Exponential sums and equidistribution

Matthew Hase-Liu

1 01/30 (Matthew): Overview and intro to equidistribution

What is equidistribution? Let's start with a famous example.

Question 1. *Start with a real number $\gamma \neq 0$ and look at the sequence of fractional parts $\langle \gamma \rangle, \langle 2\gamma \rangle, \langle 3\gamma \rangle, \ldots$. How are these distributed in the interval $[0,1]$?*

(i) If γ is rational, there are only finitely many distinct numbers.

(ii) If γ is irrational, there are infinitely many. Why? In fact, $\langle n\gamma \rangle$ is dense in $[0,1)$! We'll see why in a second by proving something even stronger.

We say a sequence of numbers $\xi_1, \xi_2, \ldots \in [0,1)$ is *equidistributed* if for every interval $(a,b) \subset [0,1)$, we have

$$\lim_{N\to\infty} \frac{\#\{1 \le n \le N : \xi_n \in (a,b)\}}{N} = b - a,$$

i.e. the entire interval is sweeped out by the sequence $\langle n\gamma \rangle$ in such a way that each sub-interval gets its fair share.

Example 2. Let $\{r_n\}_{n=1}^{\infty}$ be an enumeration of the rationals in $[0,1)$. Then the sequence $\xi_n = r_{n/2}$ for n even and 0 for n odd cannot be equidistributed (but it is dense!).

Theorem 3. If γ is irrational, then the sequence $\xi_n = \langle n\gamma \rangle$ is equidistributed in $[0,1)$.

One way to think about this is that if $\chi_{(a,b)}(x)$ is the characteristic function of the interval (a,b) on $[0,1)$, we can extend to $\mathbb{R}$ by periodicity. Then,

$$\#\{1 \le n \le N : \xi_n \in (a,b)\} = \sum_{n=1}^{N} \chi_{(a,b)}(n\gamma),$$

so the theorem can be restated as

$$\frac{1}{N}\sum_{n=1}^{N} \chi_{(a,b)}(n\gamma) \to \int_0^1 \chi_{(a,b)}(x)dx, \text{ as } N \to \infty.$$

The key fact is the following lemma:

Lemma 4. If f is continuous and periodic of period 1, and γ is irrational, then

$$\frac{1}{N}\sum_{n=1}^{N} f(n\gamma) \to \int_0^1 f(x)dx, \text{ as } N \to \infty.$$

We won't prove this, but the key point is to first check this for when f is an exponential $e^{2\pi ikx}$. By properties of Fourier series, this actually suffices. To finish the proof of the theorem, the idea is to sandwich (from above and below) $\chi_{(a,b)}$ by two continuous periodic functions of period 1, and then apply the lemma.

This motivates the more general definition of equidistribution:

Definition 5. Let X be a locally compact metric space and μ a probability measure on X so that $\mu(X) = 1$. If (X_n) is a sequence of finite sets with a map $\theta_n\colon X_n \to X$ (could be inclusions for example), then the sets (X_n) *become equidistributed with respect to* μ if for all continuous and bounded functions $f\colon X \to \mathbb{C}$, we have

$$\frac{1}{|X_n|}\sum_{x\in X_n} f(\theta_n(x)) \to \int_X f(x)d\mu(x).$$

Let's discuss another example of equidistribution that is more closely related to what the seminar is about.

Question 6. *Let p be an odd prime and χ be a non-trivial Dirichlet character mod p (i.e. $\chi\colon \mathbb{F}_p^\times \to \mathbb{C}$). Then, define the "Gauss sum"*

$$\tau(\chi) = \sum_{x\in\mathbb{F}_p^\times} \chi(x)e\left(\frac{x}{p}\right),$$

where $e(z) = e^{2\pi iz}$.

By squaring and using orthogonality of characters, one can show that $|\tau(\chi)| = \sqrt{p}$, i.e.

$$\tau(\chi) = \sqrt{p}e(\theta_p(\chi)),$$

for some unique angle $\theta_p(\chi)$ in $[0,1)$.

As $p \to \infty$, what can we say about the finite sets $\{\theta_p(\chi)\colon \chi \text{ non-trivial mod } p\}$?

It turns out that they're equidistributed with respect to the Lebesgue measure dx!

To see this, by the same kind of argument that we explained for the first example, it suffices to test this claim against the exponentials $e(jx) =: \varphi_j(x)$ for $j \in \mathbb{Z}\setminus\{0\}$, i.e. to verify that

$$\frac{1}{p-2}\sum_{\chi \bmod p, \chi\neq 1} \varphi_j(\theta_p(\chi)) \to 0.$$

Assume $j \geq 1$ by symmetry and write the LHS as

$$\begin{aligned}\frac{1}{p-2}\sum_{\chi \bmod p,\chi\neq 1}\left(\frac{\tau(\chi)}{\sqrt{p}}\right)^j &= \frac{1}{p-2}\frac{1}{p^{j/2}}\sum_{x_1,\dots,x_j} e\left(\frac{x_1+\cdots+x_j}{p}\right)\sum_{\chi\neq 1}\chi(x_1\cdots x_j)\\ &= \frac{p-1}{p-2}\frac{1}{p^{j/2}}\sum_{x_1,\dots,x_j,x_1\cdots x_j=1} e\left(\frac{x_1+\cdots+x_j}{p}\right).\end{aligned}$$

It turns out that the "Hyper-Kloosterman sum" satisfies

$$\sum_{x_1,\dots,x_j,x_1\cdots x_j=1} e\left(\frac{x_1+\cdots+x_j}{p}\right) \leq jp^{\frac{j-1}{2}},$$

so putting everything together gives

$$\frac{1}{p-2}\sum_{\chi \bmod p, \chi\neq 1}\varphi_j(\theta_p(\chi)) \leq \frac{p-1}{p-2}\frac{jp^{\frac{j-1}{2}}}{p^{j/2}} = \frac{p-1}{p-2}\cdot j\cdot p^{-1/2}\to 0$$

as $p\to\infty$.

Where did this Hyper-Kloosterman sum bound come from? Let's come back to this in a moment.

More generally, let's discuss "character sums" of the form

$$\sum_{x\in V(\mathbb{F}_q)}\Lambda_{f,g}(x),$$

where V is an algebraic variety and $\Lambda_{f,g}(x) = \chi(g(x))e(f(x)/p)$ with f, g polynomial functions on V. These cover our previous examples:

- Gauss sums are the case $V = \mathbb{G}_m$ and $(f, g) = (ax, x)$.
- Hyper-Kloosterman sums are the case $V = \mathbb{G}_m^{j-1}$ and $(f, g) = (x_1 + \cdots + x_{j-1} + a/x_1 \cdots x_{j-1}, 1)$.

Now, there is a certain compact topological group $\pi_1(V)$ called the etale fundamental group generalizing the notion of a Galois group, which contains Frobenius conjugacy classes Fr_x for $x\in V(\mathbb{F}_q)$. In many cases that we care about, $\pi_1(V)$ is literally a Galois group, and you can take the usual definition of Frobenius element. The key point is that there exists a continuous character

$$\chi_{f,g}\colon \pi_1(V)\to\mathbb{C}^\times$$

with the property that

$$\chi_{f,g}(\mathrm{Fr}_x) = \chi(g(x))\psi(f(x)).$$

Observe the unremarkable fact that $\chi_{f,g}(\mathrm{Fr}_x) = \mathrm{Tr}(\chi_{f,g}(\mathrm{Fr}_x))$, which is how we will generalize this setup to higher-dimensional representations. Indeed, there are many interesting equidistribution questions that require working beyond the case $\Lambda_{f,g}(x) = \chi(g(x))e(f(x)/p)$.

In general, we define the notion of a lisse sheaf:

Definition 7. A *lisse sheaf of rank* $r\geq 1$ *and weight* $m\in\mathbb{Z}$ on $V/\mathbb{F}_q$ is a continuous homomorphism

$$\rho\colon \pi_1(V)\to \mathrm{GL}_r(\mathbb{C})$$

such that the eigenvalues of $\rho(\mathrm{Fr}_x)$ all have absolute value $q^{m/2}$.

Grothendieck realized that a general exponential sum of the form

$$\sum_{x\in V(\mathbb{F}_q)}\Lambda(x)$$

with $\Lambda(x) = \mathrm{Tr}(\rho(\mathrm{Fr}_x))$ for some lisse sheaf ρ can be rewritten as follows:

$$\sum_{x\in V(\mathbb{F}_q)}\Lambda(x) = \sum_i(-1)^i\,\mathrm{Tr}\left(\mathrm{Fr}_q, H^i_c\left(V\otimes_{\mathbb{F}_q}\overline{\mathbb{F}_q}, \rho\right)\right)$$

(or more concisely $\mathrm{Tr}\left(\mathrm{Fr}_q, R\Gamma_c\left(V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \rho\right)\right)$), where $H_c^i\left(V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \rho\right)$ is the "*ith compactly supported cohomology group of ρ*". This is called the Grothendieck-Lefschetz trace formula.

The alternating sum on the RHS is finite:

Fact 8. *$H_c^i\left(V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \rho\right)$ is a finite-dimensional $\mathbb{C}$-vector space that vanishes unless $0 \le i \le 2 \dim V$.*

Deligne proved the following as part of the generalized Weil conjectures:

Theorem 9. If ρ is a lisse sheaf of weight m on $V/\mathbb{F}_q$, then the eigenvalues of Fr_q acting on $H_c^i\left(V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \rho\right)$ have absolute value at most $q^{(m+i)/2}$.

Let's return to our bound on Hyper-Kloosterman sums, namely

$$\sum_{x_1,\dots,x_j, x_1 \cdots x_j = 1} e\left(\frac{x_1 + \cdots + x_j}{p}\right) \le j p^{\frac{j-1}{2}}.$$

Recall $V = \mathbb{G}_m^{j-1}$. For the corresponding lisse sheaf ρ, Deligne showed that

- $H_c^i\left(V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \rho\right) = 0$ for $i \ne j - 1$ and
- $\dim H_c^{j-1}\left(V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \rho\right) = j$.

After rewriting the Hyper-Kloosterman sum in terms of co mpactly supported cohomology groups, the Weil conjectures (theorem above) then implies the bound, since only one term survives and each eigenvalue for this term has absolute value at most $p^{(j-1)/2}$.