_i \geq 0\}$. Wegen $0 \in T$ ist $T \neq \emptyset$. Außerdem ist T abgeschlossen und $T \neq \mathbb{R}$. Wähle jetzt $\tau_* \in T \cap \partial T$.
Setze $\lambda_i' = \lambda_i + \tau_*\mu_i$ für $i = 1, \ldots, n+2$. Dann ist $\lambda_1', \ldots, \lambda_{n+2}' \geq 0$,

$$\sum_{i=1}^{n+2} \lambda_i' = \underbrace{\sum_{i=1}^{n+2} \lambda_i}_{=1} + \tau_* \underbrace{\sum_{i=1}^{n+2} \mu_i}_{=0} = 1.$$

und

$$\sum_{i=1}^{n+2} \lambda_i' a_i = \underbrace{\sum_{i=1}^{n+2} \lambda_i a_i}_{=z} + \tau_* \underbrace{\sum_{i=1}^{n+2} \mu_i a_i}_{=0} = z.$$

Wegen der Wahl von τ_* muss aber $\lambda_i' = 0$ für ein $i \in [m]$ gelten. Also ist einer der Punkte $a_1, \ldots, a_{n+2}$ überflüssig, was aber der Minimalität von k widerspricht. □

Man kann sich natürlich fragen, ob die $n+1$ im Satz 4.2 überhaupt notwendig sind. Dies ist tatsächlich aber der Fall. Man nehme hierfür beispielsweise in $\mathbb{R}^2$ die Ecken $v_1, v_2, v_3 \in \mathbb{R}^2$ eines gleichseitigen Dreiecks mit dem Mittelpunkt als Ursprung. Dann kann die Null nur durch die Konvexkombination $1/3 \cdot v_1 + 1/3 \cdot v_2 + 1/3 \cdot v_3$ dargestellt werden. Diese Konstruktion lässt sich ähnlich in höheren Dimensionen verallgemeinern. In bestimmten Fällen sind aber auch n Elemente in der Konvexkombination hinreichend:

Satz 4.3. Wenn $A \subseteq \mathbb{R}^n$ höchstens n Zusammenhangskomponenten hat, dann gibt es für jeden Punkt $z \in H(A)$ Zahlen $\lambda_1, \ldots, \lambda_n \in [0,1]$ und $a_1, \ldots, a_n \in A$ mit

$$\sum_{i=1}^{n} \lambda_i = 1, \qquad \sum_{i=1}^{n} \lambda_i a_i = z.$$

Beweis. Für $n = 1$ trivial: Die Voraussetzungen implizieren dann nämlich, dass A zusammenhängend und damit $A = H(A)$ ist.
Sei nun $n \geq 2$. O.B.d.A. ist $z = 0$, sonst verschiebe das ganze Geschehen in den Ursprung. Nach Satz 4.2 gibt es $\lambda_1, \ldots, \lambda_{n+1} \in A$ mit

$$\sum_{i=1}^{n+1} \lambda_i = 1, \qquad \sum_{i=1}^{n+1} \lambda_i a_i = 0.$$

Weiterhin dürfen wir $\lambda_1, \ldots, \lambda_{n+1} > 0$ annehmen, da wir sonst fertig sind. O.B.d.A. liegen a_1, a_2 in der gleichen Zusammenhangskomponente von A. Setze

$$C = \left\{ -\sum_{i=2}^{n+1} \mu_i a_i \;\middle|\; \mu_2, \ldots, \mu_{n+1} > 0 \right\}.$$

Wegen

$$a_1 = -\sum_{i=2}^{n+1} \frac{\lambda_i}{\lambda_1} \cdot a_i$$

ist $a_1 \in C$.

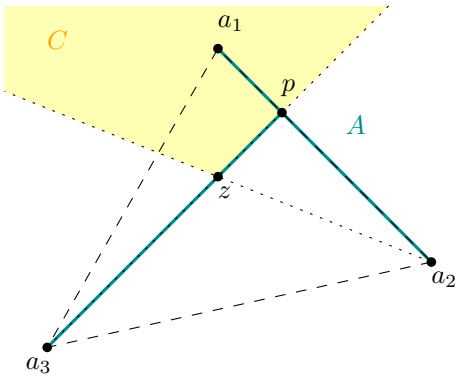


Abbildung 13: Skizze zum Beweis von Satz 4.3 in $\mathbb{R}^2$

Fall 1: $a_2 \in C$. Dann gibt es $\mu_2 > 1$ und $\mu_3, \ldots, \mu_{n+1} > 0$ mit

$$\sum_{i=2}^{n+1} \mu_i a_i = 0.$$

Setze $s = \sum_{i=2}^{n+1} \mu_i$. Dann ist

$$\sum_{i=2}^{n+1} \frac{\mu_i}{s} \cdot a_i = 0$$

wie gewünscht.

Fall 2: $a_2 \notin C$. Da a_1 und a_2 der gleichen Zusammenhangskomponente angehören, existiert ein Punkt $p \in A \cap \partial C$. O.B.d.A. gibt es $\mu_3, \ldots, \mu_{n+1} \geq 0$ mit

$$p = -\sum_{i=3}^{n+1} \mu_i a_i.$$

Setze $s = 1 + \sum_{i=3}^{n+1} \mu_i$. Dann ist

$$\frac{1}{s} \cdot p + \sum_{i=3}^{n+1} \frac{\mu_i}{s} \cdot a_i = 0$$

wie gewünscht.

Damit wäre der Beweis erbracht. □

Folgendes Lemma scheint offensichtlich, ist aber ohne obige Sätze „aus dem Stand“ nicht ganz einfach zu beweisen.

Lemma 4.4. Für jede kompakte Menge $K \subseteq \mathbb{R}^n$ ist $H(K)$ kompakt.

Beweis. Die Menge

$$\Delta = \left\{ (\lambda_1, \ldots, \lambda_{n+1}) \in [0,1]^{n+1} \,\middle|\, \sum_{i=1}^{n+1} \lambda_i = 1 \right\}$$

ist kompakt. Folglich ist auch $\Delta \times K^{n+1}$ kompakt. Die Funktion

$$\Delta \times K^{n+1} \to \mathbb{R}^n, ((\lambda_1, \ldots, \lambda_{n+1}), (a_1, \ldots, a_{n+1})) \mapsto \sum_{i=1}^{n+1} \lambda_i a_i$$

ist stetig. Daher ist ihr Bild kompakt. Nach Satz 4.2 ist dieses Bild $H(K)$. □

Für $x, y \in \mathbb{R}^n$ schreiben wir $d(x,y) = \|x - y\|$ für ihren *Abstand*. Für $x \in \mathbb{R}^n$ und $K \subseteq \mathbb{R}^n$ setze

$$d(x,K) = \inf \{ d(x,y) \,|\, y \in K \}.$$

Lemma 4.5. Es sei $K \subseteq \mathbb{R}^n$ kompakt. Für jeden Punkt $x \in \mathbb{R}^n$ existiert $y \in K$ mit $d(x,K) = d(x,y)$. Wenn K zusätzlich konvex ist, ist y eindeutig bestimmt.[18]

Beweis.

Existenz: Sei $x \in \mathbb{R}^n$ fest. Die Funktion $f\colon K \to \mathbb{R}, y \mapsto d(x,y)$ ist stetig. Nach einem Satz von Weierstraß nimmt f einen minimalen Wert an.

Eindeutigkeit: Seien $y, y' \in K$ Punkte mit $d(x,y) = d(x,y') = d(x,K)$ und K konvex. Dann ist $(y + y')/2 \in K$, da K konvex ist, und

$$\begin{aligned}
\left(d\left(x, \frac{y+y'}{2} \right) \right)^2 &= \left\| \frac{(x-y) + (x-y')}{2} \right\|^2 \\
&\leq \left\| \frac{(x-y) + (x-y')}{2} \right\|^2 + \left\| \frac{(x-y) - (x-y')}{2} \right\|^2 \\
&= \frac{\|x-y\|^2 + \|x-y'\|^2}{2} \\
&= d(x,y)^2.
\end{aligned}$$

Also ist $d(x, (y+y')/2) < d(x,y)$, Widerspruch, oder $y = y'$. □

[18] Dies ist im Allgemeinen nicht der Fall, beispielsweise wenn man K als Kugelfläche und x als Mittelpunkt nimmt.

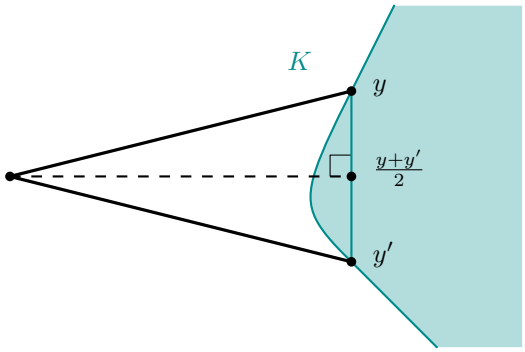


Abbildung 14: Eindeutigkeit in Lemma 4.5 für $\mathbb{R}^2$

Lemma 4.6. Es seien $x \in \mathbb{R}^n, K \subseteq \mathbb{R}^n$ und $x \notin K$. Der Punkt $y \in K$ erfülle $d(x,y) = d(x,K)$. Wenn $\overline{yz} \subseteq K$ für alle $z \in K$, dann ist K in dem Halbraum

$$\{z \in \mathbb{R}^n \mid \langle z-y, y-x\rangle \geq 0\}$$

enthalten.

Beweis. Sei $z \in K$ beliebig. Für alle $\varepsilon \in (0,1]$ liegt $y' = (1-\varepsilon)y + \varepsilon z = y + \varepsilon(z-y)$ auf $\overline{yz}$, gehört also zu K. Daher ist $\|x-y\|^2 \leq \|x-y'\|^2$ bzw. $\|y\|^2 - 2\langle y, x\rangle \leq \|y'\|^2 - 2\langle y', x\rangle$. Also gilt

$$2\varepsilon \langle z-y, x\rangle = 2\langle y'-y, x\rangle \leq \|y'\|^2 - \|y\|^2 = 2\varepsilon\langle z-y, y\rangle + \varepsilon^2 \|z-y\|^2 .$$

Daher gilt

$$0 \leq 2\langle z-y, y-x\rangle + \varepsilon \|z-y\|^2 .$$

Im Limes $\varepsilon \to 0$ erhält man schließlich $\langle z-y, y-x\rangle \geq 0$. □

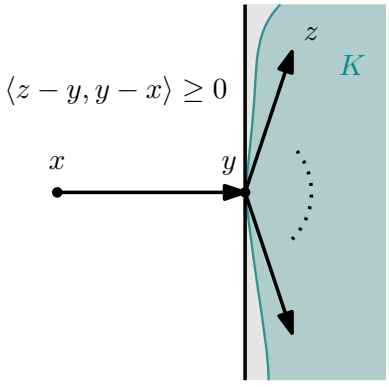


Abbildung 15: Skizze zu Lemma 4.6 in $\mathbb{R}^2$

Als nächstes zeigen wir einen Satz von Radon, demselben Radon wie vom Satz von Radon-Nikodým.

Satz 4.7 (Radon)**.** Es seien $a_1, \dots, a_{n+2} \in \mathbb{R}^n$. Dann gibt es disjunkte $I, J \subseteq [n+2]$ mit

$$H(\{a_i \mid i \in I\}) \cap H(\{a_j \mid j \in J\}) \neq \emptyset.$$

Diese Aussage macht intuitiv in der Ebene Sinn: Wir können annehmen, dass $a_1, \dots, a_4 \in \mathbb{R}^2$ verschieden und keine drei Punkte kollinear sind. Ist eines der a_i im Dreieck mit Ecken $a_j, j \neq i$, so wähle $I = \{i\}$ und $J = [4] \setminus \{i\}$. Sonst muss es $I = \{i_1, i_2\}$ und $J = \{j_1, j_2\} = [4] \setminus I$ geben, sodass sich $\overline{a_{i_1} a_{i_2}}$ und $\overline{a_{j_1} a_{j_2}}$ schneiden.

Beweis. Da $a_1 - a_{n+2}, \dots, a_{n+1} - a_{n+2}$ linear abhängig sind, gibt es $\lambda_1, \dots, \lambda_{n+2} \in \mathbb{R}$, die nicht alle Null sind, mit

$$\sum_{i=1}^{n+2} \lambda_i = 0, \qquad \sum_{i=1}^{n+2} \lambda_i a_i = 0.$$

Setze $I = \{i \in [n+2] \mid \lambda_i > 0\}$ und $J = \{j \in [n+2] \mid \lambda_j < 0\}$.
Dann ist $I \cap J = \emptyset$ klar,

$$s = \sum_{i \in I} \lambda_i = \sum_{j \in J} (-\lambda_j) > 0,$$

und der Punkt

$$S = \frac{\sum_{i \in I} \lambda_i a_i}{s} = \frac{\sum_{j \in J} (-\lambda_j) a_j}{s}$$

in $H(\{a_i \mid i \in I\}) \cap H(\{a_j \mid j \in J\})$. □

Satz 4.8 (Helly)**.** Es seien $K_1, \dots, K_m \subseteq \mathbb{R}^n$ konvex, wobei $m \geq n+1$. Für alle $I \subseteq [m]^{(n+1)}$ gelte $\bigcap_{i \in I} K_i \neq \emptyset$. Dann ist $\bigcap_{i \in [m]} K_i \neq \emptyset$.

Erster Beweis. Wir beweisen die Aussage per Induktion nach m.

$m = n+1$: Trivial.

$m = n+2$: Für $i \in [n+2]$ sei $a_i \in \bigcap_{j \neq i} K_j$ beliebig. Nach dem Satz von Radon / Satz 4.7 gibt es disjunkte Mengen $I, J \subseteq [n+2]$ und einen Punkt

$$z \in H(\{a_i \mid i \in I\}) \cap H(\{a_j \mid j \in J\}).$$

Dann ist $z \in \bigcap_{k \in [n+2]} K_k$, denn: Sei $k \in [n+2]$. O.B.d.A. sei $k \notin I$. Dann ist $\{a_i \mid i \in I\} \subseteq K_k$. Da K_k konvex ist, folgt $z \in H(\{a_i \mid i \in I\}) \subseteq K_k$.

$m \rightsquigarrow m+1$: Hier ist $m \geq n+2$. Aus dem gerade gezeigten folgt: Je $n+1$ der Mengen

$$K_1, \dots, K_{m-1}, K_m \cap K_{m+1}$$

schneiden sich.

Damit wäre der Beweis vollbracht. □

Zweiter (weniger schöner) Beweis. O.B.d.A. seien die Mengen $K_1, \ldots, K_m$ kompakt. Wir dürfen das annehmen, da für jedes $I \in [m]^{(n+1)}$ wir uns ein $z_I \in \bigcap_{i \in I} K_i$ beliebig auswählen können. Setzt man also

$$L_i = H\left(\left\{z_I \,\middle|\, i \in I \in [m]^{(n+1)}\right\}\right)$$

für $i \in [m]$, so ist $L_i \subseteq K_i$, L_i konvex und kompakt, und $z_I \in \bigcap_{i \in I} L_i$ für alle $I \in [m]^{(n+1)}$. Definiere nun $f\colon \mathbb{R}^n \to \mathbb{R}$ durch

$$f(x) = \max\{d(x, K_i) \mid i \in [m]\}.$$

Dann ist f stetig und $f(x) \to \infty$, wenn $\|x\| \to \infty$. Nach einem Satz von Weierstraß[19] existiert daher ein Punkt $y \in \mathbb{R}^n$, für den $f(y)$ minimal ist.
Wenn $f(y) = 0$, dann ist $y \in \bigcap_{i \in [m]} K_i$ und wir sind fertig.[20] Ab jetzt gelte also $f(y) > 0$. Durch eine geeignete Permutation gelte o.B.d.A.

$$\{i \in [m] \mid d(y, K_i) = f(y)\} = [k]$$

für ein $k \in [m]$. Für $i \in [k]$ wähle $x_i \in K_i$ mit $d(y, K_i) = d(y, x_i)$.

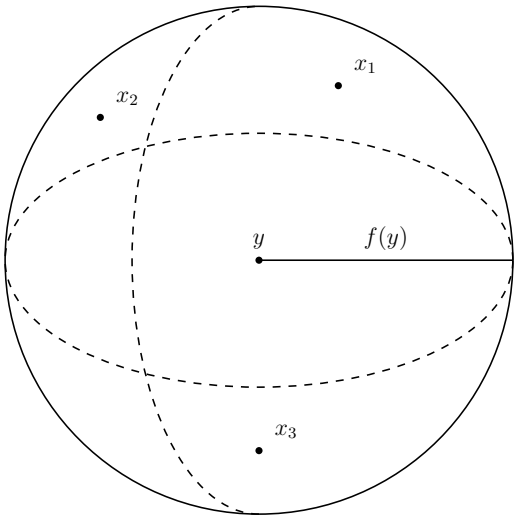


Abbildung 16: Alle $x_i, i \in [k]$, sind auf dem Rand des Balls mit Radius $f(y)$ um y ($k = 3$).

Behauptung. $y \in H(\{x_1, \ldots, x_k\})$.

Beweis der Behauptung. Angenommen $y \notin H(\{x_1, \ldots, x_k\})$. Da $H(\{x_1, \ldots, x_k\})$ kompakt und konvex ist, existiert ein eindeutiger Punkt $z \in H(\{x_1, \ldots, x_k\})$, der y am nächsten ist. Wähle $y' \in \overline{yz}$ sehr nahe y.[21] Für alle $i \in [k]$ ist dann

$$d(y', K_i) \leq d(y', x_i) < d(y, x_i) = f(y).$$

[19] Es ist schwer bei den vielen Sätzen von **dem** Satz von Weierstraß zu sprechen.
[20] Wegen der Kompaktheit folgt nämlich aus $d(x, K_i) = 0$ bereits $x \in K_i$ für alle $i \in [m]$.
[21] Wir sparen uns die Analysis-Details.

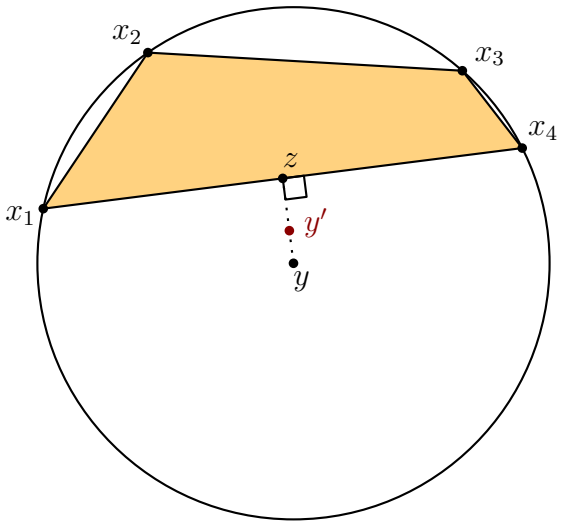


Abbildung 17: Beweisskizze zur Behauptung ($k = 4$)

Für $i \in [k+1, m]$ ist $d(y, K_i) < f(y)$ und folglich $d(y', K_i) < f(y)$.
Daher ist $f(y') < f(y)$. ↯ □

Nach dem Satz von Carathéodory / Satz 4.2 gilt o.B.d.A. $y \in H(\{x_1, \dots, x_s\})$, wobei $s \leq \min(n+1, k)$. Nach Voraussetzung existiert $z \in \bigcap_{i \in [s]} K_i$.
Nach Lemma 4.6 gilt $\langle z - x_i, x_i - y \rangle \geq 0$ für alle $i \in [s]$ und somit

$$\langle z - y, x_i - y \rangle = \langle (z - x_i) + (x_i - y), x_i - y \rangle = \langle z - x_i, x_i - y \rangle + \|x_i - y\|^2 > 0,$$

da $f(y) > 0$. Wähle $\lambda_1, \dots, \lambda_s \in [0, 1]$ mit $\sum_{i=1}^s \lambda_i = 1$ und $\sum_{i=1}^s \lambda_i x_i = y$. Nun ist $\sum_{i=1}^s \lambda_i (x_i - y) = 0$ und folglich

$$0 = \left\langle z - y, \sum_{i=1}^s \lambda_i (x_i - y) \right\rangle = \sum_{i=1}^s \lambda_i \underbrace{\langle z - y, x_i - y \rangle}_{>0} > 0. \text{ ↯} \qquad \square$$

Folgerung 4.9. Es sei $(K_i)_{i \in I}$ eine Familie kompakter, konvexer Mengen mit $|I| \geq n+1$. Für alle $J \in I^{(n+1)}$ sei $\bigcap_{j \in J} K_j \neq \emptyset$. Dann gilt $\bigcap_{i \in I} K_i \neq \emptyset$.

Beweis. Nach Satz 4.8 gilt $\bigcap_{j \in J} K_j \neq \emptyset$ für jede endliche Menge $J \subseteq I$. O.B.d.A. gebe es eine kompakte Menge K mit $K_i \subseteq K$ für alle $i \in I$: Sonst wähle ein beliebiges $i_0 \in I$ und betrachte die Familie $(K_i \cap K_{i_0})_{i \in I}$. Dann gilt immer noch $\bigcap_{j \in J} (K_j \cap K_{i_0}) = \bigcap_{j \in J \cup \{i_0\}} K_j \neq \emptyset$ für alle endlichen $J \subseteq I$ und $\bigcap_{i \in I} K_i = \bigcap_{i \in I} (K_i \cap K_{i_0})$.
Dann folgt direkt $\bigcap_{i \in I} K_i \neq \emptyset$ wegen der Kompaktheit von K.[22] □

Die Kompaktheitsbedingung ist tatsächlich notwendig.[23]

[22] Beachte, dass eine Familie von abgeschlossenen Mengen eines kompakten Raums genau dann einen gemeinsamen Schnitt hat, wenn je endliche viele einen gemeinsamen Schnitt haben.

[23] Es sei dem Leser überlassen, für den Fall ein Gegenbeispiel zu finden, siehe Aufgabe 1, Blatt 4.

Lemma 4.10. Es sei $A \subseteq \mathbb{R}^n, |A| = n+1$. Wenn $\operatorname{diam}(A) \leq 1$, dann kann man A mit einem abgeschlossenen Ball, dessen Radius $\sqrt{n/(2(n+1))}$ ist, überdecken.

Der Radius mag willkürlich wirken, jedoch ist dieser optimal, wenn man A als die Menge an Ecken eines regelmäßigen Tetraeders mit Kantenlänge 1 wählt.

Beweis. Es sei B ein abgeschlossener Ball mit $A \subseteq B$, dessen Radius r minimal ist. O.B.d.A. sei 0 der Mittelpunkt von B. Es seien $x_1, \ldots, x_k \in A$ die Punkte, die auf dem Rand von B liegen. Wie im zweiten Beweis von Satz 4.8 zeigt man $0 \in H(\{x_1, \ldots, x_k\})$. Also gibt es $\lambda_1, \ldots, \lambda_k \in [0,1]$ mit $\sum_{i=1}^k \lambda_i = 1$ und $\sum_{i=1}^k \lambda_i x_i = 0$.
Da $\max_{i,j\in[k]} \|x_i - x_j\| \leq \operatorname{diam}(A) \leq 1$, gilt für alle $i \in [k]$

$$1 - \lambda_i \geq \sum_{j=1}^k \lambda_j \|x_j - x_i\|^2 = \sum_{j=1}^k \lambda_j \underbrace{\left(\|x_j\|^2 + \|x_i\|^2\right)}_{=2r^2} - 2\left\langle x_i, \underbrace{\sum_{i=1}^k \lambda_j x_j}_{=0} \right\rangle = 2r^2.$$

Summation über $i \in [k]$ zeigt $k - 1 \geq 2kr^2$. Also folgt

$$2r^2 \leq \frac{k-1}{k} = 1 - \frac{1}{k} \leq 1 - \frac{1}{n+1} = \frac{n}{n+1},$$

das heißt $r \leq \sqrt{n/(2(n+1))}$. □

Satz 4.11 (Jung)**.** Jede Menge $A \subseteq \mathbb{R}^n$ mit $\operatorname{diam}(A) \leq 1$ lässt sich durch einen abgeschlossenen Ball mit Radius $\sqrt{n/(2(n+1))}$ überdecken.

Beweis. Für jeden Punkt $x \in \mathbb{R}^n$ sei K_x der abgeschlossene Ball um x mit Radius $\sqrt{n/(2(n+1))}$. Betrachte $\{K_x \mid x \in A\}$. Nun schneiden sich je $n+1$ dieser Mengen: Für $A' \in A, |A'| = n+1$, existiert nach Lemma 4.10 ein $z \in \mathbb{R}^n$ mit $A' \subseteq K_z$, also

$$z \in \bigcap_{x \in A'} K_x.$$

Nach Folgerung 4.9 ist also $\bigcap_{x\in A} K_x \neq \emptyset$. Wähle $z \in \bigcap_{x\in A} K_x$. Dann gilt $A \subseteq K_z$. □

Definition 4.12. Es sei $K \subseteq \mathbb{R}^n$. Man nennt $A \subseteq K$ *sichtbar in* K, wenn es einen Punkt $x \in K$ mit

$$\bigcup_{a \in A} \overline{ax} \subseteq K$$

gibt. Wenn K selbst sichtbar ist, nennt man K *sternförmig*.

Insbesonders sind natürlich konvexe Mengen sternförmig. Die Umkehrung ist nur der Fall, wenn $\bigcup_{a\in A} \overline{ax} \subseteq K$ für *alle* Punkte $x \in K$ gilt.

Die Definition kann man sich so vorstellen: Angenommen die Menge K stelle gerade den Raum einer Kunstgallerie dar. Dann ist ein Teilraum A von K sichtbar, falls ein Museumswächter ganz A gleichzeitig von seiner Position aus bewachen kann.

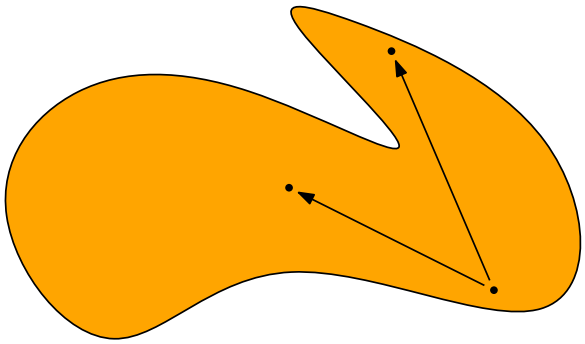


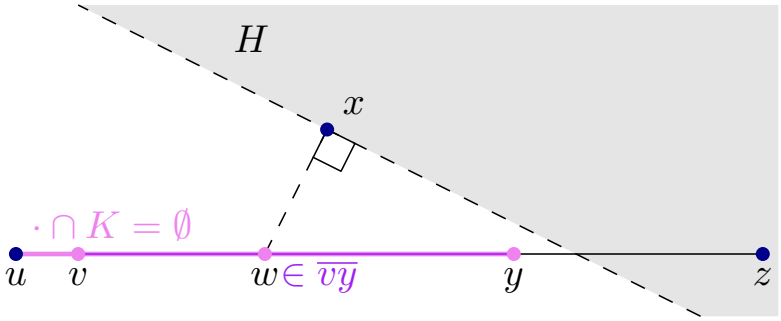
Abbildung 18: Zwei Punkte, die gleichzeitig sichtbar sind

Satz 4.13 (Krasnoselski)**.** Es sei $K \subseteq \mathbb{R}^n$ kompakt. Wenn jede Menge $A \subseteq K$ mit $|A| = n+1$ sichtbar ist, dann ist K sternförmig.

Beweis. Für alle $x \in K$ setzen wir

$$V_x = \{y \in K \mid \overline{xy} \subseteq K\}.$$

Dann ist V_x kompakt und je $n+1$ die Mengen in $\{V_x \mid x \in K\}$ schneiden sich. Nach Folgerung 4.9 und Lemma 4.4 existiert ein Punkt $z \in \bigcap_{x \in K} H(V_x)$.
Wir zeigen jetzt per Widerspruch, dass sogar $z \in \bigcap_{x \in K} V_x$ gilt.



Annahme. Es gibt $u \in K$ mit $\overline{uz} \not\subseteq K$.

Wähle $y \in \overline{uz} \setminus K$. O.B.d.A. sei das Innere der Strecke $\overline{uy}$ disjunkt zu K. (Sonst ersetze u durch den Punkt von $\overline{uy} \cap K$, der am nächsten bei y ist.) Wähle $v \in \overline{uy}$ „Nahe“ (aber ungleich) u, das heißt $0 < d(u,v) < d(y,K)$. Wähle $w \in \overline{vy}$ und $x \in K$, dass $d(w,x)$ minimal ist. x ist ein Punkt von V_x, der am nächsten an w liegt. Daher ist nach Lemma 4.6 V_x im Halbraum $H = \{q \in \mathbb{R}^n \mid \langle q - x, x - w\rangle \geq 0\}$ enthalten.
Da $z \in H(V_x) \subseteq H$ gilt, haben wir $\langle z - x, x - w\rangle \geq 0$. Das Dreieck xwz hat also keinen spitzen Winkel bei x. Somit ist sein Winkel bei w spitz. Nach Minimalität von $d(w,x)$ ist also $w = y$, sonst wäre jeder Punkt auf dem Inneren von $\overline{wy}$ näher zu x als w. Andererseits ist aber

$$d(w,K) \leq d(v,K) \leq d(v,u) < d(y,K). \; \lightning \qquad \square$$

Mit diesem Satz schließen wir mit den geometrischen Anwendungen des Satz von Helly ab und kehren zu Mengensystemen zurück.
Für jedes Mengensystem $\mathcal{A} \subseteq \mathcal{P}(X)$ sei die *Überdeckungszahl* von $\mathcal{A}$

$$\tau(\mathcal{A}) = \min\{|U| \mid \forall A \in \mathcal{A}\colon A \cap U \neq \emptyset\}.$$

In der Situation von Graphen $G = (V, E)$ ist $\tau(E)$ die Größe einer minimalsten Knotenüberdeckung. Allgemein ist für k-uniforme Hypergraphen deswegen auch die Schreibweise $\tau(G)$ statt $\tau(E)$ üblich.

Satz 4.14 (Bollobás)**.** Es sei $H = (V, E)$ ein k-uniformer Hypergraph, das heißt $E \subseteq V^{(k)}$. Wenn $\tau(E') \leq p \in \mathbb{N}$ für alle $E' \subseteq E$ mit $|E'| \leq \binom{k+p}{k}$ gilt, dann ist $\tau(E) \leq p$.

Lemma 4.15 (Bollobás)**.** Es seien $A_1, \ldots, A_m, B_1, \ldots, B_m \subseteq [n]$. Wenn $A_i \cap B_i = \emptyset$ für alle $i = 1, \ldots, m$ und $A_i \cap B_j \neq \emptyset$ für $i \neq j$, dann ist

$$\sum_{i=1}^{m} \frac{1}{\binom{|A_i|+|B_i|}{|A_i|}} \leq 1.$$

Beweis. Für $i \in [n]$ sei $\mathcal{X}_i \subseteq S_n$ die Menge der Permutationen π mit der Eigenschaft, dass in der Zeile

$$\begin{pmatrix} \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}$$

die Elemente von A_i vor allen Elementen von B_i kommen. Dann ist

$$|\mathcal{X}_i| = \binom{n}{|A_i| + |B_i|} |A_i|!\,|B_i|!(n - |A_i| - |B_i|)! = \frac{n!}{\binom{|A_i|+|B_i|}{|A_i|}}.$$

Stochastisch lässt sich diese Gleichheit auch folgendermaßen interpretieren: Die Wahrscheinlichkeit, dass bei einer zufällig gezogenen Permutation alle Elemente von A_i vor den Elementen von B_i sind, ist gerade

$$\frac{|A_i|!\,|B_i|!}{(|A_i| + |B_i|)!} = \frac{1}{\binom{|A_i|+|B_i|}{|A_i|}}.$$

Also erhalten wir insgesamt dann wie „erwartet“

$$|\mathcal{X}_i| = \frac{n!}{\binom{|A_i|+|B_i|}{|A_i|}}.$$

Außerdem ist $\mathcal{X}_i \cap \mathcal{X}_j = \emptyset$ für $i \neq j$. Ist nämlich $r \in A_i \cap B_j, s \in A_j \cap B_i$ so kommt r vor s für $\pi \in \mathcal{X}_i$ und s vor r für $\pi \in \mathcal{X}_j$. Daher gilt

$$\sum_{i=1}^{n} \frac{n!}{\binom{|A_i|+|B_i|}{|A_i|}} = \sum_{i=1}^{n} |\mathcal{X}_i| \leq |S_n| = n!.$$

Teilen wir durch $n!$ erhalten wir die gewünschte Ungleichung. □

Folgerung 4.16. Es seien $A_1, \dots, A_m \in [n]^{(r)}$ und $B_1, \dots, B_m \in [n]^{(s)}$. Wenn

- $A_i \cap B_i = \emptyset$ für alle $i \in [m]$, und
- $A_i \cap B_j \neq \emptyset$ für $i \neq j$.

Dann ist $m \leq \binom{r+s}{r}$.

Beweis. Nach Lemma 4.15 ist $m/\binom{r+s}{r} \leq 1$. □

Wir werden später die Voraussetzungen relaxieren können mit einem algebraischen Ansatz statt einem probabilistischen.[24]

Beweis von Satz 4.14. Es sei $\tau(E') \leq p$ für alle $E' \subseteq E, |E'| \leq \binom{k+p}{k}$.
Wir machen eine Induktion nach $|E|$. Dabei ist für $|E| \leq \binom{k+p}{k}$ alles klar. Für den Induktionsschritt sei $E = \{A_1, \dots, A_m\}$ mit $m > \binom{k+p}{k}$. Nach der Induktionsannahme gibt es für jedes $i \in [m]$ eine Menge B_i mit $|B_i| = p$ und $\forall\, i, j \in [m], i \neq j$, $A_j \cap B_i \neq \emptyset$. Nach Folgerung 4.16 gibt es $i \in [m]$ mit $A_i \cap B_i \neq \emptyset$. Nun bezeugt B_i, dass $\tau(E) \leq p$. □

Die *Resultante* zweier Polynome aus $\mathbb{R}[x]$[25]

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m$$
$$g(x) = b_0 + b_1 x + \cdots + b_n x^n$$

ist die $(m+n) \times (m+n)$-Determinante:

$$\operatorname{Res}(f,g) = \begin{Vmatrix} a_0 & a_1 & \cdots & \cdots & a_m & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & \cdots & a_m & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \cdots & 0 & a_0 & a_1 & \cdots & \cdots & a_m \\ b_0 & b_1 & \cdots & \cdots & b_n & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & \cdots & b_n & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & \cdots & b_n \end{Vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \end{matrix}$$

Lemma 4.17. Es seien $f, g \in \mathbb{R}[x]$ Polynome vom Grad m bzw. n. Dann haben f, g genau dann eine gemeinsame (komplexe) Nullstelle, wenn $\operatorname{Res}(f,g) = 0$.

Das Resultat lässt sich verallgemeinern auf faktorielle Ringe, was aber dann wirklich eher klassischer Algebra-Stoff wäre.

Beweis. Es ist genau dann $\operatorname{Res}(f,g) = 0$, wenn die Zeilen der obigen Matrix linear abhängig sind, das heißt, wenn es $r_0, \dots, r_{n-1}, s_0, \dots, s_{m-1} \in \mathbb{R}$ gibt, die nicht alle Null sind, mit

[24] Schließlich erhält man mehr mit Struktur als dem Gegenteil davon.
[25] Oder allgemeiner mit Elementen eines (faktoriellen) Rings als Koeffizienten.

$$r_0(a_0,\dots,a_m,\underbrace{0,\dots,0}_{n-1}) + \cdots + r_{n-1}(\underbrace{0,\dots,0}_{n-1},a_0,\dots,a_m)$$
$$+\, s_0(b_0,\dots,b_n,\underbrace{0,\dots,0}_{m-1}) + \cdots + s_{m-1}(\underbrace{0,\dots,0}_{m-1},b_0,\dots,b_n) = (0,\dots,0)$$

erfüllen. Für die Polynome $u(x) = \sum_{i=0}^{n-1} r_i x^i$ und $v(x) = \sum_{i=0}^{m-1} s_i x^i$ ist dies zu $fu+gv = 0$ äquivalent. Wenn also f, g einen gemeinsamen Faktor $q \in \mathbb{R}[x]$ haben, der keine Zahl ist, dann zeigen $u = g/q, v = -f/q$, dass $\operatorname{Res}(f,g) = 0$. Wenn f, g keinen gemeinsamen Faktor haben und Polynome u, v mit $\operatorname{grad}(u) < n, \operatorname{grad}(v) < n$ die Eigenschaft $fu+gv = 0$ haben, dann gilt $f \mid v, g \mid u$, also $u = v = 0$. □

Das Resultat ist zwar theoretisch interessant, aber wenn einen wirklich interessiert, ob zwei Polynome eine gemeinsame Nullstelle haben, sollte man lieber direkt den größten gemeinsamen Teiler der Polynome mit dem euklidischen Algorithmus einfach berechnen. Wir können jetzt aber den Satz 4.14 verallgemeinern.

Satz 4.18 (Blokhuis)**.** Es seien $A_1,\dots,A_m \in [n]^{(r)}, B_1,\dots,B_m \in [n]^{(s)}$ mit

- $A_i \cap B_i = \emptyset$ für alle $i \in [m]$, und
- $A_i \cap B_j \neq \emptyset$ für alle $1 \le i < j \le m$.

Dann ist $m \le \binom{r+s}{r}$.

Tatsächlich ist das Resultat auch so optimal. Beispielsweise könnte man für die A_i's alle möglichen r-elementigen Teilmengen von $[n]$ nehmen und für B_i das Komplement von A_i. Dann ist der Binomialkoeffizient auch optimal.

Beweis. Setze $a_i(x) = \prod_{\alpha\in A_i}(x-\alpha), b_i(x) = \prod_{\beta\in B_i}(x-\beta)$. Dann ist $\operatorname{Res}(a_i,b_i) \neq 0$ für alle $i \in [m]$ und $\operatorname{Res}(a_i,b_j) = 0$ für $1 \le i < j \le m$. Es seien $y_0,\dots,y_s$ weitere Variablen und

$$b = y_0 + y_1 x + \cdots + y_s x^s.$$

Wir fassen b als Polynom in x über $\mathbb{R}[y_0,\dots,y_s]$ auf. Für alle $i \in [m]$ ist $\operatorname{Res}(a_i,b) \in \mathbb{R}[y_0,\dots,y_s]$. Genau gesagt liegt $\operatorname{Res}(a_i,b)$ im $\mathbb{R}$-Untervektorraum V von $\mathbb{R}[y_0,\dots,y_s]$ der von allen $y_0^{\mu_0}\cdot\ldots\cdot y_s^{\mu_s}$ mit $\mu_0+\cdots+\mu_s = r$ aufgespannt wird nach der Leibniz-Formel.

Behauptung. $\operatorname{Res}(a_1,b),\dots,\operatorname{Res}(a_m,b)$ sind $\mathbb{R}$-linear unabhängig.

Beweis der Behauptung. Andernfalls wähle $\lambda_1,\dots,\lambda_m$, die nicht alle Null sind, mit

$$\sum_{i=1}^{m} \lambda_i \operatorname{Res}(a_i,b) = 0.$$

Sei j maximal mit $\lambda_j \neq 0$. Durch Einsetzen von b_j erhalten wir

$$\sum_{1\le i<j} \lambda_i \underbrace{\operatorname{Res}(a_i,b_j)}_{=0} + \underbrace{\lambda_j \operatorname{Res}(a_j,b_j)}_{\neq 0} + \sum_{m\ge i>j} \underbrace{\lambda_i}_{=0} \operatorname{Res}(a_i,b_j) = 0. \;\lightning$$ □

Also gilt $m \le \dim(V) = \binom{r+s}{r}$. □

5 Der kombinatorische Nullstellensatz

Es sei in diesem Abschitt $\mathbb{K}$ immer ein Körper. Nullstellensätze existieren zahlreich in der Mathematik. Der wohl bekannteste ist der Hilbertsche Nullstellensatz. Wir werden uns mit dem kombinatorischen Nullstellensatz beschäftigen, der viele schwierig erscheinende kombinatorische Probleme lösen kann.

Lemma 5.1. Es sei $P \in \mathbb{K}[x_1, \ldots, x_n]$ nicht das Nullpolynom. Für alle $i \in [n]$ sei $S_i \subseteq \mathbb{K}$ eine Menge derart, dass $|S_i|$ größer als der Grad von P in x_i ist. Dann gibt es $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$ mit $P(s_1, \ldots, s_n) \neq 0$.

Hier wäre kurz die Terminologie für Polynome in mehreren Variablen zu klären: Der *Grad* eines Monoms $M = x_1^{t_1} \cdot \ldots \cdot x_n^{t_n}$ ist $\operatorname{grad}(M) = t_1 + \cdots + t_n$. Ein Monom M *kommt* in einem Polynom $P \in \mathbb{K}[x_1, \ldots, x_n]$ *vor*, wenn der Koeffizient von M in P nicht Null ist. Der *Grad* $\operatorname{grad}(P)$ eines Polynoms P ist der höchste Grad eines Monoms, das in P vorkommt. Der Grad des Nullpolynoms ist $-\infty$.

Beweis. Wir machen eine Induktion nach n.

$n = 1$: Dies ist bekannt.[26]

$n - 1 \rightsquigarrow n$: Wähle $s_n \in S_n$ so, dass $P(x_1, \ldots, x_{n-1}, s_n)$ nicht das Nullpolynom ist. Wende dann die Induktionsannahme an. □

Lemma 5.2. Es seien $P \in \mathbb{K}[x_1, \ldots, x_n]$ und $S_1, \ldots, S_n \subseteq \mathbb{K}$ endlich. Es gelte für alle $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$ $P(s_1, \ldots, s_n) = 0$. Dann gibt es Polynome $Q_1, \ldots, Q_n$ mit

- $P = \sum_{i=1}^{n} Q_i \cdot \prod_{s_i \in S_i} (x_i - s_i)$,
- $\operatorname{grad}(Q_i) \leq \operatorname{grad}(P) - |S_i|$ für alle $i \in [n]$.

Beweis. Indem wir P als Polynom in x_1 auffassen, erhalten wir durch Polynomdivision

- $P = Q_1 \cdot \prod_{s_1 \in S_1} (x_1 - s_1) + R_1$, wobei
- $\operatorname{grad}(Q_1) \leq \operatorname{grad}(P) - |S_1|$, und
- der Grad von R_1 in x_1 kleiner als $|S_1|$ ist.

Als nächstes teilen wir dann R_1, aufgefasst als Polynom in x_2, durch $\prod_{s_2 \in S_2} (x_2 - s_2)$, und fahren so sukzessive fort. Insgesamt erhalten wir Polynome $Q_1, \ldots, Q_n, R$, mit

- $\operatorname{grad}(Q_i) \leq \operatorname{grad}(P) - |S_i|$ für alle $i \in [m]$,
- $P = \sum_{i=1}^{n} Q_i \cdot \prod_{s_i \in S_i} (x_i - s_i) + R$, und
- für alle $i \in [m]$ ist der Grad von R in x_i kleiner als $|S_i|$.

Für alle $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$ ist nun $R(s_1, \ldots, s_n) = 0$.
Nach Lemma 5.1 ist R das Nullpolynom. □

[26] Ein Polynom $P \neq 0$ (in einer Variablen) hat höchstens $\operatorname{grad}(P)$ viele Nullstellen.

Satz 5.3 (**Alons Nullstellensatz**[27])**.** Es seien $P \in \mathbb{K}[x_1, \ldots, x_n]$ ein Polynom,

$$x_1^{t_1} \cdot \ldots \cdot x_n^{t_n}$$

ein Monom maximalen Grades, das in P vorkommt. Ferner seien $S_1, \ldots, S_n \subseteq \mathbb{K}$ mit $|S_i| > t_i$ für $i = 1, \ldots, n$. Dann gibt es $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$ mit $P(s_1, \ldots, s_n) \neq 0$.

Beweis. Sonst wäre nach Lemma 5.2 $P = \sum_{i=1}^{n} Q_i \prod_{s_i \in S_i} (x_i - s_i)$ für Polynome Q_i mit

$$\operatorname{grad}(Q_i) \leq \operatorname{grad}(P) - |S_i|\,.$$

Dies ist ein Widerspruch, denn $x_1^{t_1} \cdot \ldots \cdot x_n^{t_n}$ muss in P vorkommen, aber alle möglichen Kandidaten sind Monome maximalen Grades in einen der Polynome

$$Q_1 \cdot x_1^{|S_1|}, \ldots, Q_n \cdot x_n^{|S_n|},$$

welche wegen $|S_i| > t_i$ für alle $i \in [n]$ aber nicht $x_1^{t_1} \cdot \ldots \cdot x_n^{t_n}$ sein können. □

Wir wollen nun den kombinatorischen Nullstellensatz in Aktion sehen.
Hierfür betrachten wir das sogenannte *Komjáth Problem*:

Was ist die kleinste Anzahl an Hyperebenen, um alle bis auf eine Ecke des Einheitswürfels zu überdecken?

Dies wird im nächsten Satz – meist Alon und Füredi zugeschrieben – beantwortet.

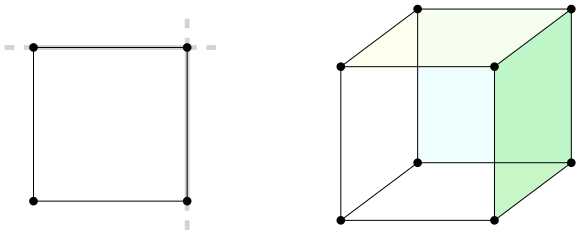


Abbildung 19: Optimale Überdeckung von allen Ecken bis auf eine

Satz 5.4. Wenn $H_1, \ldots, H_m \in \mathbb{R}^n$ Hyperebenen sind, die alle bis auf einen Punkt von $\{0,1\}^n$ überdecken, dann ist $m \geq n$.

Die Hyperebenen $H_i = \{x_i = 1\}$ zeigen, dass diese Abschätzung optimal ist, wie man in Abbilding 19 sieht.

Beweis. O.B.d.A. sei 0 der nicht überdeckte Punkt. Angenommen $m < n$. Es seien $\langle a_i, x\rangle = b_i$ $(i \in [m])$ die Gleichungen von $H_1, \ldots, H_m$. Dann ist $b_i \neq 0$ wegen $0 \notin H_i$. Betrachte das Polynom

$$P(x_1, \ldots, x_n) = \prod_{i=1}^{m} (b_i - \langle a_i, x\rangle) - \prod_{i=1}^{m} b_i \prod_{j=1}^{n} (1 - x_j).$$

[27] Interessanterweise hat Alon Reihers Dissertation begutachtet.

Offenbar hat P den Grad n und das Monom $x_1 \cdot \ldots \cdot x_n$ kommt in P vor. Nach dem kombinatorischen Nullstellensatz gibt es also $(\xi_1, \ldots, \xi_n) \in \{0,1\}^n$ mit $P(\xi_1, \ldots, \xi_n) \neq 0$. Wenn $(\xi_1, \ldots, \xi_n) \neq (0, \ldots, 0)$, dann liegt ξ auf einen der Hyperebenen und es gilt

$$\prod_{i=1}^{n} (b_i - \langle a_i, \xi \rangle) = 0.$$

Außerdem gilt $\prod_{j=1}^{n}(1 - \xi_j) = 0$ und damit $P(\xi) = 0$. ↯
Also muss $\xi = 0$ sein, aber $P(\xi) = \prod_{i=1}^{m} b_i - \prod_{i=1}^{m} b_i = 0$. ↯ □

Tatsächlich sind keine geometrischen oder einfacheren Beweise dieser Aussage bekannt. Von der kombinatorischen Geometrie gehen wir jetzt zur additiven Zahlentheorie. Für eine abelsche Gruppe Z und $A, B \subseteq Z$ setzen wir $A + B = \{a + b \mid a \in A, b \in B\}$. Wenn $A, B \subseteq \mathbb{Z}$ nicht leer sind, dann gilt $|A + B| \geq |A| + |B| - 1$. Gleichheit gilt, wenn man zwei arithmetische Folgen gleicher Schrittweite nimmt.

Beweis. Sei $A = \{a_1, \ldots, a_m\}, B = \{b_1, \ldots, b_n\}$, wobei $a_1 < \cdots < a_m$ und $b_1 < \cdots < b_n$. Dann sind

$$a_1 + b_1 < \cdots < a_m + b_1 < a_m + b_2 < \cdots < a_m + b_n$$

$m + n - 1$ verschiedene Elemente von $A + B$. □

Das lässt sich mit Einschränkung auf Körper verallgemeinern.

Satz 5.5 (Cauchy & Davenport)**.** Für alle nicht-leeren $A, B \subseteq \mathbb{F}_p$ gilt

$$|A + B| \geq \min\{|A| + |B| - 1, p\}.$$

Beweis.

Fall 1: $|A| + |B| \geq p + 1$. Sei $x \in \mathbb{F}_p$ beliebig. Wegen $|A| + |x - B| = |A| + |B| > p$, gibt es ein $a \in A \cap (x - B)$. Setze $b = x - a$. Dann ist $b \in B$ und $x = a + b \in A + B$. Dies zeigt $A + B = \mathbb{F}_p$.

Fall 2: $|A| + |B| \leq p$.

Annahme. Es gibt $C \subseteq \mathbb{F}_p$ mit $A + B \subseteq C$ mit $|C| = |A| + |B| - 2 < p$.

Betrachte das Polynom

$$P(x, y) = \prod_{c \in C} (x + y - c).$$

Für alle $a \in A, b \in B$ ist $P(a, b) = 0$. Außerdem hat P den Grad $|A| + |B| - 2$. Nach dem kombinatorischen Nullstellensatz kann das Monom $x^{|A|-1}y^{|B|-1}$ nicht in P vorkommen. Es hat aber in P den Koeffizient

$$\binom{|A| + |B| - 2}{|A| - 1} = \frac{(|A| + |B| - 2)!}{(|A| - 1)!\,(|B| - 1)!} \not\equiv 0 \pmod{p}.$$ ↯ □

Für $A_1, \ldots, A_n \subseteq \mathbb{F}_p$ sei

$$A_1 \dot{+} \ldots \dot{+} A_n = \{a_1 + \cdots + a_n \mid (\forall\, i \in [n] \colon a_i \in A_i) \wedge (\forall\, i \neq j \colon a_i \neq a_j)\}\,.$$

Damit ist $\dot{+}$ auch keine assoziative Operation, da man alle Summanden gleichzeitig betrachten muss.

Satz 5.6. Für alle nicht-leeren $A, B \subseteq \mathbb{F}_p$ mit $|A| \neq |B|$ gilt

$$|A \dot{+} B| \geq \min\{|A| + |B| - 2, p\}\,.$$

Gleichheit gilt zum Beispiel für $A = \{1, 2, \ldots, |A|\}$ und $B = \{1, 2, \ldots, |B|\}$. Dann ist $A \dot{+} B = \{3, \ldots, |A| + |B|\}$, da man $i - 1 \in A, i + 1 \in B$ für $i \in [2, \min(|A|, |B|)]$ hat.

Beweis. Da man ansonsten Elemente von A oder B löschen könnte, sodass immer noch $|A| \neq |B|$ gilt, dürfen wir o.B.d.A. $|A| + |B| \leq p + 2$ annehmen.[28]

Annahme. Es gibt $C \subseteq \mathbb{F}_p$ mit $A \dot{+} B \subseteq C$ und $|C| \leq |A| + |B| - 3 < p$.

Betrachte das Polynom

$$P(x, y) = (x - y) \prod_{c \in C} (x + y - c).$$

Offenbar hat P den Grad $|A| + |B| - 2$ und es gilt $P(a, b) = 0$ für alle $a \in A, b \in B$. Nach dem kombinatorischen Nullstellensatz hat $x^{|A|-1} y^{|B|-1}$ den Koeffizienten 0 in P. Dieser Koeffizient ist aber

$$\begin{aligned}
\underbrace{\binom{|A| + |B| - 3}{|A| - 2}}_{x \text{ in } (x-y)} - \underbrace{\binom{|A| + |B| - 3}{|A| - 1}}_{-y \text{ in } (x-y)} &= \frac{(|A| + |B| - 3)!}{(|A| - 1)!(|B| - 1)!}[(|A| - 1) - (|B| - 1)] \\
&= \frac{(|A| + |B| - 3)!}{(|A| - 1)!(|B| - 1)!}[|A| - |B|] \\
&\not\equiv 0 \pmod{p}. \; \lightning
\end{aligned}$$

□

Es sei $V_n(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ die Determinante der $(n \times n)$-Matrix $(x_j^{i-1})_{1 \leq i,j \leq n}$. $V_n(x_1, \ldots, x_n)$ ist die sogenannte *Vandermonde-Determinante*. Beispielsweise sind

$$\begin{aligned}
V_1(x_1) &= |1| &&= 1 \\
V_2(x_1, x_2) &= \begin{vmatrix} 1 & 1 \\ x_1 & x_2 \end{vmatrix} &&= x_2 - x_1.
\end{aligned}$$

Nach dem Entwicklungssatz ist

$$V_n(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} x_i^{\sigma(i)-1}.$$

Jedoch kann man die Determinante auch cleverer ausrechnen.

[28] So hätten wir auch beim Satz 5.5 vorgehen können.

Lemma 5.7 (Vandermonde)**.**

$$V_n(x_1, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Dies macht auch Sinn: Sind zwei der x_i gleich, so ist die Determinante Null. Also müssen alle paarweisen Differenzen Teiler der Determinante sein und wegen der Größe des Grads der Determinante ist das auch alles.

Beweis. Wir beweisen die Aussage per Induktion nach n.

$n = 1$: Klar.

$n - 1 \rightsquigarrow n$: Durch Entwicklung nach der letzten Spalte erhält man $V_n(x_1, \ldots, x_n)$ als Summe von $V_{n-1}(x_1, \ldots, x_{n-1}) \cdot x_n^{n-1}$ und Termen, die in x_n kleineren Grad haben. Für $x_n = x_1, \ldots, x_{n-1}$ sind die zwei Spalten gleich und die Determinante ist Null. Fasst man $V_n(x_1, \ldots, x_n)$ als Polynom in x_n mit Koeffizienten in $\mathbb{Z}[x_1, \ldots, x_{n-1}]$ auf, so sind $x_1, \ldots, x_{n-1}$ alle Nullstellen und daher ist

$$V_n(x_1, \ldots, x_n) = V_{n-1}(x_1, \ldots, x_{n-1}) \cdot \prod_{1 \le i < n} (x_n - x_i).$$

Benutze nun die Induktionsannahme. □

Um Satz 5.6 zu verallgemeinern, müssen wir noch ein paar Vorbereitungen treffen. Die Vandermonde Determinante ist hierfür von Nutzen, denn für $A_1, \ldots, A_n \subseteq \mathbb{F}_p$ ist

$$A_1 \dot{+} \ldots \dot{+} A_n = \{a_1 + \cdots + a_n \mid (\forall\, i \in [n] \colon a_i \in A_i) \wedge V_n(a_1, \ldots, a_n) \neq 0\}.$$

Folgerung 5.8. Es seien $P_1, \ldots, P_n \in \mathbb{Z}[x]$ normierte Polynome mit $\operatorname{grad}(P_i) = i - 1$ für alle $i \in [n]$. Dann ist die Determinante der Matrix $(P_i(x_j))_{1 \le i,j \le n}$ gleich

$$\prod_{1 \le i < j \le n} (x_j - x_i).$$

Beweis. Folgt durch Anwendung von elementaren Zeilenumformungen und dem letzten Lemma. □

Setze $(x)_k = x \cdot (x-1) \cdot \ldots \cdot (x-k+1)$ für alle $k \in \mathbb{N}_0$, also $(x)_0 = 1, (x)_1 = x, \ldots$

Folgerung 5.9.

$$\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} (x_i)_{\sigma(i)-1} = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Beweis. Setze $P_i = (x)_{i-1}$ in Folgerung 5.8 ein und entwickle die Determinante. □

Lemma 5.10. Es seien $n \in \mathbb{N}$ und $m, \alpha_1, \ldots, \alpha_n \in \mathbb{N}_0$. Wenn $\alpha_1 + \cdots + \alpha_n = m + \binom{n}{2}$, dann hat $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ in $(x_1 + \cdots + x_n)^m \cdot \prod_{1 \le i < j \le n} (x_j - x_i)$ den Koeffizienten

$$\frac{m!}{\alpha_1! \cdot \ldots \cdot \alpha_n!} \cdot \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i).$$

Beweis. Für ein Monom M und ein Polynom P sei $[M]\,P$ der Koeffizient von M in P. Zum Beispiel ist nach dem Multinomialtheorem

$$[x_1^{\beta_1} \cdot \ldots \cdot x_n^{\beta_n}]\,(x_1 + \cdots + x_n)^m = \frac{m!}{\beta_1! \cdot \ldots \cdot \beta_n!},$$

wann immer $\beta_1 + \cdots + \beta_n = m$, wobei $\frac{m!}{\beta_1! \cdot \ldots \cdot \beta_n!} := 0$ falls $\beta_i \notin \mathbb{N}_0$ für ein $i \in [n]$ gilt. Wegen $\prod_{1 \le i < j \le n}(x_j - x_i) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^n x_i^{\sigma(i)-1}$ ist der gesuchte Koeffizient

$$\begin{aligned}
&\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \left[x_1^{\alpha_1 - \sigma(1)+1} \cdot \ldots \cdot x_n^{\alpha_n - \sigma(n)+1}\right] (x_1 + \cdots + x_n)^m \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot \frac{m!}{(\alpha_1 - \sigma(1) + 1)! \cdot \ldots \cdot (\alpha_n - \sigma(n) + 1)!} \\
&= \frac{m!}{\alpha_1! \cdot \ldots \cdot \alpha_m!} \cdot \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^n (\alpha_i)_{\sigma(i)-1} \\
&= \frac{m!}{\alpha_1! \cdot \ldots \cdot \alpha_m!} \cdot \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)\,.
\end{aligned}$$

Damit wäre der Beweis vollbracht. □

Satz 5.11. Es seien $A_1, \ldots, A_n \subseteq \mathbb{F}_p$ nicht-leer. Wenn $|A_1|, \ldots, |A_n|$ paarweise verschieden sind, dann ist

$$|A_1 \dot{+} \ldots \dot{+} A_n| \ge \min\left(\sum_{i=1}^n |A_i| - \binom{n+1}{2} + 1, p\right).$$

Beweis. O.B.d.A. sei $\sum_{i=1}^n |A_i| \le p + \binom{n+1}{2} - 1$, da wir sonst Elemente löschen können.

Annahme. Es gibt $C \subseteq \mathbb{F}_p$ mit $A_1 \dot{+} \ldots \dot{+} A_n \subseteq C$ und $|C| = \sum_{i=1}^n |A_i| - \binom{n+1}{2} < p$.

Setze

$$P(x_1, \ldots, x_n) = \prod_{c \in C} (x_1 + \cdots + x_n - c) \prod_{1 \le i < j \le n} (x_j - x_i).$$

Dann hat P Grad $|C| + \binom{n}{2} = \sum_{i=1}^n |A_i| - n$ und $P(a_1, \ldots, a_n) = 0$ für alle $(a_1, \ldots, a_n) \in A_1 \times \cdots \times A_n$. Nach dem kombinatorischen Nullstellensatz gilt also

$$\left[x_1^{|A_1|-1} \cdot \ldots \cdot x_n^{|A_n|-1}\right] P = 0.$$

Doch dieser Koeffizient ist nach Lemma 5.10

$$\frac{|C|!}{\prod_{i=1}^n (|A_i| - 1)!} \cdot \prod_{1 \le i < j \le n} (|A_j| - |A_i|) \not\equiv 0 \pmod p. \; \lightning$$ □

Die Schranke ist optimal wie $A_i = \{1, 2, \ldots, |A_i|\}$ für alle $i \in [n]$ zeigt. Wenn nämlich o.B.d.A. $|A_1| < \cdots < |A_n|$ gilt, so entspricht jede mit $\dot{+}$ schreibbare Summe eindeutig einer strikt monotonen Folge $(a_i)_{i\in[n]}$ mit $a_i \in A_i$ für alle $i \in [n]$. Insbesondere ist

$$A_1 \dot{+} \ldots \dot{+} A_n = \left[\sum_{i=1}^{n} i, \sum_{i=1}^{n} |A_i|\right].$$

Folgerung 5.12. Es seien $A \subseteq \mathbb{F}_p$ und $n \in \mathbb{N}$. Wenn $|A| \geq n$, dann

$$|\underbrace{A \dot{+} \ldots \dot{+} A}_{n}| \geq \min\left\{n\,|A| - n^2 + 1, p\right\}.$$

Beweis. Es seien $a_1, \ldots, a_{n-1} \in A$ paarweise verschieden. Setze $A_i = A \setminus \{a_i, \ldots, a_{n-1}\}$ für alle $i \in [n]$. Wegen $|A_i| = |A| - (n-i)$ sind $|A_1|, \ldots, |A_n|$ paarweise verschieden. Aus Satz 5.11 folgt also

$$\begin{aligned}
|A \dot{+} \ldots \dot{+} A| &\geq |A_1 \dot{+} \ldots \dot{+} A_n| \\
&\geq \min\left\{\sum_{i=1}^{n} (|A| - (n-i)) - \binom{n+1}{2} + 1, p\right\} \\
&= \min\left\{n\,|A| - n^2 + 1, p\right\}.
\end{aligned}$$

□

6 Der Satz von Chevalley-Warning

Der Satz dieses Abschnitts wurde von Warning vermutet und letztlich von Chevalley bewiesen.

Lemma 6.1. Für $0 \leq i \leq p-2$ ist $\sum_{x\in\mathbb{F}_p} x^i = 0$.

Beweis. Setze $S_i = \sum_{x\in\mathbb{F}_p} x^i$. Wähle $i \geq 0$ minimal mit $S_i \neq 0$.

Annahme. $i \leq p-2$.

Da $x \mapsto x+1$ eine Permutation von $\mathbb{F}_p$ ist, gilt nach dem binomischen Lehrsatz

$$\begin{aligned}
S_{i+1} &\equiv_p \sum_{x\in\mathbb{F}_p} (x+1)^{i+1} \\
&= \sum_{x\in\mathbb{F}_p} \left(x^{i+1} + \binom{i+1}{1} x^i + \cdots + 1\right) \\
&= S_{i+1} + \binom{i+1}{1} S_i + \underbrace{\binom{i+1}{2} S_{i-1} + \ldots}_{=0 \text{ nach Minimalität von } i},
\end{aligned}$$

das heißt $(i+1) \cdot S_i \equiv 0 \pmod{p}$. Da aber $i+1 \not\equiv 0 \pmod{p}$ gilt, folgt $S_i = 0$. ↯ □

Folgerung 6.2. Für jedes Monom $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ vom Grad $\alpha_1 + \cdots + \alpha_n < n \cdot (p-1)$ ist

$$\sum_{(x_1,\ldots,x_n)\in\mathbb{F}_p^n} x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} = 0.$$

Beweis. Die linke Seite ist

$$\sum_{x_1\in\mathbb{F}_p} x_1^{\alpha_1} \cdot \ldots \cdot \sum_{x_n\in\mathbb{F}_p} x_n^{\alpha_n}.$$

Nach dem Schubfachprinzip gibt es ein $i \in [n]$ mit $\alpha_i \leq p-2$. Also ist nach Lemma 6.1 der zugehörige Faktor Null. □

Satz 6.3 (Chevalley-Warning)**.** Es seien $P_1, \ldots, P_m \in \mathbb{F}_p[x_1, \ldots, x_n]$. Wenn die Summe der Grade von $P_1, \ldots, P_m$ kleiner als n ist, dann ist die Anzahl der gemeinsamen Nullstellen von $P_1, \ldots, P_m$ (in $\mathbb{F}_p^n$) durch p teilbar.

Der Satz ist in einem gewissen Sinne optimal. So hat $P_i = x_i$ ($i \in [n]$) nur die triviale Lösung als Nullstelle.

Beweis. Setze

$$Q(x_1, \ldots, x_n) = \prod_{j=1}^{m} \left(1 - P_j(x_1, \ldots, x_n)^{p-1}\right).$$

Wenn $(x_1, \ldots, x_n) \in \mathbb{F}_p^n$ eine gemeinsame Nullstelle von $P_1, \ldots, P_m$ ist, dann gilt

$$Q(x_1, \ldots, x_n) = 1.$$

Andernfalls ist $Q(x_1, \ldots, x_n) = 0$ (nach dem kleinen Satz von Fermat).
Es sei Ω die Anzahl der gemeinsamen Nullstellen von $P_1, \ldots, P_m$. In $\mathbb{F}_p$ gilt dann

$$\Omega \equiv \sum_{(x_1,\ldots,x_n)\in\mathbb{F}_p^n} Q(x_1, \ldots, x_n) \pmod{p}.$$

Multipliziert man nun Q aus, so stellt man fest, dass jedes in Q vorkommende Monom $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ höchstens den Grad $(p-1)\sum_{j=1}^{m} \operatorname{grad}(P_j) < (p-1) \cdot n$ hat.
Nach Folgerung 6.2 gilt also $\Omega \equiv 0 \pmod{p}$. □

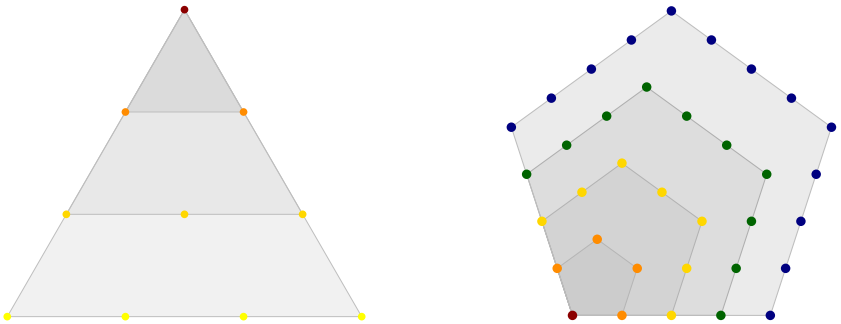
Folgerung 6.4. Für jede Primzahl p gibt es $x, y, z \in \mathbb{Z}$, die nicht alle durch p teilbar sind, mit $p \mid x^2 + y^2 + z^2$.

Hieraus kann man den 4-Quadrate-Satz von Lagrange folgern:

Jede natürliche Zahl ist Summe von 4 Quadratzahlen[29]*.*

Im Allgemeinen kann man sich fragen, ob jede natürliche Zahl Summe von drei Dreieckszahlen, Summe von fünf Fünfeckszahlen ist etc. Tatsächlich ist das immer wahr.[30]

[29] Wir zählen Null als Quadratzahl.
[30] Der Fall mit drei Dreieckszahlen sei am schwierigsten.



(a) Die Dreieckszahlen (b) Die Fünfeckszahlen

Satz 6.5 (Erdős, Ginzburg, Ziv)**.** Für alle $a_1, \ldots, a_{2n-1} \in \mathbb{Z}$ gibt es $I \subseteq \{1, \ldots, 2n-1\}$ mit $|I| = n$ und $n \mid \sum_{i \in I} a_i$.

Beweis.

Schritt 1: Wir zeigen dies zuerst, wenn $n = p$ eine Primzahl ist. Betrachte hierfür

$$x_1^{p-1} + \ldots + x_{2p-1}^{p-1} = 0, \tag{1}$$
$$a_1 x_1^{p-1} + \ldots + a_{2p-1} x_{2p-1}^{p-1} = 0. \tag{2}$$

Nach dem Satz von Chevalley-Warning ist die Anzahl der Lösungen

$$(x_1, \ldots, x_{2p-1}) \in \mathbb{F}_p^{2p-1}$$

durch p teilbar. Also gibt es auch eine nicht-triviale Lösung $(x_1, \ldots, x_{2p-1})$. Setze $I = \{i \mid x_i \not\equiv 0 \pmod p\}$. Nach (1) ist $p \mid |I|$, das heißt $|I| = p$. Nach (2) ist außerdem $p \mid \sum_{i \in I} a_i$.

Schritt 2: Für $n \in \mathbb{N}$ sei EGZ(n) die Aussage aus Satz 6.5. Wir zeigen

$$(\text{EGZ}(m) \wedge \text{EGZ}(n)) \implies \text{EGZ}(mn).$$

Seien $a_1, \ldots, a_{2mn-1}$ gegeben.

Nach EGZ(m) gelte o.B.d.A. für gewisse $b_1, \ldots, b_{2n-1} \in \mathbb{Z}$, sodass

$$\begin{aligned} a_1 + \cdots + a_m &= m \cdot b_1 \\ a_{m+1} + \cdots + a_{2m} &= m \cdot b_2 \\ &\vdots \\ a_{(2n-2)m+1} + \cdots + a_{(2n-1)m} &= m \cdot b_{2n-1}. \end{aligned}$$

Nach EGZ(n) gelte o.B.d.A. $b_1 + \cdots + b_n = n \cdot c$ mit $c \in \mathbb{Z}$. Nun ist

$$a_1 + \cdots + a_{mn} = m(b_1 + \cdots + b_n) = mnc. \qquad \square$$

Die $2n-1$ im Satz ist außerdem optimal wie

$$a_1 = \cdots = a_{n-1} = 0, a_n = \cdots = a_{2n-2} = 1$$

für $2n-2$ zeigt.
Der ursprüngliche Beweis von Satz 6.5 hat dieselbe Fallunterscheidung gemacht, aber auch den Primfall auf kombinatorische Weise gelöst. Unser Beweis liefert im Primfall dafür mehr als bloß die Existenz.

Bemerkung 6.6. Es sei $m = p$ prim. Ferner seien $a_1, \ldots, a_{2p-1} \in \mathbb{Z}$. Schließlich sei Ω die Anzahl der Mengen $I \subseteq \{1, \ldots, 2p-1\}$ mit $|I| = p, p \mid \sum_{i \in I} a_i$. Jede solche Menge entspricht nun $(p-1)^p$ Lösungen unseres Gleichungssystems (1) - (2). Insgesamt hat das Gleichungssystem also $1 + (p-1)^p \cdot \Omega$ Lösungen.
Nach Satz 6.3 ist also $0 \equiv 1 + (p-1)^p \cdot \Omega \equiv 1 - \Omega \pmod{p}$, das heißt $\Omega \equiv 1 \pmod{p}$.

Man kann die Aussage wie folgt interpretieren: Man stelle sich $\mathbb{Z}$ als eindimensionales Gitter vor. Dann besagt Satz 6.5, dass für jede Folge von $2n-1$ Punkten $a_1, \ldots, a_{2n-1} \in \mathbb{Z}$ es eine Teilmenge $I = \{i_1, \ldots, i_n\} \subseteq [2n-1]$ gibt, sodass der *Schwerpunkt* $(a_{i_1} + \cdots + a_{i_n})/n$ wieder ein Gitterpunkt ist. Das Problem lässt sich damit auf natürliche Weise für $\mathbb{Z}^2$ übertragen. Genauer hat Kemnitz vermutet:

Für jede Folge $P_1, \ldots, P_{4n-3} \in \mathbb{Z}^2$ gibt es eine Menge $I \subseteq \{1, \ldots, 4n-3\}$ mit $|I| = n$ und $n \mid \sum_{i \in I} P_i$.

Hier ist $4n-3$ optimal: Wenn man für $a_1, \ldots, a_{4n-4} \in \mathbb{Z}^2$ je $n-1$ mal die Ecken des Einheitsquadrats $\{0,1\}^2$ wählt, so gibt es keine Teilmenge $I \subseteq [4n-4], |I| = n$, sodass $\sum_{i \in I} a_i/n \notin \mathbb{Z}^2$.

Tatsächlich ist die Kemnitz-Vermutung korrekt und wir werden dies im Folgenden beweisen.[31] Das Produkt-Argument übeträgt sich dabei, das heißt es genügt, den Fall $n = p$ prim zu lösen. Für $p = 2$ geht der Beweis so:

Beweis der Kemnitz-Vermutung für $p = 2$. Gegeben seien $P_1, \ldots, P_5 \in \mathbb{Z}^2$. Nach Schubfachprinzip gibt es $i \neq j$ derart, dass beide Koordinaten von $P_i, P_j \pmod 2$ übereinstimmen. Dann tut es $I = \{i, j\}$. □

Für den Rest des Kapitels sei p immer eine ungerade Primzahl. Es sei $A = A_1, \ldots$ eine Folge von Punkten des Gitters $\mathbb{Z}^2$. $|A|$ sei die *Länge* von A. Weiter sei $(n \mid A)$ die Anzahl der n-gliedrigen Teilfolgen B von A mit $\sum B \equiv (0,0) \pmod{p}$. Ein Gegenbeispiel zur Kemnitz-Vermutung ist also eine Folge X mit $|X| = 4p-3$ und $(p \mid X) = 0$.

Lemma 6.7. Für alle A mit $|A| \in \{3p-2, 3p-1\}$ ist

$$1 - (p \mid A) + (2p \mid A) \equiv 0 \pmod{p}.$$

[31] Genauer hat dies tatsächlich Reiher persönlich 2003 gezeigt.

Beweis. A bestehe aus den Punkten $(a_1, b_1), \ldots, (a_n, b_n)$, wobei $n \in \{3p-2, 3p-1\}$. Betrachte die Gleichungen (in $\mathbb{F}_p$)

$$\sum_{i=1}^{n} x_i^{p-1} = 0, \sum_{i=1}^{n} a_i x_i^{p-1} = 0, \sum_{i=1}^{n} b_i x_i^{p-1} = 0.$$

Die Anzahl der gemeinsamen Lösungen ist

$$1 + (p-1)^p \cdot (p \mid A) + (p-1)^{2p} \cdot (2p \mid A).$$

Nach Satz 6.3 ist also

$$1 + (p-1)^p \cdot (p \mid A) + (p-1)^{2p} \cdot (2p \mid A) \equiv 0 \pmod{p}. \qquad \square$$

Bemerkung 6.8. Für A mit $|A| = 4p-2$ ist analog $1-(p \mid A)+(2p \mid A)-(3p \mid A) \equiv_p 0$.

Lemma 6.9 (Alon-Dubiner)**.** Für alle A mit $|A| = 3p$ mit $\sum A \equiv (0,0) \pmod{p}$ gilt $(p \mid A) > 0$.

Beweis. Es sei B eine Teilfolge von A mit $|B| = 3p-1$. Nach Lemma 6.7 ist $(p \mid B) \neq 0$ oder $(2p \mid B) \neq 0$. Nur der Fall $(2p \mid B) \neq 0$ ist interessant. Sei C die Teilfolge von B mit $|C| = 2p$ und $\sum C \equiv (0,0) \pmod{p}$. Nun ist $A \setminus C$ wie gewünscht. $\square$

Satz 6.10. Für alle A mit $|A| = 4p-2$ ist

$$2 - (p \mid A) + (3p \mid A) \equiv 0 \pmod{p}.$$

Beweis. Nach Lemma 6.7 ist

$$\sum_{B \subseteq A, |B| = 3p-2} (1 - (p \mid B) + (2p \mid B)) \equiv 0 \pmod{p}.$$

Kombinatorisch sieht man, dass

$$\sum_{B \subseteq A, |B| = 3p-2} 1 = \binom{4p-2}{3p-2}$$

$$\sum_{B \subseteq A, |B| = 3p-2} (p \mid B) = \binom{3p-2}{2p-2} (p \mid A)$$

$$\sum_{B \subseteq A, |B| = 3p-2} (2p \mid B) = \binom{2p-2}{p-2} (2p \mid A)$$

Die linke Seite lässt sich also wie folgt umschreiben:

$$\binom{4p-2}{3p-2} - \binom{3p-2}{2p-2}(p \mid A) + \binom{2p-2}{p-2}(2p \mid A) \equiv 0 \pmod{p}.$$

Dabei ist

$$\binom{4p-2}{3p-2} = \frac{(4p-2) \cdot \ldots \cdot (3p+1) \cdot 3p \cdot (3p-1)}{1 \cdot \ldots \cdot (p-1) \cdot p} \equiv 3 \pmod{p}$$

und analog $\binom{3p-2}{2p-2} \equiv 2 \pmod{p}$, $\binom{2p-2}{p-2} \equiv 1 \pmod{p}$. Subtrahiere Bemerkung 6.8. $\square$

Beweis der Kemnitz-Vermutung. Es genügt den Primfall $n = p \geq 3$ zu behandeln.

Annahme. Es gibt $|A| = 4p - 3$ mit $(p \mid A) = 0$.

Wir wissen $(3p \mid A) = 0$ nach Lemma 6.9. Es entstehe B aus A, indem man den Punkt $(0, 0)$ anhängt. Nach Satz 6.10 gilt

$$2 - \underbrace{(p \mid A)}_{=0} - (p-1 \mid A) + \underbrace{(3p \mid A)}_{=0} + (3p-1 \mid A) \equiv 0 \pmod{p}.$$

Dies zeigt $(p-1 \mid A) \not\equiv (3p-1 \mid A) \pmod{p}$.
Es sei χ die Anzahl der Zerlegungen $A = X \mathbin{\dot\cup} Y \mathbin{\dot\cup} Z$ mit $|X| = p-1, |Y| = p-2, |Z| = 2p$ mit $\sum X \equiv \sum Z \equiv (0,0) \pmod{p}$. Insbesondere ist $\sum Y \equiv \sum A$.
Dann ist

$$\chi = \sum_{\text{erlaubte } X} \underbrace{(2p \mid \underbrace{A \setminus X}_{\text{hat Länge } 3p-2})}_{\equiv -1 \pmod{p} \text{ nach Lemma 6.7}} \equiv -(p-1 \mid A) \pmod{p}.$$

Andererseits gilt aber

$$\chi = \sum_{\text{erlaubte } Y} \underbrace{(2p \mid \underbrace{A \setminus Y}_{\text{hat Länge } 3p-1})}_{\equiv -1 \pmod{p} \text{ nach Lemma 6.7}} \equiv -(3p-1 \mid A) \pmod{p}. \lightning \qquad \square$$

7 Snevilys Vermutung

In diesem Kapitel befassen wir uns mit der Vermutung von Hunter Snevily, über dem sonst nicht viel bekannt ist.[32]

Vermutung 7.1 (Snevily)**.** Es sei G eine (additive) abelsche Gruppe ungerader Ordnung und $A, B \subseteq G$ seien gleichmächtig. Dann gibt es eine Bijektion $\varphi\colon A \to B$ derart, dass die $a + \varphi(a)$ mit $a \in A$ paarweise verschieden sind.

Die Vermutung ist für Gruppen gerader Ordnung falsch:
Wenn $n \in \mathbb{N}$ gerade ist und $A = B = G = \mathbb{Z}/n\mathbb{Z}$, dann gibt es keine solche Bijektion, denn sonst wäre

$$\sum_{a \in G} a = \sum_{a \in G} (a + \varphi(a)),$$

das heißt $\sum_{a \in G} a = 0$, also

$$n \mid \frac{(n-1)n}{2}. \lightning$$

Alon zeigte die Vermutung für den Spezialfall $G = \mathbb{F}_p$ für irgendeine ungerade Primzahl p. Hierfür brauchen wir folgendes Resultat.

[32] „Korrupt war er aber nicht." – Christian Reiher, 11. Januar 2023

Satz 7.2 (Dysons[33] Vermutung)**.** Für alle $a_1, \ldots, a_n \in \mathbb{N}_0$ hat das Monom $\prod_{i=1}^{n} x_i^{(n-1)a_i}$ in $\prod_{i \neq j}(x_j - x_i)^{a_j}$ den (Multinomial-) Koeffizienten

$$\frac{(a_1 + \cdots + a_n)!}{a_1! \cdot \ldots \cdot a_n!} \left[= \binom{a_1 + \cdots + a_n}{a_1, \ldots, a_n} \right].$$

Für $n = 2$ steht da:

„$x_1^{a_1} x_2^{a_2}$ *hat in* $(x_1 - x_2)^{a_1}(x_2 - x_1)^{a_2}$ *den Koeffizient* $(a_1 + a_2)!/(a_1!a_2!)$.“

Dies kann man sich schnell mit dem binomischen Lehrsatz erschließen.

Beweis von Satz 7.2. Es sei $F(a_1, \ldots, a_n)$ der gesuchte Koeffizient. Wir machen eine Induktion nach $n + \sum_{i=1}^{n} a_i$.

Fall 1: $n = 1$. Dann ist $F(a_1) = 1 = a_1!/a_1!$. ✓

Fall 2: $n \geq 2$ und es gibt ein $i \in [n]$ mit $a_i = 0$. O.B.d.A. sei $a_n = 0$. Dann ist

$$\prod_{i \neq j}(x_j - x_i)^{a_j} = \prod_{\substack{i \neq j, \\ i,j<n}} (x_j - x_i)^{a_j} \cdot \prod_{j=1}^{n-1} (x_j - x_n)^{a_j}.$$

Also ist $F(a_1, \ldots, a_n)$ der Koeffizient von $\prod_{i=1}^{n-1} x_i^{(n-1)a_i}$ in

$$\prod_{\substack{i \neq j, \\ i,j<n}} (x_j - x_i)^{a_j} \cdot \prod_{i=1}^{n-1} x_i^{a_i}.$$

Dies ist der Koeffizient von $\prod_{i=1}^{n-1} x_i^{(n-2)a_i}$ in $\prod_{i \neq j, 1 \leq i,j<n}(x_j - x_i)^{a_i}$, das heißt

$$F(a_1, \ldots, a_{n-1}, 0) = F(a_1, \ldots, a_{n-1}).$$

Nach Induktionsannahme folgt

$$F(a_1, \ldots, a_{n-1}, 0) = \frac{(a_1 + \cdots + a_{n-1})!}{a_1! \cdot \ldots \cdot a_{n-1}!}. \checkmark$$

Fall 3: $n \geq 2$ und $a_i \geq 1$ für alle $i \in [n]$. Es gilt

$$\sum_{j=1}^{n} \prod_{i \neq j} \frac{y - z_i}{z_j - z_i} = 1,$$

denn: Betrachte die linke Seite als Polynom $P(y)$ in y.[34] Dann ist $\operatorname{grad}(P) = n-1$ und $P(y) - 1$ hat die Nullstellen $z_1, \ldots, z_n$.

[33] Freeman J. Dyson

[34] Stichwort: Lagrange Interpolation.

Für $y = 0$ ergibt sich

$$\sum_{j=1}^{n} \prod_{i \neq j} \frac{-z_i}{z_j - z_i} = 1.$$

Für $z_i = 1/x_i$ ist

$$\frac{-z_i}{z_j - z_i} = -\frac{\frac{1}{x_i}}{\frac{1}{x_j} - \frac{1}{x_i}} = -\frac{\frac{1}{x_i}}{\frac{x_i - x_j}{x_i x_j}} = -\frac{x_j}{x_i - x_j} = \frac{x_j}{x_j - x_i}.$$

Somit ist

$$\sum_{j=1}^{n} \frac{x_j^{n-1}}{\prod_{i \neq j}(x_j - x_i)} = 1.$$

Multiplizieren wir beide Seiten mit $\prod_{i' \neq j'}(x_{j'} - x_{i'})^{a_{j'}}$, so erhalten wir

$$\prod_{i' \neq j'} (x_{j'} - x_{i'})^{a_{j'}} = \sum_{j=1}^{n} x_j^{n-1} \prod_{i' \neq j' \neq j} (x_{j'} - x_{i'})^{a_{j'}} \cdot \prod_{i \neq j} (x_j - x_i)^{a_j - 1}.$$

Folglich gilt

$$F(a_1, \ldots, a_n) = \sum_{j=1}^{n} F(a_1, \ldots, a_{j-1}, a_j - 1, a_{j+1}, \ldots, a_n).$$

Nach der Induktionsannahme ist schließlich

$$F(a_1, \ldots, a_n) = \sum_{j=1}^{n} \frac{a_j}{a_j} \cdot \frac{(a_1 + \cdots + a_n - 1)!}{a_1! \cdot \ldots \cdot (a_j - 1)! \cdot \ldots \cdot a_n!} = \frac{(a_1 + \cdots + a_n)!}{a_1! \cdot \ldots \cdot a_n!}. \quad \square$$

Einen rein kombinatorischen Beweis der Aussage erbrachte Doron Zeilberger in *A combinatorial proof of Dyson's conjecture (1982).*

Folgerung 7.3. Der Koeffizient von $\prod_{i=1}^{n} x_i^{n-1}$ in $\prod_{i \neq j}(x_j - x_i)$ ist $n!$.

Beweis. Setze $a_1 = \cdots = a_n = 1$ in Satz 7.2 ein. $\square$

Satz 7.4 (Alon)**.** Es seien p eine Primzahl, $k < p$ und $a_1, \ldots, a_k \in \mathbb{F}_p$. Für alle k-elementigen $B \subseteq \mathbb{F}_p$ gibt es eine Bijektion $\varphi\colon [k] \to B$ derart, dass die $a_i + \varphi(i)$ paarweise verschieden sind.

Das Problem für gerade p (also $p = 2$) wird umgangen mit der Forderung $k < p$.

Beweis. Betrachte

$$P(x_1, \ldots, x_k) = \prod_{1 \leq i < j \leq k} (x_j - x_i)(x_i - x_j + a_i - a_j) = \prod_{1 \leq i < j \leq k} (x_j - x_i)\left((a_i + x_i) - (a_j + x_j)\right)$$

über $\mathbb{F}_p$. Die Koeffizienten von $(x_1 \cdot \ldots \cdot x_k)^{k-1}$ ist nach Folgerung 7.3 $k! \not\equiv 0 \pmod{p}$, da $\operatorname{grad}(P) = k \cdot (k-1)$. Nach Alons Nullstellensatz gibt es $b_1, \ldots, b_k \in B$ mit

$$P(b_1, \ldots, b_k) \neq 0.$$

Für alle $i \neq j$ ist nun $b_i \neq b_j, a_i + b_i \neq a_j + b_j$. Daher ist $i \mapsto b_i$ die gesuchte Bijektion. $\square$

Beachte, dass die Aussage etwas stärker als Snevilys Vermutung ist, da hier die $a_1, \ldots, a_k$ nicht unbedingt paarweise verschieden sein müssen. Setzen wir $a_1, \ldots, a_k$ als paarweise verschieden voraus wie in der Vermutung, so sei außerdem angemerkt, dass für ungerade p auch $k = p$ zulässig ist, da $x \mapsto 2x$ dann eine Permutation von $\mathbb{F}_p$ ist.

Da wir ein paar weitere Mittel brauchen für die Vermutung, folgt jetzt eine Wiederholung von einigen Fakten aus der Algebra und Zahlentheorie.

Wiederholung: Algebra und Zahlentheorie

Wir werden folgende Fakten ohne Beweis nutzen.[35]

1. Wenn $a, m \in \mathbb{N}$ teilerfremd sind, dann gibt es $t \in \mathbb{N}$ mit $a^t \equiv 1 \pmod{m}$. ($t = \varphi(m)$ hat diese Eigenschaft, wobei φ die eulersche Phi-Funktion ist.)
2. Jede endliche, abelsche Gruppe G ist zu einem Produkt $(\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_r\mathbb{Z})$ isomorph, wobei $d_1, \ldots, d_r \in \mathbb{N}$.
3. Für jede Primzahlpotenz p^r gibt es einen Körper $\mathbb{F}_{p^r}$, der p^r Elemente hat. Zum Beispiel ist $\mathbb{F}_{p^r}$ der Zerfällungskörper[36] von $X^{p^r} - X$ über $\mathbb{F}_p$. Außerdem ist $(\mathbb{F}_{p^r}^\times, \cdot)$ zyklisch.
4. Es seien G eine Gruppe und F ein Körper. Ein *Charakter* von G in F ist ein Gruppenhomomorphismus $G \to (F^\times, \cdot)$.

Satz 7.5 (Artin)**.** Es seien G eine Gruppe und F ein Körper. Die Charaktere von G in F sind linear unabhängig (im F-Vektorraum aller Funktionen von G nach F).

Beweis. Sonst gäbe es Charaktere $\chi_1, \ldots, \chi_n$ und $\lambda_1, \ldots, \lambda_n \neq 0$ derart, dass

$$\sum_{i=1}^{n} \lambda_i \cdot \chi_i(x) = 0$$

für alle $x \in G$. Wähle dabei die Charaktere so, dass n minimal ist. Es gilt $n \geq 2$.[37] Wähle $a \in G$ mit $\chi_1(a) \neq \chi_2(a)$. Für alle $x \in G$ ist nun

$$\sum_{i=1}^{n} \lambda_i \cdot \chi_i(ax) - \chi_1(a) \sum_{i=1}^{n} \lambda_i \cdot \chi_i(x) = 0,$$

das heißt

$$\sum_{i=2}^{n} \lambda_i \cdot (\chi_i(a) - \chi_1(a))\chi_i(x) = 0$$

wegen $\chi_i(ax) = \chi_i(a)\chi_i(x)$. Nach Minimalität von n sind die Koeffizienten Null, aber

$$\lambda_2(\chi_2(a) - \chi_1(a)) \neq 0. \; \lightning$$ □

[35] Als Referenz kann beispielsweise das Algebra-Skript von Dr. Christoph Schweigert dienen.
[36] Ein möglichst kleiner Körper, in dem ein gegebenes Polynom in Linearfaktoren zerfällt.
[37] Wir bilden ja in $(F^\times, \cdot)$ ab.

Wir betreiben jetzt eine Fourier-Analyse, die diskreter als diskrete Fourier-Analysis ist.

Satz 7.6. Es seien G eine endliche, abelsche Gruppe und F ein endlicher Körper mit $|G| \mid |F^\times|$. Dann bilden die Charaktere von G in F eine Basis des F-Vektorraums aller Abbildungen von G nach F.

Beweis. Setze $n = |G|$. Nach Satz 7.5 genügt es, n Charaktere von G nach F anzugeben. Es existieren $d_1, \dots, d_r \in \mathbb{N}$, sodass

$$G \cong (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_r\mathbb{Z})$$

Für alle $i \in [r]$ ist $d_i \mid |G| \mid |F^\times|$ und $F^\times$ ist zyklisch. Wähle $\xi_i \in F^\times$ mit Ordnung d_i. Für alle $a_1, \dots, a_r$ mit $0 \le a_i < d_i$ ist

$$(b_1 + d_1\mathbb{Z}, \dots, b_r + d_r\mathbb{Z}) \mapsto \prod_{i=1}^{r} \xi_i^{a_i b_i}$$

ein Charakter von G in F.
Hierdurch erhalten wir $\prod_{i=1}^{n} d_i = n$ verschiedene Charaktere. □

Man kann die Bedingungen etwas relaxieren, sodass aber weiterhin $d_i \mid |G| \mid |F^\times|$ gilt.

Lemma 7.7. Es seien F ein Körper, $k < |F|$ und A eine $(k \times k)$-Matrix mit Einträgen aus $z_1, \dots, z_m$. In keiner Zeile oder Spalte von A seien zwei gleiche Einträge. Dann kann man die Variablen so durch Elemente $\xi_1, \dots, \xi_m \in F$ ersetzen, dass $\det(A) \neq 0$.

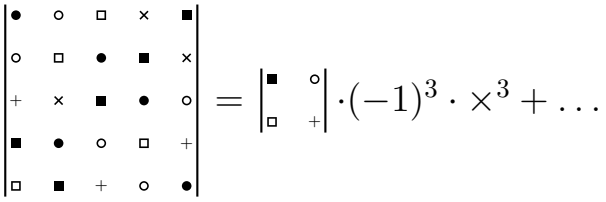


Abbildung 20: Beweisskizze zu Lemma 7.7

Beweis. O.B.d.A. komme z_1 genau $t \ge 1$ mal vor. Dabei ist $t \le k$. Dann gilt

$$\det(A) = \pm \det(A') \cdot z_1^t + o(z_1^t),$$

wobei A' eine $(k-t) \times (k-t)$-Matrix mit den gleichen Eigenschaften ist. Nach Induktionsannahme gibt es $\xi_2, \dots, \xi_m$ mit $\det(A') \neq 0$. Ersetzen wir also für $i = 2, \dots, m$ z_i durch ξ_i, so ist $\det(A)$ ein Polynom in z_1 vom Grad $t \le k < |F|$.
Wähle schließlich ξ_1 passend. □

Satz 7.8 (Bodan Asovski)**.** Snevilys Vermutung ist wahr.

Beweis. Es seien G eine abelsche Gruppe von ungerader Ordnung n und

$$A = \{a_1, \ldots, a_k\}, B = \{b_1, \ldots, b_k\}$$

seien Teilmengen von G. Wähle $m \in \mathbb{N}$ mit $n \mid 2^m - 1$[38] und setze $F = \mathbb{F}_{2^m}$.
Ordne jedem $g \in G$ eine Variable z_g zu und betrachte die $(k \times k)$-Matrix $(z_{a_i+b_j})_{1\leq i,j\leq k}$. In keiner Zeile oder Spalte kommt eine Variable doppelt vor. Wegen $k \leq n < 2^m$ gibt es nach Lemma 7.7 $\varphi\colon G \to F$ derart, dass

$$\det((\varphi(a_i + b_j))_{1\leq i,j\leq k}) \neq 0.$$

Wegen $|G| \mid |F^\times|$ gibt es Charaktere $\chi_1, \ldots, \chi_n$ von G in F, die eine Basis des F-Vektorraums aller Funktionen von G nach F bilden. Es gibt also $\lambda_1, \ldots, \lambda_m \in F$ mit $\varphi = \sum_{i=1}^n \lambda_i \cdot \chi_i$. Nun ist

$$\begin{aligned}\det((\varphi(a_i + b_j))_{1\leq i,j\leq k}) &= \det\left(\sum_{t=1}^n \lambda_t \cdot \chi_t(a_i + b_j)\right)_{1\leq i,j\leq k} \\ &= \sum_{t_1=1}^n \ldots \sum_{t_k=1}^n \lambda_{t_1} \cdots \lambda_{t_k} \det(\chi_{t_i}(a_i + b_j))_{1\leq i,j\leq k},\end{aligned}$$

wobei die letzte Gleichheit aus der Linearität von $\det(\cdot)$ in Abhängigkeit der Zeilen folgt. Hier ist immer $\chi_{t_i}(a_i + b_j) = \chi_{t_i}(a_i) \cdot \chi_{t_i}(b_j)$. Wenn also etwa $t_i = t_{i'}$ für $i \neq i'$ gilt, sind die i-te und i'-te Zeile linear abhängig, das heißt die Determinante ist Null.
Daher ist

$$\det((\varphi(a_i + b_j))_{1\leq i,j\leq k}) = \sum_{1\leq s_1<\cdots<s_k\leq n} \lambda_{s_1} \cdots \lambda_{s_k} \sum_{\pi\in S_k} \det(\chi_{s_{\pi(i)}}(a_i + b_j))_{1\leq i,j\leq k}.$$

Es gibt also feste Zahlen $1 \leq s_1 < \cdots < s_k \leq n$ mit

$$\sum_{\pi\in S_k} \det(\chi_{s_{\pi(i)}}(a_i + b_j))_{1\leq i,j\leq k} \neq 0.$$

Setze $\varphi_i = \chi_{s_i}$ für $i \in [r]$. Nun sind $\varphi_1, \ldots, \varphi_k$ verschiedene Charaktere von G in F und

$$\sum_{\pi\in S_k} \det(\varphi_{\pi(i)}(a_i + b_j))_{1\leq i,j\leq k} \neq 0.$$

Wir werten jetzt die Determinanten aus und können dabei $\operatorname{sgn}(\cdot)$ ignorieren, da F Charakteristik 2 hat. Es ergibt sich

$$\sum_{\pi\in S_k} \sum_{\tau\in S_k} \prod_{i=1}^k \varphi_{\pi(i)}(a_i + b_{\tau(i)}) \neq 0.$$

Es gibt also eine Permutation τ mit

$$\det(\varphi_j(a_i + b_{\tau(i)})_{1\leq i,j\leq k} = \sum_{\pi\in S_k} \prod_{i=1}^k \varphi_{\pi(i)}(a_i + b_{\tau(i)}) \neq 0.$$

Insbesondere sind die Zeilen die Matrix $(\varphi_j(a_i + b_{\tau(i)})_{1\leq i,j\leq k}$ verschieden.
Daher sind die Summen $a_1 + b_{\tau(1)}, \ldots, a_k + b_{\tau(k)}$ paarweise verschieden. □

[38] Möglich, da n und 2 teilerfremd sind und wir äquivalenterweise $2^m \equiv 1 \pmod{n}$ wollen.

8 Das Kakeya-Problem

Eine kompakte Menge $K \subseteq \mathbb{R}^n$ heißt *Kakeya-Menge*[39], wenn K Einheitsstrecken in allen Richtungen enthält. Zum Beispiel ist $\bar{B}_{1/2}(0)$ eine Kakeya-Menge.

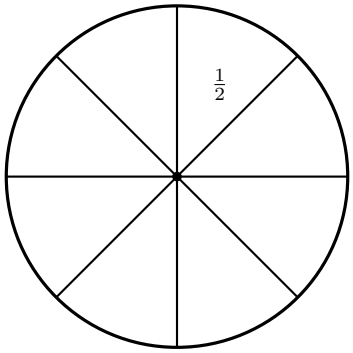


Abbildung 21: $\bar{B}_{1/2}(0)$ enthält Einheitstrecken in allen Richtungen

Wie „klein“ können jetzt Kakeya-Mengen sein? Um das Problem besser zu verstehen, brauchen wir Begriffe aus der geometrischen Maßtheorie: Für $A \subseteq \mathbb{R}^n, s \geq 0, \delta > 0$ setzen wir

$$\mathcal{H}^s_\delta(A) \coloneqq \alpha_s \cdot \inf \left\{ \sum_{i \in \mathbb{N}} \operatorname{diam}(U_i)^s \;\middle|\; A \subseteq \bigcup_{i \in \mathbb{N}} U_i, \forall\, i \in \mathbb{N} \colon \operatorname{diam}(U_i) \leq \delta \right\},$$

wobei

$$\alpha_s \coloneqq \frac{\pi^{\frac{s}{2}}}{2^s \cdot \Gamma\left(\frac{s}{2}+1\right)}.$$[40]

Diese Normierung ist notwendig, da mit U_i als Bälle tatsächlich es „bestmöglich“ ist. Für feste A, s ist weiterhin $\mathcal{H}^s_\delta(A)$ monoton wachsend für $\delta \to 0$. Daher existiert

$$\mathcal{H}^s(A) = \lim_{\delta \to 0} \mathcal{H}^s_\delta(A),$$

das sogenannte *s-dimensionale Hausdorff-Maß* von A.
Zum Beispiel ist $\mathcal{H}^n(A)$ das äußere Lebesgue-Maß von A. Man nennt $\dim_H(A) = \inf\{s \geq 0 \colon \mathcal{H}^s(A) = 0\}$ die *Hausdorff-Dimension von A*. Man kann zeigen[41], dass

$$\mathcal{H}^s(A) = \begin{cases} 0 & , s > \dim_H(A) \\ \infty & , s < \dim_H(A). \end{cases}$$

Mit anderen Worten ist das Hausdorff-Maß einer Menge nur für ihre entsprechende Hausdorff-Dimension interessant.

[39] Benannt nach dem Mathematiker Sōichi Kakeya, der diese selbst eingeführt hat.
[40] Wenn $s \in \mathbb{N}$ gilt, ist α_s das s-dimensionale Volumen des s-dimensionalen Balls mit Durchmesser 1.
[41] Dies sei dem Leser überlassen.

Vermutung 8.1 (Kakeya)**.** Jede Kakeya-Menge $K \subseteq \mathbb{R}^n$ hat Hausdorff-Dimension n.

Dieses Problem ist für $n = 1, 2$ gelöst. Vor kurzem wurde gezeigt, dass $\varepsilon > 0$ mit $\dim_H(K) \geq 5/2 + \varepsilon$ für alle Kakeya-Mengen $K \subseteq \mathbb{R}^3$ existiert. Für $n \geq 4$ weiß man

$$\dim_H(K) \geq (2 - \sqrt{2})(n-4) + 3.$$

In dieser Form werden wir uns nicht mit dem Kakeya-Problem beschäftigen: Für einen endlichen Körper F heißt $K \subseteq F^n$ *Kakeya-Menge*, wenn K Geraden in alle Richtungen enthält.

Satz 8.2 (Dvir)**.** Es seien F ein endlicher Körper und $n \in \mathbb{N}$. Für jede Kakeya-Menge $K \subseteq F^n$ gilt

$$|K| \geq \binom{|F| + n - 1}{n} \geq \frac{|F|^n}{n!}.$$

Moralisch wächst die Größe der Kakeya-Mengen mindestens in der Größenordnung $|F|^n$ mit der Normierungskonstante $1/n!$.

Beweis. Es sei $K \subseteq F^n$ eine Kakeya-Menge.

Annahme. $|K| < \binom{|F|+n-1}{n}$.

Die Anzahl der Monome $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$, dessen Grad $\alpha_1 + \cdots + \alpha_n$ höchstens $|F| - 1$ ist, beträgt (das mache man sich mit der Stars-and-Bars Methode klar)

$$\binom{|F| + n - 1}{n}.$$

Daher gibt es ein Polynom $g \in F[x_1, \ldots, x_n]$ mit $g \neq 0$ und $\operatorname{grad}(g) \leq |F| - 1$, sodass für alle $x \in K$ $g(x) = 0$ gilt, da das folgende Gleichungssystem nicht-trivial lösbar ist:

$$\forall\, (x_1, \ldots, x_n) \in K\colon \sum_{\substack{\alpha_1, \ldots, \alpha_n \in \mathbb{N}_0, \\ \alpha_1 + \cdots + \alpha_n \leq |F| - 1}} \lambda_{\alpha_1, \ldots, \alpha_n} \cdot x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} = 0.$$

Setze $d = \operatorname{grad}(g)$. Dann ist $1 \leq d \leq |F| - 1$. Es sei $\bar{g}$ die Summe aller Monome $a \cdot x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ von Grad d, die in g vorkommen. Betrachte ein beliebiges $y \in F^n$. Da K eine Kakeya-Menge ist, gibt es einen Punkt z mit

$$\{z + \lambda \cdot y\colon \lambda \in F\} \subseteq K.$$

Das Polynom $P(\lambda) = g(z + \lambda y) \in F[\lambda]$ erfüllt $\forall\, \lambda \in F\colon P(\lambda) = 0$ und $\operatorname{grad}(P) \leq d < |F|$. Somit ist $P = 0$, das heißt $\bar{g}(y)$, der Koeffizient von λ^d in P, ist Null. Dies zeigt $\bar{g}(y) = 0$ für alle $y \in F^n$. Da aber $\operatorname{grad}(\bar{g}) < |F|$ gilt, widerspricht dies dem Kombinatorischen Nullstellensatz.[42] □

[42] „Hier den Nullstellensatz zu zitieren ist wie mit Kanonen auf Spatzen schießen.“ – Christian Reiher, 18. Januar 2023, dem aber keine bessere formale Begründung einfiel.

Satz 8.3 (Schwartz, Zippel)**.** Es seien F ein endlicher Körper und $f \in F[x_1, \ldots, x_n]$ nicht das Nullpolynom. Wenn $\operatorname{grad}(f) = d$ gilt, dann ist

$$|\{(x_1, \ldots, x_n) \in F^n \colon f(x_1, \ldots, x_n) = 0\}| \leq d \cdot |F|^{n-1} .$$

Beweis. Wir führen eine Induktion nach n.

$n = 1$: Das ist bekannt.

$n - 1 \rightsquigarrow n$: O.B.d.A. komme x_n in f vor. Schreibe $f = h_0 + \cdots + h_m x_n^m$, wobei $h_0, \ldots, h_m \in F[x_1, \ldots, x_{n-1}], m \geq 1, h_m \neq 0$. Partitioniere nun

$$A = \{(x_1, \ldots, x_n) \in F^n \colon f(x_1, \ldots, x_n) = 0\}$$

in

$$A_1 = \{(x_1, \ldots, x_n) \in A \colon h_m(x_1, \ldots, x_{n-1}) \neq 0\} ,$$
$$A_2 = \{(x_1, \ldots, x_n) \in A \colon h_m(x_1, \ldots, x_{n-1}) = 0\} .$$

Für fixes $(x_1, \ldots, x_{n-1}) \in F^{n-1}, h_m(x_1, \ldots, x_{n-1}) \neq 0$, kann es höchstens m Werte für x_n geben, sodass $f(x_1, \ldots, x_{n-1}) = 0$ gilt, also

$$|A_1| \leq |F|^{n-1} \cdot m.$$

Weiter ist nach der Induktionsannahme

$$|A_2| \leq \operatorname{grad}(h_m) \cdot |F|^{n-2} \cdot |F| = \operatorname{grad}(h_m) \cdot |F|^{n-1} .$$

Da $\operatorname{grad}(h_m) \leq \operatorname{grad}(f) - m$ gilt, folgt

$$|A| = |A_1| + |A_2| \leq m \cdot |F|^{n-1} + (d - m) \cdot |F|^{n-1} \leq d \cdot |F|^{n-1} .$$

Es folgt die Behauptung. □

Es seien $\gamma, \delta \in (0, 1)$. Wir nennen $K \subseteq F^n$ eine (γ, δ)-*Kakeya-Menge*, wenn es (mindestens) $\delta |F|^n$ Geraden $l \subseteq F^n$ in paarweise verschiedene Richtungen gibt, für die $|l \cap K| \geq \gamma |F|$ gilt.

Satz 8.4 (Dvir)**.** Es seien $\gamma, \delta \in (0, 1)$, F ein endliche Körper und $n \in \mathbb{N}$. Für jede (γ, δ)-Kakeya Menge $K \subseteq F^n$ gilt $|K| \geq \binom{d+n}{n}$[43], wobei

$$d = \lfloor \min\{\gamma, \delta\} \cdot |F| \rfloor - 1.$$

Beweis. Es sei $K \subseteq F^n$ eine (γ, δ)-Kakeya-Menge.

Annahme. $|K| < \binom{d+n}{n}$.

[43] Dvir hatte ursprünglich als Schranke $\binom{d+n-1}{n-1}$, was etwas schwächer ist. Alon hat ihm aber dann einen Trick verraten.

Da es $\binom{d+n}{n}$ Monome $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ vom Grad $\alpha_1 + \cdots + \alpha_n \leq d$ gibt, existiert ein Polynom $g \in F[x_1, \ldots, x_n]$ mit $\operatorname{grad}(g) \leq d, g \neq 0$, und $g(x) = 0$ für alle $x \in K$. Setze $\bar{d} = \operatorname{grad}(g)$. Es sei $\bar{g}$ die Summe aller Monome $a \cdot x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ vom Grad $\bar{d}$, die in g vorkommen. Betrachte $y \in F^n$ derart, dass für ein $x \in F^n$ die Gerade $l = \{x + \lambda y \mid \lambda \in F\}$

$$|l \cap K| \geq \gamma |F|$$

erfüllt. Das Polynom $P(\lambda) = g(x + \lambda y)$ hat höchstens Grad $\bar{d} \leq d < \gamma |F|$, aber mindestens $\gamma |F|$ Nullstellen. Daher ist $P = 0$. Da $\lambda^{\bar{d}}$ in P den Koeffizienten $\bar{g}(y)$ hat, muss insbesondere $\bar{g}(y) = 0$ sein. Also hat $\bar{g}$ mindestens $\delta |F|^n$ Nullstellen. Dann ist aber

$$\delta |F|^n \leq \{y \in F^n \mid \bar{g}(y) = 0\} \overset{\text{Satz 8.3}}{\leq} \bar{d} \cdot |F|^{n-1} \leq d \cdot |F|^{n-1} < \delta |F|^n \,. \; \lightning \qquad \square$$

9 Äußere Produkte

Jemand hat sich wohl etwas mit Tensorprodukten gewünscht, also machen wir das jetzt.

Definition 9.1. Es seien V ein n-dimensionaler Vektorraum über F und $k \leq n$. Man nennt $\omega \colon V^k \to F$ eine *alternierende k-Form*, wenn

- $\omega(v_1, \ldots, v_k)$ bei festen $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_k$ linear in v_i ist für alle $i \in [k]$,
- $\omega(v_1, \ldots, v_k) = 0$ gilt, falls $v_i = v_j$ mit $i \neq j$.

Der F-Vektorraum der alternierenden k-Formen bezeichnen wir mit $\bigwedge^k V^*$.

Zum Beispiel ist $\bigwedge^1 V^*$ der Dualraum von V.

Bemerkung 9.2.

(1) Falls $k = 2$, $\omega \in \bigwedge^2 V^*$, ist

$$0 = \omega(v + v', v + v') = \underbrace{\omega(v, v)}_{=0} + \omega(v, v') + \omega(v', v) + \underbrace{\omega(v', v')}_{=0}$$

für alle $v, v' \in V$, das heißt $\omega(v, v') = -\omega(v', v)$.

(2) Analog gilt für $k \geq 2$: Wenn $1 \leq i < j \leq k, \omega \in \bigwedge^k V^*$, dann gilt

$$\omega(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_k) = -\omega(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_k).$$

(3) Allgemein ist

$$\omega(v_{\pi(1)}, \ldots, v_{\pi(n)}) = \operatorname{sgn}(\pi) \cdot \omega(v_1, \ldots, v_k)$$

für alle $\omega \in \bigwedge^k V^*, \pi \in S_k$ und $v_1, \ldots, v_k \in V$.

Fakt 9.3. Es seien $\alpha_1, \dots, \alpha_k \in V^*$. Dann ist

$$\begin{aligned} \omega\colon V^k &\longrightarrow F \\ (v_1, \dots, v_k) &\longmapsto \begin{Vmatrix} \alpha_1(v_1) & \dots & \alpha_1(v_k) \\ \vdots & \ddots & \vdots \\ \alpha_k(v_1) & \dots & \alpha_k(v_k) \end{Vmatrix} \end{aligned}$$

eine alternierende k-Form.[44] Wir schreiben $\omega = \alpha_1 \wedge \dots \wedge \alpha_k$.

Beweis. Da die Determinante in der i-ten Spalte linear ist, ist $\omega(v_1, \dots, v_k)$ in v_i linear. Wenn $v_i = v_j$ für $i \neq j$ gilt, hat die Determinante den Wert 0, da zwei ihrer Spalten übereinstimmen. □

Satz 9.4. Es sei $\eta_1, \dots, \eta_n \in V^*$ eine Basis von V^*. Setze $\eta_T := \eta_{t_1} \wedge \dots \wedge \eta_{t_k}$ für $T = \{t_1, \dots, t_k\} \in [n]^{(k)}, t_1 < \dots < t_k$. Dann ist $(\eta_T)_{T \in [n]^{(k)}}$ eine Basis von $\bigwedge^k V^*$. Insbesondere ist $\dim(\bigwedge^k V^*) = \binom{n}{k}$.

Beweis. Es sei $e_1, \dots, e_n \in V$ die zu $\eta_1, \dots, \eta_n$ duale Basis, das heißt es gelte

$$\eta_i(e_j) = \delta_{i,j}$$

für alle $i, j \in [n]$. Wir zeigen zuerst, dass $(\eta_T)_{T \in [n]^{(k)}}$ ein Erzeugendensystem ist. Hierfür sei $\omega \in \bigwedge^k V^*$ gegeben. Sind $v_1, \dots, v_k \in V$ beliebig, so schreibe man $v_i = \sum_{j=1}^n \alpha_{i,j} e_j$ für $i \in [k]$. Dann erhält man

$$\omega(v_1, \dots, v_k) = \sum_{s_1=1}^n \dots \sum_{s_k=1}^n \alpha_{1,s_1} \cdot \ldots \cdot \alpha_{k,s_k} \omega(e_{s_1}, \dots, e_{s_k}).$$

Wenn $s_i = s_j$ für $i \neq j$ gilt, so ist $\omega(e_{s_1}, \dots, e_{s_k}) = 0$. Also gilt

$$\omega(v_1, \dots, v_k) = \sum_{1 \leq t_1 < \dots < t_k \leq n} \sum_{\pi \in S_k} \alpha_{1,t_{\pi(1)}} \cdot \ldots \cdot \alpha_{k,t_{\pi(k)}} \omega(e_{t_{\pi(1)}}, \dots, e_{t_{\pi(k)}}).$$

Setze $\omega_T = \omega(e_{t_1}, \dots, e_{t_k})$ für alle $T = \{t_1, \dots, t_k\} \in [n]^{(k)}, t_1 < \dots < t_k$ sind. Dann ist

$$\begin{aligned} \omega(v_1, \dots, v_k) &= \sum_{1 \leq t_1 < \dots < t_k \leq n} \omega_{\{t_1, \dots, t_k\}} \cdot \sum_{\pi \in S_k} \operatorname{sgn}(\pi) \cdot \alpha_{1,t_{\pi(1)}} \cdot \ldots \cdot \alpha_{k,t_{\pi(k)}} \\ &= \sum_{1 \leq t_1 < \dots < t_k \leq n} \omega_{\{t_1, \dots, t_k\}} \cdot \left\| (\alpha_{i,t_j})_{1 \leq i,j \leq k} \right\| \\ &= \sum_{1 \leq t_1 < \dots < t_k \leq n} \omega_{\{t_1, \dots, t_k\}} \cdot \left\| (\eta_{t_j}(v_i))_{1 \leq i,j \leq k} \right\| \\ &= \sum_{1 \leq t_1 < \dots < t_k \leq n} \omega_{\{t_1, \dots, t_k\}} \cdot \eta_{\{t_1, \dots, t_k\}}(v_1, \dots, v_k). \end{aligned}$$

[44] Mit $\|\cdot\|$ ist in diesem Kontext die Determinante gemeint.

Daher ist $\omega = \sum_{T\in[n]^{(k)}} \omega_T \cdot \eta_T$, das heißt $(\eta_T)_{T\in[n]^{(k)}}$ erzeugt $\bigwedge^k V^*$.
Nun sei $(\gamma_T)_{T\in[n]^{(k)}}$ eine Familie von Elementen von F mit

$$\sum_{T\in[n]^{(k)}} \gamma_T \cdot \eta_T = 0.$$

Für alle $1 \le s_1 < \cdots < s_k \le n$ ist also

$$\sum_{T\in[n]^{(k)}} \gamma_T \cdot \eta_T(e_{s_1}, \ldots, e_{s_k}) = 0.$$

Wenn $T \neq \{s_1, \ldots, s_k\}$, also $s_i \notin T$ für ein $i \in [k]$, so ist $\eta_T(e_{s_1}, \ldots, e_{s_k}) = 0$; wenn $T = \{s_1, \ldots, s_k\}$, so ist $\eta_T(e_{s_1}, \ldots, e_{s_k}) = \|(\delta_{i,j})_{1\le i,j\le k}\| = 1$. Daher ist $\gamma_S = 0$ für $S = \{s_1, \ldots, s_k\}$. Dies zeigt, dass $(\eta_T)_{T\in[n]^{(k)}}$ linear unabhängig sind. □

Fakt 9.5. Für Linearformen $\alpha_1, \ldots, \alpha_k \in V^*$ gilt genau dann $\alpha_1 \wedge \cdots \wedge \alpha_k = 0$, wenn sie linear abhängig sind.

Beweis.

„ $\Longrightarrow$ “: Seien $\alpha_1, \ldots, \alpha_k$ linear unabhängig. Wähle $v_1, \ldots, v_k \in V$ mit $\alpha_i(v_j) = \delta_{i,j}$ für alle $i, j \in [k]$. Dann ist $(\alpha_1 \wedge \cdots \wedge \alpha_k)(v_1, \ldots, v_k) = \|\delta_{i,j}\| = 1 \neq 0$.

„ $\Longleftarrow$ “: Seien $\alpha_1, \ldots, \alpha_k$ linear abhängig. Für alle $v_1, \ldots, v_k \in F$ sind die Zeilen von

$$\begin{pmatrix} \alpha_1(v_1) & \ldots & \alpha_1(v_k) \\ \vdots & \ddots & \vdots \\ \alpha_k(v_1) & \ldots & \alpha_k(v_k) \end{pmatrix}$$

dann linear abhängig, das heißt die Determinante der Matrix ist Null. □

Lemma 9.6. Es sei U^* ein k-dimensionale Untervektorraum von V^*. Für je zwei Basen $\alpha_1, \ldots, \alpha_k$ und $\beta_1, \ldots, \beta_k$ von U^* sind $\alpha_1 \wedge \cdots \wedge \alpha_k$ und $\beta_1 \wedge \cdots \wedge \beta_k$ linear abhängig.

Beweis. Es sei $(\gamma_{i,j})_{1\le i,j\le k}$ durch $\beta_i = \sum_{j=1}^k \gamma_{i,j}\alpha_j$ für alle $i \in [k]$ gegeben. Dann ist

$$\begin{aligned}
\beta_1 \wedge \cdots \wedge \beta_k &= \sum_{t_1=1}^k \ldots \sum_{t_k=1}^k \gamma_{1,t_1} \cdot \ldots \cdot \gamma_{k,t_k} \cdot \alpha_{t_1} \wedge \cdots \wedge \alpha_{t_k} \\
&= \sum_{\pi\in S_k} \gamma_{1,\pi(1)} \cdot \ldots \cdot \gamma_{k,\pi(k)} \cdot \alpha_{\pi(1)} \wedge \cdots \wedge \alpha_{\pi(k)} \\
&= \sum_{\pi\in S_k} \operatorname{sgn}(\pi) \cdot \gamma_{1,\pi(1)} \cdot \ldots \cdot \gamma_{k,\pi(k)} \cdot \alpha_1 \wedge \cdots \wedge \alpha_k \\
&= \|(\gamma_{i,j})_{1\le i,j\le k}\| \cdot \alpha_1 \wedge \cdots \wedge \alpha_k.
\end{aligned}$$

□

Wir schreiben oft $\bigwedge_{U^*}$ für $\alpha_1 \wedge \cdots \wedge \alpha_k$ in dieser Situation. Nach Fakt 9.5 ist $\bigwedge_{U^*} \neq 0$ und nach Lemma 9.6 $\bigwedge_{U^*}$ (nur) bis auf Multiplikation mit Skalaren eindeutig bestimmt.

Satz 9.7. Für $k+l \leq n$ gibt es genau eine bilineare Abbildung

$$\wedge\colon \bigwedge^k V^* \times \bigwedge^l V^* \longrightarrow \bigwedge^{k+l} V^*$$
$$(\sigma, \omega) \longmapsto \sigma \wedge \omega$$

mit

$$(\alpha_1 \wedge \cdots \wedge \alpha_k) \wedge (\beta_1 \wedge \cdots \wedge \beta_l) = \alpha_1 \wedge \cdots \wedge \beta_l \qquad (*)$$

für alle $\alpha_1, \ldots, \beta_l \in V^*$.

Beweis. Sei $\eta_1, \ldots, \eta_n$ eine Basis von V^*. Dann sind $(\eta_T)_{T\in[n]^{(k)}}, (\eta_Q)_{Q\in[n]^{(l)}}$ Basen von $\bigwedge^k V^*, \bigwedge^l V^*$. Definiere $\eta_T \wedge \eta_Q$ so, dass $(*)$ gilt und setze dann linear fort.
Die Eindeutigkeit ist klar. □

Ab hier war es nur „Allgemeinbildung“, jetzt wollen wir diese Formen in Aktion sehen. Wir beweisen nun eine Vektorraum-Version von der Folgerung 4.16 aus dem Lemma von Bollobás / Lemma 4.15, der stärker als die Mengen-Version ist.

Lemma 9.8. Es sei V ein $(r+s)$-dimensionaler Vektorraum über F. Außerdem seien $A_1, \ldots, A_m$ r-dimensionale Untervektorräume von V und $B_1, \ldots, B_m$ s-dimensionale Untervektorräume von V. Es gelte

- $A_i \cap B_i = \{0\}$ für alle $i \in [m]$,
- $A_i \cap B_j \neq \{0\}$ für alle $1 \leq i < j \leq m$.

Dann ist $m \leq \binom{r+s}{r}$.

Beweis. Wegen $V \cong V^*$ seien $A_1, \ldots, B_l$ Untervektorräume von V^* statt V. Dann ist

- $\bigwedge_{A_i} \wedge \bigwedge_{B_i} \neq 0$ für alle $i \in [m]$,
- $\bigwedge_{A_i} \wedge \bigwedge_{B_j} = 0$ für alle $1 \leq i < j \leq m$.

Also sind $\bigwedge_{A_1}, \ldots, \bigwedge_{A_m} \in \bigwedge^r V^*$ linear unabhängig:
Seien $\gamma_1, \ldots, \gamma_m \in F, \sum_{i=1}^m \gamma_i \bigwedge_{A_i} = 0$. Sei $j = \max\{i \in [m] \mid \gamma_i \neq 0\}$. Dann ist

$$\sum_{i=1}^m \gamma_i \left(\bigwedge\nolimits_{A_i}\right) \wedge \left(\bigwedge\nolimits_{B_j}\right) = 0 \implies \gamma_j \left(\bigwedge\nolimits_{A_j}\right) \wedge \left(\bigwedge\nolimits_{B_j}\right) = 0. \lightning$$

Somit ist $m \leq \dim(\bigwedge^r V^*) = \binom{r+s}{r}$. □

Es wäre schön, wenn wir die Bedingung an die Dimension von V weglassen könnten. Dafür schauen wir uns folgenden Satz an:

Satz 9.9. Es seien W ein Vektorraum über einen unendlichen Körper K und $t \leq n = \dim(W)$. Ferner seien $U_1, \ldots, U_m$ Untervektorräume von W deren Dimension mindestens t betrage. Dann gibt es einen Untervektorraum T von W mit $\dim(T) = n - t$ und

$$\dim(U_i \cap T) = \dim(U_i) - t$$

für alle $i \in [m]$.

Beweis. O.B.d.A. sei $W = K^n$. Betrachte die $n - t$ Vektoren

$$x_j = \begin{pmatrix} x_{j,1} & \dots & x_{j,n} \end{pmatrix} \qquad (1 \leq j \leq n-t)$$

mit Variablen als Einträgen. Für $i \in [m]$ seien $u_1^{(i)}, \dots, u_t^{(i)} \in U_i$ linear unabhängig. Das Polynom

$$p_i = \det\left(u_1^{(i)}, \dots, u_t^{(i)}, x_1, \dots, x_{n-t}\right) \in K[x_{1,1}, \dots, x_{n-t,n}] \qquad (1 \leq i \leq m)$$

ist nicht das Nullpolynom, denn: W hat nach dem Basisergänzungssatz eine Basis der Form $u_1^{(i)}, \dots, u_t^{(i)}, u_{t+1}^{(i)}, \dots, u_n^{(i)}$. Insbesondere gilt $p_i(u_{t+1}^{(i)}, \dots, u_n^{(i)}) \neq 0$.
Daher ist auch

$$p = p_1 \cdot \ldots \cdot p_m$$

nicht das Nullpolynom (schließlich ist der Polynomring nullteilerfrei). Da K unendlich ist, gibt es Vektoren $\xi_1, \dots, \xi_{n-t} \in W$ mit $p(\xi_1, \dots, \xi_{n-t}) \neq 0$. Es sei T der von $\xi_1, \dots, \xi_{n-t}$ erzeugte Untervektorraum von W. Für alle $i \in [m]$ ist

$$p_i(\xi_1, \dots, \xi_{n-t}) \neq 0,$$

das heißt $u_1^{(i)}, \dots, u_n^{(i)}, \xi_1, \dots, \xi_{n-t}$ ist eine Basis von W, somit $U_i + T = W$ und

$$\dim(U_i \cap T) = \dim(U_i) + \underbrace{\dim(T)}_{=n-t} - \underbrace{\dim(U_i + T)}_{=n} = \dim(U_i) - t. \qquad \square$$

Satz 9.10 (Lovász)**.** Es seien V ein Vektorraum über einen Körper K. Die Untervektorräume $A_1, \dots, A_m$ seien r-dimensional und $B_1, \dots, B_m$ seien s-dimensional. Wenn

(i) $A_i \cap B_i = \{0\}$ für alle $i \in [m]$,

(ii) $A_i \cap B_j \neq \{0\}$ für alle $1 \leq i < j \leq m$,

dann ist $m \leq \binom{r+s}{r}$.

Beweis. O.B.d.A. sei $\dim(V) = n$ endlich.[45] Zunächst sei K unendlich. Nach (i) ist $\dim(A_i + B_i) = r + s$ für alle $i \in [m]$. Nach Satz 9.9 existiert ein Untervektorraum T von V mit $\dim(T) = n - (r + s)$ und

(iii) $\dim((A_i + B_i) \cap T) = 0$ für alle $i \in [m]$.

Betrachte die Projektion $\pi\colon V \to V/T$. Setze $A_i' = \pi[A_i], B_i' = \pi[B_i]$ für alle $i \in [m]$. Nach (iii) ist $\dim(A_i' + B_i') = r + s$ für alle $i \in [m]$. Also sind $A_1', \dots, A_m'$ r-dimensional, $B_1', \dots, B_m'$ s-dimensional, $A_i' \cap B_i' = \{0\}$ und $A_i' \cap B_j' \neq \{0\}$ für $1 \leq i < j \leq m$, denn

$$\dim(A_i' + B_j') \leq \dim(A_i + B_j) < r + s = \dim(A_i') + \dim(B_i').$$

Da $\dim(V/T) = \dim(V) - \dim(T) = r + s$ gilt, folgt $m \leq \binom{r+s}{r}$ aus Lemma 9.8.
Nun sei K endlich. Sei $L \mid K$ eine unendliche Körpererweiterung (beispielsweise könnte man L als den Körper aller rationalen Funktionen mit Koeffizienten in K wählen). Wende das bereits gezeigte auf die Skalarerweiterung $V \otimes_K L, A_i \otimes_K L, B_i \otimes_K L$ $(i \in [m])$ an. $\square$

[45] Sonst könnten wir den endlichen Vektorraum $A_1 + \dots + A_m + B_1 + \dots + B_m$ betrachten.

Satz 9.11 (Füredi)**.** Es seien V ein K-Vektorraum und $t \in \mathbb{N}_0$. Ferner seien $A_1, \dots, A_m$ r-dimensionale und $B_1, \dots, B_m$ s-dimensionale Untervektorräume von V. Wenn

(i) $\dim(A_i \cap B_i) \leq t$ für alle $i \in [m]$,

(ii) $\dim(A_i \cap B_j) > t$ für $i < j$,

dann ist $m \leq \binom{r+s-2t}{r-t}$.

Beweis. Wie vorhin seien K o.B.d.A. unendlich und $n = \dim(V)$ endlich. Aus (ii) folgt $r, s \geq t$. Nach Satz 9.9 gibt es einen Untervektorraum T von V mit

- $\dim(T) = n - t$,
- $\dim(A_i \cap T) = r - t, \dim(B_i \cap T) = s - t, \dim(A_i \cap B_i \cap T) = 0$ für alle $i \in [m]$.

Wende nun den Satz 9.10 auf $r - t, s - t$ und die Räume

$$A_1 \cap T, \dots, A_m \cap T, B_1 \cap T, \dots, B_m \cap T$$

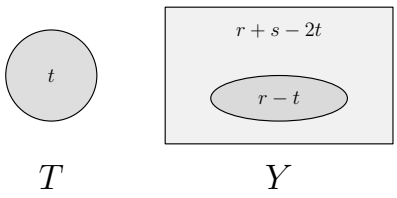
an. Das ist nur zulässig, wenn $\dim(A_i \cap B_j \cap T) > 0$ für $1 \leq i < j \leq m$.
Dies ist aber der Fall, denn

$$\dim(A_i \cap B_j \cap T) = \underbrace{\dim(A_i \cap B_j)}_{>t} + \underbrace{\dim(T)}_{=n-t} - \underbrace{\dim((A_i \cap B_j) + T)}_{\leq n} > 0. \qquad \square$$

Folgerung 9.12. Es seien X eine endliche Menge, $A_1, \dots, A_m \in X^{(r)}$, und $B_1, \dots, B_m \in X^{(s)}$. Ferner sei $t \in \mathbb{N}_0$. Wenn

- $|A_i \cap B_i| \leq t$ für alle $i \in [m]$,
- $|A_i \cap B_j| > t$ für $1 \leq i < j \leq m$,

dann ist $m \leq \binom{r+s-2t}{r-t}$.



Beispiel 9.13. $X = T \cup Y$, wobei $|T| = t, |Y| = r+s-2t$. Es seien $C_1, \dots, C_m$ die $(r-t)$-elementige Teilmengen von Y, wobei $m = \binom{r+s-2t}{r-t}$. Setze $A_i = T \cup C_i, B_i = T \cup (Y \setminus C_i)$. Dies zeigt, dass die Schranke optimal ist.

Beweis von Folgerung 9.12. Es sei V ein $\mathbb{Q}$-Vektorraum[46] mit Basis $\{e_x \colon x \in X\}$. Für $i = 1, \dots, m$ seien $\mathcal{A}_i, \mathcal{B}_i$ die von $\{e_x \colon x \in A_i\}$ bzw. $\{e_x \colon x \in B_i\}$ erzeugten Untervektorräume von V. Dann ist

$$\dim(\mathcal{A}_i \cap \mathcal{B}_i) = |A_i \cap B_i| \leq t, \qquad \dim(\mathcal{A}_i \cap \mathcal{B}_j) = |A_i \cap B_j| > t$$

für $i \in [m]$ bzw. $1 \leq i < j \leq m$. Nach Satz 9.11 gilt also $m \leq \binom{r+s-2t}{r-t}$. $\square$

[46] Welchen Körper man wählt, ist hier relativ egal.

A Lösungen zu den Übungsblättern

Disclaimer

Es sei nochmal betont, dass dies ein *inoffizieller* Mitschrieb der Vorlesung *Algebraic Methods of Combinatorics* des Wintersemesters 2022 - 2023 bei Dr. Christian Reiher ist. Ich erhebe daher keinen Anspruch auf Richtigkeit oder Vollständigkeit. Die folgenden Lösungen wurden in der Übung erarbeitet und können gegebenenfalls unvollständig sein oder Fehler enthalten.

Blatt 1

Aufgabe 1

Behauptung. Es seien $A_1, \dots, A_m$ und $B_1, \dots, B_m$ Teilmengen der endlichen Menge X. Für alle $i \in [m]$ sei $|A_i \cap B_i|$ ungerade. Für alle $1 \leq i < j \leq m$ hingegen sei $|A_i \cap B_j|$ gerade. Dann gilt $m \leq |X|$.

Beweis. O.B.d.A. sei wieder $X = [n]$, $e_1, \dots, e_n$ die Standardbasis von $\mathbb{F}_2^n$ und $\langle \cdot, \cdot \rangle$ das darauf definierte Standardskalarprodukt. Kodiere jede Menge $C \in \{A_i, B_i \mid 1 \leq i \leq m\}$ mit einem Vektor $v_C = \sum_{c \in C} e_c$. Die Eigenschaften von A_i und B_j, wobei $i \leq j$, implizieren

$$\left\langle v_{A_i}, v_{B_j} \right\rangle = \begin{cases} 1, & i = j \\ 0, & i < j. \end{cases}$$

Betrachte nun die Matrizen $M^1 \in \mathbb{F}_2^{m \times n}$ und $M^2 \in \mathbb{F}_2^{n \times m}$, wobei die Zeilen von M^1 durch $(M^1_{i,*}) = v_{A_i}^\top$ und die Spalten von M^2 durch $(M^2_{*,j}) = v_{B_j}$ gegeben sind. Obiger Fakt über das Skalarprodukt impliziert, dass $M^1 \cdot M^2$ eine untere $(m \times m)$-Dreiecksmatrix ist mit Einsen auf der Diagonalen. Da also das Produkt von beiden Matrizen regulär ist, müssen beide Matrizen einen Rang von mindestens m haben. Würde $n < m$ gelten, so wäre der Rang beider Matrizen hierfür aber zu klein, also muss $m \leq n$ gelten. □

Bemerkung A.1. Alternativ kann man wie folgt vorgehen: Wenn man eine Linearkombination $\sum_{i=1}^m \alpha_i v_{A_i}$ der Null hat, dann kann man nacheinander induktiv durch $\alpha_1 = \langle B_1, \sum_{i=1}^m \alpha_i v_{A_i} \rangle = 0$ folgern, dass $\alpha_1 = \cdots = \alpha_m = 0$ gilt. Dann wären also wie gewünscht $v_{A_1}, \dots, v_{A_m}$ linear unabhängig. □

Aufgabe 2

Behauptung. Es seien $A_1, \dots, A_m$ Teilmengen der endlichen Menge X. Für $i, j \in [m]$ sei $|A_i \cap A_j|$ genau dann durch 4 teilbar, wenn $i \neq j$ gilt.

Beweis. Es seien $A_1, \dots, A_m$ Teilmengen von einer endlichen Menge X und $n = |X|$. Wie oben sei o.B.d.A. $X = [n]$ und für $A \subseteq X$ v_A der Inzidenzvektor.
Nach den Voraussetzungen wissen wir, dass

$$\left\langle v_{A_i}, v_{A_j} \right\rangle \pmod 4 \in \begin{cases} \{1, 2, 3\}, & i = j \\ \{0\}, & i \neq j. \end{cases}$$

Anders als zuvor, fassen wir aber v_A als Vektoren des $\mathbb{Q}$-Vektorraums $\mathbb{Q}^n$ auf. Betrachte nun die Matrix $M \in \mathbb{Z}^{n\times m}$, wobei die Spalten von M durch $(M_{*,j}) = v_{A_j}$ gegeben sind. Obige Gleichung umgeschrieben ergibt $4 \mid (M^\top \cdot M)_{i,j} \iff i \neq j$.
Können wir nun zeigen, dass $N = M^\top \cdot M$ regulär ist, so wären wir fertig, denn wäre $m > n$, so könnte N höchstens Rang n haben statt vollen Rang m.

Behauptung. Es sei $N \in \mathbb{Q}^{m\times m}$ eine Matrix mit $\mathbb{Z}$-Einträgen, sodass

$$4 \mid N_{i,j} \iff i \neq j.$$

Dann ist N regulär.

Beweis. Wir zeigen dies über Induktion auf m. Wenn $m = 1$ ist, ist die Aussage klar. Sei also $m > 1$. Es sei für $r_1, \ldots, r_l \in \mathbb{Q}$ $\operatorname{diag}(r_1, \ldots, r_l)$ die $(l \times l)$-Diagonalmatrix über $\mathbb{Q}$ mit $(\operatorname{diag}(r_1, \ldots, r_l))_{i,i} = r_i$.

(i) O.B.d.A. sei $N_{i,m}$ ein Vielfaches von $N_{m,m}$ für $i < m$: Wenn nicht, multiplizieren wir im Fall, dass $N_{m,m} \equiv 0 \pmod 2$ gilt mit der Matrix

$$D = \operatorname{diag}\left(\frac{N_{m,m}}{2}, \ldots, \frac{N_{m,m}}{2}, 1\right) \in \mathbb{Q}^{m\times m}.$$

Beachte, dass D regulär ist, da $N_{m,m} \equiv 2 \pmod 4$ gilt. Zudem ist wegen jenem Fakt $N_{m,m}/2$ ungerade und damit $D \cdot N$ immer noch eine ganzzahlige Matrix mit Vielfachen von 4 genau auf den Nebeneinträgen. Ist $N_{m,m} \equiv 1 \pmod 2$, so multipliziere man N mit

$$D = \operatorname{diag}(N_{m,m}, \ldots, N_{m,m}, 1) \in \mathbb{Q}^{m\times m}.$$

In diesem Fall ist D auch regulär und $D \cdot N$ eine Matrix entsprechend der Voraussetzungen des Lemmas. Beachte, dass in beiden Fällen $D \cdot N$ genau dann regulär ist, wenn N regulär ist.

(ii) Subtrahiere von der i-ten Zeile ein geeignetes ganzzahliges Vielfaches der m-ten Zeile von N für alle $i \in [m-1]$, sodass für die resultierende Matrix N' $N'_{i,m} = 0$ gilt. Dies ist zulässig wegen (i). Beachte, dass wegen $N_{m,j} \equiv 0 \pmod 4$ N' immer noch eine Matrix entsprechend der Voraussetzungen ist. Weiterhin ist der Rang einer Matrix eine Invariante unter Zeilenumformungen, also N' genau dann regulär, wenn N regulär ist. Nun, beachte, dass durch Entwickeln der letzten Spalte wir

$$\det(N') = N'_{m,m} \cdot \det((N')_{1\leq i,j\leq m-1})$$

erhalten. Da nach der Induktionsvoraussetzung $(N')_{1\leq i,j\leq m-1}$ regulär ist, ist damit tatsächlich N' auch regulär.

Hiermit wäre der Beweis vollbracht. □

Also ist N regulär und es folgt die Behauptung. □

Bemerkung A.2. Alternativ kann man wie folgt vorgehen: Man interpretiere wieder $A_1, \dots, A_m$ als Vektoren (also $v_{A_i} \equiv A_i$), aber über den Körper $\mathbb{Q}$. Angenommen es gibt eine Linearkombination

$$\sum_{i=1}^{m} \alpha_i \cdot A_i = 0$$

mit $\alpha_1, \dots, \alpha_m \in \mathbb{Q}$. O.B.d.A. seien aber all diese α_i ganzzahlig, sonst multipliziere man mit dem Hauptnenner. Zudem seien diese α_i so gewählt, dass

$$\max\{|\alpha_1|, \dots, |\alpha_m|\}$$

minimal ist. Nun sind aber alle α_i gerade, denn

$$0 \equiv \left\langle \sum_{i=1}^{n} \alpha_i \cdot A_i, A_j \right\rangle \equiv \alpha_j \langle A_j, A_j \rangle \equiv \alpha_j \cdot |A_j| \pmod 4.$$

Damit widerspricht $\alpha_1/2, \dots, \alpha_m/2$ der Minimalität von $\alpha_1, \dots, \alpha_m$. □

Aufgabe 3

Behauptung. Es sei $n \in \mathbb{N}$ und $\mathcal{C}$ eine Menge von Teilmengen von $[n]$ mit folgenden Eigenschaften:

- Für alle $A \in \mathcal{C}$ ist $|A|$ gerade.
- Für alle verschiedenen $A, B \in \mathcal{C}$ ist $|A \cap B|$ ungerade.

Dann ist die größtmögliche Mächtigkeit von $\mathcal{C}$ n falls n ungerade ist und sonst $n-1$.

Beweis. Erstmal stellen wir fest, dass $|\mathcal{C}| = n-1$ für $n \in 2\mathbb{N}$ und $|\mathcal{C}| = n$ für $n \in (2\mathbb{N}-1)$ möglich ist. Hierfür nehme man im ungeraden Fall $\mathcal{C} = \{[n] \setminus \{i\} \mid i \in [n]\}$ und im geraden Fall beispielsweise $\mathcal{C} = \{\{1, i\} \mid 2 \le i \le n\}$ (oder $\mathcal{C} = \{[n-1] \setminus \{i\} \mid i \in [n-1]\}$). Dann hat offensichtlich $\mathcal{C}$ die gewünschte Mächtigkeit und Schnitt-Parität. Für die Optimalität kodiere man wie in Aufgabe 1 die Teilmenge durch Vektoren von $\mathbb{F}_2^n$. Angenommen $\mathcal{C} = \{C_1, \dots, C_m\}$. Betrachte nun die Matrix $M \in \mathbb{F}_2^{n \times m}$, wobei die Spalten von M durch $(M_{*,j}) = v_{C_j}$ gegeben sind. Es gilt $M^\top \cdot M = \mathbb{1}_{m \times m} - \mathrm{id}_m =: N$, wobei $\mathbb{1}_{m \times m}$ die $(m \times m)$-Matrix mit nur Eins-Einträgen ist. Mit diesem Wissen bilden wir Schranken auf den Rang von M: Zum einen gilt wegen $|C_i| \equiv 0 \pmod 2$

$$M^\top \cdot \mathbb{1}_{n \times 1} = 0,$$

also hat $M^\top$ und damit auch M keinen vollen Rang, womit dieser höchstens $n-1$ ist. Wir werden nun die Eigenvektoren von N bestimmen. Beachte, dass wir dann eine untere Schranke für den Rang von M geben können. Betrachte also die Vektoren gegeben durch

$$v^1 = \mathbb{1}_{m \times 1}$$
$$v^i_j = \begin{cases} 1, & j = 1 \text{ oder } j = i \\ 0, & \text{sonst.} \end{cases} \qquad (2 \le i \le m)$$

Man stelle fest, dass v^1 ein Eigenvektor von N zum Eigenwert $m-1$ ist und v^i für $2 \leq i \leq m$ ein Eigenvektor zum Eigenwert 1 ist. Ebenfalls ist klar, dass die angegebenen Eigenvektoren linear unabhängig sind. Da eine $(m \times m)$-Matrix (algebraische Multiplizität miteinberechnet) genau m Eigenwerte hat, sind das auch alle. Ist nun m ungerade, so ist $m-1 \equiv 0 \pmod 2$, womit also N Rang $m-1$ hat. Im Fall, dass m gerade ist, gilt wiederrum $m-1 \equiv 1 \pmod 2$, womit also N vollen Rang m hat.
Insgesamt haben wir also, weil der Rang von N höchstens der von M ist,

$$m-1 \leq n-1 \implies m \leq n$$

für ungerade n und sogar $m \leq n-1$, wenn n gerade ist. □

Alternativer Beweis. Es seien $A_1, \ldots, A_m \subseteq [n]$ mit $|A_i| \equiv 0 \pmod 2$ für alle $i \in [m]$ und $|A_i \cap A_j| \equiv 1 \pmod 2$ für alle $i \neq j$. Angenommen $m > n$. O.B.d.A. sei $m = n+1$. Da $A_1, \ldots, A_{n+1} \in \langle [n] \rangle^\perp$ gilt, wobei $\langle [n] \rangle^\perp$ $(n-1)$-dimensional ist, sind $A_1, \ldots, A_n$ und $A_1, \ldots, A_{n-1}, A_{n+1}$ linear abhängig.
Also existieren $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \mathbb{F}_2$ nicht alle Null mit

$$\sum_{i=1}^{n} \alpha_i \cdot A_i = 0, \qquad \beta_1 \cdot A_1 + \cdots + \beta_{n-1} \cdot A_{n-1} + \beta_n \cdot A_{n+1} = 0.$$

Für alle $j \in [n]$ ist $0 = \langle A_j, \sum_{i=1}^n \alpha_i \cdot A_i \rangle = \sum_{i \neq j} \alpha_i$. Somit ist $\alpha_j = \sum_{i=1}^n \alpha_i$ für alle $j \in [n]$ und, weil nicht alle Null sind, $\alpha_1 = \cdots = \alpha_n = 1$. Analog gilt $\beta_1 = \cdots = \beta_n = 1$. Dann ist aber

$$A_n = \sum_{i=1}^{n-1} A_i = A_{n+1}. \; \lightning$$

Also muss für alle $n \in \mathbb{N}$ $m \leq n$ gelten. Von nun an sei n gerade. Dann existieren wie zuvor $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_2$ nicht alle Null mit

$$\sum_{i=1}^{n} \alpha_i \cdot A_i = 0.$$

Wie zuvor können wir folgern, dass $\sum_{i=1}^n \alpha_i = \alpha_1 = \cdots = \alpha_n = 1$ gilt. Da aber n gerade ist, folgt daraus $\sum_{i=1}^n \alpha_i = 0$, Widerspruch. □

Aufgabe 4

Behauptung. Es sei $P \in \mathbb{R}[x]$ ein nicht-konstantes Polynom mit reellen Koeffizienten. Dann existiert ein durch P teilbares Polynom, bei dem alle Monome x^p mit von Null verschiedenem Koeffizienten eine Primzahl als Exponenten haben.

Beweis. Es sei d der Grad von P und $p_1, \ldots, p_d, p_{d+1} \in \mathbb{N}$ paarweise verschiedene Primzahlen. Mit Polynomdivision durch P erhalten wir für gewisse Polynome $Q_i, R_i \in \mathbb{R}[x]$

$$x^{p_i} = Q_i(x) \cdot P(x) + R_i(x)$$

für alle $i \in [d+1]$, wobei $\operatorname{grad}(R_i) \leq d-1$. Nun sind die $Q_i(x)$ Elemente des $\mathbb{R}$-Vektorraums V der Polynome vom Grad kleiner d. Dieser Vektorraum hat Dimension d, also müssen $R_1(x), \ldots, R_d(x), R_{d+1}(x)$ linear abhängig sein und $\alpha_1, \ldots, \alpha_d, \alpha_{d+1} \in \mathbb{R}$ existieren mit

$$\sum_{i=1}^{d+1} \alpha_i \cdot R_i(x) = 0.$$

Insbesondere gilt

$$\begin{aligned}\sum_{i=1}^{d+1} \alpha_i \cdot x^{p_i} &= \sum_{i=1}^{d+1} \alpha_i \cdot (Q_i(x) \cdot P(x) + R_i(x)) \\ &= \left(\sum_{i=1}^{d+1} \alpha_i \cdot Q_i(x)\right) \cdot P(x) + \sum_{i=1}^{d+1} \alpha_i \cdot R_i(x) \\ &= \left(\sum_{i=1}^{d+1} \alpha_i \cdot Q_i(x)\right) \cdot P(x).\end{aligned}$$

Hiermit wäre der Beweis vollbracht. □

Aufgabe 5

Behauptung. Es seien $A_1, \ldots, A_m$ paarweise verschiedene gleichmächtige Teilmengen einer endlichen Menge X mit der Eigenschaft, dass $\{|A_i \cap A_j| \mid 1 \leq i < j \leq m\}$ höchstens zweielementig ist. Dann ist $m \leq \binom{|X|+2}{2}$.

Beweis. Sei $A_1, \ldots, A_m \in \binom{X}{r}$ für ein gewisses $0 \leq r \leq |X|$ mit der Eigenschaft, dass $|\{|A_i \cap A_j| \mid 1 \leq i < j \leq m\}| \leq 2$. Es seien die Elemente von der letzten Menge $s, t \in [r-1]$[47]. Weiter sei $n \coloneqq |X|$ und o.B.d.A. $X = [n]$. Zu $A \subseteq X$, setze

$$v_A \coloneqq \sum_{i \in A} e_i \in \mathbb{R}^n.$$

Betrachte das Polynom

$$F \colon \mathbb{R}^n \times \mathbb{R}^n, (x, y) \mapsto (\langle x, y\rangle - s)(\langle x, y\rangle - t).$$

Wegen $\left\langle v_{A_i}, v_{A_j} \right\rangle = |A_i \cap A_j|$, gilt

$$F(v_{A_i}, v_{A_j}) = \begin{cases} 0, & i \neq j \\ (r-s)(r-t), & i = j. \end{cases}$$

Für $i \in [m]$ betrachte

$$f_i(x) = F(x, v_{A_i}).$$

[47] Hat die Menge nur ein Element, so wähle $s = t$. Zudem gilt letzte Ungleichung, weil sonst die zwei Mengen gleich wären.

Nun sind $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$ linear unabhängig, denn: Seien $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$ so, dass $\alpha_1 f_1 + \cdots + \alpha_m f_m = 0$. Durch Einsetzen von v_{A_j} erhält man $\alpha_j (r-s)(r-t) = 0$, also $\alpha_j = 0$. Beachte, dass

$$f_i(x) = (\langle x, v_{A_i} \rangle - s)(\langle x, v_{A_i} \rangle - t).$$

Durch Ausmultiplizieren sieht man, dass jedes der $f_i(x)$ im von

$$x_j x_k \ (1 \leq j \leq k \leq n), x_j \ (1 \leq j \leq n), 1$$

erzeugten $\mathbb{R}$-Untervektorraum von $\mathbb{R}[x_1, \ldots, x_n]$ ist. Somit gilt

$$m \leq \binom{n+1}{2} + n + 1 = \binom{n+1}{2} + \binom{n+1}{1} = \binom{n+2}{2}.$$

Damit wäre der Beweis vollbracht. □

Bemerkung A.3. Der Beweis ist sehr stark an den von Satz 1.7 angelehnt. Wie aber im späteren Verlauf der Vorlesung klar wurde, lässt sich diese Schranke verbessern (siehe Satz 2.13 oder gar Folgerung 2.10).

Blatt 2

Aufgabe 1

Behauptung. Es sei $\mathcal{A} \in \mathcal{P}([n])$ ein Mengensystem mit der Eigenschaft, dass für alle verschiedenen $A, B \in \mathcal{A}$ die Mächtigkeit des Schnittes $|A \cap B|$ gerade ist. Dann ist

$$|\mathcal{A}| \leq \begin{cases} 2^{\frac{n}{2}}, & n \equiv 0 \pmod 2 \\ 2^{\frac{n-1}{2}} + 1, & n \equiv 1 \pmod 2 \end{cases}$$

für $n \geq 6$.[48]

Beweis. Es sei $\mathcal{A}_g$ die Menge der geraden Mengen in $\mathcal{A}$ und $\mathcal{A}_u$ die Menge der ungeraden Mengen in $\mathcal{A}$. Weiter sei V der von $\mathcal{A}$ aufgespannte $\mathbb{F}_2$-Untervektorraum in $\mathcal{P}([n])$ und V_g und V_u entsprechend die Untervektorräume aufgespannt durch $\mathcal{A}_g$ bzw. $\mathcal{A}_u$. Da wir für Mengen $A, B \in \mathcal{A}_u$

$$\langle A, B \rangle \equiv \delta_{A=B} \pmod 2$$

haben, ist $\mathcal{A}_u$ linear unabhängig. Weiter wissen wir, dass $V_g \subseteq V^\perp$ gilt, da wir für $A \in \mathcal{A}_g$ und $B \in \mathcal{A}$

$$\langle A, B \rangle = |A \cap B| \equiv 0 \pmod 2$$

haben. Wähle nun eine Basis $\mathcal{B} \subseteq \mathcal{A}$ von V mit $\mathcal{A}_u \subseteq \mathcal{B}$. Es gilt

$$n = \dim(V) + \dim(V^\perp) \geq |\mathcal{B}| + \dim(V_g) \geq |\mathcal{A}_u| + 2 \cdot \dim(V_g) \implies 2^{\frac{n-|\mathcal{A}_u|}{2}} \geq 2^{\dim(V_g)}.$$

Also gilt

$$|\mathcal{A}| \leq |\mathcal{A}_u| + |V_g| \leq |\mathcal{A}_u| + 2^{\frac{n-|\mathcal{A}_u|}{2}} \leq \begin{cases} 2^{\frac{n}{2}}, & n \equiv 0 \pmod 2 \\ 2^{\frac{n-1}{2}} + 1, & n \equiv 1 \pmod 2. \end{cases}$$

□

[48] Die Bedingung $n \geq 6$ ist notwendig, damit die letzte Ungleichung im Beweis gilt.

Aufgabe 2 (Deza, 1973)

Behauptung. Es seien $k, t \leq n$ natürliche Zahlen und $\mathcal{A} \subseteq [n]^{(k)}$ sei ein Mengensystem. Für alle verschiedenen $A, B \in \mathcal{A}$ gelte $|A \cap B| = t$. Dann tritt mindestens eines der folgenden Fälle ein:

(i) $|\mathcal{A}| \leq k^2 - k + 1$,

(ii) Es gibt eine t-elementige Menge T mit $T \subseteq A$ für alle $A \subseteq \mathcal{A}$.

Beweis für $t = 1$.

Fall 1: $\exists\, x \in [n]\colon \deg(x) \geq k + 1$. Dann ist $x \in A$ für alle $A \in \mathcal{A}$ und somit $\{x\} \subseteq A$ für alle $A \in \mathcal{A}$.

Fall 2: $\forall\, x\colon \deg(x) \leq k$. Sei $A \in \mathcal{A}$ beliebig. Wegen $\deg(y) \leq k$ darf es pro Element $y \in A$ höchstens $(k-1)$ weitere Mengen $B \in \mathcal{A}$ geben mit $y \in B$. Zusammen haben wir damit $|\mathcal{A}| \leq 1 + k(k-1) = k^2 - k + 1$.

Es folgt die Behauptung. □

Beweis für allgemeine t. Es sei $\mathcal{A} \subseteq [n]^{(k)}$ $\{t\}$-schneidend. Setze $m = |\mathcal{A}|$.

Lemma A.4. Für alle $x \in [n]$ ist $\deg(x)(m - \deg(x)) \leq m(k-t)$.

Beweis von Lemma A.4. Setze $\mathcal{L} = \{A \in \mathcal{A} \mid x \in A\}, \mathcal{C} = \mathcal{A} \setminus \mathcal{L}$.
Für $y \in [n] \setminus \{x\}$ setze

$$r_y = |\{A \in \mathcal{L} \mid y \in A\}|, \qquad u_y = |\{A \in \mathcal{C} \mid y \in A\}|,$$
$$s_y = |\{A \in \mathcal{L} \mid y \notin A\}|, \qquad v_y = |\{A \in \mathcal{C} \mid y \notin A\}|.$$

Weiter sei $g_y = r_y/\deg(x)$ und $h_y = u_y/(m - \deg(x))$. Es gilt

$$0 \leq (g_y - h_y)^2 = g_y(1-h_y) + h_y(1-g_y) - g_y(1-g_y) - h_y(1-h_y).$$

Multipliziere mit $\deg(x)(m - \deg(x))$:

$$0 \leq r_y v_y + u_y s_y - \frac{m - \deg(x)}{\deg(x)} r_y s_y - \frac{\deg(x)}{m - \deg(x)} u_y v_y.$$

Zuletzt summiere man über y:

$$\begin{aligned}
0 \leq & \sum_{(B,C) \in \mathcal{L} \times \mathcal{C}} (|B \setminus C| - 1) + \sum_{(B,C) \in \mathcal{L} \times \mathcal{C}} |C \setminus B| \\
& - \frac{m - \deg(x)}{\deg(x)} \sum_{(B,B') \in \mathcal{L}^2} |B \setminus B'| - \frac{\deg(x)}{m - \deg(x)} \sum_{(C,C') \in \mathcal{C}^2} |C \setminus C'| \\
= & \deg(x)\,(m - \deg(x))\,(k - t - 1) + \deg(x)\,(m - \deg(x))\,(k-t) \\
& - (m - \deg(x))\,(\deg(x) - 1)\,(k-t) - \deg(x)\,(m - \deg(x) - 1)\,(k-t) \\
= & -\deg(x)(m - \deg(x)) + (m - \deg(x))\,(k-t) + \deg(x)(k-t)
\end{aligned}$$

Also ist $m(k-t) \geq \deg(x)\,(m - \deg(x))$. □

Ab jetzt sei $m \geq k^2 - k + 2$. Wegen dem Beweis für $t = 1$ sei o.B.d.A. $t \geq 2$ und $k \geq 3$. Wir müssen eine t-elementige Menge T finden, sodass $T \subseteq A$ für alle $A \in \mathcal{A}$.

Behauptung. Für alle x ist $\deg(x) \leq k - t + 1$ oder $\deg(x) \geq m - (k - t + 1)$.

Beweis der Behauptung. Sonst ist $k - t + 2 \leq \deg(x) \leq m - (k - t + 2)$. Also ist

$$(k - t + 2)[m - (k - t + 2)] \leq \deg(x)(m - \deg(x)) \leq m(k - t).$$

Dann ist $2m \leq (k - t + 2)^2 \leq k^2$. Aber dann ist

$$2k^2 - 2k + 4 \leq k^2 \implies k^2 + 4 \leq 2k. \lightning \qquad \square$$

Wir zeigen, dass $T = \{x \in [n] \mid \deg(x) \geq m - (k - t + 1)\}$ die gewünschte Menge ist.

Annahme. $|T| \geq t + 1$.

Sei $T' \subseteq T, |T'| \leq t + 1$. Die Anzahl der $A \in \mathcal{A}$ mit $T' \subseteq A$ ist größer gleich

$$\begin{aligned} m - (t+1)(k-t+1) \geq \quad & m - \left(\frac{k+2}{2}\right)^2 \geq \quad k^2 - k + 2 - \frac{k^2}{4} - k - 1 \\ = \quad & \frac{3}{4} \cdot k^2 - 2k + 1 \overset{k \geq 3}{>} \quad 1. \lightning \end{aligned}$$

Also ist $|T| \leq t$. Zuletzt genügt es zu zeigen, dass $|A \cap T| \geq t$ für alle $A \in \mathcal{A}$ ist: Sei $A \in \mathcal{A}$ beliebig. Angenommen $|A \cap T| \leq t - 1$. Eine Rechnung zeigt dann aber

$$\begin{aligned} (m-1)t + k &= \sum_{B \in \mathcal{A}} |A \cap B| \\ &= \sum_{x \in A} \deg(x) \\ &\leq |A \cap T|\, m + (k - |A \cap T|)(k - t + 1) \\ &= |A \cap T|\, (m - (k - t + 1)) + k(k - t + 1) \\ &\leq (t-1)m + (k - t + 1)^2 \\ \implies \quad k - t &\leq (k - t + 1)^2 - m \\ \implies \quad m &\leq (k - t + 1)^2 + t - k \\ &= k^2 - (2k + 1 - t)t + 1 \\ &< k^2 - k + 1 \lightning \end{aligned}$$

Damit ist T die gesuchte t-elementige Menge und der Beweis vollbracht. $\square$

Aufgabe 3

Behauptung. Es sei $\mathcal{A} \subseteq [n]^{(20)}$ ein $\{0, 13, 17\}$-schneidendes Mengensystem. Dann ist

$$|\mathcal{A}| \leq \binom{n}{2}.$$

Beweis. Sei $\mathcal{A} \subseteq [n]^{(20)}$ ein $\{0, 13, 17\}$-schneidendes Mengensystem. Es sei

$$\mathcal{B} = \{B_1, \dots, B_k\} \subseteq \mathcal{A}$$

eine maximale Familie disjunkter Mengen von $\mathcal{A}$. Es ist klar, dass $k \leq \lfloor n/20 \rfloor$. Weiterhin muss sich jedes $C \in \mathcal{A} \setminus \mathcal{B}$ mit einem Element B_i schneiden für ein $i \in [k]$, da $\mathcal{B}$ maximal ist. Weiterhin schneidet C genau ein B_i, denn würde $C \cap B_i \neq \emptyset \neq C \cap B_j$ für $1 \leq i < j \leq k$ gelten, so haben wir dann

$$20 = |C| \geq |C \cap B_i| + |C \cap B_j| \geq 26 > 20. \lightning$$

Setze $\mathcal{A}_i = \{C \in \mathcal{A} \mid C \cap B_i \neq \emptyset\}$ für $i \in [k]$. Beachte, dass $\bigcup\!\!\cdot\, _{i=1}^{k} \mathcal{A}_i = \mathcal{A}$. Wir zeigen nun, dass für alle $i \in [k]$ $\mathcal{A}_i$ ein $\{13, 17\}$-schneidendes Mengensystem ist: Es reicht zu zeigen, dass sich verschiedene $C, D \in \mathcal{A}_i$ nicht-trivial schneiden. Wäre das nun nicht der Fall, so wäre nach unseren Vorbemerkungen

$$\{B_1, \dots, B_{i-1}, C, D, B_{i+1}, \dots, B_k\} \subseteq \mathcal{A}$$

eine größere Teilfamilie von disjunkten Mengen. $\lightning$
Also findet man eine Partitionierung $[n] = X_1 \cup \ldots \cup X_n$, sodass $\mathcal{A}_i \subseteq X_i^{(20)}$ ist. Nach dem Satz von Ray-Chaudhuri-Wilson / Satz 2.13 ist dann

$$\begin{aligned} |\mathcal{A}| &= \sum_{i=1}^{m} |\mathcal{A}_i| && \leq \sum_{i=1}^{m} \binom{|X_i|}{2} \\ &= \frac{1}{2} \sum_{i=1}^{m} \left(|X_i|^2 - |X_i| \right) && = \frac{1}{2} \left(\sum_{i=1}^{m} |X_i|^2 - \sum_{i=1}^{m} |X_i| \right) \\ &\leq \frac{1}{2} \left(\left(\sum_{i=1}^{m} |X_i| \right)^2 - \sum_{i=1}^{m} |X_i| \right) = \binom{n}{2} \end{aligned}$$

nach der Cauchy-Schwarz Ungleichung. Es folgt die Behauptung. □

Alternativer Beweis. Wir wenden den Satz von Alon-Babai-Suzuki / Satz 2.17 an: Es sei o.B.d.a. $n \geq 20$. Setze $p = 13$, $L = \{0, 4\} \subseteq \mathbb{F}_p$ und $k = 7 \notin L$. Beachte, dass dann $\mathcal{A}$ als $\{0, 13, 17\}$-schneidendes System insbesondere L-schneidend ist. Also folgt direkt

$$|\mathcal{A}| \leq \binom{n}{|L|} = \binom{n}{2}.$$

Das war zu zeigen. □

Aufgabe 4

Behauptung. Es seien L_1, L_2 zwei disjunkte Teilmengen von $\mathbb{N}_0$. Für $i = 1, 2$ sei $\mathcal{A}_i \subseteq [n]^{(k)}$ ein L_i-schneidendes Mengensystem. Dann ist

$$|\mathcal{A}_1| \, |\mathcal{A}_2| \leq \binom{n}{k}.$$

Beweis. S_n wirkt auf $[n]^{(k)}$. Für $\pi \in S_n$ ist $\pi \bullet \mathcal{A}_2 = \{\pi[A] \mid A \in \mathcal{A}_2\}$ L_2-schneidend. Also ist $|\mathcal{A}_1 \cap \pi \bullet \mathcal{A}_2| \leq 1$ für alle $\pi \in S_n$. Würde nämlich $A, B \in \mathcal{A}_1 \cap \pi \bullet \mathcal{A}_2$ für gewisse $A \neq B$ gelten, so gilt, weil $\mathcal{A}_1$ und $\pi \bullet \mathcal{A}_2$ L_1-schneidend bzw. L_2-schneidend sind, $A \cap B \in L_1 \cap L_2$. Das kann aber nicht sein, da L_1 und L_2 disjunkt sind. ↯
Der Rest des Arguments geht über doppeltes Abzählen: Einerseits ist nach unseren obigen Feststellungen klar, dass

$$n! \geq \sum_{\pi \in S_n} |\mathcal{A}_1 \cap \pi \bullet \mathcal{A}_2| = \sum_{A \in \mathcal{A}_1} \sum_{B \in \mathcal{A}_2} \sum_{\pi \in S_n} \mathbb{1}_{A=\pi[B]}$$

gilt. Aus der Sicht von $A \in \mathcal{A}_1, B \in \mathcal{A}_2$ gibt es $k!$ Möglichkeiten, wie π die Elemente von B auf die von A abbildet und $(n-k)!$ Möglichkeiten, wie die restlichen Elemente abgebildet werden. Damit haben wir insgesamt

$$n! \geq |\mathcal{A}_1|\,|\mathcal{A}_2|\,k!(n-k)! \implies \binom{n}{k} \geq |\mathcal{A}_1|\,|\mathcal{A}_2|\,. \qquad \square$$

Blatt 3

Aufgabe 1

Behauptung. Es sei $\mathcal{A} \subseteq [n]^{(33)}$ ein $\{0, 18, 24\}$-schneidendes Mengensystem. Dann ist

$$\mathcal{A} \leq \binom{n}{2}.$$

Beweis 1. Nach dem OddTown Satz / Satz 1.1 folgt direkt

$$|\mathcal{A}| \leq \binom{n}{1} = n \leq \binom{n}{2}. \qquad \square$$

Beweis 2. O.B.d.A. sei $n \geq 33$, sonst ist die Aussage trivial. Wir wenden den Satz von Alon-Babai-Suzuki / Satz 2.17 an: Setze $p = 2, k = 1$, und $L = \{0\} \subseteq \mathbb{F}_2$.
Da $n \geq 33 > |L| + 1$ gilt, und

- $|A| = 33 \equiv_2 1$ für alle $A \in \mathcal{A}$, und
- $\{0, 18, 24\} \ni |A \cap B| \equiv_2 2$ für verschiedene $A, B \in \mathcal{A}$,

gilt nach dem Satz 2.17 nun $|\mathcal{A}| \leq \binom{n}{1} = n \leq \binom{n}{2}$. $\square$

Beweis 3. Es sei $\mathcal{B} = \{A_1, \ldots, A_m\} \subseteq \mathcal{A}$ eine Teilfamilie von disjunkten Mengen maximaler Größe. Beachte, dass jede andere Menge $A \in \mathcal{A} \setminus \mathcal{B}$ nur eines der Mengen in $\mathcal{B}$ schneidet. Für $A \in \mathcal{B}$ ist das klar, würde $A \notin \mathcal{B}$ zwei verschiedene $A_i, A_j \in \mathcal{B}$ schneiden, so hätten wir

$$33 = |A| \geq |A \cap A_i| + |A \cap A_j| \geq 36. \text{ ↯}$$

Es sei also $\mathcal{A}_i := \{A \in \mathcal{A} \mid A \cap A_i \neq \emptyset\}$ für $i \in [m]$, also $\mathcal{A}_1 \cup \ldots \cup \mathcal{A}_m = \mathcal{A}$. Weiter gilt natürlich $A \cap B = \emptyset$ für $A \in \mathcal{A}_i, B \in \mathcal{A}_j$, denn wäre $A \cap B \neq \emptyset$, also $|A \cap B| \in \{18, 24\}$,

so müsste wegen $|C| = 33$ für alle $C \in \mathcal{A}$ bereits $A_i \cap A_j \neq \emptyset$ gelten. ↯ Also findet man eine Partitionierung $[n] = X_1 \dot\cup \ldots \dot\cup X_n$, sodass $\mathcal{A}_i \subseteq X_i^{(33)}$ ist. Nach dem Satz von Ray-Chaudhuri-Wilson ist dann

$$\begin{aligned} |\mathcal{A}| &= \sum_{i=1}^{m} |\mathcal{A}_i| & &\leq \sum_{i=1}^{m} \binom{|X_i|}{2} \\ &= \frac{1}{2} \sum_{i=1}^{m} \left(|X_i|^2 - |X_i| \right) & &= \frac{1}{2} \left(\sum_{i=1}^{m} |X_i|^2 - \sum_{i=1}^{m} |X_i| \right) \\ &\leq \frac{1}{2} \left(\left(\sum_{i=1}^{m} |X_i| \right)^2 - \sum_{i=1}^{m} |X_i| \right) = \binom{n}{2}. \end{aligned}$$

Damit wäre der Beweis vollbracht. □

Bemerkung A.5. Tatsächlich hatte Reiher den dritten Beweis vorgesehen und meinte danach: „Hm, hätte ich 30 statt 33 gewählt, so geht der [dritte] Beweis durch, während Sie dann Schwierigkeiten hätten. Also lasst uns so tun, als wäre 30 immer gemeint gewesen."

Aufgabe 2

Behauptung. Es seien p eine Primzahl, $L = \{0, 1, p\}$ und $k = p^2$. Dann existiert eine nur von p abhängige Konstante $c > 0$ mit folgender Eigenschaft: Für alle $n \geq k$ existiert ein L-schneidendes Mengensystem $\mathcal{A} \subseteq [n]^{(k)}$ mit $|\mathcal{A}| > cn^3$.

Beweis. Betrachte zuerst den Fall $n = p^m, m \geq 2$. Dann lassen sich die Elemente als Vektoren in $\mathbb{F}_p^m$ auffassen. Nehme dann als Familie $\mathcal{A}$ die Menge der affinen Ebenen, also alle 2-dimensionalen Unterräume

$$\{a + \lambda b + \mu c \colon \lambda, \mu \in \mathbb{F}_p\}$$

für $a, b, c \in \mathbb{F}_p^m$, wobei b und c unabhängig sind. Offensichtlich enthält jede solche affine Ebene genau p^2 Elemente.
Weiter ist klar, dass $\mathcal{A}$ dann tatsächlich L-schneidend sind: Ist $1 < |U \cap V| \leq p$ für zwei affine Ebenen $U, V \in \mathcal{A}$, also $x, y \in U \cap V, x \neq y$, so muss die ganze affine Gerade $x + \lambda(y - x)$ in $U \cap V$ sein, also bereits $|U \cap V| = p$ gelten. Ist nun aber $|U \cap V| > p$, konkret $x_1, \ldots, x_p, x_{p+1} \in U \cap V$ paarweise verschieden, so sind auch $x_1 - x_{p+1}, \ldots, x_p - x_{p+1}$ paarweise verschieden und nicht Null, womit dann der affine Unterraum $W = x_{p+1} + \langle \{x_1 - x_{p+1}, \ldots, x_p - x_{p+1}\} \rangle$ mindestens Dimension 2 hat. Also gilt bereits $U = W = V$ und $|U \cap V| = p^2$.
Als nächstes bestimmen wir die Mächtigkeit von $\mathcal{A}$: In der Darstellung einer affinen Ebene durch einen Stützvektor $a \in \mathbb{F}_p^m$ und Spannvektoren $b, c \in \mathbb{F}_p^m$ haben wir

- $\left|\mathbb{F}_p^m\right| = p^m$ Möglichkeiten für a,
- $\left|\mathbb{F}_p^m \setminus \{0\}\right| = p^m - 1$ Möglichkeiten für b, und

- $\left|\mathbb{F}_p^m \setminus \langle\{b\}\rangle\right| = p^m - p$ Möglichkeiten für c.

Für die wahre Mächtigkeit von $\mathcal{A}$ müssen wir aber noch durch die Anzahl an möglichen Darstellungen einer affinen Ebene $A \in \mathcal{A}$ teilen. Dabei haben wir

- $|A| = p^2$ Möglichkeiten für a,
- $|(A-a) \setminus \{0\}| = p^2 - 1$ Möglichkeiten für b, und
- $|(A-a) \setminus \langle\{b\}\rangle| = p^2 - p$ Möglichkeiten für c.

Damit ist

$$|\mathcal{A}| = \frac{p^m(p^m-1)(p^m-p)}{p^2(p^2-1)(p^2-p)} > \frac{n^3}{4p^6}.$$

Für allgemeine $n \geq k$, wähle m gerade so, dass $p^m \leq n < p^{m+1}$.
Wählt man $\mathcal{A}$ wie zuvor, so gilt

$$|\mathcal{A}| = \frac{(p^m)^3}{4p^6} > \frac{n^3}{4p^9}.$$

Man kann als Konstante $c = c(p) = 1/(4p^9)$ wählen. □

Aufgabe 3

Behauptung. Es seien $A_1, \ldots, A_n \subseteq [n]$ paarweise verschieden. Dann existiert $x \in [n]$ derart, dass die Mengen $A_1 \setminus \{x\}, \ldots, A_n \setminus \{x\}$ paarweise verschieden sind.

Lineare Algebra Beweis. Als Elemente von $\mathcal{P}([n])$, fasse man $A_1, \ldots, A_n$ auf kanonische Weise als Vektoren in $\mathbb{F}_2^n$ auf. Da $\dim(U) \leq n-1$ für

$$U \coloneqq \langle\{A_2 - A_1, \ldots, A_n - A_1\}\rangle = \langle\{A_2 + A_1, \ldots, A_n + A_1\}\rangle$$

gilt, muss eines der Standardbasisvektoren $\{1\}, \ldots, \{n\}$ nicht in U sein. Es sei $\{x\}, x \in [n]$, dieser Basisvektor. Dann gilt

$$\{x\} \neq A_i \,\Delta\, A_j = A_i + A_j = (A_i + A_1) + (A_j + A_1)$$

für alle $i, j \in [n], i \neq j$. Also sind $A_1 \setminus \{x\}, \ldots, A_n \setminus \{x\}$ paarweise verschieden. □

Graphentheoretischer Beweis. Wir modellieren das Problem durch einen Graph: Es sei $G = (V, E)$, wobei $V = \mathcal{P}([n])$ und $E = \{AB \mid A, B \in V, |A \,\Delta\, B| = 1\}$, mit anderen Worten ist G das Hasse-Diagramm des *Boolean Lattice*. Wir färben nun die Kanten $AB \in E$ mit dem eindeutigen Element in $A \,\Delta\, B$ und erhalten so eine $[n]$-Kantenfärbung φ von G.
Beachte, dass für verschiedene $A, B \in \mathcal{P}([n])$ und $x \in [n]$ $A \setminus \{x\} = B \setminus \{x\}$ äquivalent ist zu $\varphi(AB) = x$. Wir müssen also zeigen, dass für alle n verschiedenen Mengen $A_1, \ldots, A_n \in V$ höchstens $n-1$ Farben in $G[\{A_1, \ldots, A_n\}]$ auftreten. Für eine nicht auftretende Farbe x wären dann auch $A_1 \setminus \{x\}, \ldots, A_n \setminus \{x\}$ verschieden.

Hierfür betrachten wir zuerst Kreise $C \subseteq G$. Nun ist es so, dass für $AB \in E$ wir $||A| - |B|| = 1$ und $A \cap B \in \{A, B\}$ haben, da $1 = |A \,\Delta\, B| = |A \setminus B| + |B \setminus A|$. Es sei also $A \in V(C)$ eine größte Menge in $V(C)$ und $B \in V(C)$ eine kleinste Menge in $V(C)$. C lässt sich Spalten in zwei A-B-Pfade P, P'. Um von B nach A zu kommen, muss nach unserer Vorbemerkung jedes Element $A \setminus B$ als Farbe in P und P' auftreten.
Also enthält jeder Kreis (zumindest) eine Farbe doppelt. Es seien nun $A_1, \dots, A_n \in V(G)$ paarweise verschieden und $H = G[\{A_1, \dots, A_n\}]$. Wir behaupten nun, dass es einen Spannbaum $T \subseteq H$ gibt, sodass T alle Farben enthält, die auch auf H enthalten sind. Wähle hierfür T so, dass es die größtmögliche Anzahl an Farben unter allen Spannbäumen enthält. Angenommen es gäbe eine Farbe i, die in H, aber nicht in T enthalten ist. Dann existiert $e \in E(H) \setminus E(T)$ mit $\varphi(e) = i$. Da $\{e\} \cup E(T)$ einen Kreis C_e enthält, und auf einem Kreis eine Farbe doppelt aufkommt, existiert ein $e' \in E(C_e)$, sodass $C_e \setminus \{e'\}$ mehr Farben enthält als $C_e \setminus \{e\}$. Aber dann ist $T' = (V(T), (E(T) \cup \{e\}) \setminus \{e'\})$ ein Spannbaum, der eine größere Anzahl an Farben als T hat. ↯
Also existiert ein Spannbaum T mit allen Farben von H. Da aber T als Baum genau $n - 1$ Kanten hat, ist die Anzahl an Farben in H höchstens $n - 1$.
Es folgt die Behauptung. □

Bemerkung A.6. Reiher merkte an, dass die Tatsache, dass sich der Beweis sowohl mit der linearen Algebra und der Graphentheorie erbringen lässt, damit zusammenhängt, dass man letztlich allgemeiner gesehen die Matroid-Eigenschaften der beiden Teilgebiete ausnutzt.

Beweis. Es sei $A_1, \dots, A_n \subseteq [n]$ paarweise verschieden. Es reicht zu zeigen, dass für eine Familie $\mathcal{A}$ der Größe n es dual ein Y mit $|Y| \leq n - 1$ gibt, sodass $Y \cap A_1, \dots, Y \cap A_n$ verschieden sind. Wähle dann $\mathcal{A} = \{A_1, \dots, A_n\}$ und $x \in [n] \setminus Y$. Ist $X_i \setminus \{x\} = X_j \setminus \{x\}$ für $i \neq j$, so wäre insbesondere

$$X_i \cap Y = (X_i \setminus \{x\}) \cap Y = (X_j \setminus \{x\}) \cap Y = X_j \cap Y. \text{ ↯}$$

Sei also $\mathcal{A} = \{A_1, \dots, A_n\}$ eine Familie der Größe n mit Grundmenge X. Wir zeigen die Aussage per Induktion über n: Ist $n = 1$, so kann man $Y = \emptyset$ wählen. Sei nun $n > 1$. Wähle $y \in X$, sodass

$$\mathcal{A}' \coloneqq \{A_i \mid i \in [n], y \notin A_i\}, \qquad \mathcal{A}'' \coloneqq \{A_i \setminus \{n\} \mid i \in [n], y \in A_i\}$$

nicht-leer sind. Da $|\mathcal{A}'| + |\mathcal{A}''| = n$, erhalten wir per Induktion Y', Y'' mit $|Y'| \leq |\mathcal{A}'| - 1, |Y''| \leq |\mathcal{A}''| - 1$, sodass die Mengen von $\mathcal{A}'$ geschnitten mit Y' bzw. die Mengen von $\mathcal{A}''$ geschnitten mit Y'' verschieden sind. Setze $Y = \{y\} \cup Y' \cup Y''$. Dann ist

$$|Y| \leq 1 + (|\mathcal{A}'| - 1) + (|\mathcal{A}''| - 1) = |\mathcal{A}| - 1$$

wie gewünscht. □

Bemerkung A.7. Die Aussage stimmt nicht für $n + 1$ Teilmengen von $[n]$: Betrachte die Mengen $[n] \setminus \{1\}, \dots, [n] \setminus \{n\}, [n] \subseteq [n]$. Egal welches Element $x \in [n]$ man betrachtet, es wird $([n] \setminus \{x\}) \setminus \{x\} = [n] \setminus \{x\}$ gelten. Dual könnte man natürlich auch $\{1\}, \{2\}, \dots, \{n\}, \emptyset \subseteq [n]$ anschauen. Eine aufsteigende Kette startend bei $\emptyset$ bis $[n]$ wie zum Beispiel $\emptyset, [1], [2], \dots, [n]$ wäre auch schlecht.

Aufgabe 4

Behauptung. Es gilt $\chi(\mathcal{G}_n) \leq 9^n$. Mit anderen Worten kann man $\mathbb{R}^n$ so mit 9^n Farben färben, dass je zwei Punkte mit Abstand 1 verschiedenfarbig sind.

Hinweis. Man betrachte eine maximale Menge $M \subseteq \mathbb{R}^n$ mit der Eigenschaft, dass $\|x - y\| \geq 1/2$ für alle verschiedenen $x, y \in M$ gilt. Warum kann man M so mit 9^n Farben färben, dass je zwei gleichfarbige Punkte mindestens den Abstand 2 haben?

Beweis. Wir zeigen zuerst den Hinweis: M ist abzählbar, da ein (abgeschlossener) Ball mit Radius $1/4$ höchstens zwei der Punkte in M enthält und die Bälle mit Radius und Mittelpunkt in $\sqrt{1/32} \cdot \mathbb{Z}^n$ abzählbar sind und $\mathbb{R}^n$ überdecken. Also kann man die Elemente $m_1, m_2, \ldots \in M$ auflisten. M existiert außerdem nach dem Lemma von Zorn.[49] Wir gehen jetzt *greedy* vor und geben m_1 eine beliebige Farbe und m_{i+1} eine beliebige Farbe, die keinem Punkt in $M' \coloneqq \{m_j \mid j \in [i], \|m_{i+1} - m_j\| < 2\}$ bereits zugewiesen wurde. Wir müssen nun zeigen, dass es tatsächlich möglich ist, also $|M'| < 9^n$ bzw. im (offenen) Ball um m_{i+1} es weniger als 9^n Punkte von M gibt. Hierfür beobachte man, dass $B_{1/4}(m) \subseteq B_{9/4}(m_{i+1})$ gilt für alle $m \in M'$ und für je zwei verschiedene $m_1, m_2 \in M' \subseteq M$ wir $B_{1/4}(m_1) \cap B_{1/4}(m_2) = \emptyset$ haben. Damit ist aber

$$|M'| < \frac{\lambda^n(B_{9/4}(0))}{\lambda^n(B_{1/4}(0))} = \frac{\left(\frac{9}{4}\right)^n}{\left(\frac{1}{4}\right)^n} = 9^n,$$

wobei die erste Ungleichung gilt, weil man mit den Bällen nicht perfekt der Ball mit Radius $9/4$ überdecken kann.
Um nun die eigentliche Aussage zu zeigen wähle man M wie oben und färbe entsprechend die Punkte von M. Da M maximal war, existiert für jeden Punkt $x \in \mathbb{R}^n \setminus M$ ein $m \in M$, sodass $\|x - m\| < 1/2$. Färbe x dann mit derselben Farbe wie m. Angenommen diese Färbung wäre nicht gültig. Dann existieren gleichgefärbte $x, y \in \mathbb{R}^n$ mit $\|x - y\| = 1$. Dies impliziert aber, dass $\{x, y\} \not\subseteq M$. O.B.d.A. sei deswegen $x \in \mathbb{R}^n \setminus M$. Dann wurde x entsprechend der Farbe eines $m_x \in M$ mit $\|x - m_x\| < 1/2$ gefärbt. Gleiches gilt für y für ein gewisses $m_y \in M$, wobei eventuell $m_y = y$, aber immer $\|m_y - y\| < 1/2$ gilt. Beachte, dass wegen

$$1 = \|x - y\| \leq \|x - m_x\| + \|m_x - m_y\| + \|m_y - y\| < 1 + \|m_x - m_y\|$$

$\|m_x - m_y\| > 0$ gilt, also m_x, m_y verschieden sind. Nun sind m_x und m_y zudem aber gleichgefärbt und

$$\|m_x - m_y\| \leq \|m_x - x\| + \|x - y\| + \|y - m_y\| < 2. \lightning$$

Also ist die Färbung doch gültig und der Beweis erbracht. □

[49] Sehr konstruktiv...

Aufgabe 5

Behauptung. Für $n \geq 3$ seien $S_1, \ldots, S_n \in \mathbb{R}^2$ senkrechte (d.h. zur y-Achse parallele) Strecken. Für alle $\{i,j,k\} \in [n]^{(3)}$ gebe es eine Gerade $g_{i,j,k}$, die S_i, S_j und S_k schneidet. Dann gibt es eine Gerade, die alle gegebenen Strecken schneidet.

Beweis. Es seien $S_1, \ldots, S_n \subseteq \mathbb{R}^2$ $n \geq 3$ senkrechte Strecken, sodass für alle $\{i,j,k\} \in \binom{[n]}{3}$ es eine Gerade $g_{i,j,k}$ gibt, die S_i, S_j und S_k schneidet. Da die S_i senkrecht sind, ist $S_i = \{x_i\} \times [y_i^1, y_i^2]$ für gewisse $x_i, y_i^1, y_i^2 \in \mathbb{R}$. O.B.d.A. sind alle x_i paarweise verschieden. Sonst gäbe es $i \neq j$ mit $x_i = x_j$, wo dann jede Schnittgerade, die beide schneidet, gerade $\{x_i\} \times \mathbb{R}$ ist und damit bereits $x_1 = \cdots = x_n$ gilt. Weiter sei

$$X_i \coloneqq \left\{(a,b) \in \mathbb{R}^2 \mid y_i^1 \leq ax_i + b \leq y_i^2\right\}$$

für $i \in [n]$. Beachte, dass X_i die Menge aller möglichen Parametrisierungen einer nicht senkrechten, S_i schneidenden Gerade sind.
Diese Mengen sind konvex, denn ist $(a,b), (a',b') \in X_i$, so gilt für alle $\lambda \in [0,1]$

$$(\lambda a + (1-\lambda)a')x_i + (\lambda b + (1-\lambda)b') = \lambda(ax_i + b) + (1-\lambda)(a'x_i + b') \in [y_i^1, y_i^2].$$

Weil alle S_i unterschiedliche x_i haben, gilt nach Voraussetzung

$$g_{i,j,k} \in X_i \cap X_j \cap X_k \neq \emptyset$$

für $\{i,j,k\} \in \binom{[n]}{3}$. Nach dem Satz von Helly folgt damit bereits $X_1 \cap \cdots \cap X_n \neq \emptyset$. Insbesondere existiert $(a,b) \in \mathbb{R}^2$, sodass die Gerade $a\mathbb{R} + b$ alle X_i schneidet. □

Blatt 4

Aufgabe 1

Behauptung. Es existiert eine Folge $(A_m)_{m\in\mathbb{N}}$ konvexer Teilmengen des $\mathbb{R}^n$, sodass sich je $n+1$ Mengen schneiden, aber $\bigcap_{m\in\mathbb{N}} A_m = \emptyset$.

Beweis. Setze $A_m = \{x \in \mathbb{R}^n \mid \langle x, e_1\rangle \geq m-1\}$ für alle $m \in \mathbb{N}$. Mit anderen Worten ist A_m der abgeschlossene Halbraum, die in ihrer ersten Koordinate größer gleich $m-1$ sind. Wir wissen, dass damit alle A_m konvex sind: Sind $x, y \in A_m$, so auch $\lambda x + (1-\lambda)y$ für alle $\lambda \in [0,1]$, denn

$$\langle \lambda x + (1-\lambda)y, e_1\rangle \, \lambda \langle x, e_1\rangle + (1-\lambda)\langle y, e_1\rangle \geq m-1.$$

Wir wissen zudem, dass $A_1 \subseteq A_2 \subseteq \ldots$ Insbesondere schneiden sich je $n+1$ Mengen. Andererseits ist aber klar, dass $\bigcap_{m\in\mathbb{N}} A_m = \emptyset$, denn für alle $x = (x_1, \ldots, x_n)$ existiert ein $m \in \mathbb{N}$ mit $m - 1 > x_1$, womit $x \notin A_m$ gilt. □

Bemerkung A.8. Das Beispiel zeigt genauer, dass Beschränktheit notwendig ist bei der unendlichen Version vom Satz von Helly. Für ein Beispiel der Notwendigkeit der Abgeschlossenheit, definiere $B_m = \{x \in \mathbb{R}^n \mid \|x - (1-2^{-m})\cdot e_1\| < 2^{-m}\}$ für $m \in \mathbb{N}_0$.

Aufgabe 2

Behauptung. Es seien $A, B \subseteq \mathbb{R}^n$ zwei disjunkte, endliche Punktmengen. Für jede Menge $Z \subseteq A \cup B$ von $n+2$ Punkten, gebe es eine Hyperebene H, die $A \cap Z$ streng von $B \cap Z$ trennt. Dann gibt es eine Hyperebene, die ganz A streng von B trennt.

Hinweis. Von einer Hyperebene H sagt man, sie trenne zwei Punktmengen X und Y streng, wenn von den beiden offenen Halbräumen, in die $\mathbb{R}^n \setminus H$ zerfällt, der eine X und der andere Y enthält.

Beweis. Für $a \in A$ setze $K_a = \{(c_0, c_1, \ldots, c_n) \in \mathbb{R}^{n+1} \mid \langle (c_1, \ldots, c_n), a\rangle > c_0\}$. Für $b \in B$ setze $K_b = \{(c_0, c_1, \ldots, c_n) \in \mathbb{R}^{n+1} \mid \langle (c_1, \ldots, c_n), b\rangle < c_0\}$. Beachte, dass diese Mengen konvex sind: Gilt für $x \in \mathbb{R}^n, (c_0, c_1, \ldots, c_n), (d_0, d_1, \ldots, d_n) \in \mathbb{R}^{n+1}$

$$\langle (c_1, \ldots, c_n), x\rangle \overset{>}{\underset{<}{=}} c_0 \qquad\qquad \langle (d_1, \ldots, d_n), x\rangle \overset{>}{\underset{<}{=}} d_0,$$

so folgt für alle $\lambda \in [0,1]$

$$\langle \lambda(c_1, \ldots, c_n) + (1-\lambda)(d_1, \ldots, d_n), x\rangle \overset{>}{\underset{<}{=}} \lambda c_0 + (1-\lambda) d_0.$$

Nach den Voraussetzungen wissen wir, dass je $n+2$ dieser Mengen sich schneiden. Also existiert nach dem Satz von Helly ein

$$(c_0, c_1, \ldots, c_n) \in \bigcap_{a \in A} K_a \cap \bigcap_{b \in B} K_b.$$

Die Hyperebene $\{x \in \mathbb{R}^n \mid \langle (c_1, \ldots, c_n), x\rangle = c_0\}$ tut es dann. □

Aufgabe 3

Behauptung. Es sei $K \subseteq \mathbb{R}^n$ eine kompakte, konvexe Menge. Dann existiert ein Punkt $z \in K$ mit folgender Eigenschaft: Sind u und v Randpunkte von K, für die z auf der Strecke $\overline{uv}$ liegt, so gilt

$$\|z - u\| \leq \frac{n}{n+1} \|u - v\|.$$

Beweis. Es sei K kompakt und konvex. Für $x \in K$ setze $K_x = x + \frac{n}{n+1}(K - x)$.
Je $n+1$ diesr Mengen schneiden sich: Es seien $x_1, \ldots, x_{n+1} \in K$. Es genügt

$$\frac{x_1 + \cdots + x_{n+1}}{n+1} \in K_{x_1} \cap \cdots \cap K_{x_{n+1}}$$

zu zeigen. In der Tat ist für alle $i \in [n+1]$

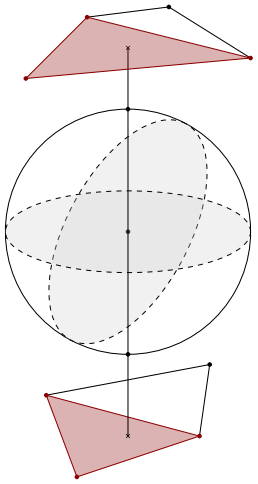
$$\frac{x_1 + \cdots + x_{n+1}}{n+1} = x_i + \frac{n}{n+1}\Bigg(\underbrace{\frac{\sum_{j \in [n], j \neq i} x_j}{n}}_{\in K} - x_i\Bigg) \in K_{x_i}.$$

Nach dem Satz von Helly existiert also $z \in \bigcap_{x \in K} K_x$. Seien $u, v \in \partial K$ mit $z \in \overline{uv}$. Wegen $z \in K_u$ gibt es $u' \in K$ mit $z - u = n/(n+1) \cdot (u' - u)$. Dann $u' \in \overline{zv}$ und

$$\|z - u\| = \frac{n}{n+1} \cdot \|u' - u\| \leq \frac{n}{n+1} \|u - v\|. \qquad \square$$

Aufgabe 4 (Satz von Steinitz)

Behauptung. Es seien $A \subseteq \mathbb{R}^n$ beliebig und x ein innerer Punkt der konvexen Hülle von A. Dann existiert eine Menge $B \subseteq A$ mit $|B| \leq 2n$ existiert, für die x ein innerer Punkt der konvexen Hülle von B ist.



Beweis. Es sei $A \in \mathbb{R}^n$. O.B.d.A. sei $x = 0$ und o.B.d.A. A endlich.
Letzteres dürfen wir ohne Einschränkung annehmen, denn – wäre dies nicht der Fall – so betrachte einen hinreichend kleinen Ball B mit Mittelpunkt x, der komplett in $H(A)$ ist. Mit den Ecken eines Hyperwürfels, der in seinen Ecken gerade so B berührt, haben wir dann innerhalb deren konvexen Hülle x. Da wir zudem nach dem Satz von Carathéodory jeden der $2n$ Ecken des Hyperwürfels als Linearkombination von $n+1$ Punkte in A nehmen können, ist damit insgesamt x in der inneren Hülle von $2n(n+1)$ Punkten in A und wären damit fertig, wenn wir zeigen können, dass wir von diesen $2n(n+1)$ $2n$ auswählen können, sodass x im Inneren dieser ist.
Es sei also A endlich und $H(A)$ damit ein Polytop. O.B.d.A. ist $x = 0 \notin A$. Wähle eine Gerade g durch x, sodass diese nie die konvexe Hülle von $n-1$ Punkten $a_1, \ldots, a_{n-1}$ aus A trifft. Beachte, dass dies möglich ist, da die Hülle von $n-1$ Punkten, als Teilmenge einer $n-1$-dimensionalen Hyperebene, eine Lebesgue Nullmenge bildet.
Durch die Wahl der Gerade schneidet g $\partial H(A)$ in dem Inneren von zwei Facetten von $H(A)$. Mit anderen Worten wird also durch diese Gerade x auf das Innere von zwei verschiedenen Facetten von $H(A)$ projiziert. Seien x^1, x^2 die Schnittpunkte und $\lambda \in (0,1)$, sodass $\lambda x^1 + (1-\lambda)x^2 = x$. Da eine Facette von $H(A)$ die Konvexkombination von n Punkten in A ist, existieren $\lambda_1^i, \ldots, \lambda_n^i \in (0,1), \sum_{j=1}^n \lambda_j^i = 1$ und $a_1^i, \ldots, a_n^i \in A$, sodass $x^i = \sum_{j=1}^n \lambda_j^i a_j^i$, $i \in [2]$. Somit ist

$$x = \sum_{j=1}^{n} \underbrace{\lambda \cdot \lambda_j^1}_{\in(0,1)} a_j^1 + \sum_{j=1}^{n} \underbrace{(1-\lambda)\lambda_j^2}_{\in(0,1)} a_j^2, \qquad \sum_{j=1}^{n} \lambda \cdot \lambda_j^1 (1-\lambda)\lambda_j^2 = 1.$$

Also ist x ein innerer Punkt der konvexen Hülle von den (höchstens) $2n$ Punkten. □

Bemerkung A.9. $A = \{\pm e_1, \dots, \pm e_n\} \subseteq \mathbb{R}^n$ und $0 \in \mathbb{R}^n$ zeigen, dass $2n$ optimal ist.

Aufgabe 5

Man nennt $\mathcal{A} \subseteq \mathcal{P}([n])$ eine *Antikette*, wenn $A \not\subseteq B$ für alle verschiedenen $A, B \in \mathcal{A}$ gilt. Ein Satz von Sperner besagt, dass $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$ für jede Antikette $\mathcal{A} \subseteq \mathcal{P}([n])$ gilt.

Behauptung. Der Satz von Sperner folgt aus dem Lemma von Bollobás / Lemma 4.15.

Beweis. Es sei $\mathcal{A} = \{A_1, \dots, A_m\}$ eine Antikette. Setze $B_i = [n] \setminus A_i$ für alle $i \in [m]$. Da $\mathcal{A}$ eine Antikette ist, gilt $A_i \cap B_j = A_i \setminus A_j \neq \emptyset \neq A_j \setminus A_i = A_j \cap B_i$ für $i, j \in [m], i \neq j$. Nach Lemma 4.15 gilt also

$$1 \geq \sum_{i=1}^{m} \frac{1}{\binom{|A_i|+|B_i|}{|A_i|}} = \sum_{i=1}^{m} \frac{1}{\binom{n}{|A_i|}}.$$

Beachte, dass $\binom{n}{|A_i|} \leq \binom{n}{\lfloor n/2 \rfloor}$ für alle $i \in [m]$ gilt. Also ist

$$1 \geq \frac{m}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} \implies m \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}. \qquad \square$$

Blatt 5

Aufgabe 1

Behauptung. Folgende Version vom Lemma von Bollobás / Lemma 4.15 ist falsch: Es seien $A_1, \dots, A_m, B_1, \dots, B_m$ endliche Mengen. Wenn $A_i \cap B_i = \emptyset$ für alle $i = 1, \dots, m$ und $A_i \cap B_j \neq \emptyset$ für $1 \leq i < j \leq m$, dann ist

$$\sum_{i=1}^{m} \frac{1}{\binom{|A_i|+|B_i|}{|A_i|}} \leq 1.$$

Beweis. Es sei $n \in \mathbb{N}$ mit $n > 2$. Definiere für $i \in [n]$

$$A_i \coloneqq \{i+1, i+2, \dots, n\} \qquad\qquad B_i \coloneqq [i].$$

Dann gilt für $1 \leq i \leq j \leq n$

$$A_i \cap B_j = \begin{cases} \emptyset, & i = j \\ \{i+1, i+2, \dots, j\}, & i < j. \end{cases}$$

Insbesondere erfüllen $A_1, \dots, A_n, B_1, \dots, B_n$ die Voraussetzung der Version des Lemmas. Da zudem $|A_i| = n - i$ und $|A_i \cup B_i| = n$ gilt, folgt

$$\sum_{i=1}^{n} \frac{1}{\binom{|A_i|+|B_i|}{|A_i|}} = \sum_{i=1}^{n} \underbrace{\frac{1}{\binom{n}{n-i}}}_{>0} \overset{n>1}{>} \frac{1}{\binom{n}{0}} = 1. \; \lightning \qquad \square$$

Bemerkung A.10. Das simpelste Gegenbeispiel ist wahrscheinlich $A_1 = B_2 = \{1\}$ und $A_2 = B_1 = \emptyset$. Hier ist

$$\sum_{i=1}^{2} \frac{1}{\binom{|A_i|+|B_i|}{|A_i|}} = 2.$$

Laut Reiher ist es tatsächlich so, dass die Summe der Kehrwerte sogar beliebig groß werden kann.

Aufgabe 2

Behauptung. Es seien X_1, X_2 zwei disjunkte Mengen und $X = X_1 \cup X_2$ ihre Vereinigung. Ferner seien $r_1, r_2, s_1, s_2 \in \mathbb{N}$ und $A_1, \ldots, A_m, B_1, \ldots, B_m$ Teilmengen von X.
Es gelte

- $|A_i \cap X_k| = r_k$ und $|B_i \cap X_k| = s_k$ für alle $i \in [m], k \in [2]$,
- $A_i \cap B_i = \emptyset$ für alle $i \in [m]$,
- $A_i \cap B_j \neq \emptyset$ wann immer $1 \leq i < j \leq m$.

Dann gilt

$$m \leq \binom{r_1 + s_1}{r_1}\binom{r_2 + s_2}{r_2}.$$

Beweis. Wir emulieren den Beweis von Satz 4.18: Wir definieren für $i \in [m]$

$$a_i(x) \coloneqq \begin{pmatrix} \prod_{\alpha \in A_i \cap X_1}(x - \alpha) \\ \prod_{\alpha \in A_i \cap X_2}(x - \alpha) \end{pmatrix} \qquad b_i(x) \coloneqq \begin{pmatrix} \prod_{\beta \in B_i \cap X_1}(x - \beta) \\ \prod_{\beta \in B_i \cap X_2}(x - \beta) \end{pmatrix}.$$

Wir setzen $\tilde{\mathrm{Res}}\colon (\mathbb{R}[x])^2 \times (\mathbb{R}[x])^2 \to \mathbb{R}, ((p_1, p_2), (q_1, q_2)) \mapsto \mathrm{Res}(p_1, q_1) \cdot \mathrm{Res}(p_2, q_2)$, wobei $\mathrm{Res}(\cdot, \cdot)$ die Resultante ist. Nach den Voraussetzungen und Lemma 4.17 ist

- $\tilde{\mathrm{Res}}(a_i, b_i) \neq 0$ für alle $i \in [m]$, und
- $\tilde{\mathrm{Res}}(a_i, b_j) = 0$ für alle $1 \leq i < j \leq m$.

Weiter seien $y_0, \ldots, y_{s_1}, z_0, \ldots, z_{s_2}$ weitere Variablen und

$$b = \begin{pmatrix} y_0 + y_1 x + \cdots + y_{s_1} x^{s_1} \\ z_0 + z_1 x + \cdots + z_{s_2} x^{s_2} \end{pmatrix}.$$

Komponentenweise fassen wir dann b als ein Polynom in x über $\mathbb{R}[y_0, y_1, \ldots, y_{s_1}]$ bzw. $\mathbb{R}[z_0, z_1, \ldots, z_{s_2}]$ auf. Für alle $i \in [m]$ ist $\tilde{\mathrm{Res}}(a_i, b) \in V$, wobei V der $\mathbb{R}$-Untervektorraum von $\mathbb{R}[y_0, \ldots, y_{s_1}, z_0, \ldots, z_{s_2}]$ ist, welcher von allen

$$y_0^{\mu_0} \cdot \ldots \cdot y_{s_1}^{\mu_{s_1}} \cdot z_0^{\nu_0} \cdot \ldots \cdot z_{s_2}^{\nu_{s_2}}$$

mit $\mu_0 + \cdots + \mu_{s_1} = r_1, \nu_0 + \cdots + \nu_{s_2} = r_2$ aufgespannt wird.
Wir zeigen als nächstes, dass $(\tilde{\mathrm{Res}}(a_i))_{i \in [m]}$ linear unabhängig sind:

Angenommen, es gäbe $\lambda_1, \dots, \lambda_m \in \mathbb{R}$, die nicht alle Null sind, sodass

$$\sum_{i=1}^{m} \lambda_i \tilde{\mathrm{Res}}(a_i, b) = 0.$$

Sei $j \in [m]$ maximal mit $\lambda_j \neq 0$. Durch Einsetzen von b_j erhalten wir

$$\sum_{1 \leq i < j} \lambda_i \underbrace{\tilde{\mathrm{Res}}(a_i, b_j)}_{=0} + \underbrace{\lambda_j \, \mathrm{Res}(a_j, b_j)}_{\neq 0} + \sum_{m \geq i > j} \underbrace{\lambda_i}_{=0} \tilde{\mathrm{Res}}(a_i, b_j) = 0. \; \lightning$$

Wegen der linearen Unabhängigkeit gilt also $m \leq \binom{r_1+s_1}{r_1} \cdot \binom{r_2+s_2}{r_2}$. □

Aufgabe 3

Behauptung. Es sei $n \in \mathbb{N}$ und m die kleinste natürliche Zahl ist, sodass (affine) Ebenen $E_1, \dots, E_m \subseteq \mathbb{R}^3$ mit den folgenden Eigenschaften existieren:

- Keine der Ebenen enthält $(0, 0, 0)$.
- Bis auf dem Ursprung wird jeder Punkt des Würfels $\{0, 1, \dots, n\}^3$ von einer der Ebenen überdeckt.

Dann ist $m = 3n$.

Beweis. Wir zeigen zuerst $m \leq 3n$: Die Familie an (affinen) Ebenen gegeben durch $(\{x_i = j\})_{i \in [3], j \in [n]}$ tut das gewünschte und besitzt $3n$ Elemente.
Für $m \geq 3n$ gehen wir wie im Satz 5.4 vor: Angenommen $m < 3n$. Es seien

$$\langle a_i, x \rangle = b_i \; (i \in [m])$$

die Gleichungen von $E_1, \dots, E_m$. Dann ist $b_i \neq 0$ wegen $0 \notin H_i$. Betrachte das Polynom

$$P(x_1, x_2, x_3) = \prod_{i=1}^{m} (b_i - \langle a_i, x \rangle) - \left(\prod_{i=1}^{m} b_i \right) \prod_{j=1}^{3} \left(\prod_{k=1}^{n} \frac{k - x_j}{k} \right).$$

Offensichtlich hat P Grad $3n$ und das Monom $x_1^n \cdot x_2^n \cdot x_3^n$ kommt in P vor. Nach dem kombinatorischen Nullstellensatz gibt es also $v := (v_1, v_2, v_3) \in \{0, 1, \dots, n\}^3$ mit $P(v_1, v_2, v_3) \neq 0$. Angenommen $v \neq (0, 0, 0)$. Dann wird v von einen der Ebenen überdeckt, womit

$$\prod_{i=1}^{m} (b_i - \langle a_i, v \rangle) = 0$$

gilt. Da aber es eine Koordinate von v nicht Null ist, muss zudem

$$\left(\prod_{i=1}^{m} b_i \right) \prod_{j=1}^{3} \left(\prod_{k=1}^{n} \frac{k - v_j}{k} \right)$$

gelten. Also ist $P(v_1, v_2, v_3) = 0$. $\lightning$ Daher muss $v = (0, 0, 0)$ sein, aber

$$P(0, 0, 0) = \prod_{i=1}^{m} b_i - \left(\prod_{i=1}^{m} b_i \right) \prod_{j=1}^{3} \left(\prod_{k=1}^{n} 1 \right) = 0. \; \lightning$$

Also ist $m \geq 3n$ und insgesamt $m = 3n$. □

Aufgabe 4

Behauptung. Es seien p eine Primzahl und G ein Graph. Es sei $\Delta(G) \leq 2p-1$ und $d(G) > 2p-2$. Dann besitzt G einen nicht-leeren p-regulären Teilgraphen.

Hinweis. Man ordne jeder Kante e von G eine Variable x_e zu und betrachte ein Polynom P über $\mathbb{F}_p$.

Beweis. Es sei $G = (V, E)$ mit $\Delta(G) \leq 2p-1$ und $d(G) > 2p-2$. Für $v \in V$ sei $E_v \coloneqq \{e \in E \mid v \in e\}$. Wie im Hinweis beschrieben, ordnen wir jeder Kante e von G eine Variable $x_e \in \{0,1\}$ zu. Setze

$$P(x) \coloneqq \prod_{v \in V} \left[-\prod_{i=1}^{p-1} \left(i - \left(\sum_{e \in E_v} x_e \right) \right) \right] - \prod_{e \in E} (1 - x_e) \in \mathbb{F}_p[\{x_e \mid e \in E\}].$$

Wegen den Voraussetzungen[50] ist klar, dass $P(x) = 0$ ist, wenn die Eins-Komponenten von x entweder der Kantenmenge des leeren Graphens oder eines nicht p-regulären Graphens entsprechen. Andererseits, wenn die Eins-Komponenten einem nicht-leeren, p-regulären Graphen entsprechen, so gilt nach dem Satz von Wilson

$$P(x) = \prod_{v \in V} (-\underbrace{(p-1)!}_{\equiv -1 \pmod p}) - 0 \equiv 1 \pmod p.$$

Klar ist, dass $\deg(P(x)) \leq |E|$. Wir werden jetzt zeigen, dass tatsächlich Gleichheit gilt, also das Monom $\prod_{e \in E} x_e$ in $P(x)$ enthalten ist. Es genügt hierfür zu zeigen, dass

$$Q(x) = \prod_{v \in V} \left[-\prod_{i=1}^{p-1} \left(i - \left(\sum_{e \in E_v} x_e \right) \right) \right]$$

nicht $\prod_{e \in E} x_e$ enthält. Hierfür mache man folgende Beobachtung: Für fixes $v \in V$ hat der innere Term höchstens Grad $p-1$. Durch das Bilden des ganzen Produktes ist also der Grad höchstens $|V|\,(p-1)$. Aus $d(G) > 2p-2$ folgt aber mit dem Handschlaglemma

$$\frac{2\,|E|}{|V|} = \frac{\sum_{v \in V} \deg(v)}{|V|} = d(G) > 2p-2 \implies |E| > (p-1)\,|V|\,.$$

Also kann einfach wegen dem zu kleinen Maximalgrades $\prod_{e \in E} x_e$ nicht in $Q(x)$ enthalten sein.
Demnach ist $\prod_{e \in E} x_e$ *das* Monom maximalen Grades in P, womit nach dem kombinatorischen Nullstellensatz $x \in \{0,1\}^E$ mit $P(x) \neq 0$ existiert. Dieses x entspricht unserem gesuchten nicht-leeren, p-regulären Teilgraphen von G. □

[50] Hauptsächlich $\Delta(G) \leq 2p-1$.

Beweis mit anderem, ähnlichen Trick. Man wähle stattdessen

$$P(x) \coloneqq \prod_{v \in V} \left[1 - \left(\sum_{e \in E_v} x_e \right)^{p-1} \right] - \prod_{e \in E} (1 - x_e).$$

Man nutzt statt den Satz von Wilson dann den kleinen Satz von Fermat, das Prinzip ist aber dasselbe. □

Aufgabe 5

Behauptung. Es seien p eine Primzahl, $d \in \mathbb{N}$ und G ein Graph mit mehr als $d(p-1)$ Ecken. Dann existiert eine nicht-leere Menge $U \subseteq V(G)$ existiert, für die die Anzahl der U schneidenden d-Cliquen in G durch p teilbar ist.

Hinweis. Man ordne jeder Knoten v von G eine Variable x_v zu und betrachte ein Polynom P über $\mathbb{F}_p$.

Beweis. Es seien p eine Primzahl, $d \in \mathbb{N}$ und $G = (V, E)$ ein Graph mit $|V| > d(p-1)$. Setze $\mathcal{D}$ für die Familie (der Knotenmengen) aller d-Cliquen in G. Wie im Hinweis beschrieben, ordnen wir jedem Knoten $v \in V$ eine Variable $x_v \in \{0, 1\}$ zu. Setze

$$P(x) = \prod_{v \in V} (1 - x_v) + \prod_{i=1}^{p-1} \left[i - \sum_{D \in \mathcal{D}} \left(1 - \prod_{v \in D} (1 - x_v) \right) \right] \in \mathbb{F}_p[\{x_v \mid v \in V\}].$$

Ist $x \equiv 0$, so gilt nach dem Satz von Wilson

$$P(x) = 1 + \prod_{i=1}^{p-1} \left(i - \sum_{D \in \mathcal{D}} (1 - 1) \right) = 1 + (p-1)! \equiv 0 \pmod{p}.$$

Wäre $U \subseteq V$ nicht-leer, sodass die Anzahl an U schneidenden d-Cliquen nicht durch p teilbar ist, so gilt zum korrespondierenden x

$$\sum_{D \in \mathcal{D}} \left(1 - \prod_{v \in D} (1 - x_v) \right) \not\equiv 0 \pmod{p}.$$

Also ist dann

$$P(x) = 0 + \prod_{i=1}^{p-1} \left[i - \sum_{D \in \mathcal{D}} \left(1 - \prod_{v \in D} (1 - x_v) \right) \right] \equiv 0 \pmod{p}.$$

Andererseits gilt für nicht-leere $U \subseteq V$, wo die Anzahl an U schneidenden d-Cliquen durch p teilbar ist,

$$\sum_{D \in \mathcal{D}} \left(1 - \prod_{v \in D} (1 - x_v) \right) \equiv 0 \pmod{p}$$

für das korrespondierende x. Also ist dann

$$P(x) \equiv 0 + \prod_{i=1}^{p-1} (i-0) \equiv -1 \pmod{p}$$

nach dem Satz von Wilson. Wir sehen also, dass für $x \in \{0,1\}^V$ $P(x)$ genau dann Null ist, wenn x zu einer nicht-leeren Teilmenge $U \subseteq V$ korrespondiert, wo die Anzahl an U schneidenden d-Cliquen durch p teilbar ist.
Wir betrachten jetzt genauer P. Klar ist, dass von

$$\prod_{i=1}^{p-1} \left[i - \sum_{D \in \mathcal{D}} \left(1 - \prod_{v \in D} (1 - x_v) \right) \right]$$

der innere Term höchstens Grad d hat, also der Term insgesamt höchstens Grad $d(p-1)$ hat. Da aber $|V| > d(p-1)$, ist der Grad von P gerade $|V|$ und $\prod_{v \in V} x_v$ ein in P enthaltenes Monom maximalen Grads.
Also existiert nach dem kombinatorischen Nullstellensatz $x \in \{0,1\}^V$ mit $P(x) \neq 0$. Damit existiert ein nicht-leeres $U \subseteq V$, sodass die Anzahl der U schneidenden d-Cliquen durch p teilbar ist. □

Bemerkung A.11. Man kann wie bei Aufgabe 4 auch hier wieder umformen. Die „Brücke“ vom kleinen Satz von Fermat zum Satz von Wilson ist die Polynomgleichung

$$\prod_{i=1}^{p-1} (i - y) = y^{p-1} - 1$$

über $\mathbb{F}_p$. Man sieht, dass die beiden Polynome denselben Grad haben und nach dem kleinen Satz von Fermat sie in ihren Nullstellen ($\mathbb{F}_p \setminus \{0\}$) übereinstimmen. Also sind sie (über $\mathbb{F}_p$) gleich. Insbesondere liefert er für $y = 0$ gerade den Satz von Wilson, und äquivalent hätte man in Aufgabe 5 auch

$$P(x) = \prod_{v \in V} (1 - x_v) + \left[\sum_{D \in \mathcal{D}} \left(1 - \prod_{v \in D} (1 - x_v) \right) \right]^{p-1} - 1$$

setzen können.

Blatt 6

Aufgabe 1

Behauptung. Es seien p eine Primzahl und $n \in \mathbb{N}$. Dann besitzt jede Folge $P_1, \ldots, P_{n(p-1)+1} \in \mathbb{F}_p^n$ von Vektoren eine nicht-leere Teilfolge, deren Summe Null ergibt.

Bemerkung A.12. Man darf $n(p-1)+1$ nicht durch $n(p-1)$ ersetzen, denn

$$P_1, \ldots, P_{n(p-1)}$$

mit $P_i = e_{\lceil i/(p-1) \rceil}$ besitzen keine nicht-leere Teilfolge, deren Summe Null ergibt.

Beweis. Es seien $P_1, \ldots, P_{n(p-1)+1} \in \mathbb{F}_p^n$ beliebig. Für Konkretheit sei $a_{i,j}$ die i-te Komponente von P_j. Äquivalenterweise suchen wir

$$v = (v_1, \ldots, v_{n(p-1)+1}) \in \{0,1\}^{n(p-1)+1} \setminus \{0\}^{n(p-1)-1},$$

sodass für alle $i \in [n]$

$$\sum_{j=1}^{n(p-1)+1} a_{i,j} \cdot v_j \equiv 0 \pmod{p}.$$

Hierfür definieren wir Polynome $f_1, \ldots, f_n \in \mathbb{F}_p[x_1, \ldots, x_{n(p-1)+1}]$ durch

$$f_i(x_1, \ldots, x_{n(p-1)+1}) = \sum_{j=1}^{n(p-1)+1} a_{i,j} \cdot x_j^{p-1}.$$

Die Summe der Grade der f_i ist $n(p-1) < n(p-1)+1$, also ist nach dem Satz von Chevalley-Warning die Anzahl der gemeinsamen Nullstellen durch p teilbar. Da $x \equiv 0$ eine gemeinsame Nullstelle ist, muss es insbesondere also auch gemeinsame Nullstellen $x \not\equiv 0$ geben. Wählt man nun $v_i = x_i^{p-1}$, so ist das dann ein gewünschter Vektor v nach dem kleinen Satz von Fermat. □

Bemerkung A.13. Bis auf das angegebene Beispiel kann man natürlich für eine Basis $b_1, \ldots, b_n$ dann als Folge jedes der b_i $(p-1)$ mal nehmen. Allgemein bleibt die Eigenschaft für affin lineare Abbildungen (mit vollem Rang) erhalten.
Tatsächlich ist aber ungeklärt, wie allgemein all diese Konfigurationen aussehen.
Der Fall $n = 2$ ist aber gelöst. Da gibt es im Grunde 2 Typen.

Typ 1: Man hat (bis auf die Anwendung einer affin linearen Abbildung vollen Rang) $p-1$ mal in der Folge $(1,0)$ und $p-1$ Punkte der Form $(b_1, 1), \ldots, (b_{p-1}, 1)$, wobei $b_i \in \mathbb{F}_p$ für alle $i \in [p-1]$. Da man nur $p-1$ mal den Punkt $(1,0)$ hat, muss man einen der $(b_i, 1)$ nehmen. Aber von denen hat man nur $p-1$ Stück, sodass also die hintere Komponente der Summe nicht Null ist.

Typ 2: Man hat (bis auf die Anwendung einer affin linearen Abbildung vollen Rang) $p-2$ mal den Punkt $(1,0)$ und p Punkte $(b_1, 1), \ldots, (b_p, 1)$, sodass $\sum_{i=1}^{p} b_i \equiv 1 \pmod{p}$. Eine sich zu Null aufsummierende Folge kann nicht nur aus den $(1,0)$'en bestehen, also muss sie einen Punkt $(b_i, 1)$ enthalten. Dann muss man wegen der zweiten Koordinate alle $(b_i, 1)$'s enthalten. Da die Summe der b_i's gerade Eins ist, bräuchten wir dann $p-1$ mal den Punkt $(1,0)$, haben aber nur $p-2$ mal diesen.

Tatsächlich gilt folgender Satz:

Ist $P_1, \ldots, P_{2p-2} \in \mathbb{F}_p^2$ eine Folge ohne nicht-leere Teilfolge mit Summe Null, dann muss die Folge von Typ 1 oder Typ 2 sein.

Dieser Satz kann beispielsweise (sehr kompliziert) mit dem kombinatorischen Nullstellensatz bewiesen werden.

Aufgabe 2

Behauptung. Es sei p eine Primzahl. Dann besitzt jede Folge $P_1, \dots, P_{4p-2} \in \mathbb{F}_p^2$ eine Teilfolge der Länge $2p$, deren Summe Null ergibt.

Beweis. Es sei $|X| = 4p-2$. Der Notation aus dem Skript folgend wollen wir $(2p \mid X) > 0$ zeigen. Hierfür liefert Bemerkung 6.8

$$1 - (p \mid X) + (2p \mid X) - (3p \mid X) \equiv 0 \pmod{p}.$$

Also muss mindestens einer der $(p \mid X), (2p \mid X), (3p \mid X)$ nicht Null sein.
Ist $(2p \mid X) > 0$, so sind wir fertig. Ist $(3p \mid X) > 0$, so existiert eine Teilfolge X' von X der Länge $3p$ mit $\sum X' = 0$. Das Lemma von Alon-Dubiner liefert, dass $(p \mid X') > 0$ ist. Ist X'' eine entsprechende Teilfolge X'' der Länge p aus X, so ist dann $X' \setminus X''$ eine Teilfolge der Länge $2p$ und $\sum(X' \setminus X'') = \sum X' - \sum X'' = 0 - 0 = 0$.
Ist $(p \mid X) > 0$, so existiert eine Teilfolge A von X der Länge p und $\sum A = 0$. Es sei $Y = X \setminus A$ die zu A komplementäre Teilfolge. Nach Lemma 6.7 ist dann $1 - (p \mid Y) + (2p \mid Y) \equiv 0 \pmod{p}$. Ist $(2p \mid Y) > 0$, so sind wir wieder fertig. Sonst ist $(p \mid Y) > 0$ und damit können wir die entsprechende Teilfolge mit der Teilfolge A vereinen zu einer Teilfolge von X der Länge $2p$ mit Summe Null. □

Bemerkung A.14. $4p-2$ ist wieder optimal: Für ein Gegenbeispiel wähle man $p-1$ mal den Punkt $(0,1)$, $p-1$ mal den Punkt $(1,0)$ und $2p-1$ mal den Punkt $(1,1)$.
Angenommen wir hätten eine Teilfolge mit Summe Null. Würde die einer der $(1,0)$-er ($(0,1)$-er) enthalten, so muss man entsprechend mit den $(1,1)$-en ausgleichen. Deren Gesamtanzahl deutet daraufhin, dass man dann (in $\mathbb{Z}$) sich in der ersten (zweiten) Koordinate zu p oder $2p$ aufsummieren muss. Nun, man kann nicht nur die $(1,1)$-en enthalten, denn wir wollen eine Folge der Länge $2p$. Ohne Einschränkung enthalte die Folge noch $(1,0)$ $k \in [p-1]$ mal. Da man mit den $(1,1)$'en dann ausgleichen muss, enthält die Folge $p-k \in [p-1]$ oder $2p-k \in \{p+1, \dots, 2p-1\}$ mal $(1,1)$. Dann sind wir aber in der zweiten Koordinate nicht Null. Im ersten Fall müssen wir, um nicht Null zu sein dann auch k mal $(0,1)$ enthalten, was aber dann $p+k < 2p$ Terme in der Folge gibt. Im zweiten Fall erhält man dann $2p+k > 2p$ viele Terme. ↯ □

Aufgabe 3

Behauptung. Es sei p eine Primzahl. Jede Folge $P_1, \dots, P_{3p-2}$ von Vektoren der Ebene $\mathbb{F}_p^2$ eine nicht-leere Teilfolge mit Summe Null besitzt, deren Länge höchstens p beträgt.

Beweis. Es sei X eine Folge der Länge $3p-2$. Nach Lemma 6.7 ist

$$1 - (p \mid A) + (2p \mid A) \equiv 0 \pmod{p}.$$

Ist $(p \mid X) > 0$, so sind wir fertig. Sonst ist $(2p \mid X) > 0$. Es sei also B eine Teilfolge von X der Länge $2p$ mit Summe 0. Da insbesondere $|B| > 2p-1$ gilt, existiert nach Aufgabe 1 eine nicht-leere Teilfolge C von B mit Summe 0. Also tut es entweder C oder die komplementäre Folge $B \setminus C$. □

Bemerkung A.15. $3p-2$ ist tatsächlich bestmöglich. Hierfür betrachte man die Folge mit $p-1$ mal $(1,0)$, $p-1$ mal $(0,1)$ und $p-1$ mal $(1,1)$. Angenommen es gäbe eine nicht-leere Teilfolge mit Summe 0. Eine Folge kann nicht nur aus $(1,1)$-en bestehen. O.B.d.A. enthalte die Folge also $(1,0)$. Man muss, damit es in der ersten Koordinate Null ist, mit $(1,1)$ ausgleichen. Die Gesamtanzahl an $(1,0)$-en und $(1,1)$-en deutet daraufhin, dass man vorne (in $\mathbb{Z}$) sich zu p aufsummieren muss. Enthält die Teilfolge $k \in [p-1]$ mal $(1,0)$, so muss man auch $p-k \in [p-1]$ mal $(1,1)$ enthalten. Dann muss man aber zum Ausgleich in der zweiten Koordinate k mal $(0,1)$ enthalten. Damit wäre die Teilfolge dann von der Länge $k+(p-k)+k = p+k > p$. □

Aufgabe 4

Behauptung. Es sei G eine endliche abelsche Gruppe der Ordnung n. Dann besitzt jede Folge $a_1, \dots, a_n$ von Elementen von G eine nicht-leere Teilfolge, deren Summe Null ergibt.

Beweis. Es sei G eine endliche, abelsche Gruppe der Ordnung $n \in \mathbb{N}$ und $a_1, \dots, a_n$ eine Folge von Elementen in G. Wir setzen $s_l = \sum_{k=1}^{l} a_k$ für $k \in [n]$.
Gilt $s_i = s_j$ für gewisse $1 \leq i < j \leq n$, so wähle als Teilfolge $a_{i+1}, \dots, a_j$. Dann ist nämlich $0 = s_j - s_i = \sum_{k=i+1}^{j} a_k$.
Sind alle $s_i, i \in [n]$, verschieden, so muss insbesondere $i \in [n]$ existieren mit $s_i = \sum_{k=1}^{i} a_k = 0$ sein. Wähle also dann als Teilfolge $a_1, \dots, a_i$. □

Bemerkung A.16. Die Aussage folgt fast schon direkt aus Aufgabe 5.

Aufgabe 5

Behauptung. Es sei G eine endliche abelsche Gruppe der Ordnung n. Die Folge

$$a_1, \dots, a_{n-1}$$

von Elementen von G besitze keine nicht-leere Teilfolge mit Summe Null. Dann ist $G \cong \mathbb{Z}/n\mathbb{Z}$ und $a_1 = \dots = a_{n-1}$ ein erzeugendes Element von G.

Beweis. Es sei G eine endliche, abelsche Gruppe der Ordnung $n \in \mathbb{N}$ und $a_1, \dots, a_{n-1}$ eine Folge, welche keine Teilfolge enthält, die Summe Null hat.
Wir wenden denselben Trick wie zuvor an und erhalten, dass $a_1, a_1+a_2, \dots, a_1+\dots+a_{n-1}$ paarweise verschieden und nicht Null sind. Somit muss

$$\{a_1, a_1+a_2, \dots, a_1+\dots+a_{n-1}\} = G \setminus \{0\}$$

gelten. Jetzt wenden wir denselben Trick wie zuvor an, wobei wir aber die Rollen von a_1 und a_2 tauschen. Wir erhalten

$$\{a_2, a_1+a_2, \dots, a_1+\dots+a_{n-1}\} = G \setminus \{0\}\,.$$

Also muss $a_1 = a_2$ sein. Wendet man denselben Trick für $(a_2, a_3), (a_3, a_4), \dots$ an, erhält man schließlich $a := a_1 = \dots = a_{n-1}$. a hat nach den obigen Beobachtungen Ordnung n, und damit ist $G \cong \mathbb{Z}/n\mathbb{Z}$. □