§4. Vorüberlegungen zum Satz von Freiman.

Frage. Beschreibe alle additiven Mengen mit kleiner Verdopplungskonstante.

Beispiele. (1) Sei $A = \{a, a+d, a+2d, \dots, a+(k-1)d\}$.

Dann $A+A = \{2a, 2a+d, \dots, 2a+(2k-2)d\}$,

also $\sigma[A] = \frac{|A+A|}{|A|} = \frac{2k-1}{k} < 2$.

(2) Sei A eine arithm. Folge und $B \subseteq A$ mit $|B| \geq \frac{2|A|}{K}$.

Dann $\sigma[B] \leq K$.

Dfn 4.1. Sei G eine abelsche Gruppe und $a, d_1, \dots, d_r \in G$.

Ferner seien $k_1, \dots, k_r \in \mathbb{N}$. Dann heißt

$$P = \{a + m_1 d_1 + \dots + m_r d_r : 0 \leq m_i < k_i \text{ für alle } i \in [r]\}$$

eine verallgemeinerte arithmetische Folge (GAP) mit Rang r, Schritte $(d_1, \dots, d_r)$ und Länge $(k_1, \dots, k_r)$. Wenn $|P| = \prod_{1 \leq i \leq r} k_i$ heißt P eine echte GAP.

Fakt 4.2. Für jede echte GAP A vom Rang r gilt $\sigma[A] \le 2^r$.

Beweis. Wenn

$$P = \{ a + m_1 d_1 + \dots + m_r d_r : 0 \le m_i < k_i \text{ für alle } i \in [r] \}$$

und $|P| = k_1 \cdot \dots \cdot k_r$, dann

$$P + P = \{ 2a + m_1 d_1 + \dots + m_r d_r : 0 \le m_i < 2k_i - 1 \text{ für alle } i \in [r] \},$$

also

$$\sigma[P] = \frac{|P+P|}{|P|} \le \prod_{1 \le i \le r} \frac{2k_i - 1}{k_i} < 2^r. \qquad \square$$

Auch dichte Teilmengen echter GAP haben kleine Verdopplungskonstanten.

Satz 4.3 (Freiman & Ruzsa) Für jede reelle Zahl $K \ge 1$ gibt's $r(K), s(K) \in \mathbb{N}$ mit: Für jede additive Menge $A \subseteq \mathbb{Z}$ mit $\sigma[A] \le K$ gibt's eine echte GAP P vom Rang $r(K)$ mit $A \subseteq P$ und $|P| \le s(K) \cdot |A|$.

. . . . . .

Beobachtung 4.4. Sei $A \subseteq \mathbb{R}^d$ konvex und Lebesgue-messbar.

Dann $\lambda(A+A) \leq 2^d \lambda(A)$.

Beweis. Für alle $a, a' \in A$ ist $\frac{a+a'}{2} \in A$.

Also $A + A \subseteq \{ 2a : a \in A \}$.

Die Menge auf der rechten Seite hat Maß $2^d \lambda(A)$. □

In dieser Situation hat $A \cap \mathbb{Z}^d$ "gute Chancen", kleine Verdopplungskonstante zu haben. Wie in der Übung kann man solche Mengen nach $\mathbb{Z}$ abbilden.

. . . . . .

Dfn 4.5. Sei $t \in \mathbb{N}$. Eine additiv geschriebene Gruppe G heißt

t- Torsionsgruppe, wenn $\underbrace{x + x + \ldots + x}_{t} = 0$ für alle $x \in G$.

Lemma 4.6. (Ruzsa) Sei A eine additive Menge in einer t-Torsionsgruppe G mit $|A+A| \leq K|A|$. Dann gibt's Untergruppe $H \subseteq G$ und $x \in G$ mit $A \subseteq H+x$ und $|H| \leq K^2 t^{K^5} |A|$.

Lemma 4.7 (Ruzsa) Seien A, B additive Mengen mit $|A+B| \leq K|A|$. Dann gibt's $X \subseteq B$ mit $|X| \leq K$ und $B \subseteq A-A+X$.

Beweis. Sei $X \subseteq B$ maximal mit $|A+X| = |A| \cdot |X|$. Dann $|A| \cdot |X| \leq |A+B| \leq K|A|$, also $1 \leq |X| \leq K$.

Sei $b \in B$ beliebig. Wenn $b \in X$, dann ist $b \in A-A+X$ klar.

Sei nun $b \notin X$. Da $X \cup \{b\}$ nicht der Maximalität von X widerspricht gibt's $a, a' \in A$, $x \in X$ mit $a+x = a'+b$,

d.h. $b = a-a'+x \in A-A+X$. □

Beweis von Lemma 4.6.

Aus der Plünnecke - Ungleichung folgt

$$|3A - 2A| \leq K^5 |A|.$$

Wende Lemma 4.7 mit $B = 2A - 2A$ an. Dies liefert $X \subseteq 2A - 2A$ mit $|X| \leq K^5$ und

$$2A - 2A \subseteq A - A + X. \qquad (*)$$

Die von X erzeugte Untergruppe $\langle X \rangle$ erfüllt also $|\langle X \rangle| \leq t^{K^5}$ und wg (*) ist

$$H = A - A + \langle X \rangle$$

eine Untergruppe von G. Außerdem

$$|H| \leq |A - A| \langle X \rangle \leq K^2 |A| \, t^{K^5}.$$

Ist $x \in A - \langle X \rangle$ bel., so gilt $H \geq A - x$, d.h.

$$A \subseteq H + x.$$

□

Lemma 4.8. Sei $A \subseteq \mathbb{F}_2^n$ eine additive Menge mit $|A| \geq \alpha \cdot 2^n$. Dann gibt's einen UVR $U \subseteq \mathbb{F}_2^n$ mit $U \subseteq 4A$ und $\operatorname{codim}(U) \leq \alpha^{-2}$.

Beweis. OBdA ~~=~~ $|A| = \alpha \cdot 2^n$. Sei $\cdot$ das Standardskalarprodukt $\mathbb{F}_2^n \times \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$, d.h.

$$(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) = \sum_{i=1}^{n} x_i y_i .$$

Für $x \in \mathbb{F}_2^n \setminus \{0\}$ sei $W_x = \{y \in \mathbb{F}_2^n : x \cdot y = 0\}$, $W_x' = \mathbb{F}_2^n \setminus W_x$.

Sei $\mathcal{W} = \{W_x : x \in \mathbb{F}_2^n \setminus \{0\}\}$. Jeder Vektor $z \in \mathbb{F}_2^n \setminus \{0\}$ ist in $2^{n-1} - 1$ dieser Räume enthalten.

Daher

$$\sum_{W \in \mathcal{W}} \left(|W \cap A| - |W' \cap A| \right)^2$$

$$= \sum_{W \in \mathcal{W}} \sum_{a_1, a_2 \in A} \begin{cases} +1 & \text{wenn } a_1 + a_2 \in W \\ -1 & \text{wenn } a_1 + a_2 \in W' \end{cases}$$

$$= \sum_{a_1, a_2 \in A} \begin{cases} 2^n - 1 & \text{wenn } a_1 + a_2 = 0 \\ (2^{n-1} - 1) - 2^{n-1} & \text{wenn } a_1 + a_2 \neq 0 \end{cases}$$

$$= |A| \cdot (2^n - 1) - (|A|^2 - |A|) < 2^n |A| = \alpha \cdot 4^n .$$

Für

$$Q = \{ z \in \mathbb{F}_2^n \setminus \{0\} : \left| |W_z \cap A| - |W_z' \cap A| \right| \geq \alpha^{3/2} 2^n \}$$

gilt also $|Q| \cdot \alpha^3 \cdot 4^n < \alpha \cdot 4^n$, also $|Q| < \alpha^{-2}$.

Der Raum $U = \bigcap_{z \in Q} W_z$ erfüllt $\operatorname{codim}(U) < \alpha^{-2}$.

Es genügt $U \leq 4A$ zu beweisen.

Angenommen $u \in U \setminus 4A$. Dann $u \neq 0$.

Wir interessieren uns für

$$\Delta = \sum_{\substack{W \in \mathcal{W} \\ u \notin W}} \left(|W \cap A| - |W' \cap A|\right)^4 - \sum_{\substack{W \in \mathcal{W} \\ u \in W}} \left(|W \cap A| - |W' \cap A|\right)^4 .$$

Einerseits ist

$$\Delta = \sum_{\substack{W \in \mathcal{W} \\ u \notin W}} \sum_{a_1, \ldots, a_4 \in A} \begin{cases} 1 & \text{wenn } a_1 + a_2 + a_3 + a_4 \in W \\ -1 & \text{wenn } a_1 + a_2 + a_3 + a_4 \in W' \end{cases}$$

$$- \sum_{\substack{W \in \mathcal{W} \\ u \in W}} \quad \cdots \cdots$$

$$= \sum_{W \in \mathcal{W}} \sum_{a_1 \ldots a_4 \in A} \begin{cases} +1 \\ -1 \end{cases} \qquad \begin{matrix} a_1 + a_2 + a_3 + a_4 - u \notin W \\ \in W \end{matrix}$$

$$= \sum_{a_1, a_2, a_3, a_4 \in A} \underbrace{\left(2^{n-1} - (2^{n-1} - 1)\right)}_{1} = |A|^4$$

↑ da $u \notin 4A$.

Für $x \in Q$ ist $u \in W_x$.

Daher gilt $\big| |W \cap A| - |W' \cap A| \big| < \alpha^{312} \cdot 2^4$

für alle $W \in \mathcal{W}$ mit $u \notin W$.

Also ist andererseits

$$\Delta \leq \sum_{\substack{W \in \mathcal{W} \\ u \notin W}} (|W \cap A| - |W' \cap A|)^2 \cdot \alpha^3 \cdot 4^4$$

$$\leq \sum_{W} (|W \cap A| - |W' \cap A|)^2 \cdot \alpha^3 \cdot 4^4$$

$$< \alpha \cdot 4^4 \cdot \alpha^3 \cdot 4^4 = (\alpha \cdot 2^4)^4 = |A|^4 .$$

Widerspruch! □

Bem. Ähnlich kann man zeigen: Für jede Menge $A \subseteq \mathbb{F}_p^n$ mit $|A| \geq \alpha \cdot p^n$ gibt's UVR $U \leq \mathbb{F}_p^n$ mit $U \leq 2A - 2A$ und $\operatorname{codim}(U) \leq \alpha^{-2}$. (→ Fouricranalysis).

Plan für den Beweis des Satzes von Freiman.

I. Zeige, dass $2A - 2A$ eine große echte GAP (mit kleinem Rang) enthält.

- Finde eine große Teilmenge $A' \subseteq A$, die sich wie eine dichte Teilmenge von $\mathbb{Z}/N\mathbb{Z}$ benimmt.
- Finde in $2A' - 2A'$ eine große "Bohr-Menge". (≈ konvexe Teilmenge von $\mathbb{R}^d$)
- Finde die gesuchte GAP in der Bohr-Menge (Minkowski ....)

II. Überdeckungsargumente zeigen dann, dass A in einer kleinen GAP enthalten ist.