11. Vorlesung

Folgerung 10.6. Es gibt ein $\varepsilon > 0$ mit folgender Eigenschaft: Wenn $A \subseteq \mathbb{F}_3^n$ keine Gerade enthält, dann $|A| \leq (3-\varepsilon)^n$.

Beweis. Für r, s, t mit $r+s+t = n$ ist

$$n^n = (r+s+t)^n \geq \binom{n}{r\,s\,t} r^r s^s t^t$$

und mithin

$$\binom{n}{r\,s\,t} \leq \frac{n^n}{r^r s^s t^t} = \left(\frac{n}{r}\right)^r \left(\frac{n}{s}\right)^s \left(\frac{n}{t}\right)^t .$$

Schreibt man $\frac{r}{n} = \rho$, $\frac{s}{n} = \sigma$, $\frac{t}{n} = \tau$, so folgt

$$\frac{1}{n} \log \binom{n}{r\,s\,t} \leq \rho \log \frac{1}{\rho} + \sigma \log \frac{1}{\sigma} + \tau \log \frac{1}{\tau}$$

Für die Funktion $J : [0,1] \longrightarrow \mathbb{R}$, definiert durch

$$J(x) = \begin{cases} x \log \frac{1}{x} & \text{wenn } x > 0 \\ 0 & \text{wenn } x = 0 \end{cases}$$

ist wegen

$$J'(x) = \log \frac{1}{x} - 1$$

$$J''(x) = -\frac{1}{x} < 0$$

streng konkav. Wenn $\rho + \sigma + \tau = 1$ ist also

$$J(\rho) + J(\sigma) + J(\tau) \leq 3\,J\left(\tfrac{1}{3}\right) = \log 3,$$

wobei Gleichheit nur für $\rho = \sigma = \tau = \frac{1}{3}$ gilt.

Somit gibt's $\delta > 0$ mit

$$J(\rho) + J(\sigma) + J(\tau) \leq \log(3-\delta)$$

wenn $\rho + \sigma + \tau = 1$, $\sigma + 2\tau \leq \frac{2}{3}$.

Nun ist $\binom{n}{r\,s\,t} \leq (3-\delta)^n$ für alle r, s, t mit $r + s + t = n$, $s + 2t \leq \frac{2}{3} n$. Somit

$$|A| \leq \binom{n+2}{2} (3-\delta)^n.$$ Wenn n hinreichend groß folgt

$$|A| \leq \left(3 - \tfrac{\delta}{2}\right)^n.$$ $\square$

§11. Der Satz von Roth.

Dfn 11.1. Für $n, k \in \mathbb{N}$ sei $r_k(n)$ die größtmögliche Mächtigkeit einer Menge $A \subseteq [n]$, die keine arithm. Folge der Länge k (AP_k) enthält.

Beob 11.2. Für alle $k, m, n \in \mathbb{N}$ ist $r_k(m+n) \leq r_k(m) + r_k(n)$.

Beweis. Wähle $A \subseteq [m+n]$ mit $|A| = r_k(m+n)$ ohne AP_k.

Setze $B = A \cap [m]$,

$C = \{c \in [n] : c + m \in A\}$.

Weder B noch C enth. eine AP_k. Also

$$|A| = |B| + |C| \leq r_k(m) + r_k(n). \qquad \square$$

Lemma 11.3. Wenn $F : \mathbb{N} \to \mathbb{R}_{\geq 0}$ subadditiv ist

(d.h. wenn $F(m+n) \leq F(m) + F(n)$ f. alle $m, n \in \mathbb{N}$ gilt)

dann existiert $\gamma = \lim_{n \to \infty} \frac{F(n)}{n}$ und es gilt $F(n) \geq \gamma n$

für alle $n \in \mathbb{N}$.

Beweis. Setze $\gamma = \inf \left\{ \frac{F(n)}{n} : n \in \mathbb{N} \right\}$.

Sei $\gamma' > \gamma$ beliebig. Wähle $m \in \mathbb{N}$ mit $\frac{F(m)}{m} < \gamma'$.

Setze $K = \max \{ F(1), \ldots, F(m) \}$. Für alle $n \in \mathbb{N}$

ist

$$F(n) \leq \frac{n}{m} F(m) + K .$$

[Warum? Division mit Rest liefert $n = qm + r$,

wobei $1 \leq r \leq m$. Da F subadditiv ist, gilt

$$F(n) = F(\underbrace{m + \ldots + m}_{q} + r) \leq q \, F(m) + F(r)$$

$$\leq \frac{n}{m} F(m) + K \quad]$$

Im Limes $n \to \infty$ erhalten wir

$$\limsup_{n \to \infty} \frac{F(n)}{n} \leq \frac{F(m)}{m} < \gamma' .$$

Da γ' beliebig war, folgt $\limsup_{n \to \infty} \frac{F(n)}{n} \leq \gamma$.

Daher $$\lim_{n \to \infty} \frac{F(n)}{n} = \gamma . \qquad \square$$

<u>Folgerung 11.4.</u> Für alle $k \geq 2$ existiert

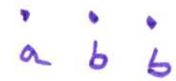
$$\lim_{n \to \infty} \frac{r_k(n)}{n} .$$

Szemerédi zeigte, dass diese Limites alle gleich Null sind,

<u>Satz 11.5 (Roth)</u> $\quad r_3(n) = O\left(\frac{n}{\log\log n}\right)$.

<u>Lemma 11.6.</u> Es seien $N \geq 20\delta^{-2}$ ungerade Zahl und $A \subseteq \{1,\dots,N\}$ eine Menge mit $|A| = \delta N$, die keine arithmetische Folge der Länge 3 enthält. Wenn $\left|A \cap \left[\frac{N}{3}, \frac{2N}{3}\right]\right| \geq \frac{\delta N}{4}$, dann gibt's $r \in \mathbb{Z}/N\mathbb{Z}$ mit $|\hat{A}(r)| \geq \frac{\delta^2 N}{5}$, $r \neq 0$.

<u>Beweis.</u> Setze $B = A \cap \left[\frac{N}{3}, \frac{2N}{3}\right]$.



Wir betrachten arithm. Folgen $(x,y,z) \in A \times B \times B$ mit $y = \frac{x+z}{2}$, d.h. $x = 2y - z$.

Für $y, z \in B$ ist

$$0 < 2\frac{N}{3} - \frac{2N}{3} < 2y - z < 2 \cdot \frac{2N}{3} - \frac{N}{3} = N$$

Daher ist $(x,y,z) \in A \times B \times B$ genau dann arithm. Folge in $\mathbb{Z}$, wenn es arithm. Folge in $\mathbb{Z}/N\mathbb{Z}$ ist. Es gibt nur die $|B|$ trivialen solchen Folgen. Daher

$$N|B| = \sum_{x \in A} \sum_{y \in B} \sum_{z \in B} \sum_{r \in \mathbb{Z}/N\mathbb{Z}} e((x-2y+z)r/N)$$

$$= \sum_{r \in \mathbb{Z}/N\mathbb{Z}} \sum_{x \in A} e(xr/N) \sum_{y \in B} e(-2yr/N) \sum_{z \in B} e(zr/N)$$

$$= \sum_{r \in \mathbb{Z}/N\mathbb{Z}} \hat{A}(-r)\, \hat{B}(2r)\, \hat{B}(-r)$$

$$\geq \hat{A}(0)\, \hat{B}(0)^2 - \sum_{r \neq 0} |\hat{A}(-r)|\, |\hat{B}(2r)|\, |\hat{B}(-r)|.$$

Dabei $\hat{A}(0) = |A|$, $\hat{B}(0) = |B|$ und

$$\sum_{r\neq 0} |\hat{B}(2r)|\cdot|\hat{B}(-r)| \overset{\text{CSU}}{\leq} \Big(\sum_{r\neq 0}|\hat{B}(2r)|^2\Big)^{1/2}\Big(\sum_{r\neq 0}|\hat{B}(-r)|^2\Big)^{1/2}$$

$$\leq \sum_{r} |\hat{B}(r)|^2 = |B|\cdot N$$

(Parseval)

Setzt man $K = \max\{|\hat{A}(r)| : r \neq 0\}$ so gilt also

$$N\,|B| \geq |A|\,|B|^2 - K\,|B|\,N,$$

d.h. $(1+K)\,N \geq |A|\,|B| \geq \delta\cdot N \cdot \frac{\delta N}{4} = \frac{\delta^2 N^2}{4}.$

Somit $K \geq \frac{\delta^2 N}{4} - 1 \geq \frac{\delta^2 N}{5}.$ $\square$

<u>Lemma 11.7.</u> Es seien $N > (\frac{16}{\alpha})^4$, $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ eine Funktion mit $\|f\|_\infty \leq 1$ und $\varphi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ linear. Wenn

$$\Big| \sum_{x \in \mathbb{Z}/N\mathbb{Z}} f(x)\, e(-\varphi(x)/N) \Big| \geq \alpha N ,$$

dann gibt eine Partition $\{1, \dots, N\} = P_1 \dot\cup \dots \dot\cup P_m$ in echte arithm. Folgen der Länge $\lfloor \sqrt[4]{N} \rfloor$ oder $\lfloor \sqrt[4]{N} \rfloor - 1$ für die

$$\sum_{j=1}^{m} \Big| \sum_{x \in P_j} f(x) \Big| \geq \frac{\alpha N}{2} .$$

<u>Beweis.</u> Nach Lemma 9.6 gibt's eine Partition $\{1, \dots, N\} = P_1 \dot\cup \dots \dot\cup P_m$ mit $|P_j| \in \{\lfloor \sqrt[4]{N} \rfloor, \lfloor \sqrt[4]{N} \rfloor - 1\}$ und $\operatorname{diam}(\varphi[P_j]) \leq N^{3/4}$ für alle $j \in [m]$.

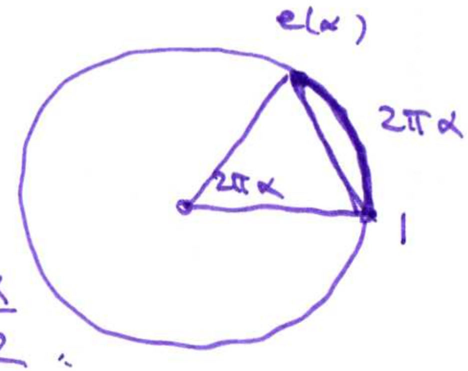
Für jede dieser arithm. Folgen gilt

$$\Big|\sum_{x\in P_j} f(x)\Big| \geq \Big|\sum_{x\in P_j} f(x)\, e(-\varphi(x)/N)\Big| - \frac{\alpha}{2}|P_j| \quad \dots (*)$$

[Warum? Sei $x_j \in P_j$ beliebig. Da $\varphi[P_j] \leq N^{3/4}$

ist

$$\begin{aligned} &|e(-\varphi(x)/N) - e(-\varphi(x_j)/N)| \\ &= |1 - e((\varphi(x) - \varphi(x_j))/N)| \\ &\leq |1 - e(N^{-1/4})| \\ &\leq 2\pi N^{-1/4} \leq 8 N^{-1/4} \leq \frac{\alpha}{2}. \end{aligned}$$



und daher

$$|f(x)e(-\varphi(x)/N) - f(x)\, e(-\varphi(x_j)/N)| \leq \frac{\alpha}{2}\|f\|_\infty \leq \frac{\alpha}{2}$$

für alle $x \in P_j$. Summiere über alle $x \in P_j$.]

Summiere (*) über alle $j \in [m]$.

$$\sum_{j=1}^{m} \Big| \sum_{x \in P_j} f(x) \Big| \geq \Big| \sum_{j=1}^{m} \sum_{x \in P_j} f(x)\, e(-\varphi(x)/N) \Big| - \frac{\alpha}{2} N$$

$$\geq \alpha N - \frac{\alpha N}{2} = \frac{\alpha N}{2}. \qquad \square$$