Ramseyan Theorems for Numbers

Contents

Sum-Free Sets

Some definitions

- A is a sum-free set, if:

  $A \subseteq \mathbb{N}$ s.t. $x,y \in A \Rightarrow x+y \notin A$

- G: abelian group; $S \subseteq G$ a subset
  - $\alpha(S)$ is the cardinality of the largest sum-free subset S of G
  - for A, $B \subseteq G$: $A+B=\{a+b \mid a \in A, b \in B\}$
  - a subgroup H of G is called proper if $H \neq G$

Observation

- $A \subseteq G$, A sum-free, then:

$$|A| \leq \frac{|G|}{2}$$

Proof by contradiction: supp: $|A| > |G|/2$

- for $a \in A$: $|a+A| = |A|$
- $x \in a+A \Rightarrow \exists\, \tilde{a} \in A$: $x = a+\tilde{a} \Rightarrow x \notin A$
- $2|A| = |a+A| + |A| > |G|$
- $\Rightarrow \exists\, g \in G$: $g \in a+A$ and $g \in A$ ⇥⇤

Theorem

Let G be a finite abelian group and let p be the smallest prime divisor of |G|. Then:

$$\alpha(G) \leq \frac{(p+1)|G|}{3p}$$

Lower Bounds for α(G)

- G = $\mathbb{Z}_n$, n even, then α(G) = |G|/2
- G = $\mathbb{Z}$, then for any finite S ⊆ $\mathbb{Z}$\{0} :

  α(S) > |S|/3
- $\alpha(G) \geq \sqrt{|G| - 1}$

➔The best known lower bound for an arbitrary finite abelian group G is:

α(G) ≥ 2|G|/7

Kneser‘s Theorem

Let G be an abelian group. $G \neq \{0\}$, and let A, B be nonempty finite subsets of G.

If $|A| + |B| \leq |G|$, then there exists a proper subgroup H of G such that

$$|A+B| \geq |A| + |B| - |H|$$

Proof of Kneser's Theorem

Induction on $|B|$:

ii) $|B| = 1$; Then:

$|A+B| = |A| = |A| + |B| - 1 \geq |A| + |B| - |H|$ for every subgroup H

iv) Let $|B| > 1$ and suppose theorem holds for all finite nonempty subsets A', B' of G for which $|B'| < |B|$

Case 1: $a + b - c \in A \ \forall a \in A;\ b, c \in B$

Then: $A + b - c = A \ \forall b,c \in B$

Let $H \coloneqq \langle b-c \mid b,c \in B \rangle$

Then: $|B| \leq |H|$ and $A + H = A \neq G$

Therefore: H is a proper subgroup of G and:

$|A + B| \geq |A| \geq |A| + |B| - |H|$

Proof of Kneser's Theorem

Case 2: $\exists a \in A$, $b,c \in B$ s.t. $(a + b - c) \notin A$

Let $e := a - c$; $A' := A \cup (B+e)$; $B' := B \cap (A-e)$

note: B' is a proper subset of B

$c \in B'$ (as $0 \in A - a$) $\Rightarrow$ B' is nonempty

$\Rightarrow$ with the induction hypothesis:

$\exists H$ proper subgroup of G, s.t.

$|A' + B'| \geq |A'| + |B'| - |H|$

Proof of Kneser's Theorem

Observation:

2. $A' + B' = [A \cup (B+e)] + [B \cap (A-e)]$

   $\subseteq (A + B) \cup [(B+e) + (A-e)] = A + B$

4. $|A'| + |B'| = |A \cup (B+e)| + |B \cap (A-e)|$

   $= \underbrace{|A \cup (B+e)|}_{|A| + |B+e| - |A \cap (B+e)|} + |(B+e) \cap A|$

   $= |A| + |B+e| = |A| + |B|$ ■

Proof of Theorem

- supp: $A \subseteq G$ sum-free
- Then: $A \cap (A+A) = \varnothing \Rightarrow |A+A| \leq |G| - |A|$
- Observe that $|A| \leq |G|/2$
- Then: $|G| - |A| \geq |A+A| \geq 2|A| - |H|$ for some proper subgroup H of G.
- Lagrange: $|H|$ divides $|G|$
- $\Rightarrow |H| \leq |G|/p$ since p is the smallest prime divisor of G
- Therefore: $3|A| \leq |G| + |H| \leq (1 + 1/p)|G|$ ■

Zero-Sum Sets

Definition

- A sequence of (not necessarily) distinct numbers $b_1, \ldots, b_m$ is a zero-sum sequence (modulo n) if the sum $b_1 + \ldots + b_m$ is 0 (modulo n)

Proposition

- Suppose we are given a sequence of n integers $a_1,..a_n$, which need not be distinct. Then there is always a set of consecutive numbers a_{r+1}, a_{r+2}, … , a_s whose sum is divisible by n.

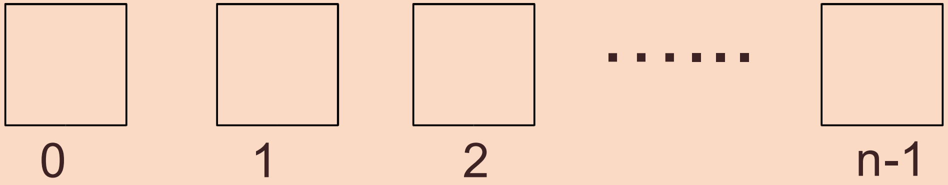
  → For a sequence of less than n integers this is not necessarily true:

  $\underbrace{(1,1,\ldots,1)}_{n-1} \bmod n$

Proof:

Pigeonhole Principle

- n pigeonholes:



- sequences (a_1), (a_1, a_2), …, $(a_1, …, a_n)$
- place a sequence $(a_1,.., a_i)$ into pigeonhole k, if $a_1+…+a_i = k \bmod n$
- i) $\exists$ sequence in the pigeonhole 0 $\Rightarrow$ sequence is divisible by n
- ii) $\nexists$ sequence in the pigeonhole 0 $\Rightarrow$ n sequences are placed in (n-1) pigeonholes $\Rightarrow$ some two of them must lie in the same pigeonhole
- Let $(a_1, …, a_r)$ and $(a_1, …, a_s)$ be these two sequences
- With $r < s$: $a_{r+1}+…+ a_s$ is divisible by n

∎

Question

- We know:

  Every sequence of n numbers has a zero-sum subsequence modulo n

→

Question:

How long must a sequence be so that we can find a subsequence of n elements whose sum is divisible by n?

Theorem: Erdös-Ginzburg-Ziv

Any sequence of $2n - 1$ integers contains a subsequence of cardinality n, the sum of whose elements is divisible by n

Cauchy-Davenport Lemma

If p is a prime, and A, B, are two non-empty subsets of $\mathbb{Z}_p$, then

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

Proof: Follows directly from Kneser‘s Theorem

Proof of the Theorem

Case 1: $n=p$ a prime number

w.l.o.g: $a_1 \le a_2 \le \ldots \le a_{2p-1}$

i) $\exists i \le p-1$ s.t. $a_i = a_{i+p-1} \Rightarrow a_i + a_{i+1} + \ldots + a_{i+p-1} = pa_i = 0 \bmod p$

ii) otherwise: $A_i \coloneqq \{a_i, a_{i+p-1}\}$ for $1 \le i \le p-1$

Repeatedly apply the Cauchy- Davenport lemma:

$\Rightarrow |A_1 + \ldots + A_{p-1}| = p \Rightarrow \mathbb{Z}_p = A_1 + \ldots + A_{p-1}$

i.e. Every element of $\mathbb{Z}_p$ is a sum of precisely p-1 of the first 2p-2 elements of our sequence

in particular: $-a_{2p-1}$ is such a sum: $-a_{2p-1} \in A_1 + \ldots + A_{p-1}$

$\Rightarrow$This supplies us with our p-element subset whose sum is 0

Proof of the Theorem

2) general case:

induction on the number of primes in the prime factorization of n

- given $(a_1, \ldots, a_{2n-1})$ with $n = pm$; p: prime
- case i) ⇒ each subset of 2p-1 members of the sequence contains a p-element subset whose sum is 0 mod p
- ℓ ≔ # pairwise disjoint p-element subsets $I_1, \ldots, I_\ell$ of {1, …, 2n-1}, with $\sum_{j \in I_i} a_j \equiv 0 \pmod p$ $i=1,..,\ell$
- $\ell \geq 2m - 1$

Proof of the Theorem

- from now on: ℓ=2m-1
- define a sequence $b_1, \ldots, b_{2m-1}$ where

$$b_i = \sum_{j \in I_i} \frac{a_j}{p} \quad \forall\, i = 1, .. \ell$$

- Induction hypothesis: sequence has a subset $\{b_i : i \in J\}$ of $|J| = m$ whose sum is divisible by m

$\Rightarrow$ $\{a_j : j \in \cup I_i\}$ supplies n-element subset of the original sequence divisible by n = pm

■

Szemerédi's Cube Lemma

Definition: Affine d-cube

A collection C of integers is called an affine d-cube if there exists d+1 positive integers $x_0, x_1, \ldots, x_d$ so that

$$C = \{x_0 + \sum_{i \in I} x_i : I \subseteq \{1, 2, ..., d\}\}$$

→ We write $C=C(x_0, x_1, \ldots, x_d)$ if an affine cube is generated by $x_0, x_1, \ldots, x_d$.

- example: a, a + b, a + 2b, … a + db

→ C=C(a,b,b,…,b)

Szemerédi's Lemma

For any $0 < \epsilon < 1$ and positive integer d, there exists $n_0 = n_0(\epsilon, d)$ such that, for all $n \geq n_0$, every subset A of $\{1, ..., n\}$ of size $|A| > \epsilon n$ contains an affine d-cube.

Ramsey-Type Version of Szemerédi's Lemma

For every $d, r \geq 1$ there exists an $n = N(d,r)$ with the following property. If we color the set $1, \ldots n$ in r colors then all the elements of at least one affine d-cube lying in this set will receive the same color.

Proof

- Induction on d

i) d = 1: N(1,r) = r+1

ii) assume: n = N(r, d-1) exists

$N = N(r,d) \coloneqq r^n + n$

Now:

Color {1, …, N} with r colors

Proof

- Consider strings of length n:

  i, i+1, … , i+n-1 for $1 \leq i \leq r^n + 1$

- Observation:

1. There are $r^n + 1$ such strings.
2. There are r^n possibilities to color one string.

   ⇒ 2 strings will receive the same sequence of colors (pigeon hole principle)

Proof

- Consider these two sequences with $i < j$

- i.e. for each x in $\{i, i+1, \dots, i+n-1\}$ the numbers x and $x + (j-i)$ receive the same color.
- By induction: The set $\{i, i+1, \dots, i+n-1\}$ contains an affine (d-1)-cube $C=C(x_0, x_1, \dots, x_{d-1})$
- Then: All the numbers of $C(x_0, x_1, \dots, x_{d-1}, j-i)$ have the same color
- $j-i \le r^n \Rightarrow$ cube lies in $\{1,\dots, N\}$ ■

Density-Version of the Lemma

Let $d \geq 2$ be given.
Then, for every sufficiently large n, every subset A of $\{1, ..., n\}$ of size

$$|A| \geq (4n)^{1-1/2^{d-1}}$$

contains an affine d-cube.

Proof

- $B_i := \{b \in B: b+i \in B\}$
- Note that $$\sum_{i=1}^{n-1} |B_i| = \binom{|B|}{2}$$

⇒ For $B \subseteq \{1,\ldots N\}$ and $|B| \geq 2$ $\exists$ $i \geq 1$ so that

$$|B_i| > \frac{|B|^2}{4n}$$

- For A: $\exists$ $i_1 \geq 1$ s.t.

$$|A_{i_1}| > \frac{|A|^2}{4n} \geq \frac{(4n)^{2-2/2^{d-1}}}{4n} = (4n)^{1-1/2^{d-2}}$$

Proof

- Find i_2 so that

$$|A_{i_1,i_2}| = |(A_{i_1})_{i_2}| > \frac{|A_{i_1}|^2}{4n} \geq \frac{(4n)^{2-2/2^{d-2}}}{4n} = (4n)^{1-1/2^{d-3}}$$

- Proceed like this until

$$|A_{i_1,i_2,\ldots,i_{d-1}}| > (4n)^{1-1/2^{d-d}} = 1$$

- Set $A_{i1,\ldots,id-1}$ has still at least 2 elements

⇒ Apply the fact once more:

Now: $A_{i1,\ldots,id}$ contains at least on element b_0

Proof

- $A_{i_1} = \{b: b \in A, b + i_1 \in A\}$

  $A_{i_1, i_2} = \{b: b \in A, b+i_1 \in A, b+i_2 \in A, b+i_1+i_2 \in A\}$

  etc.
- $A_{i_1,\ldots,i_d}$ determines an affine d-cube

  $C=C(b_0, i_1, \ldots, i_d)$
- C lies entirely in A

■

End