Additive Kombinatorik

Wintersemester 2020/21

Christian Reiher

T. Tao, Van Vu: Additive Combinatorics

Cambridge studies in advanced mathematics 105

Leitfragen.

Satz (Green & Tao) Es gibt beliebig lange arithmetische Folgen von Primzahlen.

11, 41, 71, 101, 131

Problem: Gibt es unendlich viele Primzahlzwillinge?

Goldbach?

Satz (van der Waerden) Für alle $k, r \in \mathbb{N}$ gibt's $N \in \mathbb{N}$ mit der Eigenschaft: Für jede Färbung $f: [N] \longrightarrow [r]$ gibt's eine einfarbige arithmetische Folge der Länge k.

$\longrightarrow$ Ramseytheorie

Satz (Szemerédi) Für alle $k \in \mathbb{N}$, $\delta > 0$ gibt's $N \in \mathbb{N}$ mit der Eigenschaft: Jede Teilmenge $A \subseteq [N]$ mit $|A| \geq \delta N$ enthält eine arithmetische Folge der Länge k.

$\longrightarrow$ Ergodentheorie

$\longrightarrow$ höhere Fourieranalysis

$\longrightarrow$ Hypergraphenregularität

$\longrightarrow$ Dichte Hales - Jewett

Satz (van der Waerden) Für alle $k, r \in \mathbb{N}$ gibt's $N \in \mathbb{N}$ mit der Eigenschaft: Für jede Färbung $f: [N] \longrightarrow [r]$ gibt's einfarbige arithmetische Folge der Länge k.

$\longrightarrow$ Ramseytheorie

Satz (Szemerédi) Für alle $k \in \mathbb{N}$, $\delta > 0$ gibt's $N \in \mathbb{N}$ mit: Jede Teilmenge $A \subseteq [N]$ mit $|A| \geq \delta N$ enthält eine arithmetische Folge der Länge k.

$\longrightarrow$ Ergodentheorie

$\longrightarrow$ höhere Fourieranalyse

$\longrightarrow$ Hypergraphenregularität

$\longrightarrow$ Dichte Hales-Jewett

Vermutung (Erdős, Turán) Es sei $A \subseteq \mathbb{N}$ eine Menge mit $\sum_{a \in A} \frac{1}{a} = \infty$. Dann enthält A bel. lange arithm. Folgen.

Frage: Welche Teilmengen von $\mathbb{Z}$ sind "additiv strukturiert"?

Beispiel: Arithm. Folgen, Mengen der Form

$$\{a + d_1 r_1 + d_2 r_2 : 0 \leq r_1, r_2 < r\}$$

sind "strukturiert".

$\{n^2 : 0 \leq n < N\}$ hat "wenig additive Struktur".

§1. Summen additiver Mengen.

Dfn 1.1. Es sei G eine abelsche Gruppe. Eine **additive Menge** (mit umgebender Gruppe G) ist eine endliche nichtleere Teilmenge $A \subseteq G$.

- Meistens ist $G = \mathbb{Z}$ "typisch".
- Oft wird G nicht erwähnt
- Wenn mehrere additive Mengen $A, B, C, \ldots$ im Spiel sind, haben alle die gleiche umgebende Gruppe.

Dfn 1.2. Für additive Mengen A, B setzen wir

$$A + B = \{ a + b : a \in A \ \& \ b \in B \}$$

$$A - B = \{ a - b : a \in A \ \& \ b \in B \}.$$

Analog $A + B + C$, $nA = \underbrace{A + A + \ldots + A}_{n}$, $A + x$, u.s.w.

Beobachtung 1.3. Für je zwei additive Mengen A, B gilt

$$\max(|A|,|B|) \le |A+B|, |A-B| \le |A|\cdot|B|$$

Außerdem
$$|A| \le |A+A| \le \binom{|A|+1}{2}$$
$$|A| \le |A-A| \le |A|^2 - |A| + 1.$$

Beweis. 1) Für die untere Schranke $|A| \le |A+B|, |A-B|$ wählen wir $b_* \in B$ und benutzen, dass $a \longmapsto a+b_*$, $a \longmapsto a-b_*$ injektiv sind. Analog $|B| \le |A+B|, |A-B|$.

2) Für $|A+B| \le |A|\cdot|B|$ benutze, dass $(a,b) \longmapsto a+b$ eine surjektive Fkt. von $A\times B$ nach $A+B$ ist.

Analog $|A-B| \le |A|\cdot|B|$

3) Wg. Kommutativität $|A+A| \le |A| + \binom{|A|}{2} = \binom{|A|+1}{2}$

Wg. $a-a=0$ für alle $a\in A$ ist $|A-A| \le |A|^2 - (|A|-1)$. □

Dfn 1.4. Für eine additive Menge A heißt $\sigma[A] = \frac{|A+A|}{|A|}$ die Verdopplungskonstante von A. Außerdem heißt $\delta[A] = \frac{|A-A|}{|A|}$ die Differenzenkonstante von A.

- Aus Beob. 1.3 folgt

$$1 \leq \sigma[A] \leq \frac{|A|+1}{2}, \quad 1 \leq \delta[A] \leq |A| - 1 - \frac{1}{|A|}.$$

- Man kann A als "strukturiert" ansehen, wenn $\sigma[A]$ "klein" ist.

Satz 1.5. Für jede additive Menge A gilt $\delta[A] \leq \sigma[A]^2$ und $\sigma[A] \leq \delta[A]^3$.

- Später zeigen wir sogar $\sigma[A] \leq \delta[A]^2$.
- Die Beh. sind zu $|A||A-A| \leq |A+A|^2$, $|A|^2|A+A| \leq |A-A|^3$ äqu.

Lemma 1.6. (Dreiecksungleichung von Ruzsa) Für je drei additive Mengen A, B, C gilt $|B| \cdot |A-C| \leq |A-B| \cdot |B-C|$.

Beweis. Wähle für jede Differenz $d \in A-C$ eine Darstellung $d = a_d - c_d$ mit $a_d \in A$, $c_d \in C$. Definiere

$$\varphi : B \times (A-C) \longrightarrow (A-B) \times (B-C)$$
$$(b, d) \longmapsto (a_d - b, b - c_d).$$

Genügt z.z. dass φ injektiv. Sei $\varphi(b,d) = \varphi(b',d')$.

Dann $a_d - b = a_{d'} - b'$, $c_d - b = c_{d'} - b'$.

Also $d = a_d - c_d = (a_d - b) - (c_d - b)$

$$\| $$

$$d' = a_{d'} - c_{d'} = (a_{d'} - b') - (c_{d'} - b'),$$

Aus $d = d'$ folgt $b = b'$. □

Folgerung 1.7. $\delta[A] \leq \sigma[A]^2$.

Beweis. Setze $B = -A$, $C = A$ in Lemma 1.6 ein.

Dann $|A| \cdot |A-A| \leq |A+A| \cdot |-A-A| = |A+A|^2$. □

Warum Dreiecksungleichung? Der Ruzsa-Abstand additiver Mengen A, B ist

$$d(A,B) = \log \frac{|A-B|}{\sqrt{|A| \cdot |B|}}.$$

Da $\sqrt{|A| \cdot |B|} \leq \max(|A|, |B|) \leq |A-B|$ ist $d(A,B) \geq 0$.

Es gibt $d(A,A) = \log \delta[A]$.

Merke: ⇝ Add. Mengen bilden mit Ruzsa-Abstand keinen metrischen Raum.

Aber: d ist symmetrisch (d.h. $d(A,B) = d(B,A)$)

und erfüllt $d(A,C) \leq d(A,B) + d(B,C)$.

(dies ist $\Leftarrow\!\Rightarrow \frac{|A-C|}{\sqrt{|A||C|}} \leq \frac{|A-B|}{\sqrt{|A||B|}} \cdot \frac{|B-C|}{\sqrt{|B||C|}}$ $\Leftarrow\!\Rightarrow$ Lemma 1.6.)

Lemma 1.8. (Vsevolod). Es seien A, B additive Mengen in G. Für jedes $x \in G$ hat die Gleichung $x = a + b$ höchstens

$$\frac{|A-B|^2}{|A+B|}$$

Lösungen mit $a \in A$, $b \in B$.

Beweis. Setze $X = \{ (a,b) \in A \times B : a + b = x \}$. Für jedes $s \in A+B$ fixiere $a_s \in A$, $b_s \in B$ mit $a_s + b_s = s$. Definiere

$$\varphi : X \times (A+B) \longrightarrow (A-B) \times |A-B|$$

$$(a, b, s) \longmapsto (a - b_s, a_s - b).$$

Wenn φ injektiv ist, folgt $|X| \cdot |A+B| \leq |A-B|^2$ und wir sind fertig. Sei $\varphi(a,b,s) = \varphi(a',b',s')$. Dann

$$x - s = (a+b) - (a_s + b_s) = (a - b_s) - (a_s - b)$$

$$\parallel$$

$$x - s' = (a' + b') - (a_{s'} + b_{s'}) = (a' - b_{s'}) - (a_{s'} - b').$$

Also $s = s'$ und folglich $a = a'$, $b = b'$. $\square$

Dfn 1.9. Für additive Mengen A, B in G und $x \in G$ schreiben wir

$$r_{A+B}(x) = |\{(a,b) \in A \times B : x = a+b\}|$$

$$r_{A-B}(x) = |\{(a,b) \in A \times B : x = a-b\}|.$$

Klarerweise ist

$$\sum_{x \in G} r_{A+B}(x) = \sum_{x \in A+B} r_{A+B}(x) = |A||B|$$

$$\sum_{x \in G} r_{A-B}(x) = \sum_{x \in A-B} r_{A-B}(x) = |A||B|.$$