Geometry and probability of exponential sums

E. Kowalski

ETH Zürich

November 6, 2014

What are exponential sums?

Consider finite sums

$$S = \sum_{n=1}^{N} \alpha_n$$

where $\alpha_n \in \mathbf{C}$ satisfies $|\alpha_n| \leq 1$.

What are exponential sums?

Consider finite sums

$$S = \sum_{n=1}^{N} \alpha_n$$

where $\alpha_n \in \mathbf{C}$ satisfies $|\alpha_n| \leq 1$.

Question: How large can $|S|$ be?

What are exponential sums?

Consider finite sums

$$S = \sum_{n=1}^{N} \alpha_n$$

where $\alpha_n \in \mathbf{C}$ satisfies $|\alpha_n| \leq 1$.

Question: How large can $|S|$ be?

In this generality, the only possible bound is

$$|S| \leq N.$$

What are exponential sums?

Consider finite sums

$$S = \sum_{n=1}^{N} \alpha_n$$

where $\alpha_n \in \mathbf{C}$ satisfies $|\alpha_n| \leq 1$.

Question: How large can $|S|$ be?

In this generality, the only possible bound is

$$|S| \leq N.$$

But in applications, this is not usually the case, and we can hope to prove

$$|S| \leq \frac{N}{\theta(N)}$$

where $\theta(N) > 1$ is "large".

First example

For $n \geq 1$, define

$$\lambda(n) = (-1)^{\Omega(n)}$$

where $\Omega(n)$ is the total number of prime divisors of n. (E.g., $\Omega(12) = 3$).

First example

For $n \geq 1$, define

$$\lambda(n) = (-1)^{\Omega(n)}$$

where $\Omega(n)$ is the total number of prime divisors of n. (E.g., $\Omega(12) = 3$). Then one knows that

$$\frac{1}{N}\Big|\sum_{1\leq n\leq N} \lambda(n)\Big| \longrightarrow 0$$

as $N \to +\infty$.

First example

For $n \geq 1$, define

$$\lambda(n) = (-1)^{\Omega(n)}$$

where $\Omega(n)$ is the total number of prime divisors of n. (E.g., $\Omega(12) = 3$). Then one knows that

$$\frac{1}{N}\Big|\sum_{1 \leq n \leq N} \lambda(n)\Big| \longrightarrow 0$$

as $N \to +\infty$. This is equivalent to the Prime Number Theorem.

First example

For $n \geq 1$, define

$$\lambda(n) = (-1)^{\Omega(n)}$$

where $\Omega(n)$ is the total number of prime divisors of n. (E.g., $\Omega(12) = 3$). Then one knows that

$$\frac{1}{N}\Big|\sum_{1 \leq n \leq N} \lambda(n)\Big| \longrightarrow 0$$

as $N \to +\infty$. This is equivalent to the Prime Number Theorem.
One *expects* that, for some constant $C \geq 0$ and all $N \geq 2$, we have

$$\Big|\sum_{1 \leq n \leq N} \lambda(n)\Big| \leq C\sqrt{N}(\log N)^2,$$

First example

For $n \geq 1$, define
$$\lambda(n) = (-1)^{\Omega(n)}$$
where $\Omega(n)$ is the total number of prime divisors of n. (E.g., $\Omega(12) = 3$). Then one knows that
$$\frac{1}{N}\Big|\sum_{1\leq n\leq N} \lambda(n)\Big| \longrightarrow 0$$
as $N \to +\infty$. This is equivalent to the Prime Number Theorem.
One *expects* that, for some constant $C \geq 0$ and all $N \geq 2$, we have
$$\Big|\sum_{1\leq n\leq N} \lambda(n)\Big| \leq C\sqrt{N}(\log N)^2,$$
but this is *equivalent* to the Riemann Hypothesis for the Riemann zeta function.

Digression: why is that so?

Using the Euler product

$$\sum_{n\geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

for $\mathrm{Re}(s) > 1$,

Digression: why is that so?

Using the Euler product

$$\sum_{n\geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

for $\mathrm{Re}(s) > 1$, one gets

$$\sum_{n\geq 1} \frac{\lambda(n)}{n^s} = \frac{\zeta(2s)}{\zeta(s)}.$$

Digression: why is that so?

Using the Euler product

$$\sum_{n\geq 1}\frac{1}{n^s}=\prod_{p\text{ prime}}\frac{1}{1-p^{-s}}$$

for $\mathrm{Re}(s)>1$, one gets

$$\sum_{n\geq 1}\frac{\lambda(n)}{n^s}=\frac{\zeta(2s)}{\zeta(s)}.$$

Then by summation by parts, note that

$$\frac{\zeta(2s)}{\zeta(s)}=s\int_1^{+\infty}\Big(\sum_{n\leq x}\lambda(n)\Big)x^{-s-1}dx,$$

Digression: why is that so?

Using the Euler product

$$\sum_{n\geq 1}\frac{1}{n^s}=\prod_{p\text{ prime}}\frac{1}{1-p^{-s}}$$

for $\mathrm{Re}(s)>1$, one gets

$$\sum_{n\geq 1}\frac{\lambda(n)}{n^s}=\frac{\zeta(2s)}{\zeta(s)}.$$

Then by summation by parts, note that

$$\frac{\zeta(2s)}{\zeta(s)}=s\int_1^{+\infty}\Big(\sum_{n\leq x}\lambda(n)\Big)x^{-s-1}dx,$$

and if

$$\Big|\sum_{1\leq n\leq N}\lambda(n)\Big|\leq C\sqrt{N}(\log N)^2,$$

for all $N\geq 2$,

Digression: why is that so?

Using the Euler product

$$\sum_{n\geq 1}\frac{1}{n^s}=\prod_{p \text{ prime}}\frac{1}{1-p^{-s}}$$

for $\mathrm{Re}(s)>1$, one gets

$$\sum_{n\geq 1}\frac{\lambda(n)}{n^s}=\frac{\zeta(2s)}{\zeta(s)}.$$

Then by summation by parts, note that

$$\frac{\zeta(2s)}{\zeta(s)}=s\int_1^{+\infty}\Bigl(\sum_{n\leq x}\lambda(n)\Bigr)x^{-s-1}dx,$$

and if

$$\Bigl|\sum_{1\leq n\leq N}\lambda(n)\Bigr|\leq C\sqrt{N}(\log N)^2,$$

for all $N\geq 2$, the right-hand side is holomorphic for $\mathrm{Re}(s)>1/2$.

Digression: why is that so?

Using the Euler product

$$\sum_{n\geq 1}\frac{1}{n^s}=\prod_{p \text{ prime}}\frac{1}{1-p^{-s}}$$

for $\mathrm{Re}(s)>1$, one gets

$$\sum_{n\geq 1}\frac{\lambda(n)}{n^s}=\frac{\zeta(2s)}{\zeta(s)}.$$

Then by summation by parts, note that

$$\frac{\zeta(2s)}{\zeta(s)}=s\int_1^{+\infty}\Big(\sum_{n\leq x}\lambda(n)\Big)x^{-s-1}dx,$$

and if

$$\Big|\sum_{1\leq n\leq N}\lambda(n)\Big|\leq C\sqrt{N}(\log N)^2,$$

for all $N\geq 2$, the right-hand side is holomorphic for $\mathrm{Re}(s)>1/2$. So $\zeta(s)\neq 0$ for $\mathrm{Re}(s)>1/2$.

Next examples

Let p be a prime number. For integers a, b, not divisible by p, define

$$K(a,b;p)=\sum_{1\le x\le p-1} e\Big(\frac{ax+b\bar{x}}{p}\Big),\quad B(a;p)=\sum_{0\le x\le p-1} e\Big(\frac{ax+x^3}{p}\Big),$$

where $e(z)=e^{2i\pi z}$, and $x\bar{x}\equiv 1 \pmod{p}$ if p does not divide x. (E.g., for $p=11$, $\bar{3}=4$).

Next examples

Let p be a prime number. For integers a, b, not divisible by p, define

$$K(a,b;p)=\sum_{1\le x\le p-1} e\Big(\frac{ax+b\bar{x}}{p}\Big),\quad B(a;p)=\sum_{0\le x\le p-1} e\Big(\frac{ax+x^3}{p}\Big),$$

where $e(z)=e^{2i\pi z}$, and $x\bar{x}\equiv 1 \pmod p$ if p does not divide x. (E.g., for $p=11$, $\bar{3}=4$).
These are called *Kloosterman sums* and *Birch sums* respectively. They are classical examples of exponential sums over finite fields.

Next examples

Let p be a prime number. For integers a, b, not divisible by p, define

$$K(a, b; p) = \sum_{1 \leq x \leq p-1} e\Big(\frac{ax + b\bar{x}}{p}\Big), \quad B(a; p) = \sum_{0 \leq x \leq p-1} e\Big(\frac{ax + x^3}{p}\Big),$$

where $e(z) = e^{2i\pi z}$, and $x\bar{x} \equiv 1 \pmod{p}$ if p does not divide x. (E.g., for $p = 11$, $\bar{3} = 4$).
These are called *Kloosterman sums* and *Birch sums* respectively. They are classical examples of exponential sums over finite fields.

Question: How large can $|K(a, b; p)|$ or $|B(a; p)|$ be, in terms of p?

Digression: why “geometry” and “probability”?

Geometry:

- Many properties of sums like $K(a, b; p)$ and $B(a; p)$ turn out to be best studied using methods from algebraic geometry;

Digression: why “geometry” and “probability”?

Geometry:

- Many properties of sums like $K(a, b; p)$ and $B(a; p)$ turn out to be best studied using methods from algebraic geometry;
- And they have applications to problems of arithmetic geometry (finding rational points on algebraic varieties),

Digression: why "geometry" and "probability"?

Geometry:

- Many properties of sums like $K(a, b; p)$ and $B(a; p)$ turn out to be best studied using methods from algebraic geometry;
- And they have applications to problems of arithmetic geometry (finding rational points on algebraic varieties), and hyperbolic geometry (spectral gap for the Laplace operator on arithmetic hyperbolic surfaces).

Digression: why "geometry" and "probability"?

Geometry:

- Many properties of sums like $K(a, b; p)$ and $B(a; p)$ turn out to be best studied using methods from algebraic geometry;
- And they have applications to problems of arithmetic geometry (finding rational points on algebraic varieties), and hyperbolic geometry (spectral gap for the Laplace operator on arithmetic hyperbolic surfaces).

Probability:

- Heuristic reasoning about these sums is often phrased in probabilistic terms;

Digression: why "geometry" and "probability"?

Geometry:

- Many properties of sums like $K(a, b; p)$ and $B(a; p)$ turn out to be best studied using methods from algebraic geometry;
- And they have applications to problems of arithmetic geometry (finding rational points on algebraic varieties), and hyperbolic geometry (spectral gap for the Laplace operator on arithmetic hyperbolic surfaces).

Probability:

- Heuristic reasoning about these sums is often phrased in probabilistic terms;
- And they satisfy probabilistic limit theorems that justify these heuristics.

History

Kloosterman sums were first written down by Poincaré around 1911 as coefficients in Fourier expansions of Poincaré series. They are discrete analogues of Bessel functions.

Nous allons maintenant grouper ensemble les termes qui correspondent aux diverses valeurs de δ non congrues entre elles suivant le module γ. Si nous appelons $\omega(\gamma)$ la somme de ces termes, le coefficient de q^j dans $\omega(\gamma)$ sera

$$\mu_j \mathrm{J}(m, \mathrm{G}) \sum \mathrm{E}.$$

Il faut donc calculer $\sum \mathrm{E}$, c'est-à-dire

$$\sum e^{\frac{2i\pi}{\gamma}(j\delta - p\alpha)}.$$

Les entiers j, p et γ sont donnés; mais on donne à α toutes les valeurs entières premières avec γ et incongrues entre elles par rapport au module γ, et à δ les valeurs correspondantes, de telle façon que

$$\alpha\delta \equiv 1 \pmod{\gamma}.$$

Je me bornerai à constater que $\sum \mathrm{E}$ n'est pas nul en général. Il reste à sommer

Kloosterman re-defined them in 1925 and used them to establish the solubility of equations

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = n$$

for fixed positive integers $(a_1, \ldots, a_4)$ and $x_i \in \mathbf{Z}$ and suitable $n \geq 1$.

2. 4. The sum $S(u, v; \lambda, \Lambda; q)$.

We shall show afterwards, that the approximation for large values of q of the sum occurring on the right hand side of the formula of lemma 3*, can be reduced to the calculation for large values of q of the sum

$$S(u, v; \lambda, \Lambda; q) = \sum_{p \equiv \lambda \pmod{\Lambda}}' \exp\left(\frac{2\pi i u p}{q} + \frac{2\pi i v p'}{q}\right).$$

But before performing the reduction, we shall first consider this sum S. The object of this section is the proof of lemma 4. The lemmas 4 b—4 e are special cases of lemma 4, from which the general lemma 4 will be deduced.

“Square-root cancellation” philosophy

The standard heuristic for guessing the size of a sum

$$S = \sum_{n \leq N} \alpha_n, \qquad |\alpha_n| \leq 1,$$

is that if the arguments of the complex numbers α_n vary “randomly”, then the sum should have size about $\sqrt{N}$.

“Square-root cancellation” philosophy

The standard heuristic for guessing the size of a sum

$$S = \sum_{n \le N} \alpha_n, \qquad |\alpha_n| \le 1,$$

is that if the arguments of the complex numbers α_n vary “randomly”, then the sum should have size about $\sqrt{N}$.

This is certainly true if “randomly” is interpreted in a rigorous probabilistic sense.

“Square-root cancellation” philosophy

The standard heuristic for guessing the size of a sum

$$S = \sum_{n \leq N} \alpha_n, \qquad |\alpha_n| \leq 1,$$

is that if the arguments of the complex numbers α_n vary “randomly”, then the sum should have size about $\sqrt{N}$.
This is certainly true if “randomly” is interpreted in a rigorous probabilistic sense. If $(\alpha_n)_{n \geq 1}$ are independent uniformly distributed on the unit circle, for instance, then the Central Limit Theorem implies that

$$\mathbf{P}\Big(\Big|\sum_{n \leq N} \alpha_n\Big| \geq t\sqrt{N}\Big) \longrightarrow e^{-t^2}$$

for $t \geq 0$ fixed.

“Square-root cancellation” philosophy

The standard heuristic for guessing the size of a sum

$$S = \sum_{n \leq N} \alpha_n, \qquad |\alpha_n| \leq 1,$$

is that if the arguments of the complex numbers α_n vary “randomly”, then the sum should have size about $\sqrt{N}$.

This is certainly true if “randomly” is interpreted in a rigorous probabilistic sense. If $(\alpha_n)_{n \geq 1}$ are independent uniformly distributed on the unit circle, for instance, then the Central Limit Theorem implies that

$$\mathbf{P}\Big(\Big|\sum_{n \leq N} \alpha_n\Big| \geq t\sqrt{N}\Big) \longrightarrow e^{-t^2}$$

for $t \geq 0$ fixed.

The problem is to show that this heuristic applies to deterministic sums, like Kloosterman sums, or to the Möbius function.

First bounds

The trivial bound $|K(a, b; p)| \leq p - 1$ was already improved by Kloosterman using an elementary method.

First bounds

The trivial bound $|K(a,b;p)| \leq p-1$ was already improved by Kloosterman using an elementary method. He proved that

$$\sum_{1 \leq a \leq p-1} |K(a,b;p)|^4 = 2p^3 - 3p^2 - p - 1$$

First bounds

The trivial bound $|K(a,b;p)| \leq p-1$ was already improved by Kloosterman using an elementary method. He proved that

$$\sum_{1 \leq a \leq p-1} |K(a,b;p)|^4 = 2p^3 - 3p^2 - p - 1$$

and deduced by dropping all but one term that

$$|K(a,b;p)| \leq 2p^{3/4},$$

and that *some* Kloosterman sum modulo p has modulus at least $\sqrt{p}$.

First bounds

The trivial bound $|K(a, b; p)| \leq p - 1$ was already improved by Kloosterman using an elementary method. He proved that

$$\sum_{1 \leq a \leq p-1} |K(a, b; p)|^4 = 2p^3 - 3p^2 - p - 1$$

and deduced by dropping all but one term that

$$|K(a, b; p)| \leq 2p^{3/4},$$

and that *some* Kloosterman sum modulo p has modulus at least $\sqrt{p}$.

H. Weyl introduced a general technique for exponential sums that leads to

$$|B(a; p)| \leq C_\varepsilon p^{7/8+\varepsilon}$$

for any $\varepsilon > 0$.

The Weil bounds

As an application of the *Riemann Hypothesis for curves over finite fields*, Weil proved in the 1940's quite general bounds for one-variable exponential sums that show that they behave according to the square-root cancellation philosophy.

The Weil bounds

As an application of the *Riemann Hypothesis for curves over finite fields*, Weil proved in the 1940's quite general bounds for one-variable exponential sums that show that they behave according to the square-root cancellation philosophy.

Particular cases:

- For all primes p and $1 \leq a, b \leq p-1$, we have

$$|K(a, b; p)| \leq 2\sqrt{p},$$

The Weil bounds

As an application of the *Riemann Hypothesis for curves over finite fields*, Weil proved in the 1940's quite general bounds for one-variable exponential sums that show that they behave according to the square-root cancellation philosophy.

Particular cases:

- For all primes p and $1 \leq a, b \leq p-1$, we have

$$|K(a, b; p)| \leq 2\sqrt{p},$$

- For all primes p and $0 \leq a \leq p-1$, we have

$$|B(a; p)| \leq 2\sqrt{p}.$$

The geometric idea is to relate the Kloosterman sums to the algebraic curve with equation

$$C_a \,:\, y^p - y = ax + \frac{b}{x}$$

where (x, y) belong to an algebraic closure of the finite field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

The geometric idea is to relate the Kloosterman sums to the algebraic curve with equation

$$C_a : y^p - y = ax + \frac{b}{x}$$

where (x, y) belong to an algebraic closure of the finite field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. The geometry of algebraic curves is key to the proof.

The geometric idea is to relate the Kloosterman sums to the algebraic curve with equation

$$C_a \,:\, y^p - y = ax + \frac{b}{x}$$

where (x, y) belong to an algebraic closure of the finite field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. The geometry of algebraic curves is key to the proof. Later, Stepanov found a proof which is elementary; as interpreted by Bombieri, the key point is the Riemann-Roch theorem.

Equidistribution

So, for some deep geometric reason, the summands $e((ax + b\bar{x})/p)$ behave extremely randomly as x varies over the interval $1 \leq x \leq p - 1$.

Equidistribution

So, for some deep geometric reason, the summands $e((ax + b\bar{x})/p)$ behave extremely randomly as x varies over the interval $1 \leq x \leq p - 1$. *But* randomly in a subtle way that leads to $K(a, b; p)/\sqrt{p}$ lying always in $[-2, 2]$, instead of being (rarely) unbounded, as the Central Limit Theorem suggests.

Equidistribution

So, for some deep geometric reason, the summands $e((ax + b\bar{x})/p)$ behave extremely randomly as x varies over the interval $1 \leq x \leq p - 1$. *But* randomly in a subtle way that leads to $K(a, b; p)/\sqrt{p}$ lying always in $[-2, 2]$, instead of being (rarely) unbounded, as the Central Limit Theorem suggests.

Deligne proved in the 1980's a general equidistribution theorem that gives some hint of the probabilistic nature of these exponential sums.

Equidistribution

So, for some deep geometric reason, the summands $e((ax + b\bar{x})/p)$ behave extremely randomly as x varies over the interval $1 \leq x \leq p - 1$. *But* randomly in a subtle way that leads to $K(a, b; p)/\sqrt{p}$ lying always in $[-2, 2]$, instead of being (rarely) unbounded, as the Central Limit Theorem suggests.

Deligne proved in the 1980's a general equidistribution theorem that gives some hint of the probabilistic nature of these exponential sums.

Theorem (Deligne; Katz)

As $p \to +\infty$, the normalized Kloosterman sums $K(a, b; p)/p^{1/2}$ for $1 \leq a, b \leq p - 1$ become equidistributed with respect to the measure

$$\mu_{ST} = \frac{1}{\pi}\sqrt{1 - \frac{x^2}{4}}dx$$

on $[-2, 2]$. The same holds for Birch sums $B(a; p)/p^{1/2}$.

What does this mean?

(1) For any continuous function $f : [-2, 2] \longrightarrow \mathbf{C}$, we have

$$\lim_{p\to+\infty} \frac{1}{(p-1)^2} \sum_{1\leq a,b\leq p-1} f\Big(\frac{K(a,b;p)}{\sqrt{p}}\Big) = \int_{-2}^{2} f(x) d\mu_{ST}(x).$$

What does this mean?

(1) For any continuous function $f : [-2, 2] \longrightarrow \mathbf{C}$, we have

$$\lim_{p \to +\infty} \frac{1}{(p-1)^2} \sum_{1 \leq a, b \leq p-1} f\Big(\frac{K(a, b; p)}{\sqrt{p}}\Big) = \int_{-2}^{2} f(x) d\mu_{ST}(x).$$

(2) Or equivalently: the sequences of random variables

$$(a, b) \mapsto \frac{K(a, b; p)}{\sqrt{p}}$$

on $\{1 \leq a, b \leq p-1\}$ with uniform probability measure converges weakly to μ_{ST}.

The shape of exponential sums

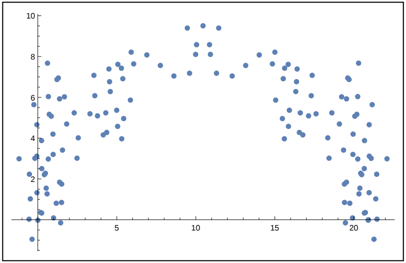
Out of curiosity, one can play the following game.

The shape of exponential sums

Out of curiosity, one can play the following game. Given a prime p and parameters $1 \leq a, b \leq p-1$, plot in the complex plane the successive partial sums

$$\sum_{1 \leq x \leq j} e\Big(\frac{ax + b\bar{x}}{p}\Big)$$

for $0 \leq j \leq p-1$,

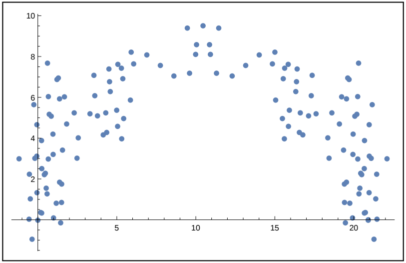


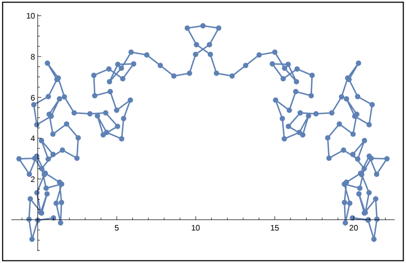
The shape of exponential sums

Out of curiosity, one can play the following game. Given a prime p and parameters $1 \leq a, b \leq p-1$, plot in the complex plane the successive partial sums

$$\sum_{1 \leq x \leq j} e\left(\frac{ax + b\bar{x}}{p}\right)$$

for $0 \leq j \leq p-1$,





and join these points by line segments, to obtain a polygonal curve in the plane.

History

D.H. Lehmer and J.H. Loxton (1970's–1980's) looked at and studied similar graphs for more regular exponential sums, especially quadratic Gauss sums

$$\sum_{0 \le x \le j} e\left(\frac{x^2}{p}\right).$$

History

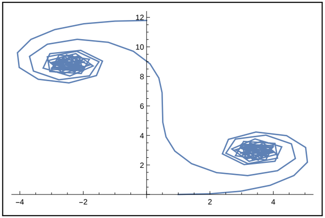
D.H. Lehmer and J.H. Loxton (1970's–1980's) looked at and studied similar graphs for more regular exponential sums, especially quadratic Gauss sums

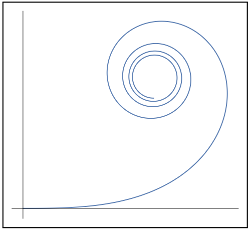
$$\sum_{0 \leq x \leq j} e\left(\frac{x^2}{p}\right).$$

These behave more regularly, staying close to Cornu spirals

$$\int_0^j e^{2i\pi x^2/p} dx$$

up to j about $p/2$.





“Absolutely chaotic”

Loxton mentions in a paper the case of Kloosterman sums:

> The other extreme may be exemplified by the incomplete Kloosterman sum
>
> $$K(h) = \sum_{\substack{a \leq x < a+h \\ (x,q)=1}} e_q(mx + n\bar{x}),$$
>
> where $\bar{x}$ denotes the solution of $x\bar{x} \equiv 1 \pmod{q}$. The graph of $K(h)$ seems to be absolutely chaotic and it is natural to think of it as a random walk in the plane.

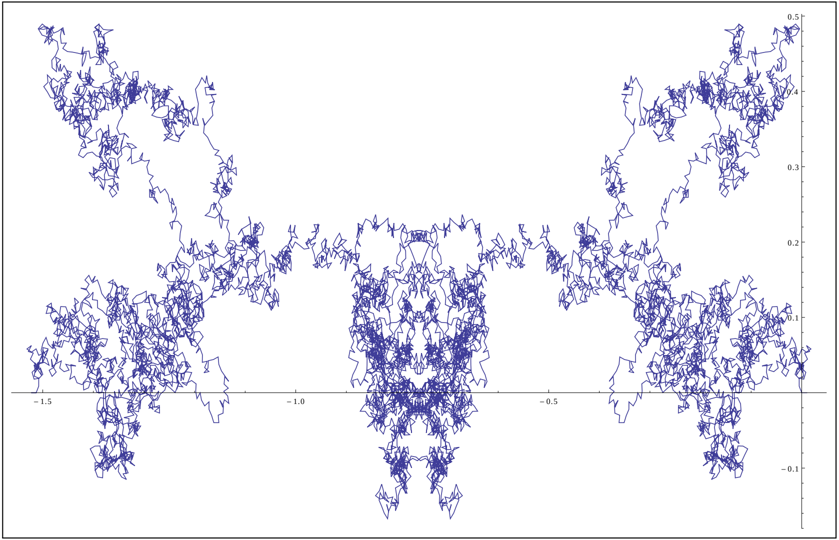
“Absolutely chaotic”

Loxton mentions in a paper the case of Kloosterman sums:

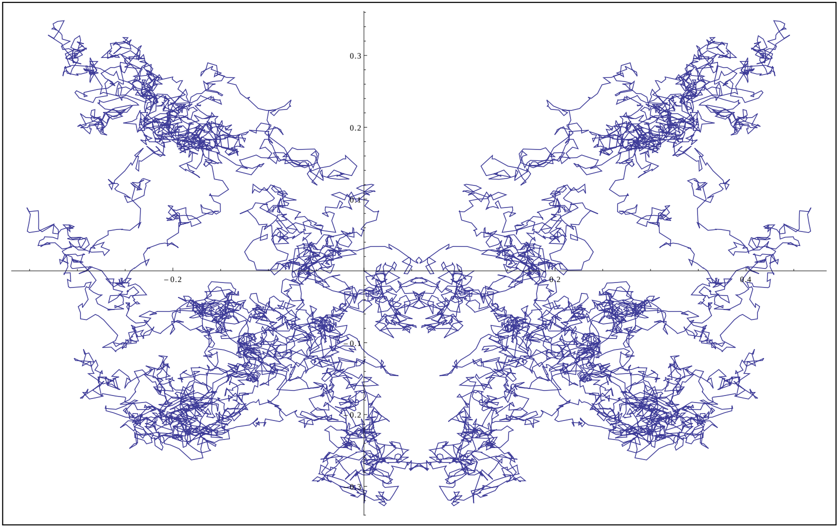
> The other extreme may be exemplified by the incomplete Kloosterman sum
>
> $$K(h) = \sum_{\substack{a \leq x < a+h \\ (x,q)=1}} e_q(mx + n\bar{x}),$$
>
> where $\bar{x}$ denotes the solution of $x\bar{x} \equiv 1 \pmod{q}$. The graph of $K(h)$ seems to be absolutely chaotic and it is natural to think of it as a random walk in the plane.

Is he right, or wrong?

Right...



and wrong...



A probabilistic limit theorem

For p prime and $1 \leq a, b \leq p-1$, we define a continuous map

$$\mathcal{K}\ell_p(a,b) \,:\, [0,1] \longrightarrow \mathbf{C}$$

by linear interpolation between the normalized partial sums

$$\frac{1}{\sqrt{p}} \sum_{1 \leq x \leq j} e\Big(\frac{ax + b\bar{x}}{p}\Big).$$

A probabilistic limit theorem

For p prime and $1 \leq a, b \leq p-1$, we define a continuous map

$$\mathcal{K}\ell_p(a,b) \,:\, [0,1] \longrightarrow \mathbf{C}$$

by linear interpolation between the normalized partial sums

$$\frac{1}{\sqrt{p}} \sum_{1 \leq x \leq j} e\Big(\frac{ax + b\bar{x}}{p}\Big).$$

For each p, we view $(\mathcal{K}\ell_p(\cdot,\cdot)(t))_{t\in[0,1]}$ as a stochastic process, defined on the finite probability space

$$\Omega_p = \{1 \leq a, b \leq p-1\}$$

with uniform probability.
We can also view this as a $C([0,1])$-valued random variable on this space.

Theorem (K.–Sawin, 2014)

- *The sequence* $(\mathcal{K}\ell_p)$ *converges in law, as random variables with values in* $C([0,1])$*, to a limiting process* V*.*

Theorem (K.–Sawin, 2014)

- *The sequence* $(\mathcal{K}\ell_p)$ *converges in law, as random variables with values in* $C([0,1])$, *to a limiting process* V.
- *This limiting process is the random Fourier series*

$$V(t) = \sum_{h \in \mathbf{Z}} \frac{e^{2i\pi ht} - 1}{2i\pi h} X_h,$$

where (X_h) *is a sequence of independent random variables, identically distributed according to* μ_{ST}.

(Note: the term $h = 0$ should be interpreted as tX_0).

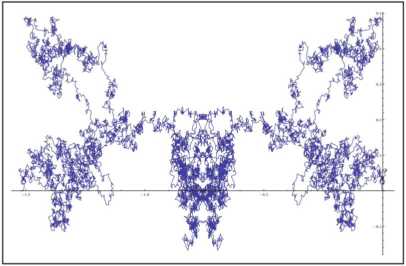
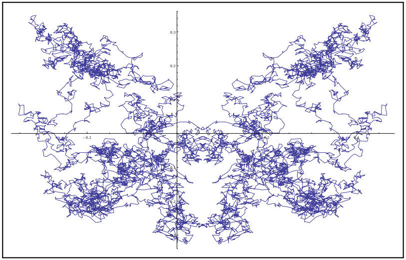
Theorem (K.–Sawin, 2014)

- *The sequence $(\mathcal{K}\ell_p)$ converges in law, as random variables with values in $C([0,1])$, to a limiting process V.*
- *This limiting process is the random Fourier series*

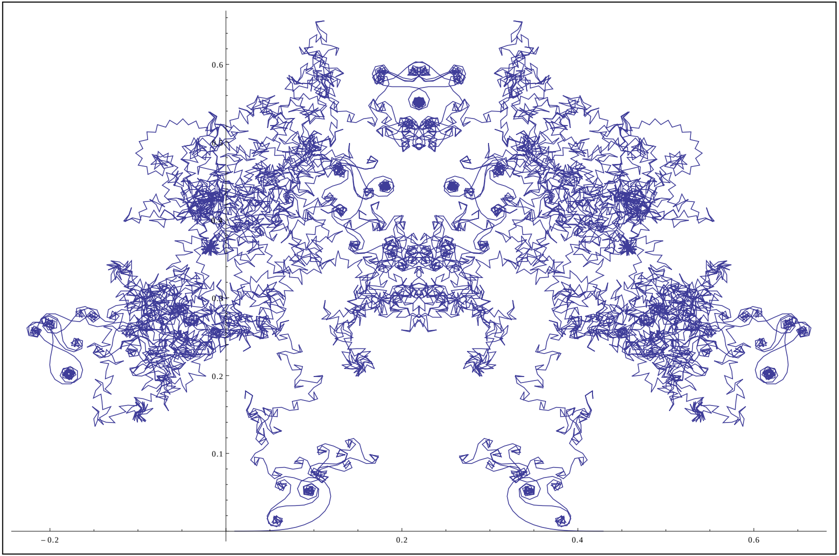
$$V(t) = \sum_{h\in\mathbf{Z}} \frac{e^{2i\pi ht}-1}{2i\pi h} X_h,$$

where (X_h) is a sequence of independent random variables, identically distributed according to μ_{ST}.

(Note: the term $h=0$ should be interpreted as tX_0).

Different look...



Limit for Birch sums

Theorem (K.–Sawin, 2014)

Define $C([0,1])$-valued random variables $\mathcal{B}_p$ from normalized partial sums of Birch sums on $\{1 \leq a \leq p-1\}$.

Limit for Birch sums

Theorem (K.–Sawin, 2014)

Define $C([0,1])$-valued random variables $\mathcal{B}_p$ from normalized partial sums of Birch sums on $\{1 \leq a \leq p-1\}$.
The sequence $(\mathcal{B}_p)$ converges in law, as random variables with values in $C([0,1])$, to the same limiting process V.

Limit for Birch sums

Theorem (K.–Sawin, 2014)

Define $C([0,1])$*-valued random variables* $\mathcal{B}_p$ *from normalized partial sums of Birch sums on* $\{1 \leq a \leq p-1\}$.
The sequence $(\mathcal{B}_p)$ *converges in law, as random variables with values in* $C([0,1])$*, to the same limiting process* V.

The different appearance between these graphs and those of Kloosterman sums is only at *smaller scales* than those that are retained in the limit.

Ideas of the proof

There are two parts, following Prokhorov's Theorem:

- Step 1: convergence of finite distributions:

Ideas of the proof

There are two parts, following Prokhorov's Theorem:

- Step 1: convergence of finite distributions: for any $k \geq 1$, and

$$0 \leq t_1 < t_2 < \cdots < t_k \leq 1,$$

the vectors

$$(\mathcal{K}\ell_p(t_1), \ldots, \mathcal{K}\ell_p(t_k))$$

converge in law to $(V(t_1), \ldots, V(t_k))$.

Ideas of the proof

There are two parts, following Prokhorov's Theorem:

- Step 1: convergence of finite distributions: for any $k \geq 1$, and

$$0 \leq t_1 < t_2 < \cdots < t_k \leq 1,$$

  the vectors

$$(\mathcal{K}\ell_p(t_1), \ldots, \mathcal{K}\ell_p(t_k))$$

  converge in law to $(V(t_1), \ldots, V(t_k))$.
- Step 2: tightness / weak-compactness in $C([0, 1])$:

Ideas of the proof

There are two parts, following Prokhorov's Theorem:

- Step 1: convergence of finite distributions: for any $k \geq 1$, and

  $$0 \leq t_1 < t_2 < \cdots < t_k \leq 1,$$

  the vectors

  $$(\mathcal{K}\ell_p(t_1), \ldots, \mathcal{K}\ell_p(t_k))$$

  converge in law to $(V(t_1), \ldots, V(t_k))$.
- Step 2: tightness / weak-compactness in $C([0,1])$: by Kolmogorov's criterion, it is enough to prove that

  $$\mathbf{E}(|\mathcal{K}\ell_p(t) - \mathcal{K}\ell_p(s)|^{\alpha}) \leq C|t-s|^{1+\delta}$$

  for $0 \leq s, t \leq 1$ and $C \geq 0$, $\alpha > 0$ and $\delta > 0$ independent of (p, t, s).

Finite distributions

- One can deal with the actual partial sums (no linear interpolation);

Finite distributions

- One can deal with the actual partial sums (no linear interpolation);
- Properties of $V(t)$ show that one can use the method of moments;

Finite distributions

- One can deal with the actual partial sums (no linear interpolation);
- Properties of $V(t)$ show that one can use the method of moments;
- Discrete Fourier expansion:

$$\frac{1}{\sqrt{p}} \sum_{1 \leq x \leq j} e\left(\frac{ax + b\bar{x}}{p}\right) = \frac{1}{p} \sum_{-p/2 < h < p/2} \alpha_p(h, j) K(a + h, b; p)$$

Finite distributions

- One can deal with the actual partial sums (no linear interpolation);
- Properties of $V(t)$ show that one can use the method of moments;
- Discrete Fourier expansion:

$$\frac{1}{\sqrt{p}} \sum_{1 \leq x \leq j} e\Big(\frac{ax + b\bar{x}}{p}\Big) = \frac{1}{p} \sum_{-p/2 < h < p/2} \alpha_p(h, j) K(a + h, b; p)$$

- Compute moments and get sums like

$$S = \frac{1}{(p-1)^2} \sum_{1 \leq a, b \leq p-1} \frac{K(a + h_1, b; p) \cdots K(a + h_k, b; p)}{p^{k/2}}$$

Finite distributions

- One can deal with the actual partial sums (no linear interpolation);
- Properties of $V(t)$ show that one can use the method of moments;
- Discrete Fourier expansion:

$$\frac{1}{\sqrt{p}}\sum_{1\leq x\leq j} e\Big(\frac{ax+b\bar{x}}{p}\Big) = \frac{1}{p}\sum_{-p/2<h<p/2} \alpha_p(h,j)K(a+h,b;p)$$

- Compute moments and get sums like

$$S = \frac{1}{(p-1)^2}\sum_{1\leq a,b\leq p-1} \frac{K(a+h_1,b;p)\cdots K(a+h_k,b;p)}{p^{k/2}}$$

- Deligne's Riemann Hypothesis *in very strong form* gives asymptotic formulas for S:

$$S = \mathbf{E}(X_{h_1}\cdots X_{h_k}) + O(p^{-1/2})$$

Finite distributions

- One can deal with the actual partial sums (no linear interpolation);
- Properties of $V(t)$ show that one can use the method of moments;
- Discrete Fourier expansion:

$$\frac{1}{\sqrt{p}} \sum_{1 \leq x \leq j} e\Big(\frac{ax + b\bar{x}}{p}\Big) = \frac{1}{p} \sum_{-p/2 < h < p/2} \alpha_p(h, j) K(a + h, b; p)$$

- Compute moments and get sums like

$$S = \frac{1}{(p-1)^2} \sum_{1 \leq a, b \leq p-1} \frac{K(a + h_1, b; p) \cdots K(a + h_k, b; p)}{p^{k/2}}$$

- Deligne's Riemann Hypothesis *in very strong form* gives asymptotic formulas for S:

$$S = \mathbf{E}(X_{h_1} \cdots X_{h_k}) + O(p^{-1/2})$$

- Then unwind...

Tightness

The goal is

$$\mathbf{E}(|\mathcal{K}\ell_p(t) - \mathcal{K}\ell_p(s)|^{\alpha}) \leq C|t-s|^{1+\delta}.$$

Write $|t-s| = p^{-\gamma}$ where $\gamma \geq 0$.

Tightness

The goal is

$$\mathbf{E}(|\mathcal{K}\ell_p(t) - \mathcal{K}\ell_p(s)|^\alpha) \leq C|t-s|^{1+\delta}.$$

Write $|t-s| = p^{-\gamma}$ where $\gamma \geq 0$. Then

- If $\gamma \geq 1$: the linear interpolation gives the result;

Tightness

The goal is

$$\mathbf{E}(|\mathcal{K}\ell_p(t) - \mathcal{K}\ell_p(s)|^\alpha) \leq C|t-s|^{1+\delta}.$$

Write $|t-s| = p^{-\gamma}$ where $\gamma \geq 0$. Then

- If $\gamma \geq 1$: the linear interpolation gives the result;
- If $1/2 + \varepsilon_1 \leq \gamma \leq 1$ (where $\varepsilon_1 > 0$): use trivial bound by number of terms;

Tightness

The goal is

$$\mathbf{E}(|\mathcal{K}\ell_p(t) - \mathcal{K}\ell_p(s)|^\alpha) \leq C|t - s|^{1+\delta}.$$

Write $|t - s| = p^{-\gamma}$ where $\gamma \geq 0$. Then

- If $\gamma \geq 1$: the linear interpolation gives the result;
- If $1/2 + \varepsilon_1 \leq \gamma \leq 1$ (where $\varepsilon_1 > 0$): use trivial bound by number of terms;
- If $0 \leq \gamma \leq 1/2 - \varepsilon_1$: use equidistribution as for Step 1;

Tightness

The goal is

$$\mathbf{E}(|\mathcal{K}\ell_p(t) - \mathcal{K}\ell_p(s)|^{\alpha}) \leq C|t-s|^{1+\delta}.$$

Write $|t-s| = p^{-\gamma}$ where $\gamma \geq 0$. Then

- If $\gamma \geq 1$: the linear interpolation gives the result;
- If $1/2 + \varepsilon_1 \leq \gamma \leq 1$ (where $\varepsilon_1 > 0$): use trivial bound by number of terms;
- If $0 \leq \gamma \leq 1/2 - \varepsilon_1$: use equidistribution as for Step 1;
- If γ is close to $1/2$: take $\alpha = 4$, and apply Kloosterman's method!

First application

Using some relatively basic probability in Banach spaces, we get a limiting distribution μ for

$$\max_{1\leq j\leq p-1} \frac{1}{\sqrt{p}}\Big|\sum_{1\leq x\leq j} e\Big(\frac{ax+b\bar{x}}{p}\Big)\Big|$$

and doubly-exponential tail bounds

$$c^{-1}\exp(-\exp(ct)) \leq \mu([t,+\infty[) \leq c\exp(-\exp(c^{-1}t)).$$

Similar results

- Bober, Goldmakher, Granville, Koukoulopoulos, Soundararajan: "classical" character sums (functional limit theorem in progress, with very different limiting random Fourier series, much work on tail bounds);

Similar results

- Bober, Goldmakher, Granville, Koukoulopoulos, Soundararajan: "classical" character sums (functional limit theorem in progress, with very different limiting random Fourier series, much work on tail bounds);
- Jurkat and van Horne; Marklof, Akarsu, Cellarosi: quadratic Gauss sums with arbitrary real coefficients (functional limit theorem in progress, again different limiting process);

Similar results

- Bober, Goldmakher, Granville, Koukoulopoulos, Soundararajan: "classical" character sums (functional limit theorem in progress, with very different limiting random Fourier series, much work on tail bounds);
- Jurkat and van Horne; Marklof, Akarsu, Cellarosi: quadratic Gauss sums with arbitrary real coefficients (functional limit theorem in progress, again different limiting process);
- Others?

Questions

- Has anyone already encountered the random series $V(t)$?

Questions

- Has anyone already encountered the random series $V(t)$?
- What are further properties of $V(t)$ that would have nice consequences for Kloosterman sums?