University of Georgia REU - Additive Combinatorics - Summer 2010

Roth's theorem in random subsets of $\mathbb{Z}_N$

In this exercise sheet, we outline the proof of Roth's theorem for random sets.

We will assume N is a large odd integer throughout. Suppose $f : \mathbb{Z}_N \to \mathbb{C}$. Then we define the normalized *Fourier transform* $\widehat{f} : \mathbb{Z}_N \to \mathbb{C}$ by the formula

$$\widehat{f}(\xi) := \frac{1}{N} \sum_{x \in \mathbb{Z}_N} f(x) e(-x\xi/N).$$

We define the ℓ_p *norm* of the Fourier transform $\widehat{f}$ to be

$$\|\widehat{f}\|_p := \Big(\sum_{\xi \in \mathbb{Z}_N} |\widehat{f}(\xi)|^p \Big)^{1/p},$$

for $1 \leq p < \infty$ and

$$\|\widehat{f}\|_\infty := \max_{\xi \in \mathbb{Z}_N} |\widehat{f}(\xi)|.$$

1. **Roth's theorem in $\mathbb{Z}_N$**

   Prove the following version of Roth's theorem, due to Varnavides:

   Theorem 1. *Let $\delta > 0$ and $N \geq 1$ prime. If $f : \mathbb{Z}_N \to [0,1]$ such that*

   $$\frac{1}{N} \sum_{x \in \mathbb{Z}_N} f(x) \geq \delta,$$

   then there exists a constant $c(\delta) > 0$ such that

   $$\sum_{x,d \in \mathbb{Z}_N} f(x) f(x+d) f(x+2d) \geq c(\delta) N^2.$$

   Hint: If f is the characteristic function of a set this result follows from Varnavides. In general we can reduce to this case by considering the set $A := \{x \in \mathbb{Z}_N : f(x) \geq \delta/2\}$.

2. **Restriction estimate for random subsets of $\mathbb{Z}_N$**

   Lemma 2 (Lemma 10.22, Tao-Vu)**.** *Suppose $f : \mathbb{Z}_N \to \mathbb{C}$ satisfies $|f(x)| \leq \nu(x)$ for all $x \in \mathbb{Z}_N$ where $\nu : \mathbb{Z}_N \to [0, \infty)$ obeys the pseudorandom condition*

   $$|\widehat{\nu}(\xi)| \leq \eta \text{ for every } \xi \neq 0,$$

   and

   $$|\widehat{\nu}(0) - 1| \leq \eta,$$

   for some $0 < \eta \leq 1$. Then

   $$\Big| \Big\{ \xi \in \mathbb{Z}_N : |\widehat{f}(\xi)| \geq \alpha \Big\} \Big| \leq \frac{4}{\alpha^2}$$

   provided $\alpha \geq 2\eta^{1/2}$.

Exercise: Use Plancherel to verify that the conclusion above holds (easily) for all $\alpha > 0$ in the case where $\nu(x) = 1$ for all $x \in \mathbb{Z}_N$.

Lemma 3. *Let $0 < \eta \leq 1$. Suppose $f : \mathbb{Z}_N \to [0, \infty)$ satisfies*

$$\|\widehat{f}\|_2 \leq C\eta^{-\varepsilon/4}$$

for some $\varepsilon > 0$. Assume $f \leq \nu$ where $\nu : \mathbb{Z}_N \to [0, \infty)$ obeys the pseudorandom condition

$$|\widehat{\nu}(\xi)| \leq \eta \text{ for every } \xi \neq 0,$$

and

$$|\widehat{\nu}(0) - 1| \leq \eta.$$

Then there exists a constant M so that

$$\|\widehat{f}\|_{2+\varepsilon} \leq M.$$

3. **Structure and randomness: A decomposition $f = f_1 + f_2$**

Prove the following decomposition lemma:

Lemma 4. *Assume that $f : \mathbb{Z}_N \to [0, \infty)$ satisfies*

$$\|\widehat{f}\|_q \leq M \tag{1}$$

for some $2 < q < 3$ and $f \leq \nu$, where $\nu : \mathbb{Z}_N \to [0, \infty)$ obeys the pseudorandom condition

$$|\widehat{\nu}(\xi)| \leq \eta \text{ for every } \xi \neq 0, \tag{2}$$

and

$$|\widehat{\nu}(0) - 1| \leq \eta,$$

for some $0 < \eta \leq 1$. Let

$$f_1(x) = \frac{1}{|B|^2} \sum_{y_1, y_2 \in B} f(x + y_1 - y_2),$$

where

$$B := B(\Gamma, \varepsilon) = \{x \in \mathbb{Z}_N : \ |e(-x\xi/N) - 1| \leq \varepsilon \text{ for all } \xi \in \Gamma\}$$

and

$$\Gamma = \left\{\xi : \ |\widehat{f}(\xi)| \geq \varepsilon\right\}$$

for some $\varepsilon > 0$ to be fixed later. Let $f_2(x) = f(x) - f_1(x)$. Then

(i) $0 \leq f_1 \leq \widehat{\nu}(0) + \frac{\eta N}{|B|}$

(ii) $\frac{1}{N} \sum_{x \in \mathbb{Z}_N} f_1(x) = \frac{1}{N} \sum_{x \in \mathbb{Z}_N} f(x)$

(iii) $|\widehat{f_i}(\xi)| \leq |\widehat{f}(\xi)|$ *for all* $\xi \in \mathbb{Z}_N$ *and* $i = 1, 2$.

(vi) $\|\widehat{f_2}(\xi)\|_\infty \leq 3(1 + \eta)\varepsilon$

4. **Roth's theorem for random sets**

Using Parts 1, 2 and 3, prove the following version of Roth's theorem for random sets:

Theorem 5. *Let $\delta > 0$, $0 < \theta \leq 1/100$ and $W \subseteq \mathbb{Z}_N$ with $|W| = N^{1-\theta}$ that satisfies the condition $|\widehat{W}(\xi)| \leq N^{-1/3}$ for all $\xi \neq 0$. If $A \subseteq W$ with $|A| \geq \delta |W|$ and N is sufficiently large, then A must contain a nontrivial three term arithmetic progression.*

Sketch of the proof of Theorem 5: Define $f(x) = N^{\theta} A(x)$ and $\nu(x) = N^{\theta} W(x)$.

(a) Let B and Γ be as in Part 3 above.
   i. Use estimate (1) to show that $|\Gamma| \leq (M/\varepsilon)^q$.
   ii. Use the pigeonhole principle to prove that $|B| \geq C\varepsilon^{|\Gamma|}$.

(b) i. Verify that $\|f\|_2 \leq N^{\theta}$.
   ii. Deduce from Lemma 3 that the restriction estimate (1) holds for $q = 5/2$, say.