University of Georgia REU - Additive Combinatorics - Summer 2010

Exercise sheet 4

Some Definitions

Definition 1. *Let $f : \mathbb{Z}_N \to \mathbb{C}$. We define the* Fourier transform *of f to be*

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

where $e(\alpha) := e^{2\pi i \alpha}$.

Definition 2. *Let $f, g : \mathbb{Z}_N \to \mathbb{C}$. We define the* convolution *of f with g to be*

$$f * g(x) = \frac{1}{N} \sum_{y \in \mathbb{Z}_N} f(y) g(x-y).$$

Definition 3. *Given a set $A \subseteq \mathbb{Z}_N$ we denote its characteristic function*

$$A(x) = \begin{cases} 1 & \text{if} \quad x \in A \\ 0 & \text{otherwise} \end{cases}$$

Definition 4. *We say that a set $A \subseteq \mathbb{Z}_N$ is* ε-uniform *if $|\widehat{A}(\xi)| \leq \varepsilon$ for all $\xi \neq 0$.*

Problems and Exercises

1. Prove the orthogonality relation

$$\frac{1}{N} \sum_{\xi \in \mathbb{Z}_N} e(x\xi/N) = \begin{cases} 1 & \text{if} \quad x \equiv 0 \pmod N \\ 0 & \text{otherwise} \end{cases}$$

2. Let $f, g : \mathbb{Z}_N \to \mathbb{C}$. Verify the following identities/inequalities.

   (a) (Fourier inversion formula)

$$f(x) = \sum_{\xi \in \mathbb{Z}_N} \widehat{f}(\xi) e(x\xi/N)$$

   (b) (Parseval's identity)

$$\frac{1}{N} \sum_{x \in \mathbb{Z}_N} f(x) \overline{g(x)} = \sum_{\xi \in \mathbb{Z}_N} \widehat{f}(\xi) \overline{\widehat{g}(\xi)}$$

   (c) (Plancherel's identity)

$$\frac{1}{N} \sum_{x \in \mathbb{Z}_N} |f(x)|^2 = \sum_{\xi \in \mathbb{Z}_N} |\widehat{f}(\xi)|^2$$

(d) (Convolution identity)

$$\widehat{f * g}(\xi) = \widehat{f}(\xi)\widehat{g}(\xi)$$

(e) (Uniform boundedness)

$$\max_{\xi \in \mathbb{Z}_N} |\widehat{f}(\xi)| \leq \frac{1}{N} \sum_{x \in \mathbb{Z}_N} |f(x)|$$

3. (a) Show that for any $A \subseteq \mathbb{Z}_N$ one always has

$$\max_{\xi \in \mathbb{Z}_N} |\widehat{A}(\xi)| \leq \widehat{A}(0) = \frac{|A|}{N}.$$

(b) Show that if $A = \mathbb{Z}_N$, then

$$\widehat{A}(\xi) = \begin{cases} 1 & \text{if} \quad \xi \equiv 0 \pmod{N} \\ 0 & \text{otherwise} \end{cases}$$

(c) Let $P := \{a, a+q, \ldots, a+(L-1)q\} \subseteq \mathbb{Z}_N$. Show that if $\xi q \equiv 1 \pmod{N}$, then

$$\widehat{P}(\xi) = \frac{L}{N} e(-a\xi/N) + O\left(\frac{L^2}{N^2}\right).$$

4. Fix $\xi \in \mathbb{Z}_N \setminus \{0\}$.

(a) Let $1 \leq Q \leq N$.

i. Show that there exists $1 \leq q \leq Q$ such that

$$\left\| q \frac{\xi}{N} \right\| \leq \frac{1}{Q}$$

where $\|\alpha\|$ denotes, for each $\alpha \in \mathbb{R}$, the distance from α to the nearest integer.

ii. Let $1 \leq L \leq N$. Show that there exists an arithmetic progression P of length L and step size q, with $1 \leq q \leq Q$, such that

$$|\widehat{P}(\xi)| \geq \frac{L}{N} - \frac{2\pi L^2}{NQ}.$$

(b) Let $1 \leq L \leq N/4\pi$ and set $\eta = L/N$. Show that there exists $1 \leq q \leq 4\pi L$ so that the arithmetic progression

$$P_q := \{-q, -2q, \ldots, -Lq\} \subseteq \mathbb{Z}_N$$

satisfies

$$|\widehat{P_q}(\xi)| \geq \eta/2.$$

5. (a) Given any 2-coloring of $\mathbb{Z}_N$, using the colors red and blue (say), we define the function

$$f(x) = \begin{cases} 1 & \text{if } x \text{ is red} \\ -1 & \text{if } x \text{ is blue} \end{cases}.$$

i. Show that the *discrepancy* function

$$\Delta_q(x) := N|f * P_q(x)|$$

counts the difference (in absolute value) between the number of red and blue elements in the progression

$$\{x+q, x+2q, \ldots, x+Lq\} \subseteq \mathbb{Z}_N$$

where $P_q := \{-q, -2q, \ldots, -Lq\}$.

ii. Using Question 4b, verify that if $1 \leq L \leq N/4\pi$, then

$$\frac{1}{N}\sum_{q=1}^{4\pi L}\sum_{x\in\mathbb{Z}_N}|f * P_q(x)|^2 \geq \left(\frac{L}{2N}\right)^2$$

and hence that there exists $1 \leq q_0 \leq 4\pi L$ and $x_0 \in \mathbb{Z}_N$ such that

$$\Delta_{q_0}(x_0) \geq \sqrt{L/16\pi}.$$

(b) Prove **Roth's $\frac{1}{4}$-Theorem**: In any 2-coloring of $[1, N]$ there exists an arithmetic progression that contains at least $cN^{1/4}$ more elements in one color than the other.

Hint: Identify $[1, N]$ with $\mathbb{Z}_N$ and set $L = \lfloor\sqrt{N/4\pi}\rfloor$. This will ensure that the progressions $x_0 - P_{q_0}$ obtained above is "non-overlapping". Deduce that there must exist a genuine arithmetic progression in $[1, N]$ with discrepancy at least $\sqrt{L/16\pi}/2$.

For more on Roth's $\frac{1}{4}$-Theorem, see Chazelle's book "The discrepancy method" [1].

6. Let $A \subseteq \mathbb{Z}_N$ and $d \in \mathbb{Z}_N$. Show that if we set $A_d = A + d$, then

$$\widehat{A_d}(\xi) = \widehat{A}(\xi)e(-d\xi/N).$$

7. (Expressing combinatorial counts using the Fourier transform).

Let $A, B \subseteq \mathbb{Z}_N$.

(a) Show that

$$\frac{|A \cap B|}{N} = \sum_{\xi\in\mathbb{Z}_N}\widehat{A}(\xi)\overline{\widehat{B}(\xi)}$$

noting in particular that

$$\sum_{\xi\in\mathbb{Z}_N}|\widehat{A}(\xi)|^2 = \frac{|A|}{N}.$$

(b) Let

$$r_4(A) := |\{(a, b, c, d \in A^4 : a - c = d - b\}|$$

denote the number of additive quadruples in A. Show that

$$\frac{r_4(A)}{N^3} = \sum_{\xi\in\mathbb{Z}_N}|\widehat{A}(\xi)|^4.$$

(c) Let

$$\mathcal{N}_3(A) := |\{(x,y,z) \in A^3 : x - z = z - y\}|$$

denote the number of 3-term arithmetic progressions in A. Show that

$$\frac{\mathcal{N}_3(A)}{N^2} = \sum_{\xi \in \mathbb{Z}_N} \widehat{A}(\xi)^2 \widehat{A}(-2\xi).$$

8. (Illustrations that ε-uniformity can be interpreted as a measure of quasi-randomness). Let $A \subseteq \mathbb{Z}_N$ and set $\delta := |A|/N$.

(a) Verify that if A is ε-uniform, then

$$0 \leq \frac{r_4(A)}{N^3} - \delta^4 \leq \varepsilon^2 \delta$$

(b) Verify that if A is ε-uniform and N is odd, then

$$\left| \frac{\mathcal{N}_3(A)}{N^2} - \delta^3 \right| \leq \varepsilon\delta$$

(c) Verify that if A is ε-uniform, then

$$\frac{1}{N} \sum_{d \in \mathbb{Z}_N} \left| \frac{|A \cap (A+d)|}{N} - \delta^2 \right| \leq \varepsilon \delta^{1/2} \leq \varepsilon$$

and hence that

$$\left| \left\{ d \in \mathbb{Z}_N : \left| \frac{|A \cap (A+d)|}{N} - \delta^2 \right| \geq \varepsilon^{1/2} \right\} \right| \leq \varepsilon^{1/2} N$$

(d) Let

$$P := \{a, a+q, \ldots, a+(L-1)q\} \subseteq \mathbb{Z}_N$$

and set $\eta = L/N$.

i. Show that for each $\xi \in \mathbb{Z}_N$ one has

$$|\widehat{P}(\xi)| \leq \frac{1}{N} \min \left\{ L, \frac{1}{2\|q\xi/N\|} \right\},$$

where $\|\alpha\|$ denotes, for each $\alpha \in \mathbb{R}$, the distance from α to the nearest integer.

ii. Verify that if A is ε-uniform and N is prime, then

$$\left| \frac{|A \cap P|}{N} - \delta\eta \right| \leq C\varepsilon^{1/2}(\delta\eta)^{1/4} \leq C\varepsilon^{1/2}$$

Hint: Use Hölder's inequality.

9. Explain why each part of Question 8 illustrates that the notion of ε-uniformity of a set $A \subseteq \mathbb{Z}_N$ can interpreted as a measure of quasi-randomness.

In Questions 10-14 we outline the key steps of a (Fourier analytic) proof of Roth's theorem on arithmetic progressions of length three, namely

Roth's Theorem[2]

Let $\delta > 0$. If $N \geq \exp\exp(C\delta^{-1})$, then any subset $A \subseteq [1, N]$ with $|A| \geq \delta N$ will necessarily contain a non-trivial arithmetic progression of length three.

10. Let $A \subseteq [1, N]$ and set $\delta := |A|/N$. Let $B := A \cap [N/3, 2N/3]$.

    (a) Is it true that if A is ε-uniform/not ε-uniform (when considered as a subset of $\mathbb{Z}_N$), then B is also ε-uniform/not ε-uniform? What about other subsets of A?

    (b) Show that the number of genuine 3-term arithmetic progressions in A is greater than

    $$\widetilde{\mathcal{N}_3}(A) := |\{(x, y, z) \in B \times A \times B : x + y \equiv 2z \pmod N\}|$$

    (c) Arguing as in Question 8b, verify that if N is odd and A is ε-uniform, then

    $$\left|\widetilde{\mathcal{N}_3}(A) - \delta|B|^2\right| \leq \varepsilon|B|N.$$

    In particular, if A is ε-uniform with $\varepsilon \leq \delta|B|/2N$, then A must contains at least $\delta|B|^2/2$ genuine 3-term arithmetic progressions.

11. Let $A \subseteq \mathbb{Z}_N$ and set $\delta = |A|/N$. We define the *balanced* function of A to be

    $$f_A(x) = A(x) - \delta.$$

    (a) i. Show that

    $$\sum_{x \in \mathbb{Z}_N} f_A(x) = 0$$

    ii. Show that

    $$\sum_{x \in \mathbb{Z}_N} f_A * g(x) = 0$$

    for any $g : \mathbb{Z}_N \to \mathbb{C}$.

    (b) Show that

    $$\widehat{f_A}(\xi) = \begin{cases} \widehat{A}(\xi) & \text{if } \xi \neq 0 \\ 0 & \text{if } \xi = 0 \end{cases}$$

12. Let $A \subseteq \mathbb{Z}_N$ and set $\delta = |A|/N$.

    (a) Verify that

    $$f_A * P_q(x) = \frac{|A \cap (x - P_q)|}{N} - \delta\eta$$

    (b) Show that if A is <u>not</u> ε-uniform, then

    $$\frac{1}{N} \sum_{x \in \mathbb{Z}_N} |f_A * P_q(x)| \geq \frac{\varepsilon\eta}{2}$$

    and hence that there must exist $x \in \mathbb{Z}_N$ such that

    $$\left|\frac{|A \cap (x - P_q)|}{N} - \delta\eta\right| \geq \frac{\varepsilon\eta}{2}.$$

    ** Compare this result with Question 8(d)ii **

(c) Use the fact that $|f_A * P_q(x)| \leq \eta$ for all $x \in \mathbb{Z}_N$ (verify this if it is not clear to you) to conclude that if A is <u>not</u> ε-uniform, then in fact

$$\left|\left\{x \in \mathbb{Z}_N \,:\, \left|\frac{|A \cap (x - P_q)|}{N} - \delta\eta\right| \geq \frac{\varepsilon\eta}{4}\right\}\right| \geq \frac{\varepsilon}{4}N.$$

13. (A <u>not</u> ε-uniform $\Longrightarrow$ A has <u>increased</u> (relative) density on some long arithmetic progression)

(a) Let $A \subseteq \mathbb{Z}_N$ and P_q be the progression of length L obtained in the previous question. Set $\delta = |A|/N$ and $\eta = |P_0|/N$.

i. Verify that for any $g : \mathbb{Z}_N \to \mathbb{R}$ we have

$$g_+(x) = \frac{1}{2}\left(|g(x)| + g(x)\right)$$

where $g_+(x) = \max\{g(x), 0\}$.

ii. Show that if A is <u>not</u> ε-uniform, then

$$\frac{1}{N}\sum_{x \in \mathbb{Z}_N} (f_A * P_q)_+(x) \geq \frac{\varepsilon\eta}{4}$$

and hence

$$\left|\left\{x \in \mathbb{Z}_N \,:\, \frac{|A \cap (x - P_q)|}{|P_q|} \geq \frac{|A|}{N} + \frac{\varepsilon}{8}\right\}\right| \geq \frac{\varepsilon}{8}N.$$

(b) Let $A \subseteq [1, N]$. Prove that if A is <u>not</u> ε-uniform (when considered as a subset of $\mathbb{Z}_N$), then there exists a *genuine* arithmetic progression $P \subseteq [1, N]$ with $L = |P| \geq \sqrt{\varepsilon N/32\pi}$, such that

$$\frac{|A \cap P|}{|P|} \geq \frac{|A|}{N} + \frac{\varepsilon}{8}$$

14. Let $A \subseteq [1, N]$ and set $\delta = |A|/N$.

(a) If A contains <u>no</u> non-trivial 3-term arithmetic progressions, then either $N \leq 32\delta^{-2}$ or there exists a *genuine* arithmetic progression $P \subseteq [1, N]$ with $L = |P| \geq c\delta\sqrt{N}$, such that

$$\frac{|A \cap P|}{|P|} \geq \frac{|A|}{N} + \frac{\delta^2}{64}.$$

Hint: Use Questions 13b and 10c together with the fact that if $|A \cap [N/3, 2N/3]| < \delta N/4$, *then*

$$\max\{|A \cap [1, N/3]|, |A \cap [2N/3, N]|\} \geq \frac{9}{8}\delta N/3.$$

(b) Assume that $N > 32\delta^{-2}$ and A contains <u>no</u> non-trivial 3-term arithmetic progressions. Let $A_0 := A$, $N_0 := N$ and $\delta_0 := \delta$. Apply the above result to obtain (by translating and dilating the set $A_0 \cap P$) a new set $A_1 \subseteq [1, N_1]$ with $N_1 \geq c\delta N^{1/2}$ and size $|A_1| = \delta_1 N_1$ where $\delta_1 \geq \delta + \delta^2/64$ that also contains <u>no</u> non-trivial 3-term arithmetic progressions.

(c) Verify, by iterating this argument, that one can establish Roth's Theorem.

References

[1] Bernard Chazelle. *The discrepancy method*. Cambridge University Press, Cambridge, 2000. Randomness and complexity.

[2] K. F. Roth. On certain sets of integers. *J. London Math. Soc.*, 28:104–109, 1953.