

# Introduction to Discrete Analysis

Lecturer : Prof. Tim Gowers

=====

(4th October 2018, Thursday)

## Chapter 1. The discrete Fourier transform

Let  $N$  be some fixed positive integer. Write  $\omega$  for  $e^{2\pi i/N}$ . and  $\mathbb{Z}_N$  for  $\mathbb{Z}/N\mathbb{Z}$ . Let  $f : \mathbb{Z}_N \rightarrow \mathbb{C}$ . Given  $r \in \mathbb{Z}_N$  define  $\widehat{f}(r)$  to be  $\frac{1}{N} \sum_{x \in \mathbb{Z}_N} f(x) \omega^{-rx}$ . From now on, we shall use the notation  $\mathbb{E}_{x \in \mathbb{Z}_N}$  for  $\frac{1}{N} \sum_{x \in \mathbb{Z}_N}$  (so that  $\widehat{f}(r) = \mathbb{E}_x f(x) \omega^{-rx}$ ). If we write  $\omega_r$  for the function  $x \mapsto \omega^{rx}$  and  $\langle f, g \rangle$  for  $\mathbb{E}_x f(x) \overline{g(x)}$ , then  $\widehat{f}(r) = \langle f, \omega_r \rangle$ .

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

**Important convention** : we use averages for the "original functions" in "physical space" and sums for their Fourier transforms in "frequency spaces".

**Lemma 1** (Parseval's identity) If  $f, g : \mathbb{Z}_N \rightarrow \mathbb{C}$ , then  $\langle \widehat{f}, \widehat{g} \rangle = \langle f, g \rangle$ .

**proof)**

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

where  $\Delta_{xy} = N$  if  $x = y$  and 0 if  $x \neq y$  (in analogy with  $\delta$ -distribution).

(End of proof)  $\square$

Beware that inner product in the Fourier space and the physical space are defined in a different way :  $\langle \widehat{f}, \widehat{g} \rangle = \sum_r \widehat{f}(r) \overline{\widehat{g}(r)}$  while  $\langle f, g \rangle = \mathbb{E}_x f(x) \overline{g(x)}$

**Lemma 2** (Convolution identity)  $\widehat{f * g}(r) = \widehat{f}(r) \widehat{g}(r)$

**proof)** The convolution  $f * g(x)$  is defined to be  $\mathbb{E}_{y+z=x} f(y) g(z) = \mathbb{E}_y f(y) g(x-y)$ . Then,

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

(End of proof)  $\square$

**Lemma 3** (Inversion formula)  $f(x) = \sum_r \widehat{f}(r) \omega^{rx}$ .

**proof)**

$$\sum_r \widehat{f}(r) \omega^{rx} = \sum_r \mathbb{E}_y f(y) \omega^{r(x-y)} = \mathbb{E}_y f(y) \sum_r \omega^{r(x-y)} = \mathbb{E}_y f(y) \Delta_{xy} = f(x)$$

(End of proof)  $\square$

**Further Observations :**

- If  $f$  is real-valued, then  $\widehat{f}(-r) = \mathbb{E}_x f(x) \omega^{rx} = \overline{\mathbb{E}_x f(x) \omega^{-rx}} = \overline{\widehat{f}(r)}$ .
- If  $A \subset \mathbb{Z}_N$ , write  $A$  (instead of  $1_A$  or  $\chi_A$ ) for the characteristic function of  $A$ . Then  $\widehat{A}(0) = \mathbb{E}_x A(x) = \frac{|A|}{N}$ , the **density** of  $A$ . Also,  $\|\widehat{A}\|_2^2 = \langle \widehat{A}, \widehat{A} \rangle = \langle A, A \rangle = \mathbb{E}_x A(x)^2 = |A|/N$ .
- Let  $f : \mathbb{Z}_N \rightarrow \mathbb{C}$ . Given  $\mu \in \mathbb{Z}_N$  with  $(\mu, N) = 1$ , define  $f_\mu(x)$  to be  $f(\mu^{-1}x)$ . Then  $\widehat{f}_\mu(r) = \mathbb{E}_x f_\mu(x) \omega^{-rx} = \mathbb{E}_x f(x/\mu) \omega^{-rx} = \mathbb{E}_x f(x) \omega^{-r\mu x} = \widehat{f}(\mu r)$ .

## Roth's Theorem

**Theorem 4)** (Szemerédi's theorem for  $k = 3$ ) For every  $\delta > 0$ , there exists  $N$  such that if  $A \subset \{1, \dots, N\}$  is a set of size at least  $\delta N$ , then  $A$  must contain an arithmetic progression of length 3.

Basic strategy : show that if  $A$  has density  $\geq \delta$  and no 3AP, then there is a long arithmetic progression  $P \subset \{1, \dots, n\}$  such that

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

=====

(9th October, Tuesday)

**Theorem 4)** (Roth's theorem, or Szemerédi's theorem for  $k = 3$ ) For every  $\delta > 0$ , there exists  $N$  such that if  $A \subset \{1, \dots, N\}$  is a set of size at least  $\delta N$ , then  $A$  must contain an arithmetic progression of length 3.

**Lemma 5)** Let  $A, B, C \subset \mathbb{Z}_N$  have densities  $\alpha, \beta, \gamma$ . If  $\max_{r \neq 0} |\widehat{A}(r)| \leq \frac{\alpha(\beta\gamma)^{1/2}}{2}$  and  $\frac{\alpha\beta\gamma}{2} > \frac{1}{N}$  then there exist  $x, d \in \mathbb{Z}_N$  with  $d \neq 0$  s.t.  $(x, x+d, x+2d) \in A \times B \times C$ .

**proof)** Assume  $N$  is odd.

Consider the function  $A(x)B(x+d)C(x+2d)$ , which is non-zero if and only if there is a arithmetic progression of length 3. So  $\mathbb{E}_{x,d} A(x)B(x+d)C(x+2d)$  counts the density of  $x, d$  satisfying such condition.

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

(Recall,  $B_\mu(x)$  is defined to be  $B(\mu^{-1}x)$  whenever  $(\mu, N) = 1$ . We can generalize this to write  $B_\mu(x) = \mathbb{E}_{\mu u = x} B(u)$  )

The first term  $\alpha\beta\gamma$  gives a rough estimate of the value just in terms of the densities and the second term gives an estimate for how random the sets  $A, B, C$  behave.

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

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.  
(End of proof)  $\square$

Now let  $A$  be a subset of  $\mathbb{Z}_N$  of 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  $\frac{2\delta}{5}$  so in that case we find an AP(arithmetic progression),  $P$ (one of  $\mathbb{Z}_N \cap [1, N/3]$  and  $\mathbb{Z}_N \cap [2N/3, N]$ ), of length about  $N/3$  such that  $|A \cap P|/|P| \geq 6\delta/5$ .
- Otherwise, if  $\max_{r \neq 0} |\hat{A}(r)| \leq \frac{\delta^2}{10}$ . We may pick  $N$  large so that  $\frac{\delta^3}{50} > \frac{1}{N}$ . Then  $A \times B \times C$  contains a 3AP by the **Lemma 5** and therefore  $A$  contains a 3AP.
- So if  $A$  does not contain a 3AP, then either we find  $P$  of length about  $N/3$  with  $|A \cap P|/|P| \geq 6\delta/5$  or we find  $r \neq 0$  such that  $|\hat{A}(r)| \geq \delta^2/10$ . (This is sometimes called the *dichotomy of order and chaos*)

**Definition)** If  $X$  is a finite set and  $f : X \rightarrow \mathbb{C}$ ,  $Y \subset X$ , write  $\text{osc}(f|_Y)$  to mean  $\max_{y_1, y_2 \in Y} |f(y_1) - f(y_2)|$ .

**Lemma 6)** Let  $r \in \widehat{\mathbb{Z}_N}$  (or just  $\mathbb{Z}_N$ ) and let  $\epsilon > 0$ . Then there is a partition of  $\{1, 2, \dots, N\}$  into arithmetic progressions  $P_i$  of length at least  $c(\epsilon)\sqrt{N}$  such that  $\text{osc}(\omega_r|_{P_i}) \leq \epsilon$  for each  $i$ .

**proof)** Let  $t = \lfloor \sqrt{N} \rfloor$ . Of the numbers  $1, \omega^r, \dots, \omega^{tr}$  there must be two that differ by at most  $2\pi/t$  (by sort-of-pigeon hole principle.) If  $|\omega^{ar} - \omega^{br}| \leq 2\pi/t$  with  $a < b$ , then  $|1 - \omega^{dr}| \leq 2\pi/t$  where  $d = b - a$ . Now, by the triangular inequality, if  $u < v$  then

$$|\omega^{urd} - \omega^{vrd}| \leq |\omega^{urd} - \omega^{(u+1)rd}| + \dots + |\omega^{(v-1)rd} - \omega^{vrd}| \leq \frac{2\pi}{t}(v - u)$$

So if  $P$  is a progression with common difference  $d$  and length  $l$ , then  $\text{osc}(\omega_r|_P) \leq \frac{2\pi l}{t}$ . So divide up  $\{1, \dots, N\}$  into residue classes root  $d$  and partition each residue class into parts of length between  $\frac{\epsilon t}{4\pi}$  and  $\frac{\epsilon t}{2\pi}$  (this is possible, since  $d \leq t \leq \sqrt{N}$ .) We are done, with  $c(\epsilon) = \frac{\epsilon}{16} (< \frac{\epsilon}{4\pi})$ .

(End of proof)  $\square$

Now let us use the information that  $r \neq 0$  and  $|\hat{A}(r)| \geq \delta^2/10$ .

Define the **balanced function**  $f$  of  $A$  by  $f(x) = A(x) - |A|/N$  for each  $x$ . Note that  $\hat{f}(0) = 0$  and  $\hat{f}(r) = \hat{A}(r)$  for all  $r \neq 0$ .

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

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

So  $\sum_{i=1}^m \left| \sum_{x \in P_i} f(x) \right| \geq \delta^2 N/20$ . Also,  $\sum_{i=1}^m \sum_{x \in P_i} f(x) = 0$ . 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,  $\exists i$  s.t.  $\left| \sum_{x \in P_i} f(x) \right| + \sum_{x \in P_i} f(x) \geq \frac{\delta^2}{20} |P_i|$  by pigeon hole principle and hence  $\sum_{x \in P_i} f(x) \geq \frac{\delta^2}{40} |P_i|$ . This implies  $|A \cap P_i| = \left| \sum_{x \in P_i} f(x) + \frac{|A|}{N} \right| \geq (\delta + \delta^2/40) |P_i|$

=====  
(11th October, 2018)

(Example sheets handed out - do not try to use particular theorem, but to apply the idea of using Fourier analysis in combinatorics.

Why does Fourier analysis have anything to do with combinatorics? Because we can formulate various problems in terms of Fourier transformation, e.g. by convolution and Parseval's law.)

•What we have showed : Let  $A \subset \mathbb{Z}_N$ ,  $|A| \geq \delta N$ . Then,

- (1)  $A$  contains a 3AP or
- (2)  $N$  is even or
- (3)  $\exists P \subset \{1, \dots, N\}$ ,  $|P| \geq N/3$  s.t.  $|A \cap P| \geq \frac{6\delta}{5}|P|$  or
- (4)  $\exists P \subset \{1, \dots, N\}$ ,  $|P| \geq \frac{\delta^2}{320}\sqrt{N}$  s.t.  $|A \cap P| \geq (\delta + \delta^2/40)|P|$

If (2) holds, write  $N = N_1 + N_2$  with  $N_1, N_2$  odd,  $N_1, N_2 \simeq N/2$ . Then  $A$  has density at least  $\delta$  in one of  $\{1, \dots, N_1\}$  or  $\{N_1 + 1, \dots, N_1 + N_2\}$ .

If (4) holds (NB (3) $\Rightarrow$ (4)) then we pass to  $P$  and start again(that is, replace  $\mathbb{Z}_N$  with  $P$  and  $A$  with  $A \cap P$ ). After  $40/\delta$  iterations, the density at least doubles. So the total number of iterations we can have is at most  $\leq \frac{40}{\delta} + \frac{40}{2\delta} + \frac{40}{4\delta} + \dots \leq \frac{80}{\delta}$ .

If  $\frac{\delta^2}{320}\sqrt{N} \geq N^{1/3}$  at each iteration, and  $\delta^3/25 \geq N^{-1}$  (which follow from the first condition) then after  $\frac{80}{\delta}$  iterations, we have is  $N \geq N^{(1/3)^{80/\delta}}$ . So the argument works provided

$$\begin{aligned}
 N^{(1/3)^{80/\delta}} &\geq \left(\frac{320}{\delta^2}\right)^6 \Leftrightarrow \left(\frac{1}{3}\right)^{80/\delta} \log N \geq 6(\log 320 + 2 \log \frac{1}{\delta}) \\
 \Leftrightarrow \frac{-80}{\delta} \log 3 + \log \log N &\geq \log 6 + \log(\log 320 + 2 \log \frac{1}{\delta}) \\
 \Leftrightarrow \log \log N &\geq \frac{160}{\delta} \\
 \Leftrightarrow \delta &\geq \frac{160}{\log \log N}
 \end{aligned}$$

(just the follow the idea of calculation,, do not try to learn a particular thing from this calculation)  
(In fact 320 above should be corrected to 640 because of (2))

## Bogolyubov's Method

**Definition)** Let  $K \subset \widehat{\mathbb{Z}}_N$  and let  $\delta > 0$ . The **Bohr set**  $B(K, \delta)$  has two definitions.

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

It turns out that Bohr set has a lot of structure.

**Definition)** Let  $G$  be an Abelian group and let  $A, B$  be subsets of  $G$ . Then

$$\begin{aligned}
 A + B &= \{a + b : a \in A, b \in B\} \\
 A - B &= \{a - b : a \in A, b \in B\} \\
 rA &= \{a_1 + \dots + a_r : a_1, \dots, a_r \in A\}
 \end{aligned}$$

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

**proof)** Observe that  $x \in 2A - 2A$  if and only if  $A * A * (-A) * (-A)(x) \neq 0$ (think for a second). But

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

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 the final term can be bounded by

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

It follows that  $\operatorname{Re}\left(\sum_r |\hat{A}(r)|^4 \omega^{rx}\right) > 0$ , so  $x \in 2A - 2A$ .

(End of proof)  $\square$

**Lemma 8)** Let  $K \subset \mathbb{Z}_N$  and let  $\delta > 0$ . Then

- (i)  $B(K, \delta)$  has density at least  $\delta^{|K|}$ .
- (ii)  $B(K, \delta)$  contains a mod- $N$  arithmetic progression of length  $\geq \delta N^{1/|K|}$ .

**proof)**

- (i) Let  $K = \{r_1, \dots, r_k\}$ . Consider the  $N$  number of  $k$ -tuples  $(r_1x, \dots, r_kx) \in \mathbb{Z}_N^k$  (for  $x \in \mathbb{Z}_N$ ). If we intersect this set of  $k$ -tuples with a random "box"  $Q = [t_1, t_1 + \delta N] \times \dots \times [t_k, t_k + \delta N]$ . Then the expected number of  $k$ -tuples in the box is  $\delta^k N$  (since each intersection has probability  $\delta^k$ ).

But if  $(r_1x, \dots, r_kx)$  and  $(r_1y, \dots, r_ky)$  belong to this box, then  $x - y \in B(K, \delta)$ , so the expected number of in  $(r_1y, \dots, r_ky)$  is smaller or equal to the expected number of  $y$  in  $B(K, \delta)$ . i.e. if we let  $q$  be a random point in  $Q \cap \mathbb{Z}_N^k$ , then

$$\mathbb{E}\left(\sum_y 1_{y \in B(K, \delta)}\right) \geq \mathbb{E}\left(\sum_y 1_{q \in Q} 1_{q+y \in Q}\right) = \sum_y \mathbb{P}(y \in Q) = N|\delta|^K$$

(there must be an easy argument... in fact, in the lecture, it was concluded before so the expected number of, so there must be more intuitive way of understanding this)

- (ii) If we take  $\eta > N^{-1/k}$ , then by (i) we get that  $|B(K, \eta)| > 1$  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  $B(K, d\eta) \subset B(K, \delta)$  so  $dx \in B(K, \delta)$ , that gives us an AP of length at least  $\delta/\eta$ . So we get one of length at least  $\delta N^{1/k}$ .

(End of proof)  $\square$

=====

(16th October, Tuesday)

(about the example sheet - Question 2, has to fix  $\alpha^2 \beta^2 N^4$  to  $\alpha^2 \beta^2 N^3$  : a natural way to think about this is "normalizing". We decide one element from other three, so the factor of  $N$  should be 3.)

Recall :  $B(K, \delta) = \{x \in \mathbb{Z}_N : rx \in [-\delta N, \delta N] \text{ for all } r \in K\}$

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

$$a_1 + \dots + a_k = a_{k+1} + \dots + a_{2k} \Rightarrow \phi(a_1) + \dots + \phi(a_k) = \phi(a_{k+1}) + \dots + \phi(a_{2k})$$

If  $k = 2$ , we call this a **Freiman homomorphism**. In that case, the condition is equivalent to

$$a - b = c - d \Rightarrow \phi(a) - \phi(b) = \phi(c) - \phi(d)$$

If  $\phi$  has an inverse which is also a Freiman homomorphism of order  $k$  then  $\phi$  is a **Freiman isomorphism of order  $k$** .

Consider  $\begin{smallmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{smallmatrix}$  and  $\dots, \dots, \dots$ . They have same additive structure, in some sense, and the Freiman isomorphism describes this. Freiman isomorphism is intended to describe a hidden lattice structure of a additive system.

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

**proof)** Let  $K = \{r_1, \dots, r_k\}$  and let  $\Lambda = N\mathbb{Z}^k + \{(r_1x, \dots, r_kx) : x \in \mathbb{Z}\}$ . Write  $\underline{r}$  for  $(r_1, \dots, r_k)$ . Claim that  $B(K, \delta) \cong \Lambda \cap [-\delta N, \delta N]^k$ .

Define a map  $\phi : B(K, \delta) \rightarrow \Lambda \cap [-\delta N, \delta N]^k$  by

$$x \mapsto (\langle r_1x \rangle, \dots, \langle r_kx \rangle)$$

where  $\langle u \rangle$  means the least-modulus residue of  $u \bmod N$ . If  $x + y = z + w$ , then  $\underline{r}x + \underline{r}y = \underline{r}z + \underline{r}w$  in  $\mathbb{Z}_N^k$ . But for each  $i$ ,  $\langle r_ix \rangle + \langle r_iy \rangle - \langle r_iz \rangle - \langle r_iw \rangle \in [-4\delta N, 4\delta N]$ . Since  $\delta < 1/4$ , that implies that  $\langle r_ix \rangle + \langle r_iy \rangle - \langle r_iz \rangle - \langle r_iw \rangle = 0$ . So  $\langle \underline{r}x \rangle + \langle \underline{r}y \rangle - \langle \underline{r}z \rangle - \langle \underline{r}w \rangle = \underline{0}$ .

That already implies that  $\phi$  is an injection.

If  $\underline{r}x + \underline{a}N \in [-\delta N, \delta N]^k$  (this is a way of writing a typical point in a lattice), then  $r_ix \in [-\delta N, \delta N] \bmod N$  for each  $i$ , so  $x \in B(K, \delta)$  and  $\phi(x) = \underline{r}x + \underline{a}N$ . So  $\phi$  is a surjection.

If  $\underline{r}x + \underline{a}N + \underline{r}y + \underline{b}N = \underline{r}z + \underline{c}N + \underline{r}w + \underline{d}N$ , then  $r_i(x + y) = r_i(z + w) \bmod N$ , so  $x + y = z + w \bmod N$ , so the inverse of  $\phi$  is also a Freiman homomorphism.

(End of proof)  $\square$

(we will not prove in this course, but later in next term, we will prove a generalized version of AP contained in an intersection of  $K$  and a box - this requires more knowledge in geometry of numbers, so cannot be dealt here)

**Lemma 10)** Let  $\Lambda$  be a lattice and let  $C$  be a symmetric convex body, both in  $\mathbb{R}^k$ . Then  $|\Lambda \cap C| \leq 5^k |\Lambda \cap \frac{C}{2}|$  (5 is not an optimal bound, but convenient to prove - how do we reduce this?)

**proof)** Let  $x_1, \dots, x_n$  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  $x_i + C/2$  cover all of  $\Lambda \cap C$ . So we see that

$$|\Lambda \cap C| = |\cup_i (x_i + C/2) \cap \Lambda| \leq n |\Lambda \cap C/2|$$

Also, the sets  $x_i + C/4$  are disjoint subsets of  $\mathbb{R}^k$ , and they are all contained in  $C + \frac{C}{4} = 5C/4$ . That is  $\cup_i (x_i + C/4) \subset 5C/4$  and therefore

$$|\cup_i (x_i + C/4)| = n |C/4| \leq |5C/4|$$

Hence  $n \leq \frac{\text{vol}(5C/4)}{\text{vol}(C/4)} = 5^k$ , and we have the conclusion along with the previous inequality.

**Corollary 11)** If  $N$  is primes,  $0 \notin K$ ,  $|K| = k$ ,  $\delta < 1/4$ , then  $|B(K, \delta)| \delta 5^k |B(k, \delta/2)|$

## 2. Sum Sets and their Structure

Suppose  $A$  is a subset of integers, and has  $k$  such that  $|A + A| \leq k|A|$ . What can we say about the set  $A$ ? What can we say about the bound of  $|rA - sA|$ ? (will prove  $|rA - sA| \leq k^{r+s}|A|$ )

**Lemma 1)** (George Petridis - a former student of T.W.Gowers) Let  $A_0$  and  $B$  be finite subsets of an Abelian group such that  $|A_0 + B| \leq K_0|A_0|$ . Then there exists a subset  $A \subset A_0$  and  $K \leq K_0$  such that  $|A + B + C| \leq K|A + C|$  for every finite subset  $C$  of the group.

-the style of proof is so different from other combinatorics proofs. It uses induction on  $C$ . (Lesson to take : do not dispose a method for proof even before thinking about it)

**proof)** Choose  $A \subset A_0$  that minimizes the ratio  $|A + B|/|A|$  and let the minimal ratio be  $K$ .

★ Claim : This particular choice of  $A$  and  $K$  works - We prove this by induction on  $C$ .

**proof)** If  $C = \emptyset$ , we are all happy.

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

$$|A + (C \cup \{x\})| = |A + C| + |A| - |A'|$$

Also,  $A + B + (C \cup \{x\}) = (A + B + C) \cup ((A + B + x) \setminus (A' + B + x))$  since if  $a + x \in A + C$ , then  $a + B + x \subset A + B + C$ .

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

by induction and minimality property of  $A$

(End of proof)  $\square$

=====

(18th October, Thursday)

(Example class next Wednesday afternoon, 24th October)

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

**proof)** Choose  $A'$  as we chose  $A$  in **Lemma 1**, that is, minimizing  $|A' + B|/|A'|$ . 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.

(End of proof)  $\square$

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

**proof)** Just set  $B = A$  or  $-A$  in **Corollary 2**, and note that  $|A \pm rA| \geq |rA|$ .

(End of proof)  $\square$

**Lemma 4)** (*Ruzsa triangle inequality*) Let  $A, B, C$  be finite subsets of an Abelian group. Then

$$A|B - C| \leq |A - B||A - C|$$

**proof)** Define a map  $\phi : A \times (B - C) \rightarrow (A - B) \times (A - C)$  as follows : For each  $x \in B - C$ , choose functions  $b(x) \in B$  and  $c(x) \in C$  such that  $b(x) - c(x) = x$ . Now given  $(a, x)$  with  $a \in A$ ,  $x \in B - C$ , set  $\phi(a, x) = (a - b(x), a - c(x))$ .

Note that given  $(a - b(x), a - c(x)) \in (A - B) \times (A - C)$ , we may find  $x = b(x) - c(x) = (a - c(x)) - (a - b(x))$ . And then, having worked with  $x$ , we know  $b(x)$ , and  $a = a - b(x) + b(x)$ , so  $a$  is determined too, so  $\phi$  is an injection, and the inequality follows.

(End of proof)  $\square$

Why does this lemma deserves its name 'triangular 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**  $d(A, B)$  to be  $\frac{|A - B|}{|A|^{1/2}|B|^{1/2}}$ , then the inequality says  $d(B, C) \leq d(A, B)d(A, C)$ . (be aware that,  $\log(d(A, B))$  still does not define a metric... this defines a metric if and only if  $A$  is a coset of a subgroup. But this inequality is still useful, since this helps to measure a distance between two sets using other two relations.)

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

**proof)** Pick  $A'$  as before. Then by **Corollary 2** with  $B$  replaced by  $-B$ , has

$$|A' - rB| \leq K^r |A'| \quad \text{and} \quad |A' - sB| \leq K^s |A'|$$

Therefore by Ruzsa triangle inequality,

$$|A'| |rB - sB| \leq K^{r+s} |A'|^2 \Rightarrow |rB - sB| \leq K^{r+s} |A|$$

(End of proof)  $\square$

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

**proof)** Apply **Corollary 5** with  $B = -A$  or  $B = A$ .

(End of proof)  $\square$

If you follow the lines of proof, you'll find them trivial but the proof themselves are highly non-trivial.

**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  $p > 4C|A|$  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  $\mathbb{Z}_p$ .

(In fact, the proof tells us that such subset  $A' \subset A$  exists for any prime  $p > 2C|A|$ , with  $|A'| \geq \lfloor |A|/k \rfloor$ )

This gives a pretty dense subgroup of a cyclic group. This is beneficial later one

**proof)** Consider the following composition of maps, with prime  $q > 2k \max\{|a| : a \in A\}$

$$\phi : \mathbb{Z} \xrightarrow{\text{reduce mod } q} \mathbb{Z}_q \xrightarrow{\times \text{ by some (random) } r \neq 0} \mathbb{Z}_q \xrightarrow{\text{least non-neg. residue}} \mathbb{Z} \xrightarrow{\text{reduce mod } p} \mathbb{Z}_p$$

where  $q$  is a prime bigger than  $\text{diam}(A)$  (the largest element of  $A - A$ ) and  $p$  is a prime  $\in (2C|A|, 4C|A|]$ . Call  $\phi$  for this composition. The first, second and fourth parts are group homomorphisms, and thus Freiman homomorphism of all orders. Also, the third map is a Freiman homomorphism of order  $k$  if you restrict to a subinterval of  $[0, q - 1]$  of length  $\leq q/k$ . To see this, write  $\langle u \rangle$  for least non-negative residue, let  $I$  be an interval of length  $\leq q/k$  (and therefore  $< q/k$ ) and  $u_1, \dots, u_{2k} \in I$ . If  $u_1 + \dots + u_k - u_{k+1} - \dots - u_{2k} = 0$ , then

$$\langle u_1 \rangle + \dots + \langle u_k \rangle - \langle u_{k+1} \rangle - \dots - \langle u_{2k} \rangle \equiv 0 \pmod{q}$$

and also  $\langle u_1 \rangle + \dots + \langle u_k \rangle - \langle u_{k+1} \rangle - \dots - \langle u_{2k} \rangle \in (-q, q)$ . So it is zero.

By the pigeon hole principle, for any  $r$  we can find  $I$  of length  $\leq q/k$  such that  $A' = \{a \in A : ra \in I \pmod{q}\}$  has size at least  $|A|/k$  (In fact, this is not true : Let  $q = ku + s$  and  $|A| = kw + v$ , where  $s, v \in [0, k - 1]$ .  $I_1, \dots, I_k$  be disjoint intervals of each length  $u \leq q/k$ . Then  $|\cup_j \{a \in A : ra \in I_j\}| \geq |A| - s = kw + (v - s)$ . Then by pigeon hole principle, one can choose  $I_j$  with  $|\{a \in A : ra \in I_j\}| \geq w = \lfloor |A|/k \rfloor$ . So  $|A|/k$  should be replaced by  $\lfloor |A|/k \rfloor$ . How do I fix this problem?) Then  $\phi|_{A'}$  is a Freiman homomorphism of order  $k$ .

It remains to prove that  $\phi$  is an isomorphism to its image. That is, we must show that if

$$a_1 + \dots + a_k - a_{k+1} - \dots - a_{2k} \neq 0 \quad (a_i \in A)$$

$$\text{then} \quad \langle a_1 \rangle + \dots + \langle a_k \rangle - \langle a_{k+1} \rangle - \dots - \langle a_{2k} \rangle \not\equiv 0 \pmod{p}$$

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

$$\left| \langle ra_1 \rangle + \dots + \langle ra_k \rangle - \langle ra_{k+1} \rangle - \dots - \langle ra_{2k} \rangle \right| < q$$

and

$$\langle ra_1 \rangle + \dots + \langle ra_k \rangle - \langle ra_{k+1} \rangle - \dots - \langle ra_{2k} \rangle \equiv r(a_1 + \dots + a_k - a_{k+1} - \dots - a_{2k}) \pmod{q}$$

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

(End of proof)  $\square$



=====

(23rd October, Wednesday)

(Tomorrow example class MR3, 2pm)

(Question 10 in examples sheets - need condition that  $B$  has property  $P$ )

## Freiman's theorem (a version of)

We shall now start with a set  $A \subset \mathbb{Z}$  with  $|A + A| \leq C|A|$  and put together several of the previous results to say a lot about the structure of  $A$ .

(The theorem proved here is not the most general version. For a stronger version, see the attached note of Brad Hannigan-Daley)

- By Plünnecke's theorem,  $|8A - 8A| \leq C^{16}|A|$
- By Ruzsa's embedding lemma,  $A$  has a subset  $A'$  of size at least  $|A|/8$  that is 8-isomorphic to a subset  $A'' \subset \mathbb{Z}_p$  with  $p \leq 4C^{16}|A|$ . The density of  $A''$  in  $\mathbb{Z}_p$  is  $\alpha \geq \frac{1}{32C^{16}}$ .
- By Bogolyubov's lemma,  $2A'' - 2A''$  contains a Bohr set  $B(K, 1/4)$  with  $|K| \leq \alpha^{-2}$ , which is 2-isomorphic to a set  $B$  that is the intersection of a symmetric convex with a lattice of dimension at most  $\alpha^{-2}$ . But  $2A'' - 2A'' \stackrel{2}{=} 2A' - 2A'$  (think for a minute - if  $A' \stackrel{8}{=} A''$  then we should have  $2A' - 2A' \stackrel{2}{=} 2A'' - 2A''$ ), and therefore  $2A' - 2A'$  has a subset  $B$  that is isomorphic to  $B'$ .
- Now let  $X \subset A$  be maximal such that the sets  $x + B$  with  $x \in X$  are disjoint. Then  $A \subset X + B - B$ , by maximality. Also,

$$|X||B| = |X + B| \leq |3A - 2A| \leq C^5|A| \Rightarrow |X| \leq C^5|A|/|B|$$

But by **Lemma 8** about Bohr sets,  $|B| \geq 4^{\alpha^{-2}}|A|$ , so  $|X| \leq 4^{\alpha^{-2}}C^5 \leq 4^{1024C^{32}}C^5$ . So  $A$  is contained in the union of at most  $4^{1024C^{32}}C^5$  translates of  $B - B$

- If  $B = \Lambda \cap K_0$  (where  $K_0$  is a symmetric convex body) then  $B - B \subset \Lambda \cap 2K_0$ , and also  $|B - B| \leq C^2|A| \leq 5^{\alpha^{-2}}|B|$ . So this

We need a additional statement about the geometry of numbers to prove the real Freiman's theorem.

\*\*\*\*\*

(not lectured)

**Minkowski's Second Theorem** : Let  $K$  be a symmetric convex body and  $\Lambda$  a lattice in  $\mathbb{R}^k$ . Let  $\lambda_1 \leq \dots \leq \lambda_k$  be the successive minima of  $C$  with respect to  $\Lambda$ . Then  $\lambda_1 \dots \lambda_k \leq 2^k \det(\Lambda)/\text{vol}(K)$ .

**Lemma** (Volume Packing Lemma) Let  $\Lambda, \Lambda'$  be lattices with  $\lambda \subset \Lambda' \subset \mathbb{R}^n$ . Then

$$\det(\Lambda) = \det(\Lambda')[\Lambda : \Lambda']$$

**Proposition**) Let  $N$  be a large prime,  $r_1, \dots, r_k$  be distinct residue classes mod  $N$  with  $k \geq 2$ , and let  $\delta \in (0, 1)$ . Then the Bohr set  $\mathcal{B}(r_1, \dots, r_k; \delta)$  in  $\mathbb{Z}/N$  contains a proper generalized arithmetic progression of dimension  $k$  and size at least  $(\delta/k)^k N$ .

It follows the Freiman's theorem.

**Freiman's Theorem** : Let  $A$  be a finite subset of  $\mathbb{Z}$  with  $|A + A| \leq C|A|$ . Then there exist constants  $d'$  and  $S$  depending only on  $C$  such that  $A$  is contained in a generalized arithmetic progression of dimension at most  $d'$  and size at most  $S$ .

\*\*\*\*\*

## The Balog-Szemerédi-Gowers theorem

**Definition)** Let  $A$  be a subset of an Abelian group. An **additive quadruple** in  $A$  is a quadruple  $(a, b, c, d) \in A^4$  such that  $a + b = c + d$ . (Equivalently, it's a quadruple such that  $a - b = c - d$ )

If  $|A| = n$ , then the number of additive quadruples in  $A$  is at most  $n^3$  (this is obtained if  $A$  is a subgroup or a coset of a subgroup.) We shall show that if  $A^4$  contains at least  $cn^3$  additive quadruples, then  $A$  has a subset  $A'$  of size at least  $c'n$  with  $|A - A'| \leq C|A'|$  where  $c'$  and  $C$  depend (nicely) on  $c$  only.

=====

(25th October, Thursday)

**Lemma 8)** Let  $A_1, A_2, \dots, A_m$  be subsets of  $[n] = \{1, 2, \dots, n\}$  of average density at least  $\delta$ . Then for any  $\eta > 0$  we can find a set  $B \subset [m]$  of size at least  $\delta m / \sqrt{2}$  such that the proportion of pairs  $(i, j) \in B^2$  with  $|A_i \cap A_j| \geq \eta \delta^2 n / 2$  is at least  $1 - \eta$ .

**proof)** Choose  $y \in [n]$  uniformly at random, and set  $B = \{i : y \in A_i\}$ . The probability that we pick both  $i$  and  $j$  is  $|A_i \cap A_j| / n$ , which we can write as  $\langle A_i, A_j \rangle$ . So the expected number of pairs we pick is

$$\sum_{i,j} \langle A_i, A_j \rangle = \left\| \sum_i A_i \right\|_2^2 \geq \left\| \sum_i A_i \right\|_1^2 = (\delta m)^2 = \delta^2 m^2$$

The probability that we pick  $i, j$  with  $|A_i \cap A_j| \leq \eta \delta^2 n / 2$  is at most  $\eta \delta^2 / 2$ . Call such a pair  $(i, j)$  **bad**. Then

$$\mathbb{E}|B|^2 - \eta^{-1} \mathbb{E}(\# \text{ bad pairs picked}) \geq \delta^2 m^2 - \eta^{-1} \frac{\eta \delta^2}{2} m^2 = \frac{\delta^2 m^2}{2}$$

Therefore, there exists  $B$  such that  $|B| \geq \delta m / \sqrt{2}$  and the proportion of pairs in  $B^2$  that are bad is at most  $\eta$ .

(End of proof)  $\square$

The following is an equivalent statement.

**Corollary 9)** Let  $G$  be a bipartite graph with finite vertex sets  $X, Y$  and density at least  $\delta$ . Then there is a subset  $B \subset X$  of size at least  $\delta|X|/\sqrt{2}$  such that for at least  $(1 - \eta)|B|^2$  pairs  $(x_1, x_2) \in B^2$ , there are at least  $\frac{\eta \delta^2}{2}|Y|$  paths of length 2 from  $x_1$  to  $x_2$ .

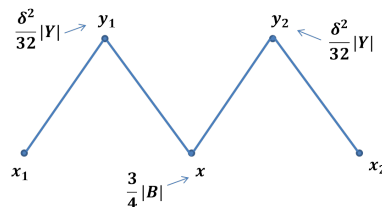
(Note : density of a bipartite graph =  $|E(G)|/(|X||Y|)$ )

**proof)** Put  $X = [m]$  and  $Y = [n]$  and  $A_i = \{y \in Y : (i, y) \in E, i \in X, y \in Y\} \subset Y$  be as in the setting of **Lemma 8**. If we choose a subset  $B$  of  $X$ , then there is a path of length 2 from  $x_1 \in B$  to  $x_2 \in B$  passing through  $B$  if and only if  $|A_{x_1} \cap A_{x_2}|$  is non-empty, therefore we can just apply **Lemma 8** to conclude.

(End of proof)  $\square$

**Corollary 10)** Let  $G$  be a bipartite graph as above with density  $\delta$ . Then there is a subset  $B' \subset X$  of size at least  $\delta|X|/2\sqrt{2}$  such that for every  $x_1, x_2 \in B'$  there are at least  $\frac{\delta^5}{2048\sqrt{2}}|X||Y|^2$  paths of length 4 from  $x_1$  to  $x_2$ .

**proof)** Choose  $B$  as in **Corollary 9** with  $\eta = 1/16$ . Define a graph  $\Gamma$  with vertex set  $B$ , joining  $x_1$  to  $x_2$  if there are at least  $\frac{\delta^2}{32}|Y|$  paths of length 2 from  $x_1$  to  $x_2$  in  $G$ . By **Corollary 9**, the average degree in  $\Gamma$  is at least  $\frac{15}{16}|B|$ . Therefore, there are at least  $|B|/2$  vertices in  $B$  of degree at least  $\frac{7}{8}|B|$ . Let  $B'$  be the set of all such vertices. If  $x_1, x_2 \in B'$ , then there are at least  $\frac{3}{4}|B|$  vertices in  $B$  joined to both  $x_1$  and  $x_2$  in  $\Gamma$ . Therefore, there at least



$$\frac{\delta^4}{1024}|Y|^2 \frac{3}{4} \frac{\delta|X|}{\sqrt{2}} \quad \text{paths of length 4 from } x_1 \text{ to } x_2$$

[Note : setting  $\eta = 1/8$  would(?) give a bound of  $\frac{\delta^4}{256}|Y|^2 \frac{1}{2} \frac{\delta|X|}{\sqrt{2}}$ ]

(End of proof)  $\square$

**Lemma 11)** (*The BSG Lemma*) Let  $A$  be a subset of size  $n$  of an Abelian group  $H$ . Suppose that there are at least  $cn^3$  additive quadruples in  $A$ . Then  $A$  has subset  $A'$  of size at least  $c'n$  with  $|A' - A'| \leq C|A'|$ , where  $c'$  and  $C$  depend on  $c$  only.

**proof)** For each  $d$ , let  $f(d)$  be the number of ways of writing  $d = a_1 - a_2$  with  $a_1, a_2 \in A$ . Then  $\sum_d f(d)^2 \geq cn^3$ , because  $f(d)^2$  is the number of quadruples  $(a_1, a_2, a_3, a_4)$  with  $d = a_1 - a_2 = a_3 - a_4$  for each  $d$ . Call  $d$  **popular** if  $f(d) \geq cn/2$ . Then

$$\begin{aligned} cn^3 &\leq \sum_d f(d)^2 = \sum_{d \text{ popular}} f(d)^2 + \sum_{d \text{ unpopular}} f(d)^2 \\ &\leq (\# \text{ popular } d) \times n^2 + \frac{cn}{2} n^2 \quad (\text{since } \sum_d f(d) = n^2) \end{aligned}$$

Therefore, the number of popular  $d$  is at least  $cn/2$ .

Now define a graph with vertex set  $A$ , by joining  $a_1$  to  $a_2$  if  $a_1 - a_2$  (or  $a_2 - a_1$ ) is popular. Each popular difference contributes at least  $cn/2$  edges so the average degree of the graph is at least  $c^2/4$ .

By duplicating the vertex set, create a corresponding bipartite graph  $G$ . By **Corollary 10** with  $\delta = c^2/4$ , we can find a subset  $B \subset A$  of size at least  $\frac{c^2}{8\sqrt{2}}|A|$  such that for any  $a_1, a_2 \in B$  there are at least  $\frac{\delta^5}{2048\sqrt{2}}|A|^3$  paths of length 4 from  $a_1$  to  $a_2$ . Each such paths of length 4 gives us at least  $(\frac{c}{2}|A|)^4$  ways of writing  $a_2 - a_1$  as  $b_1 - b_2 + b_3 - b_4 + b_5 - b_6 + b_7 - b_8$  with all  $b_i \in A$ . So

$$|B - B| \times \frac{\delta^5}{2048\sqrt{2}}|A|^3 \left(\frac{c}{2}|A|\right)^4 \leq |A|^8$$

so  $|B - B| \leq C'|A| \leq C|B|$

(End of proof)  $\square$