Probabilistic aspects of character sums
Lecture 1: Classics

Adam J Harper
University of Warwick

SSANT Paris, June 2021

Plan of the talk:

- Introduction to character sums
- Motivation
- Pólya–Vinogradov inequality
- Preview of future lectures

Introduction

Throughout these lectures: Let r be a large prime, and χ a Dirichlet character mod r.

In other words:

- $\chi : \mathbb{N} \to \mathbb{C}$;
- $\chi(n) = 0$ if and only if $r|n$;
- χ is *periodic* mod r, i.e. $\chi(n + r) = \chi(n)$ for all n;
- χ is *totally multiplicative*, i.e. $\chi(nm) = \chi(n)\chi(m)$ for all n, m.

There are $\phi(r) = r - 1$ such functions χ, including the principal character $\chi_0(n) = \mathbf{1}_{(n,r)=1}$ and the Legendre symbol $\left(\frac{n}{r}\right)$.

We always have $\chi(1) = 1$, and $|\chi(n)| \in \{0, 1\}$.

Dirichlet characters have two important orthogonality properties:

- $\frac{1}{r-1} \sum_{n=1}^{r} \chi(n) = \mathbf{1}_{\chi=\chi_0}$.
  (This is fairly easy to prove, by multiplying LHS by $\chi(n)$ for some n with $\chi(n) \neq 0, 1$.)
- $\frac{1}{r-1} \sum_{\chi \bmod r} \chi(n) = \mathbf{1}_{n \equiv 1 \bmod r}$.
  (This is a bit harder to prove, I don't know an argument that doesn't involve the explicit construction of the characters χ.)

Thanks to the second orthogonality property, we can use Dirichlet characters to detect behaviour in arithmetic progressions.

For example, if (a_n) is some complex sequence then

$$\begin{aligned}\sum_{\substack{n\le x,\\ n\equiv 1 \bmod r}} a_n &= \sum_{n\le x} a_n \frac{1}{r-1}\sum_{\chi \bmod r}\chi(n)\\ &= \frac{1}{r-1}\sum_{\chi \bmod r}\sum_{n\le x} a_n\chi(n)\\ &= \frac{1}{r-1}\sum_{n\le x} a_n\chi_0(n) + \frac{1}{r-1}\sum_{\substack{\chi \bmod r,\\ \chi\ne\chi_0}}\sum_{n\le x} a_n\chi(n).\end{aligned}$$

Some motivation

We might want to understand the distribution of primes in arithmetic progressions.

Thanks to the identity $\Lambda(n) = -\sum_{d|n} \mu(d) \log d$ (or more sophisticated versions like Vaughan's Identity), this is more or less equivalent to investigating the *Möbius function* $\mu(n)$ in arithmetic progressions.

Recall:

$$\mu(n) := \begin{cases} 0 & \text{if } n \text{ has any repeated prime factors,} \\ (-1)^{\omega(n)} & \text{if } n \text{ has } \omega(n) \text{ prime factors, all distinct.} \end{cases}$$

For example, $\mu(1) = \mu(6) = 1$, and $\mu(2) = \mu(3) = \mu(5) = -1$, and $\mu(4) = 0$.

We have

$$\sum_{\substack{n\le x,\\ n\equiv 1 \bmod r}} \mu(n) = \frac{1}{r-1}\sum_{n\le x}\mu(n)\chi_0(n) + \frac{1}{r-1}\sum_{\substack{\chi \bmod r,\\ \chi\neq\chi_0}}\sum_{n\le x}\mu(n)\chi(n).$$

The Prime Number Theorem implies that

$$\sum_{n\le x}\mu(n)\chi_0(n) = \sum_{n\le x}\mu(n) - \sum_{\substack{n\le x,\\ r|n}}\mu(n) = o(x).$$

We expect that $\sum_{n\le x}\mu(n)\chi(n) = o(x)$ for all non-principal χ as well (provided x isn't tiny compared with r).
"Can a Dirichlet character $\chi(n)$ pretend to be $\mu(n)$?"
For real Dirichlet characters: closely connected to the *Siegel zeros* problem.

Before grappling with $\mu(n)$, we might just try to understand the behaviour of $\sum_{n \leq x} \chi(n)$. By periodicity mod r, we only need to investigate $1 \leq x \leq r$.

For the principal character $\chi_0(n) = \mathbf{1}_{(n,r)=1}$, this is an easy problem.

For $\chi \neq \chi_0$, we always have the trivial bound

$$|\sum_{n \leq x} \chi(n)| \leq \sum_{n \leq x} |\chi(n)| \leq x,$$

but we generally expect this to be *far from the truth*.

Define

$$n(r) := \min\{1 \leq n \leq r : n \text{ is a quadratic non-residue mod } r\},$$

the *least quadratic non-residue* mod r.

Conjecture 1 (Vinogradov)

For any fixed $\epsilon > 0$, we have $n(r) \ll_\epsilon r^\epsilon$.

We expect (but cannot prove) that much more should be true: $\sum_{n \leq r^\epsilon} \chi(n) = o(r^\epsilon)$ uniformly for all non-principal characters χ mod r (including $\chi(n) = \left(\frac{n}{r}\right)$).

Pólya–Vinogradov inequality

Theorem 1 (Pólya–Vinogradov inequality, 1918)

Uniformly for all large primes r, all $\chi \neq \chi_0$ mod r, and all x, we have

$$|\sum_{n \leq x} \chi(n)| \ll \sqrt{r} \log r.$$

This is a fundamental result, as is the method of proof.

The Pólya–Vinogradov inequality immediately implies that if $\frac{x}{\sqrt{r}\log r} \to \infty$, then $\sum_{n \leq x} \chi(n) = o(x)$.

Our key tool in proving the Pólya–Vinogradov inequality, and an important tool in lectures 2 and 3, will be the *Pólya Fourier expansion (PFE)*: for any parameter K, we have

$$\sum_{n \le x} \chi(n) = \frac{\tau(\chi)}{2\pi i} \sum_{0<|k| \le K} \frac{\overline{\chi}(-k)}{k} (e(kx/r) - 1) + O(1 + \frac{r \log r}{K}),$$

where $e(t) := e^{2\pi i t}$ is the complex exponential, and $\tau(\chi) := \sum_{a=1}^{r} \chi(a) e(a/r)$ is the *Gauss sum* corresponding to χ.

We will sketch the proof of the PFE (assuming a bit of standard Fourier analysis), and then deduce Theorem 1.

For a fixed non-principal character χ mod r, we (temporarily) define

$$S(t) = S_\chi(t) := \sum_{1 \le n \le tr} \chi(n), \quad 0 \le t \le 1.$$

We have $S(0) = 0$ (trivially, empty sum), and $S(1) = \sum_{1 \le n \le r} \chi(n) = 0$ using one of the orthogonality properties.

Next we compute the Fourier coefficients of the function $S(t)$ (thought of as a 1-periodic function on $\mathbb{R}$):

$$\hat{S}(k) := \int_0^1 S(t) e(-kt) dt = \sum_{1 \le n \le r} \chi(n) \int_{n/r}^1 e(-kt) dt, \quad k \in \mathbb{Z}.$$

When $k = 0$, we obviously have $\hat{S}(0) = \sum_{1 \le n \le r} \chi(n)(1 - \frac{n}{r})$.
Using the fact that $\sum_{1 \le n \le r} \chi(n) = 0$, we can simplify this:
$\hat{S}(0) = -\frac{1}{r} \sum_{1 \le n \le r} \chi(n) n$.

When $k \neq 0$, we get

$$\hat{S}(k) = \sum_{1 \le n \le r} \chi(n) \left[\frac{e(-kt)}{-2\pi i k} \right]_{n/r}^{1} = \sum_{1 \le n \le r} \chi(n) \frac{e(-kn/r) - 1}{2\pi i k}.$$

Again, we can simplify this:

$$\hat{S}(k) = \frac{1}{2\pi i k} \sum_{1 \le n \le r} \chi(n) e(-kn/r).$$

Now we shall exploit the special structure of Dirichlet characters/residues mod r.

If k is coprime to r, then

$$\begin{aligned}\overline{\chi}(-k)\tau(\chi) = \overline{\chi}(-k)\sum_{a=1}^{r}\chi(a)e(a/r) &= \sum_{a=1}^{r}\chi(-a/k)e(a/r) \\ &= \sum_{a=1}^{r}\chi(a)e(-ak/r),\end{aligned}$$

because replacing a by $-ak$ just permutes the residue classes mod r. **So we get**

$$\hat{S}(k) = \tau(\chi)\frac{\overline{\chi}(-k)}{2\pi ik}.$$

This is still true when $r|k$, because then both sides equal zero.

Finally, (a quantitative form of) Fourier inversion gives

$$S(t) = \frac{S(t+) + S(t-)}{2} + O(1) = \sum_{|k| \le K} \hat{S}(k) e(kt) + O(1 + \frac{r \log r}{K})$$

$$= \quad -\frac{1}{r} \sum_{1 \le n \le r} \chi(n) n + \frac{\tau(\chi)}{2\pi i} \sum_{0 < |k| \le K} \frac{\overline{\chi}(-k)}{k} e(kt) + O(1 + \frac{r \log r}{K}).$$

(The r in the error term is a bound on the variation of $S(t)$.)

Since $S(0) = 0$, we can get rid of the first sum by subtracting $S(0)$ from both sides:

$$S(t) = \frac{\tau(\chi)}{2\pi i} \sum_{0 < |k| \le K} \frac{\overline{\chi}(-k)}{k} (e(kt) - 1) + O(1 + \frac{r \log r}{K}).$$

Setting $t = x/r$ yields the PFE. $\square$

Lemma 1

For all primes r and all $\chi \neq \chi_0$ mod r, we have $|\tau(\chi)| = \sqrt{r}$.

Proof of Lemma 1.

The key point, as we already saw, is that

$$\overline{\chi}(n)\tau(\chi) = \overline{\chi}(n)\sum_{a=1}^{r}\chi(a)e(a/r) = \sum_{a=1}^{r}\chi(a)e(an/r)$$

for all n (LHS=RHS=0 if $r|n$). And $|\overline{\chi}(n)| = 1$ for n coprime to r, so

$$(r-1)|\tau(\chi)|^2 = \sum_{n=1}^{r}|\sum_{a=1}^{r}\chi(a)e(an/r)|^2 = \sum_{a,b=1}^{r}\chi(a)\overline{\chi}(b)r\mathbf{1}_{a=b}.$$

The RHS is equal to $r(r-1)$. □

Proof of the Pólya–Vinogradov inequality.

We can choose $K = r$, say, in the PFE. Then simply applying the triangle inequality,

$$
\begin{aligned}
\Big|\sum_{n\le x}\chi(n)\Big| &= \frac{\sqrt{r}}{2\pi}\Big|\sum_{0<|k|\le r}\frac{\overline{\chi}(-k)}{k}(e(kx/r)-1)\Big| + O(1+\log r) \\
&\le \frac{\sqrt{r}}{2\pi}\sum_{0<|k|\le r}\frac{2}{|k|} + O(\log r) \\
&\ll \sqrt{r}\log r.
\end{aligned}
$$

$\square$

Further developments

- *Burgess bound (1957, 1962)*: for $\chi \neq \chi_0$ we have $|\sum_{n \leq x} \chi(n)| = o(x)$ provided $x \geq r^{1/4+o(1)}$.
- This directly implies that the least quadratic non-residue $n(r) \leq r^{1/4+o(1)}$.
- With some combinatorial trickery, one can in fact deduce the stronger (best known) result that $n(r) \leq r^{1/(4\sqrt{e})+o(1)}$.
- Better character sum estimates are possible for special non-prime moduli r (e.g. smooth/friable r).
- Assuming the Generalised Riemann Hypothesis is true, Granville and Soundararajan (2001) showed that $|\sum_{n \leq x} \chi(n)| = o(x)$ provided $\frac{\log x}{\log \log r} \to \infty$. (cf. Lecture 3)

Key points to take away:

- *The PFE encodes the periodicity of $\chi(n)$ mod r. We need to use it to understand the behaviour of $\chi(n)$ properly.*
- We have $(e(kx/r)-1) \approx \frac{2\pi ikx}{r}$ when $|k| \le r/x$. So the PFE implies that

$$\begin{aligned}\sum_{n\le x}\chi(n) &\approx \frac{\tau(\chi)}{2\pi i}\sum_{0<|k|\le r/x}\frac{\overline{\chi}(-k)}{k}\frac{2\pi ikx}{r} + O(\log r) + \\ &\quad + \frac{\tau(\chi)}{2\pi i}\sum_{r/x<|k|\le r}\frac{\overline{\chi}(-k)}{k}(e(kx/r)-1) \\ &\approx \frac{\tau(\chi)x}{r}\sum_{0<|k|\le r/x}\overline{\chi}(-k).\end{aligned}$$

- In particular, $|\sum_{n\le x}\chi(n)| \approx \frac{x}{\sqrt{r}}|\sum_{k\le r/x}\chi(k)|$.

- So there is a "symmetry" between character sums up to x and up to r/x:
$$|\sum_{n\le x}\chi(n)| \approx \frac{x}{\sqrt{r}}|\sum_{k\le r/x}\chi(k)|,$$
at least for most χ and/or most x.
- In particular, $|\sum_{n\le x}\chi(n)|\approx\sqrt{x}$ is roughly equivalent to $|\sum_{n\le r/x}\chi(n)|\approx\sqrt{r/x}$.
- This symmetry is sometimes called the "Fourier flip", or a "reflection principle". It is also closely related to the functional equation of Dirichlet L-functions.

Preview of Lectures 2–4

Main Theme: We will combine the PFE with a *random multiplicative function* model to understand various aspects of character sums.

- Lecture 2: distribution of $\max_{1\le x\le r} |\sum_{n\le x} \chi(n)|$ as χ varies.
- Lecture 3: distribution of character sums over moving intervals.
- Lecture 4: distribution of $\sum_{n\le x} \chi(n)$ as χ varies.