Introduction to Discrete Analysis

October 18, 2018

Contents

0 Introduction

asdasd

1 The discrete Fourier transform

Let N be a fixed positive integer. Write ω for $e^{2\pi i/N}$, and $\mathbb{Z}_N$ for $\mathbb{Z}/n\mathbb{Z}$. Let $f : \mathbb{Z}_N \to \mathbb{C}$. Given $r \in \mathbb{Z}_N$, define $\hat{f}(r)$ to be

$$\frac{1}{N}\sum_{x\in\mathbb{Z}_N} f(x)\omega^{-rx}$$

From now on we use the notation $\mathbb{E}_{x\in\mathbb{Z}_N}$ for $\frac{1}{N}\sum_{x\in\mathbb{Z}_N}$, so $\hat{f}(r) = \mathbb{E}_x f(x)e^{-\frac{2\pi i r x}{N}}$.

If we write ω_r for the function $x \to \omega^{rx}$, and $\langle f, g\rangle$ for $\mathbb{E}_x f(x)\overline{g(x)}$, then $\hat{f}(r) = \langle f, \omega_r\rangle$. So the discrete fourier transforn is basically expanding the function f in the set of orthonormal basis ω_r.

Let us write $||f||_p$ for $\mathbb{E}_x|f(x)|^p)^{1/p}$ (the L_p-norm), and call the resulting space $L_p(\mathbb{Z}_n)$.

Important convention: we use *averages* for the 'original functions' in 'physical spaces', and *sums* for their Fourier transforms in 'frequency space' (referring to $\mathbb{E}$: $\langle , \rangle$ is average in the original space but just $\sum$ in frequency space, i.e. for $\hat{f}, \hat{g}$ etc.)

Lemma. (1, Parseval's identity)
If $f, g : \mathbb{Z}_n \to \mathbb{C}$, then $\langle \hat{f}, \hat{g}\rangle = \langle f, g\rangle$.

Proof.

$$\begin{aligned}
\langle \hat{f}, \hat{g}\rangle &= \sum_r \hat{f}(r)\overline{\hat{g}(r)} \\
&= \sum_r (\mathbb{E}_x f(x)\omega^{-rx})(\overline{\mathbb{E}_y g(y)\omega^{-ry}}) \\
&= \mathbb{E}_x\mathbb{E}_y f(x)\overline{g(y)}\sum_r \omega^{-r(x-y)} \\
&= \mathbb{E}_x\mathbb{E}_y f(x)\overline{g(y)} n\delta_{xy} \\
&= \langle f, g\rangle
\end{aligned}$$

□

Lemma. (2, Convolution identity)

$$\widehat{f * g}(r) = \hat{f}(r)\hat{g}(r)$$

where

$$(f * g)(x) = \mathbb{E}_{y+z=x} f(y)g(z) = \mathbb{E}_y f(y)g(x-y)$$

Proof.

$$\begin{aligned}\widehat{f*g}(r) &= \mathbb{E}_x f*g(x)\omega^{-rx} \\ &= \mathbb{E}_x\mathbb{E}_{y+z=x} f(y)g(z)\omega^{-rx} \\ &= \mathbb{E}_x\mathbb{E}_{y+z=x} f(y)g(z)\omega^{-ry}\omega^{-rz} \\ &= \mathbb{E}_y\mathbb{E}_z f(y)\omega^{-ry}g(z)\omega^{-rz} \\ &= \hat{f}(r)\hat{g}(r)\end{aligned}$$

□

Lemma. (3, Inversion formula)

$$f(x) = \sum_r \hat{f}(r)\omega^{rx}$$

(note the sign of ω^{rx}).

Proof.

$$\begin{aligned}\sum_r \hat{f}(r)\omega^{rx} &= \sum_r \mathbb{E}_y f(y)\omega^{r(x-y)} \\ &= \mathbb{E}_y f(y)\sum_r \omega^{r(x-y)} \\ &= \mathbb{E}_y f(y) n\delta_{xy} \\ &= f(x)\end{aligned}$$

This is really just the statement that we get the original vector back when we sum up its components. □

Further observations: If f is real-valued, then $\hat{f}(-r) = \mathbb{E}_x f(x)\omega^{rx} = \overline{\mathbb{E}_x f(x)\omega^{-rx}} = \overline{\hat{f}(r)}$.

If $A \subset \mathbb{Z}_n$, write A (instead of $1_A, \chi_A$) for the characteristic function of A. Then $\hat{A}(0) = \mathbb{E}_x A(x) = \frac{|A|}{N}$, the *density* of A.

Also, $||\hat{A}||_2^2 = \langle \hat{A}, \hat{A}\rangle = \langle A, A\rangle = \mathbb{E}_x A(x)^2 = \mathbb{E}_x A(x) = \frac{|A|}{N}$, again the density.

Let $f : \mathbb{Z}_n \to \mathbb{C}$. Given $\mu \in \mathbb{Z}_n$, define $f_\mu(x)$ to be $f(\mu^{-1}x)$ (so we need $(\mu, N) = 1$). Then

$$\begin{aligned}\hat{f}_\mu(r) &= \mathbb{E}_x f_\mu(x)\omega^{-rx} \\ &= \mathbb{E}_x f(x/\mu)\omega^{-rx} \\ &= \mathbb{E}_x f(x)\omega^{-r\mu x} \\ &= \hat{f}(\mu r)\end{aligned}$$

1.1 Roth's theorem

Theorem. (4) For every $\delta > 0$, $\exists N$ s.t. if $A \subset \{1, ..., N\}$ is a set of size at least δN, then A must contain an arithmetic progression of length 3.

This is also true for 4,5,..., but the proof is much harder – Szemeredi's theorem. Basic strategy of proof: show that if A has density δ and no AP of length 3 (3AP), then there's a long AP in $P \subset \{1, 2, ..., n\}$ s.t.

$$|A \cap P| \geq (\delta + c(\delta))|p|$$

where $c(\delta)$ is some positive number. But then we can continue this argument to expand $A \cap P$ to infinity (note that $|A \cap P|$ is an integer, so each time increase by 1 at least).

The best known relationship between δ and the N required is around $\delta \sim \frac{c}{\log \log N}$ for some constant c.

—Lecture 2—

Lemma. (5)
Let N be odd, $A, B, C \subset \mathbb{Z}_N$ have densties α, β, γ.
If $\max_{r \neq 0} |\hat{A}(r)| \leq \frac{\alpha(\beta\gamma)^{1/2}}{2}$ and $\frac{\alpha\beta\gamma}{2} > \frac{1}{N}$, then there exists $x, d \in \mathbb{Z}_N$ with $d \neq 0$ s.t. $(x, x+d, x+2d) \in A \times B \times C$.

Proof.

$$\begin{aligned}
\mathbb{E}_{x,d} A(x)B(x+d)C(x+2d) &= \mathbb{E}_{x+z=2y} A(x)B(y)C(z) \\
&= \mathbb{E}_u (\mathbb{E}_{x+z=u} A(x)C(z)) \mathbb{E}_{2y=u} B(y) \\
&= \mathbb{E}_u A * C(u) B_2(u) \\
&= \langle A * C, B_2 \rangle \\
&= \langle \widehat{A * C}, \hat{B}_2 \rangle \\
&= \langle \hat{A}\hat{C}, \hat{B}_2 \rangle \\
&= \sum_r \hat{A}(r)\hat{C}(r)\hat{B}(-2r) \\
&= \alpha\beta\gamma + \sum_{r \neq 0} \hat{A}(r)\hat{C}(r)\hat{B}(-2r)
\end{aligned}$$

Recall here the notation is $B_2(u) = B(u/2)$. now

$$\begin{aligned}
|\sum_{r \neq 0} \hat{A}(r)\hat{B}(-2r)\hat{C}(r)| &\leq \frac{\alpha(\beta\gamma)^{1/2}}{2} \sum_{r \neq 0} |\hat{B}(-2r)||\hat{C}(r)| \\
&\leq \frac{\alpha(\beta\gamma)^{1/2}}{2} \left(\sum_r |\hat{B}(-2r)^2 \right)^{1/2} \left(\sum_r |\hat{C}(r)|^2 \right)^{1/2} \quad \text{By Cauchy-Schwarz} \\
&= \frac{\alpha(\beta\gamma)^{1/2}}{2} ||\hat{B}||_2 ||\hat{C}||_2 \\
&= \frac{\alpha(\beta\gamma)^{1/2}}{2} ||B||_2 ||C||_2 \\
&= \frac{\alpha\beta\gamma}{2}
\end{aligned}$$

The contribution to $\mathbb{E}_{x,d} A(x)B(x+d)C(x+2d)$ from $d = 0$ is at most $\frac{1}{N}$, so if $\frac{\alpha\beta\gamma}{2} > \frac{1}{N}$, we are done. □

Now let A be a subset of $\{1, ..., N\}$ with density $\geq \delta$ and let $B = C = A \cap [\frac{N}{3}, \frac{2N}{3})$. If B has density $< \frac{\delta}{5}$ (??), then either $A \cap [1, \frac{N}{3}]$ or $A \cap [\frac{2N}{3}, N]$ has density at least $\frac{2\delta}{5}$. In that case we find an AP P of length about $N/3$ such that $|A \cap P|/|P| \geq \frac{6\delta}{5}$.
Otherwise, we find that if $\max_{r \neq 0} |\hat{A}(r)| \leq \frac{\delta}{10}$ and $\frac{\delta^3}{50} > \frac{1}{N}$, then $A \times B \times C$ contains a 3AP, so A contains a 3AP.
So if A does not contain a 3AP, then either we find P of length about $N/3$ with $|A \cap P|/|P| \geq \frac{6\delta}{5}$, or ther exists $r \neq 0$ s.t. $|\hat{A}(r)| \geq \frac{\delta}{10}$.

Definition. If X is a finite set and $f : X \to \mathbb{C}$, $Y \subset X$, write $osc(f|_Y)$ to mean $\max_{y_1, y_2 \in Y} |f(y_1) - f(y_2)|$ (I think *amplitude* is a better word for this).

Lemma. (6)
Let $r \in \mathbb{Z}_n$ and let $\varepsilon > 0$. Then there is a partition of $\{1, 2, ..., N\}$ into arithmetic progressions P_i of length at least $c(\varepsilon)\sqrt{N}$ such that

$$osc(\omega_r|_{P_i}) \leq \varepsilon$$

for each i.

Proof. Let $t = \lfloor \sqrt{N} \rfloor$. Of the numbers $1, \omega^r, ..., \omega^t r$, there must be two that differ by at most $\frac{2\pi}{t}$.
If $|\omega^{ar} - \omega^{br}| \leq \frac{2\pi}{t}$ with $a < b$, then $|1 - \omega^{dr}| \leq \frac{2\pi}{t}$ where $d = b - a$. Then $|\omega^{urd} - \omega^{vrd}| \leq |\omega^{urd} - \omega^{(u+1)rd}| + ... + |\omega^{(v-1)rd} - \omega^{vrd}| \leq \frac{2\pi}{t}(v - u)$.
So if P is a progression with common differnece d and length l, then $osc(\omega_r|_P) \leq \frac{2\pi l}{t}$. So divide up $\{1, ..., N\}$ into residue classes mod d, and partition each residue class into parts of length between $\frac{\varepsilon t}{4\pi}$ and $\frac{\varepsilon t}{2\pi}$ (possible, since $d \leq t \leq \sqrt{N}$).
We are done, with $c(\varepsilon) = \frac{\varepsilon}{16}$ (a casual choice). □

Now let us use the information that $r \neq 0$ and $|\hat{A}(r)| \geq \frac{\delta^2}{10}$.
Define the *balanced function* f of A by $f(x) = A(x) = \frac{|A|}{N}$ for each x.
Note that $\hat{f}(0) = 0$ and $\hat{f}(r) = \hat{A}(r)$ for all $r \neq 0$.

Now let $P_1, ..., P_m$ be given by Lemma 6 with $\varepsilon = \delta^2/20$. Then

$$\begin{aligned}
\frac{\delta^2}{10} &\leq |\hat{f}(r)| \\
&= \frac{1}{N} |\sum_x f(x)\omega^{-rx}| \\
&\leq \frac{1}{N} \sum_{i=1}^{m} |\sum_{x \in P_i} f(x)\omega^{-rx}| \\
&\leq \frac{1}{N} \sum_{i=1}^{N} \left[\left| \sum_{x \in P_i} f(x)\omega^{-rx_i} \right| + \left| \sum_{x \in P_i} f(x)(\omega^{-rx} - \omega^{-rx_i}) \right| \right] \quad x_i \in P_i \text{ arbitrary} \\
&\leq \frac{1}{N} \sum_{i=1}^{m} |\sum_{x \in P_i} f(x)| + \frac{\delta^2}{20}
\end{aligned}$$

Therefore $\sum_{i=1}^{m} \left| \sum_{x \in P_i} f(x) \right| \geq \frac{\delta^2 N}{20}$.

We also have $\sum_{i=1}^{m}\sum_{x\in P_i} f(x) = 0$, so

$$\sum_{i=1}^{m}\left(\left|\sum_{x\in P_i} f(x)\right| + \sum_{x\in P_i} f(x)\right) \geq \frac{\delta^2}{20}\sum_{i=1}^{m}|P_i|$$

Therefore,

$$\begin{aligned}
|\sum_{x\in P_i} f(x)| + \sum_{x\in P_i} f(x) &\geq \frac{\delta^2}{20}|P_i| \\
\implies \sum_{x\in P_i} f(x) &\geq \frac{\delta^2}{40}|P_i| \\
\implies |A\cap P_i| &\geq \left(\delta + \frac{\delta^2}{40}\right)|P_i|
\end{aligned}$$

—Lecture 3—

Now let $A \subset \mathbb{Z}_N$, $|A| \geq \delta N$. Then:
- either A contains a 3AP,
- or N is even,
- or $\exists P \subset \{1, ..., N\}$, $|P| \geq N/3$ s.t. $|A \cap P| \geq \frac{6\delta}{5}|P|$,
- or $\exists P \subset \{1, ..., N\}$, $|P| \geq \frac{\delta^2}{640}\sqrt{N}$ (casual) s.t. $|A\cap P| \geq (\delta + \frac{\delta^2}{40})|P|$.

Note that the third case is strictly worse than the fourth.
Well if the first is true then we're done. Suppose now the seconds hols. Write $N = N_1 + N_2$ with N_1, N_2 odd, $N_1, N_2 \approx \frac{N}{2}$. Then A has density at least δ in one of $\{1, ..., N_1\}$ or $\{N_1 + 1, ..., N_1 + N_2\}$.
If (4) holds (note (3) $\implies$ (4)), then we pass to P and start to again. After $\frac{40}{\delta}$ iterations, the density at least doubles. Therefore the toatl number of iterations we can have is at most $\frac{40}{\delta} + \frac{40}{2\delta} + ... \leq \frac{80}{\delta}$.
If $\frac{\delta^2}{640}\sqrt{N} \geq N^{1/3}$ (to account for the above, and also for the possible use of (2)) at each iteration, and $\frac{\delta^3}{25} \geq N^{-1}$ (which follows from the first condition), then after $\frac{80}{\delta}$ iterations we have $N \geq N^{(1/3)^{80/\delta}}$, so the argument works provided

$$N^{(1/3)^{80\delta}} \geq \left(\frac{640}{\delta^2}\right)^6$$

taking logs and simplify a bit, we need

$$\begin{aligned}
&-\frac{80}{\delta}\log 3 + \log\log N \geq \log 6 + \log(\log 640 + 2\log\frac{1}{\delta})) \\
&\Leftarrow \log\log N \geq \frac{160}{\delta} \\
&\Leftarrow \delta \geq \frac{160}{\log\log N}
\end{aligned}$$

1.2 Bogolyubov's method

Let $K \subset \hat{\mathbb{Z}}_N$ and let $\delta > 0$. The *Bohr set* $B(K, \delta)$ has two definitions (not exactly equivalent, but quite equivalent):

• (1) $B(K,\delta) = \{x \in \mathbb{Z}_N : rx \in [-\delta N, \delta N] \forall r \in K\}$ (arc-length definition);
• (2) $B(K,\delta) = \{x \in \mathbb{Z}_N : |1-\omega^{rx}| \leq \delta \forall r \in K\}$ (chord-length definition).

Definition. Let G be an abelian group and let A, B be subsets of G. Then write $A + B = \{a + b : a \in A, b \in B\}$ and the obvious definition for $A - B$. We also write $rA = \{a_1 + ... + a_r : a_1, ..., a_r \in A\}$ (note this might be different than what you think this notation should mean).

Lemma. (7)
Let $A \subset \mathbb{Z}_N$ be a set of density α. Then $2A - 2A$ contains a Bohr set $B(K, 1/4)$ (arc) with $|K| \leq \alpha^{-2}$.

Proof. Observe that $x \in 2A - 2A$ iff $A * A * (-A) * (-A)(x) \neq 0$ (this makes more sense if we write it as $\mathbb{E}_{a+b-c-d=x} A(a)A(b)A(c)A(d) \neq 0$, i.e. we are basically just counting the number of ways x can be written as $a + b - c - d$ where $a, b, c, d \in A$.)
But

$$\begin{aligned} A * A * (-A) * (-A)(x) &= \sum_r A * A * \widehat{(-A)} * (-A)(r)\omega^{rx} \text{ inversion formula} \\ &= \sum |\hat{A}(r)|^4 \omega^{rx} \end{aligned}$$

Let $K = \{r : |\hat{A}(r)| \geq \alpha^{3/2}\}$. Then $\alpha = ||\hat{A}||_2^2 = \sum_r |\hat{A}(r)|^2 \geq \alpha^3|K|$.
So $|K| \leq \alpha^{-2}$.
Now suppose that $x \in B(K, 1/4)$. Then

$$\sum_r |\hat{A}(r)|^4\omega^{rx} = \alpha^4 + \sum_{r\in K, r\neq 0} |\hat{A}(r)|^4\omega^{rx} + \sum_{r\notin K} |\hat{A}(r)|^4\omega^{rx}$$

The real part of the second term is non-negative since $rx \in [-N/4, N/4]$ when $r \in K$.
Also

$$\begin{aligned} \left|\sum_{r\notin K} |\hat{A}(r)|^4\omega^{rx}\right| &\leq \sum_{r\notin K} |\hat{A}(r)|^4 \\ &< \alpha^3 \sum_{r\notin K} |\hat{A}(r)|^2 \\ &\leq \alpha^4 \end{aligned}$$

So it follows that the real part of $\sum_r |\hat{A}(r)|^4\omega^{rx} > 0$, i.e. it is non-zero. So $x \in 2A - 2A$. □

Lemma. (8)
Let $K \subset \mathbb{Z}_N$ and let $\delta > 0$. Then:
(i) $B(K, \delta)$ (arc) has density at least $\delta^{|K|}$;
(ii) $B(K, \delta)$ contains a mod-N artihmetic progression of length at least $\delta N^{1/|K|}$.

Proof. (i) Let $K = \{r_1, ..., r_k\}$. Consider the N k-tuples $(r_1x, ..., r_kx) \in \mathbb{Z}_N^k$. If we intersect this set of k-tuples with a random 'box' $[t_1, t_1+\delta N] \times ... \times [t_k, t_k+\delta N]$

(here we are thinking t_i as real numbers), then the expected number of the k-tuples in the box is $\delta^k N$ (since each one has a probability δ^k).
But if $(r_1 x, ..., r_k x)$ and $(r_1 y, ..., r_k y)$ belong to this box, then $x - y \in B(K, \delta)$.
(ii) If we take $\eta > N^{-1/k}$, then by (i) we get that $|B(K, \eta)| > 1$, therefore at least 2. So $\exists x \in B(K, \eta)$ s.t. $x \neq 0$. But then $dx \in B(K, d\eta)$ for every d.
So if $d\eta \leq \delta$ then $dx \in B(K, \delta)$. That gives us an AP of length at least $\frac{\delta}{\eta}$. So we get one of length at least $\delta N^{1/k}$. $\square$

Definition. Let A, b be subsets of Abelian groups and let $\phi : A \to B$. Then ϕ is a *Freiman homomorphism of order k* if

$$a_1 + ... + a_k = a_{k+1} + ... + a_{2k} \implies \phi(a_1) + ... + \phi(a_k) = \phi(a_{k+1}) + ... + \phi(a_{2k})$$

If $k = 2$, we call this just a *Freiman homomorphism.* In that case, the condition is equivalent to $a - b = c - d \implies \phi(a) - \phi(b) = \phi(c) - \phi(d)$.
If ϕ has an inverse which is also a F-homomorphism of order k, then ϕ is a F-*isomorphism* of order k.

Lemma. (9)
Assume $0 \notin K$, and N is prime. If $\delta < 1/4$, then $B(K, \delta)$ (arc) is Freiman isomorphic to the intersection in $\mathbb{R}^{|K|}$ of $[-\delta N, \delta N]^{|K|}$ with some lattice Λ.

Proof. Let $K = \{r_1, ..., r_k\}$, and let $\Lambda = N\mathbb{Z}^k + \{(r_1 x, ..., r_k x) : x \in \mathbb{Z}\}$. Write $\mathbf{r}$ for $(r_1, ..., r_k)$. Claim that $B(K, \delta) \cong \Lambda \cap [-\delta N, \delta N]^k$.
Define a map $\phi : B(K, \delta) \to \Lambda \cap [-\delta N, \delta N]^k$ by sending x to $(\langle r_1 x \rangle, ..., \langle r_k x \rangle)$ where $\langle u \rangle$ means the least-modulus residue u mod N.
If $x + y = z + w$, then $\mathbf{r}x + \mathbf{r}y = \mathbf{r}z + \mathbf{r}w$ in $\mathbb{Z}_N^k$. But for each i, $\langle r_i x \rangle + \langle r_i y \rangle - \langle r_i z \rangle - \langle r_i w \rangle \in [-4\delta N, 4\delta N]$. Since $\delta < 1/4$, that implies that $\langle r_i x \rangle + \langle r_i y \rangle - \langle r_i z \rangle - \langle r_i w \rangle = 0$. So $\langle \mathbf{r}x \rangle + \langle \mathbf{r}y \rangle = \langle \mathbf{r}z \rangle + \langle \mathbf{r}w \rangle$.
That already implies that ϕ is an injection.
If $\mathbf{r}x + \mathbf{a}N \in [-\delta N, \delta N]^k$, then $r_i x \in [-\delta N, \delta N]$ mod N for each i. So $x \in B(K, \delta)$ and $\phi(x) = \mathbf{r}x + \mathbf{a}N$. So ϕ is a surjection as well.
If $\mathbf{r}x + \mathbf{a}N + \mathbf{r}y + \mathbf{b}N = \mathbf{r}z + \mathbf{c}N + \mathbf{r}w + \mathbf{d}N$, then $r_1(x + y) = r_1(z_w)$ mod N, so $x + y = z + w$ mod N. So the inverse of ϕ is also a Freiman homomorphism. $\square$

Lemma. (10)
Let Λ be a lattice and C be a symmetric convex body, both in $\mathbb{R}^k$. Then $|\Lambda \cap C| \leq 5^k |\Lambda \cap \frac{C}{2}$—.

Proof. let $x_1, ..., x_m$ be a maximal subset of $\Lambda \cap C$ such that for all $i \neq j$, $x_j \notin x_i + \frac{C}{2}$. Then by maximality, the sets $x_i + \frac{C}{2}$ over(are?) all of $\Lambda \cap C$. Also, the sets $x_i + \frac{C}{4}$ are disjoint subsets of $\mathbb{R}^k$, and they are all contained in $C + \frac{C}{4} = \frac{5}{4}C$. So $m \leq \frac{vol(\frac{5}{4}C)}{vol(\frac{1}{4}C)} = 5^k$. $\square$

Corollary. (11)
If N is prime, $0 \notin K$, $|K| = k$, $\delta < 1/4$, then $|B(K, \delta)| \leq 5^k |B(K, \frac{\delta}{2})|$.

2 Sumsets and their structure

It's to be shown that $|A+A| \leq K|A| \implies |rA-sA| \leq K^{r+s}|A|$ (Ruzsa).

Lemma. (1, Petridis)
Let A_0, B be finite subsets of an Abelian group such that $|A_0+B| \leq K_0|A_0|$. Then there exist a non-empty subset $A \subset A_0$ and $K \leq K_0$ s.t. $|A+B+C| \leq K|A+C|$ for every finite subset C of the group.

Proof. Let A minimize the ratio $\frac{|A+B|}{|A|}$, and let the minimal ratio be K.
Claim: this works. We prove this by induction on C.
If $C = \phi$, then the result holds. Now assume it for C and let $x \notin C$. Then $A+(C\cup\{x\}) = (A+C)\cup[(A+x)\setminus(A'+x)]$ where $A' = \{a \in A : a+x \in A+C\}$. This is a disjoint union, so $|A+(C\cup\{x\})| = |A+C|+|A|-|A'|$, $A+B+(C\cup\{x\}) = (A+B+C)\cup((A+B+x)\setminus(A'+B+x))$, since if $a+x \in A+C$ then $a+B+x \subset A+B+C$. So

$$\begin{aligned}|A+B+(C\cup\{x\})| &\leq |A+B+C| + |A+B| - |A'+B| \\ &\leq K|A+C| + K|A| - K|A'|\end{aligned}$$

by induction and minimality property of A. □

—Lecture 5—

Corollary. (2)
If A, B are finite subsets of an abelian group, and $|A+B| \leq K^r|A|$, then there exists $A' \subset A$, $A' \neq \phi$ such that $|A'+rB| \leq K|A'|$ for every positive integer r.

Proof. Choose A' as we choose A in lemma 1. Then $|A'+rB| = |A'+B+(r-1)B| \leq K|A'+(r-1)B|$.
And $|A'+B| \leq K|A'|$, so we are done by induction. □

Corollary. (3)
If $|A+A| \leq K|A|$ or $|A-A| \leq K|A|$, then $|rA| \leq K^r|A|$.

Proof. Set $B = A$ or $-A$ in corollary 2. (think about this) □

Lemma. (4, Ruzsa triangle inequality)
Let A, B, C be finite subsets of an abliean group. Then $|A||B-C| \leq |A-B||A-C|$.

Proof. Define a map $\phi : A\times(B-C) \to (A-B)\times(A-C)$. Given (a,x) with $a \in A, x \in B-C$, choose, *somehow*, $b(x) \in B$ and $c(x) \in C$ s.t. $b(x)-c(x) = x$, and set $\phi(a,x) = (a-b(x), a-c(x))$. Note that $(a-c(x))-(a-b(x)) = b(x)-c(x) = x$ (!). And then, having worked out x, we know $b(x)$, and $a = a-b(x)+b(x)$, so a is determined too. So ϕ is an injection. □

The proof was easy, but why is this called the triangle inequality? We can rewrite it as

$$\frac{|B-C|}{|B|^{1/2}|C|^{1/2}} \leq \frac{|A-B|}{|A|^{1/2}|B|^{1/2}} \cdot \frac{|A-C|}{|A|^{1/2}|C|^{1/2}}$$

So if we define the *Ruzsa distance* $d(A,B) = \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}$, then the inequality says $d(B,C) \leq d(A,B)d(A,C)$.

Corollary. (5)
If $|A+B| \leq K|A|$, then $|rB - sB| \leq K^{r+s}|A|$ for all r, s.

Proof. Pick a' as before. Then by corollary 2 with B replaced by $-B$, $|A' - rB| \leq K^r|A'|$ and $|A' - sB| \leq K^s|A'|$.
Therefore, by Rusza triangle inequality (lemma 4), $|A'||rB - sB| \leq K^{r+s}|A'|^2$, so $|rB - sB| \leq K^{r+s}|A|$. □

One finally corollary:

Corollary. (6, Plunnecke's theorem)
If $|A+A| \leq K|A|$ or $|A-A| \leq K|A$, then $|rA - sA| \leq K^{r+s}|A|$.

Proof. Just apply corollary 5 with $B = -A$ or $B = A$. □

Lemma. (7, Ruzsa's embedding lemma)
Let $A \subset \mathbb{Z}$ be finite and suppose that $|kA - kA| \leq C|A|$. Then there exists a prime $p \leq 4C|A|$ and a subset $A' \subset A$ of size at least $|A|/k$ such that A' is Freiman isomorphic of order k to a subset of $\mathbb{Z}_p$.

Proof. Consider the following composition of maps $\mathbb{Z} \xrightarrow{\text{reduce mod } q} \mathbb{Z}_q \xrightarrow{\times \text{ by random non-zero } r} \mathbb{Z}_q \xrightarrow{\text{least non-negative residue}} \mathbb{Z} \xrightarrow{\text{reduce mod } p} \mathbb{Z}_p$, where q is a prime bigger than $diam A$ and p is a prime $\in (2C|A|, 4C|A|]$ by Bertrand's postulate.
Let $|phi$ be the composition. THe first, second and fourth parts are group homomorphisms, and thus Freiman homomorphisms of all order. Also, the third map is a Freiman homomorphism of order k if you restrict to a subinterval of $[0, q-1]$ of lemgth $\leq q/k$. To see this, write $\langle u \rangle$ for least non-negative residue. Then if I has length $\leq q/k$ (and therefore $< q/k$) and $u_1, ..., u_{2k} \in I$, then if $i_1 + ... + u_k - u_{k+1} - ... - k_{2k} = 0$, then $\langle u_1 \rangle + ... + \langle u_k \rangle - \langle u_{k+1} \rangle - ... - \langle u_{2k} \rangle \equiv 0 \pmod q$, and also has modulus less than q. So it is zero.
By the pigeonhole principle, for any r we can find I of length $\leq q/k$ such that $A' = \{a \in A : ra \in I\}$ has size at least $|A|/k$.
Then $\phi|_{A'}$ is a Freiman homomorphism of order k. It's now remain to prove that ϕ is an isomorphism to its image, i.e. we must show that if $a_1 + ... + a_k - a_{k+1} - ... - a_{2k} \neq 0 (a_i \in A)$, then

$$\langle ra_1 \rangle + ... + \langle ra_k \rangle - \langle ra_{k+1} \rangle - ... - \langle ra_{2k} \rangle \not\equiv 0 \pmod p$$

But if the a_i are chosen sucth that the ra_i all belong to the same interval of length $\leq q/k$, then

$$|\langle ra_1 \rangle + ... + \langle ra_k \rangle - \langle ra_{k+1} \rangle - ... - \langle ra_k \rangle| < q$$

and is congruent to $r(a_1 + ... + a_k - a_{k+1} - ... - a_{2k}) \pmod q$.
So all that can go wrong is if $r(a_1 + ... + a_k - a_{k+1} - ... - a_{2k}$ is xp for some $x \neq 0$, with $|x| < q/p$. The number of values to avoid is at most $2q/p$, so for each $a_1 + ... + a_k - a_{k+1} - ... - a_{2k}$, the probability of going wrong if r is chosen randomly is at most $2/p$. So since $|kA - kA| \leq C|A|$, the probability of going wrong is at most $\frac{2}{p}C|A|$. Since $p > 2C|A|$, there exists r s.t. we get an Freiman isomorphism of order k. $\square$