31.5.2021

Remark

(1) The theorem shows that the "paths" of Kloosterman sums are not really random walks, because they are not Markovian [$\approx$ one cannot say that the values at $t+\varepsilon$ only depend on the value at t, and not on "the past"].

(2) The most famous random continuous function is Brownian motion $(B(t))_{t\in[0,1]}$, which are gaussian processes with $B(0)=0$, $\mathbb{E}[B(t)B(s)] = \inf(t,s)$

There is a minor analogy because complex-valued Brownian motion is given by

$$B_{\mathbb{C}}(t) = t\,G_0 + \sum_{h\neq 0} \frac{e(ht)-1}{2i\pi h} G_h$$

where $(G_h)_{h\in\mathbb{Z}}$ i.i.d standard gaussians

3 _ Motivating the Theorem

We look first at

$$Kl_p(a, b)$$

at a fixed value of t, namely

$$t = \frac{j}{p-1} \qquad (\Leftrightarrow j = (p-1)t)$$

Then the value is

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

We use a standard technique to relate this partial sum to "complete" sums (over all of $\mathbb{F}_p$), by writing

$$z_j = \frac{1}{\sqrt{p}} \sum_{1 \leq x \leq p-1} \varphi_t(x)\, e\left(\frac{ax + b\bar{x}}{p}\right)$$

where φ_t is the characteristic function of the interval $1 \leq x \leq (p-1)t$; then we use a discrete Fourier expansion represented by integers in $-p/2, \dots, p/2$

of φ_t :

$$\varphi_t(x) = \sum_{h \in \mathbb{F}_p} \alpha_p(h;t)\, e\left(\frac{-hx}{p}\right)$$

where
$$\alpha_p(h;t) = \frac{1}{p} \sum_{1 \leq x \leq (p-1)t} e\left(\frac{hx}{p}\right)$$

So

$$z_j = \sum_{-p/2 < h \leq p/2}{}' \alpha_p(h;t)\, \frac{1}{\sqrt{p}} \sum_{1 \leq x \leq p-1} e\left(\frac{(a-h)x + b\bar{x}}{p}\right)$$

$$= \boxed{\sum_{-p/2 < h \leq p/2} \alpha_p(h;t)\, Kl_2(a-h, b; p)}$$

For fixed t, we have

$$\alpha_p(h;t) \xrightarrow[p \to \infty]{} \int_0^t e(hx)\, dx = \begin{cases} \dfrac{e(ht) - 1}{2i\pi h}, & h \neq 0 \\[2ex] t, & h = 0 \end{cases}$$

so the question becomes that of the

statistical distribution of the "shifted" Kloosterman sums

$$\mathrm{Kl}_2(a-h, b; p)$$

for $h \in \mathbb{F}_p$, as r.v. on Ω_p.

<u>Th.</u> [essentially Katz]

Consider the "infinite" random vectors

$$(a,b) \longmapsto (\mathrm{Kl}_2(a-h, b; p))_{h \in \mathbb{Z}}$$

on Ω_p. These converge in law as $p \to \infty$ to a family $(ST_h)_{h \in \mathbb{Z}}$ of independent Sato-Tate r.v.

(in the sense that for $H \geq 1$, the r.v. $(a,b) \longmapsto (\mathrm{Kl}_2(a-h,b;p))_{|h| \leq H}$ converge to $(ST_h)_{|h| \leq H}$).

Combining this, one might expect that

K_p should converge in law to

$$\boxed{K(t) = t\, ST_0 + \sum_{k \neq 0} \frac{e(kt) - 1}{2i\pi k}\, ST_k}$$

4 – Convergence in law for $C([0,1])$ – r.v

Random continuous functions are much better understood than some other infinite-dim. r.v., because of stochastic processes (esp. Brownian motion).

A standard approach to prove convergence in law uses two steps. Say we have X_n sequence of r.v. with values in $C([0,1])$ and some potential limit X.

Step 1 – Prove "convergence in finite distributions", i.e.

$\forall\, k \geq 1,\ \forall\ \ 0 \leq t_1 < \dots < t_k \leq 1$

$$(X_n(t_i))_{1\leq i \leq k} \xrightarrow[n\to\infty]{\text{law}} (X(t_i))_{1\leq i\leq k}$$

as $\mathbb{C}^k$ - valued r.v.

[Step 1' - Prove convergence in law of "Fourier coefficients"]

For this, we can use e.g.

- method of moments (was the approach in original proof)
- Lévy's Criterion
- CLT

Step 2 - Prove "tightness" of the sequence (X_n), i.e.

$\forall\, \varepsilon > 0,\ \exists\ K \subset C([0,1])$ compact

$\forall\, n \geq 1,\quad \mathbb{P}(X_n \in K) \geq 1-\varepsilon.$

cf. Ascoli-Arzela Theorem

In practice, one can use the following criterion of Kolmogorov:

Prop. [B.11.10]

Suppose there exist:

$$\alpha > 0, \quad \delta > 0, \quad C \geq 0$$

s.t.

$\forall \ 0 \leq s < t \leq 1,$

$$\mathbb{E}\left(|X_n(t) - X_n(s)|^{\alpha} \right) \leq C\, |t-s|^{1+\delta}.$$

Then the sequence (X_n) is tight.

5_ Existence of the random Fourier series

(cf. Kahane, "Some random series of functions")

Proposition. (1) For every $t \in [0,1]$, $K(t)$ converges a.s. and in L^2.

(2) The symmetric partial sums

$$K_H(t) = t\, ST_0 + \sum_{1 \le |h| \le H} \frac{e(ht)-1}{2i\pi h} ST_h$$

$\underbrace{\text{converge}}_{}^{\text{as } H \to \infty}$ as $C([0,1])$ - r.v to some $K(t)$.

<u>Proof.</u> (1) We use Kolmogorov's 3-series Th., writing the series as

$$t\, ST_0 + \sum_{h \ge 1} \underbrace{\left(\frac{e(ht)-1}{2i\pi h} ST_h - \frac{e(-ht)-1}{2i\pi h} ST_{-h} \right)}_{\text{summands } Y_h \text{ are independent, and bounded}}$$

so it suffices to check that

$$\left.\begin{array}{l} \mathbb{E}(Y_h) \\ \mathbb{V}(Y_h) \end{array}\right\} \text{ define convergent series}$$

But $\mathbb{E}(Y_h) = 0$ because

$$\mathbb{E}(ST_{\pm h}) = 0$$ and

$$\mathbb{V}(Y_h) = \left| \frac{e(ht)-1}{2i\pi h} \right|^2 \mathbb{V}(ST_h)$$

$$+ \left| \frac{e(-ht)-1}{2i\pi h} \right|^2 \mathbb{V}\left(ST_{-h}\right)$$

$$\leq \frac{1}{h^2}$$

(check that $\mathbb{V}(ST_h) = \mathbb{E}(ST_h^2) = 1$),

so these series converge.

(2) We use the two step process to check convergence in law in $C([0,1])$.

<u>Step 1.</u> Convergence of finite distributions follows from the convergence in L^1 of $K_H(t)$ to $K(t)$ for fixed t (Lemma B. 11. 3)

<u>Step 2.</u> We use Kolmogorov's Tightness Criterion. One can check that $\alpha = 2$ does not work (because by orthogonality we get that $\mathbb{E}\left(|K_H(t) - K_H(s)|^2\right)$ is of size $|t-s|$). The next value of α is $\alpha = 4$. We use here

The fact that since

$$K_H(t) - K_H(s) = (t-s)\,\xi T_0 + \sum_{1\leq|h|\leq H} \frac{e(ht)-e(hs)}{2i\pi h}\,\xi T_h$$

variance 1

is bounded and has expectation 0, it is σ_H^2 - subgaussian with

$$\sigma_H^2 = |t-s|^2 + \sum_{1\leq|h|\leq H} \left|\frac{e(ht)-e(hs)}{2i\pi h}\right|^2$$

$$\leq |t-s|^2 + \sum_{|h|\geq 1} \left|\frac{e(ht)-e(hs)}{2i\pi h}\right|^2$$

Parseval formula

$\sum |\hat{f}(h)|^2 = \int_0^1 |f(x)|^2 dx$

$$= \int_s^t dx = |t-s|$$

and one knows then that

$$\mathbb{E}\left(|K_H(t) - K_H(s)|^4\right) \leq C\,|t-s|^2$$

for some constant $C \geq 0$ independent of s and t, proving Kolmogorov's criterion.

$\square$

Remark. Kahane's results imply for instance that

(i) the random series K is a.s. nowhere differentiable (like Brownian motion)

(ii) it is a.s. Hölder with exponent $\frac{1}{2}-\varepsilon$, where $\varepsilon>0$ is fixed:

a.s.
$$|K(t)-K(s)| \leq C(\omega)\,|t-s|^{\frac{1}{2}-\varepsilon}$$

(again as Brownian motion).

6. Step 1 of proof of the Theorem

Instead of convergence of finite distributions, we use a variant better adapted to random Fourier series.

Prop. (special case of B. 11. 8)

If the following hold

$$(*)\begin{cases} \underset{\overset{\shortparallel}{Kl_2(a,b;p)}}{\underline{K}_p(1)} \xrightarrow{\text{law}} K(1) = ST_0 \\ \forall H \geq 1, \quad \left(\int_0^1 (\underline{K}_p(t) - t\underline{K}_p(1))\, e(-ht)\, dt \right)_{|h| \leq H} \\ \qquad \Big\downarrow {\scriptstyle H \to +\infty} \text{ law} \\ \left(\int_0^1 (K(t) - tK(1))\, e(-ht)\, dt \right)_{|h| \leq H} \end{cases}$$

and if $(\underline{K}_p)$ is tight, then

$\underline{K}_p$ converges in law to K.

Note:
$$\int_0^1 (K(t) - tK(1))\, e(-ht)\, dt$$
$$= \int_0^1 \left(\sum_{m \neq 0} ST_m \frac{e(mt) - 1}{2i\pi m} \right) e(-ht)\, dt$$
$$= \frac{1}{2i\pi h} ST_h$$

Idea: show, using Fejér's theorem or uniform of Cesàró-means of Fourier series of continuous functions, that if two $C([0,1])$-valued r.v. X_1 and X_2 have same Fourier coefficients (in law), then X_1 and X_2 have the same law.

It remains to prove:

(i) convergence of Fourier coefficients in the sense (*)

(ii) tightness

Sketch of proof of (i) (see p. 102 and following)

$$\underline{K}_p(1) = Kl_2(a, b; p)$$

$$\Big\downarrow \; p \to \infty \qquad [\mathrm{Kat}_3]$$

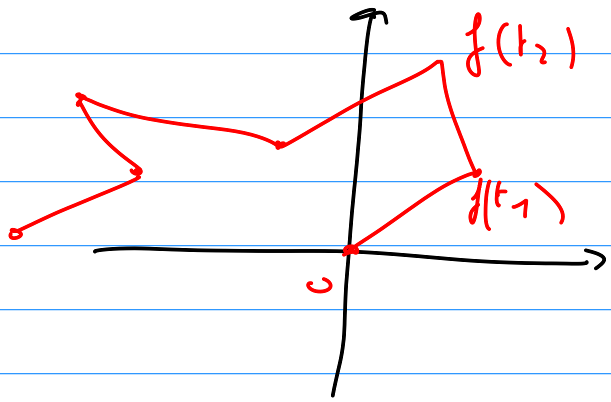
ST_0 , Sato-Tate r.v.

gives the first part of (*)

Then we use explicit computation of Fourier of $f(t) - tf(1)$ when $f(0) = 0$, f continuous, f polygonal [i.e. $f(t_i)$ are given for some

$$0 = t_0 < t_1 < \dots < t_m = 1$$

and one uses linear interpolation between successive values]



to check that

$$\int_0^1 \left(\underline{K}_p(t) - t\underline{K}_p(1)\right) e(-ht)\, dt$$

$$\approx \frac{1}{2i\pi h} Kl_2(a-h, b; p)$$

(compare with the discrete Fourier

expansion

$$\underline{K}_p\left(\frac{j}{p-1}\right) = \sum_{-p/2 < h \le p/2} \overset{\frac{e(hr)-1}{2i\pi h}}{\overset{\shortparallel}{\alpha_p}}\left(h;\underset{\underset{j/_{p-1}}{\shortparallel}}{r}\right) \mathrm{Kl}_2(a-h,b;p)$$