18.156, Projection theory, problem set 5

This problem set is about projections, convolution, and smoothing. These are core ideas in the course, and they come up in particular in the Renyi-Bombieri-Vinogradov theorem.

Projections tend to make things smoother, and we have been exploring exactly how much. Convolution tends to make things smoother, although not always. And projections and convolutions can cooperate with each other. We will explore that on this problem set.

1a. (Projections can make things smoother) Convolutions are related to counting the number of solutions of equations such as $m_1^2 + ... + m_r^2 = n \bmod p$. Let $S(n)$ be the number of solutions to $m^2 = n \bmod p$. (So $S(n)$ is 2 if n is a quadratic residue, 1 if $n = 0$, and 0 if n is a non-residue.) We write S^{*r} for S convolved with itself r times. On your own check that

$$S^{*r}(n) = \#\{m_1, ..., m_r \in \mathbb{Z}_p : m_1^2 + ... + m_r^2 = n\}.$$

We will study this using the Fourier transform in $\mathbb{Z}_p$. Recall that if $f : \mathbb{Z}_p \to \mathbb{C}$ we have the conventions

$$\hat{f}(\alpha) = \sum_{a \in \mathbb{Z}_p} f(a) e^{-2\pi i \frac{a\alpha}{p}}.$$

$$f(a) = \frac{1}{p} \sum_{\alpha \in \mathbb{Z}_p} \hat{f}(\alpha) e^{2\pi i \frac{a\alpha}{p}}.$$

It is known that $\hat{S}(0) = p$ and $|\hat{S}(\alpha)| \leq \sqrt{p}$ for $\alpha \neq 0$. Using this, prove that

$$\|(S^{*r})_h\|_{L^\infty(\mathbb{Z}_p)} \leq p^{r/2}.$$

Also check that $(S^{*r})_0 = p^{r-1}$.

So for $r \geq 3$, the function S^{*r} is almost constant. In this situation, repeated convolution makes S smoother and smoother.

1b. (Convolutions don't always make things smoother). Suppose that m divides n and let $G \subset \mathbb{Z}_n$ be the multiples of m. Check that

$$1_G^{*r}(n) = |G|^{r-1} 1_G(n).$$

So in this case, repeated convolution does not make 1_G any smoother.

This is related to the fact that $\widehat{1_G}$ behaves quite differently from $\hat{S}$. Let $G' \subset \mathbb{Z}_n$ be the multiples of n/m. Check that

$$\widehat{1_G}(\alpha) = |G| 1_{G'}(\alpha)$$

2. (Projections and convolutions together)

Suppose that $X \subset [N]$. Consider $\pi_p 1_X : \mathbb{Z}_p \to \mathbb{C}$. For a single prime p, it may not happen that convolving this function with itself many times makes it smoother. But if X is big enough, then for most primes p, convolving $\pi_p 1_X$ with itself many times does make it smoother.

Let $P_{N^{1/2}}$ be the set of primes $p \sim N^{1/2}$. You can use that $|P_{N^{1/2}}| \approx N^{1/2}$.

On your own, check that if $p \in P_{N^{1/2}}$, then

$$(\pi_p 1_X)_0^{*r} = |X|^r/p \sim |X|^r N^{-1/2}. \tag{1}$$

a. Recall that for a prime p, $\mathbb{Z}_p^* = \{a \in \mathbb{Z}_p, a \neq 0\}$. Using the idea of the proof of the large sieve, show that

$$\sum_{p \in P_{N^{1/2}}} \|\widehat{\pi_p 1_X}\|^2_{L^\infty(\mathbb{Z}_p^*)} \lesssim N|X|.$$

Conclude that for 90 % of $p \in P_{N^{1/2}}$, we have

$$\|\widehat{\pi_p 1_X}\|_{L^\infty(\mathbb{Z}_p^*)} \lessapprox N^{1/4}|X|^{1/2}.$$

(You can use that $|P_{N^{1/2}}| \approx N^{1/2}$.)

b. Now using the idea from problem 1, show that for 90 % of $p \in P_{N^{1/2}}$,

$$\|(\pi_p 1_X)_h^{*r}\|_{L^\infty(\mathbb{Z}_p)} \lessapprox N^{r/4}|X|^{r/2}. \tag{2}$$

Using this, check that if $|X| = N^\alpha$ with $\alpha > 1/2$, then most $p \in P_{N^{1/2}}$, $\pi_p 1_X^{*r}$ becomes smooth when r is large enough.

c. On the other hand, if $|X| = N^\alpha$ with $\alpha < 1/2$, then there is no smoothing effect. Suppose $\alpha < 1/2$. If X is an arithmetic progression of length N^α, then show that for each $p \in P_{N^{1/2}}$, the support of $(\pi_p 1_X)^{*r}$ has size $\lesssim rN^\alpha$, which is much smaller than p.

d. The bound (**??**) can actually be improved a little, especially if r is small like $r = 2$. This is good practice for a common Fourier analysis tactic: noticing when L^2 norms appear and estimating them with Plancherel. First recall that the large sieve inequality tells us that

$$\sum_{p \in P_{N^{1/2}}} \|(\pi_p 1_X)_h\|^2_{L^2(\mathbb{Z}_p)} \lesssim N^{1/2}|X| \tag{3}$$

By Plancherel, this is equivalent to the following estimate (which was part of the proof of the large sieve):

$$\sum_{p \in P_{N^{1/2}}} \frac{1}{p} \sum_{\alpha \in \mathbb{Z}_p^*} \widehat{\pi_p 1_X}(\alpha)^2 \lesssim N^{1/2}|X|, \tag{4}$$

If you look back at the proof you did in Part b, a quantity similar to the left-hand side of (**??**) appears, and so you can take advantage of this bound. In this way, you can improve (**??**) to the following. For 90 % of $p \in P_{N^{1/2}}$,

$$\|(\pi_p 1_X)_h^{*r}\|_{L^\infty(\mathbb{Z}_p)} \lessapprox N^{\frac{r-2}{4}}|X|^{r/2}. \tag{5}$$

Optional exploration. In the example in 2c, X is an arithmetic progression and so 1_X^{*r} is itself very concentrated. This causes $\pi_p 1_X^{*r}$ to be concentrated. But what if 1_X^{*r} is not concentrated? Can we get a better estimate for $\pi_p 1_X^{*r}$?

For a precise question, suppose that $X \subset [N]$ with $|X| \sim N^{1/2}$, and suppose that $\|1_X^{*2}\|_{L^\infty} \lessapprox 1$. For most $p \in P_{N^{1/2}}$, can we prove a bound for $\|(\pi_p 1_X)_h^{*2}\|_{L^\infty(\mathbb{Z}_p)}$ which improves on (**??**)?

I don't know the answer to this question. I'm curious about it and I'm not sure how difficult it is.

This optional question is somewhat analogous to improving the Bombieri-Vinogradov theorem to the range $q > N^{1/2}$. In the setting of the Bombieri-Vinogradov theorem, we would want a similar estimate with multiplicative convolution instead of additive convolution. In that setup, we would have $X \subset [N^{1/2}]$ with $|X| \approx N^{1/2}$ and we would study $1_X *_M 1_X$. Because a number $n \leq N$ has $\lessapprox 1$ factors, we automatically get $\|1_X *_M 1_X\|_{L^\infty} \lessapprox 1$. Using the large sieve as in Bombieri-Vinogradov, we get the following bound, which matches (**??**) when $r = 2$: for most $p \in P_{N^{1/2}}$,

$$\|(\pi_p(1_X *_M 1_X))_h\|_{L^\infty(\mathbb{Z}_p^*)} \lessapprox |X|. \tag{6}$$

I believe that it is a difficult open question whether this bound can be improved.

18.156 Projection Theory

Spring 2025