Exercise Set #10
Combinatorial Number Theory (2025)

E1. For $f, g, h : \mathbb{Z}_N \to \mathbb{C}$, define

$$\Gamma(f,g,h) = \frac{1}{N^2} \sum_{n,m \in \mathbb{Z}_N} f(n)g(m)h(n+m).$$

(i) Prove

$$\Gamma(f,g,h) = \sum_{\xi \in \mathbb{Z}_N} \hat{f}(\xi)\hat{g}(\xi)\hat{h}(-\xi).$$

(ii) Suppose $\|f\|_\infty, \|g\|_\infty, \|h\|_\infty \leq 1$. Show that

$$|\Gamma(f,g,h)\| \leq \min\{\|\hat{f}\|_\infty, \|\hat{g}\|_\infty, \|\hat{h}\|_\infty\}.$$

Solution: (i) We start from the right hand side. Using the definition of the Fourier transform and the Fourier inversion formula, we have

$$\begin{aligned}
\sum_{\xi \in \mathbb{Z}_N} \hat{f}(\xi)\hat{g}(\xi)\hat{h}(-\xi) &= \sum_{\xi \in \mathbb{Z}_N} \left(\frac{1}{N} \sum_{n \in \mathbb{Z}_N} f(n) e\left(-\frac{\xi n}{N}\right) \right) \left(\frac{1}{N} \sum_{m \in \mathbb{Z}_N} g(m) e\left(-\frac{\xi m}{N}\right) \right) \hat{h}(-\xi) \\
&= \frac{1}{N^2} \sum_{n,m \in \mathbb{Z}_N} f(n)g(m) \left(\sum_{\xi \in \mathbb{Z}_N} \hat{h}(-\xi) e\left(\frac{-\xi(n+m)}{N}\right) \right) \\
&= \frac{1}{N^2} \sum_{n,m \in \mathbb{Z}_N} f(n)g(m) \left(\sum_{\xi \in \mathbb{Z}_N} \hat{h}(\xi) e\left(\frac{\xi(n+m)}{N}\right) \right) \\
&= \frac{1}{N^2} \sum_{n,m \in \mathbb{Z}_N} f(n)g(m)h(n+m) \\
&= \Gamma(f,g,h).
\end{aligned}$$

(ii) We focus only on the proof of $|\Gamma(f,g,h)| \leq \|\hat{f}\|_\infty$ and note that the proofs of the others two follow from similar arguments. Using part (i), we have that

$$\Gamma(f,g,h) = \sum_{\xi \in \mathbb{Z}_N} \hat{f}(\xi)\hat{g}(\xi)\hat{h}(-\xi).$$

To finish the proof, we utilize the Cauchy–Schwarz inequality and Plancherel's identity to

get

$$\begin{aligned}
|\Gamma(f,g,h)|^2 &\le \|\hat{f}\|_\infty^2 \left| \sum_{\xi \in \mathbb{Z}_N} \hat{g}(\xi)\hat{h}(-\xi) \right|^2 \\
&\le \|\hat{f}\|_\infty^2 \left(\sum_{\xi \in \mathbb{Z}_N} |\hat{g}(\xi)|^2 \right) \left(\sum_{\xi \in \mathbb{Z}_N} \left|\hat{h}(-\xi)\right|^2 \right) \\
&= \|\hat{f}\|_\infty^2 \left(\sum_{\xi \in \mathbb{Z}_N} |\hat{g}(\xi)|^2 \right) \left(\sum_{\xi \in \mathbb{Z}_N} \left|\hat{h}(\xi)\right|^2 \right) \\
&= \|\hat{f}\|_\infty^2 \left(\frac{1}{N} \sum_{n \in \mathbb{Z}_N} |g(n)|^2 \right) \left(\frac{1}{N} \sum_{n \in \mathbb{Z}_N} |h(n)|^2 \right) \\
&\le \|\hat{f}\|_\infty^2 \|g\|_\infty^2 \|h\|_\infty^2 \le \|\hat{f}\|_\infty^2
\end{aligned}$$

as desired.

E2. By a *randomly generated* subset of $\mathbb{Z}_N$ we mean a set A where each $n \in \mathbb{Z}_N$ has a 50% probability of being an element in A. Imagine flipping a coin N times and including the number n in A if the nth coin flip is "heads" and excluding the number n from A if the nth coin flip is "tails". The next problem says that, almost surely, a randomly generated set is pseudorandom.

Let $\epsilon > 0$. Prove that the probability that a randomly generated subset of $\mathbb{Z}_N$ is ϵ-pseudorandom converges to 1 as $N \to \infty$.
Hint: Use Hoeffding's inequality: For independent random variables $X_1, \ldots, X_k$ with $|X_i| \le 1$,

$$\mathbb{P}\left[|S_k - \mathbb{E}\left[S_k\right]| \ge t\right] \le 2\exp\left(-\frac{t^2}{2k}\right),$$

where $S_k = \sum_{i=1}^k X_i$.

Solution: We want to prove

$$\mathbb{P}\left[\sup_{\xi \in \mathbb{Z}_N \setminus \{0\}} \left|\hat{A}(\xi)\right| > \epsilon\right] \to 0$$

as $N \to \infty$.
Fix $\xi \in \mathbb{Z}_N \setminus \{0\}$. From the definition of the Fourier transform, we have that

$$\hat{A}(\xi) = \frac{1}{N} \sum_{n \in \mathbb{Z}_N} \mathbb{1}_A(n) e\left(-\frac{\xi n}{N}\right).$$

Let X_n be the random variable $X_n = \mathbb{1}_A(n) e\left(-\frac{\xi n}{N}\right)$ so that $N\hat{A}(\xi) = S_N = \sum_{n=1}^N X_n$. The

variables $X_1, \ldots, X_N$ are independent and satisfy $|X_n| \leq 1$. Moreover,

$$\mathbb{E}\left[S_N\right] = \sum_{n=1}^{N} \mathbb{E}\left[\mathbb{1}_A(n)\right] e\left(-\frac{\xi n}{N}\right) = \frac{1}{2}\sum_{n=1}^{N} e\left(-\frac{\xi n}{N}\right) = 0,$$

since $\xi \neq 0$. Therefore, by Hoeffding's inequality,

$$\mathbb{P}\left[\left|\hat{A}(\xi)\right| > \epsilon\right] = \mathbb{P}\left[|S_N - \mathbb{E}\left[S_N\right]| > N\epsilon\right] \leq 2\exp\left(-\frac{\epsilon^2 N}{2}\right).$$

Now, $\sup_{\xi\in\mathbb{Z}_N\setminus\{0\}} \left|\hat{A}(\xi)\right| > \epsilon$ if and only if there exists $\xi \in \mathbb{Z}_N \setminus \{0\}$ with $\left|\hat{A}(\xi)\right| > \epsilon$. Hence,

$$\begin{aligned}
\mathbb{P}\left[\sup_{\xi\in\mathbb{Z}_N\setminus\{0\}} \left|\hat{A}(\xi)\right| > \epsilon\right] &= \mathbb{P}\left[\exists\ \xi \in \mathbb{Z}_N \setminus \{0\},\ \left|\hat{A}(\xi)\right| > \epsilon\right] \\
&\leq \sum_{\xi\in\mathbb{Z}_N\setminus\{0\}} \mathbb{P}\left[\left|\hat{A}(\xi)\right| > \epsilon\right] \\
&\leq 2(N-1)\exp\left(-\frac{\epsilon^2 N}{2}\right).
\end{aligned}$$

This goes to 0 when N goes to infinity, so we are done.

E3. Prove *Dirichlet's approximation theorem*: for any $\alpha \in \mathbb{R}$ and any $Q \in \mathbb{N}$, there exist $p, q \in \mathbb{Z}$ with $1 \leq q \leq Q$ such that

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ}.$$

Solution: For $k \in \{0, 1, \ldots, Q\}$, decompose $k\alpha$ into its integer and fractional parts, i.e.

$$k\alpha = \lfloor k\alpha \rfloor + \{k\alpha\},$$

with $\{k\alpha\} \in [0, 1)$. Divide the interval $[0, 1)$ into Q sub-intervals of length $\frac{1}{Q}$ each:

$$[0, 1) = \left[0, \frac{1}{Q}\right) \cup \left[\frac{1}{Q}, \frac{2}{Q}\right) \cup \cdots \cup \left[\frac{Q-1}{Q}, 1\right).$$

Since we have $Q + 1$ fractional parts, by the pigeonhole principle, two of them belong to the same sub-interval, i.e. there there exist $k, k' \in \{0, 1, \ldots, Q\}$ such that $k < k'$ and

$$|\{k'\alpha\} - \{k\alpha\}| < \frac{1}{Q}.$$

Set $p := \lfloor k'\alpha \rfloor - \lfloor k\alpha \rfloor$ and $q := k' - k$. Then we have

$$\begin{aligned} |q\alpha - p| &= |k'\alpha - k\alpha - (\lfloor k'\alpha \rfloor - \lfloor k\alpha \rfloor)| \\ &= |\{k'\alpha\} - \{k\alpha\}| \\ &< \frac{1}{Q}. \end{aligned}$$

Dividing by q yields the result.