3.6.2021

Mon.

Exam : Fri 27.8 or ✓ 30.8

20 minutes oral exam

Two parts :

(1) You pick 2 out of

① Schoenberg / Erdős-Wintner ths.

② Erdős-Kac Theorem
③ Chebychev Bias
④ Bagchi's Th.
⑤ Kloosterman path

and be prepared to explain them

in ≃ 10 to 15 minutes.

I will pick one of the two.

(2) If time remains, some questions

about the other topics

7. Step 2: tightness

Prop. $\exists\ C \geq 0$ s.t.

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

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

This implies tightness of $(\underline{K}_p)_{p \text{ prime}}$ by Kolmogorov's Criterion.

Remark: check that taking $\alpha = 2$ (instead of 4) does not work, the RHS is only $|t-s|$.

Proof. Let $\gamma \geq 0$ be s.t.

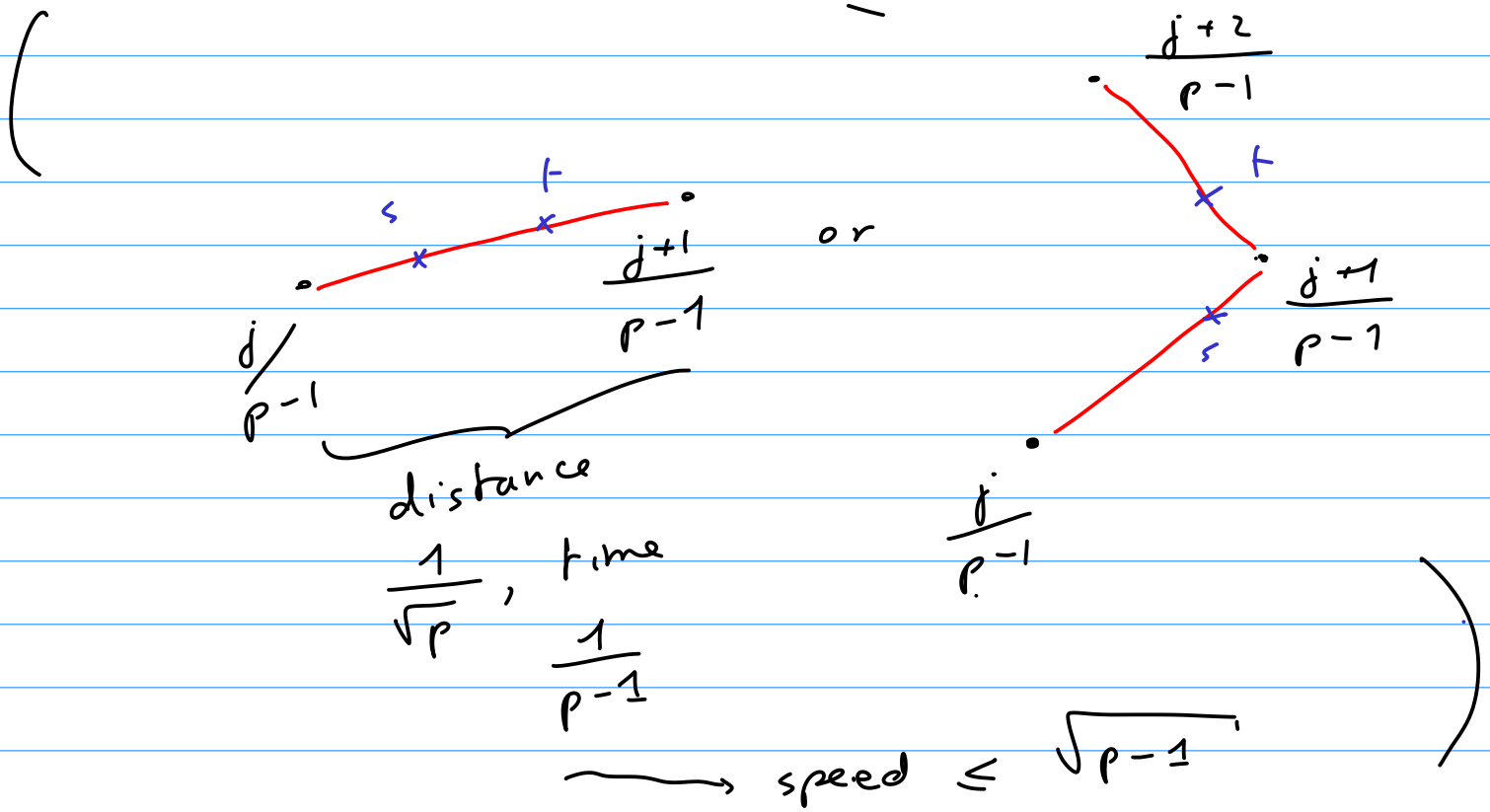
$$|t-s| = t-s = (p-1)^{-\gamma}.$$

We distinguish two cases.

Case 1 - If t and s are **close**, in the sense that $\gamma > 1$ $\left(\Leftrightarrow |t-s| < \frac{1}{p-1}\right)$

Then the polygonal definition implies that

$$|\underline{K}_p(t) - \underline{K}_p(s)| \leq \sqrt{p-1}\,|t-s| \leq \sqrt{t-s}$$



$\Rightarrow$ speed $\leq \sqrt{p-1}$

$$\Rightarrow$$

$$\mathbb{E}_p\left(|\underline{K}_p(t) - \underline{K}_p(s)|^4\right) \leq |t-s|^2$$

Case 2 - If t and s are "far", i.e. $\gamma \leq 1$ ($\Leftrightarrow \frac{1}{p-1} \leq |t-s| \leq 1$)

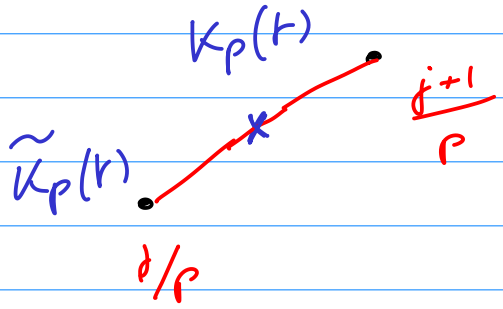
We can then check (with Hölder/Minkowski inequalities) that it is enough to

prove that $\exists\ C > 0$ s.t.

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

where

$$\widetilde{K}_p(t) = \frac{1}{\sqrt{p}} \sum_{1 \leq x \leq (p-1)t}{}^{*} e\left(\frac{ax+b\bar{x}}{p}\right)$$



So

$$\widetilde{K}_p(t) - \widetilde{K}_p(s) = \frac{1}{\sqrt{p}} \sum_{x \in I} e\left(\frac{ax+b\bar{x}}{p}\right)$$

where $I = \{ x \mid (p-1)s < x \leq (p-1)t \}$, i.e. is an interval of integers of length

$\approx (p-1)(t-s) \geq 1$.

So we need to compute

$$M_4 = \frac{1}{(p-1)^2} \sum_{(a,b) \in (\mathbb{F}_p^{\times})^2} \left| \frac{1}{\sqrt{p}} \sum_{x \in I} e\left(\frac{ax+b\bar{x}}{p}\right) \right|^4$$

(The following computation is the same idea used by Kloosterman in 1924 to prove $|Kl_2(a,b;p)| \leq 2p^{1/4}$.)

Precisely:

$$M_4 = \frac{1}{p^2(p-1)^2} \sideset{}{'}\sum_{a,b \neq 0} \sum_{\substack{x_1,\dots,x_4 \\ \in I}} \sum \cdots \sum e\left(\frac{a(x_1+x_2-x_3-x_4)}{p}\right) e\left(\frac{b(\bar{x}_1+\bar{x}_2-\bar{x}_3-\bar{x}_4)}{p}\right)$$

$$= \frac{1}{p^2(p-1)^2} \sum_{\substack{x_1,\dots,x_4 \\ \text{in } I}} \cdots \sum \sum_{a \neq 0} e\left(\frac{a(x_1+x_2-x_3-x_4)}{p}\right) \sum_{b \neq 0} e\left(\frac{b(\bar{x}_1+\bar{x}_2-\bar{x}_3-\bar{x}_4)}{p}\right)$$

By orthogonality of characters of $\mathbb{F}_p$

we have

$$\sum_{a \neq 0} e\left(\frac{ah}{p}\right) = \sum_{a} e\left(\frac{ah}{p}\right) - 1$$

$$= p\,\delta(h) - 1$$

where $\begin{cases} \delta(h) = 1 & \text{if } h = 0 \\ \delta(h) = 0 & \text{if } h \neq 0 \end{cases}$.

So

$$M_4 = \frac{1}{p^2(p-1)^2} \sum_{(x_1,\dots,x_4) \in I^4} \cdots \sum$$

$$\left(p\,\delta(x_1 + x_2 - x_3 - x_4) - 1\right)$$

$$\left(p\,\delta(\bar{x}_1 + \bar{x}_2 - \bar{x}_3 - \bar{x}_4) - 1\right)$$

$$= \frac{1}{(p-1)^2} \sum_{(x_1,\dots,x_4) \in I^4} \cdots \sum 1$$

$$x_1 + x_2 = x_3 + x_4$$

$$\bar{x}_1 + \bar{x}_2 = \bar{x}_3 + \bar{x}_4$$

$$+ O\left(\frac{1}{p(p-1)^2}|I|^3 + \frac{1}{p^2(p-1)^2}|I|^4\right)$$

(↳ because the nb. of $(x_i) \in I^4$

s.t. $\bar{x}_1 + \bar{x}_2 = \bar{x}_3 + \bar{x}_4$

is <u>at most</u> $|I|^3$, since (x_1, x_2, x_3)

determine x_4).

Note $\frac{1}{p(p-1)^2} |I|^3 \leq \frac{1}{(p-1)^3} |I|^3$

$\leq |t-s|^3$

$\frac{1}{p^2(p-1)^2} |I|^4 \leq |t-s|^4 \leq |t-s|^3$.

So the error terms are at most

$C |t-s|^3 \leq C |t-s|^2$

for some $C \geq 0$ (independent of p, s, t).

So we have to bound the number of solutions of

$$\begin{cases} x_1 + x_2 = x_3 + x_4 \\ \bar{x}_1 + \bar{x}_2 = \bar{x}_3 + \bar{x}_4 \end{cases}.$$

" $\cdot \frac{1}{x_1}$

The second equation is

$$\frac{x_2 + x_1}{x_1 x_2} = \frac{x_4 + x_3}{x_3 x_4}$$

so

(i) either $\boxed{x_2 + x_1 = 0} \Rightarrow x_3 + x_4 = 0$

so the solutions are

$$(x_1, -x_1), \quad (x_3, -x_3)$$

restricted to $x_1 \in I$ s.t. $-x_1 \in I$,

and so there are $\leq |I|^2$ solutions of this kind.

(ii) either $x_2 + x_1 \neq 0$, so $x_3 + x_4 \neq 0$

then

$$\begin{cases} x_1 + x_2 = x_3 + x_4 \\ x_1 x_2 = x_3 x_4 \end{cases}$$

$\rightsquigarrow$ (x_1, x_2), (x_3, x_4) are roots of the same quadratic equation / $\mathbb{F}_p$

$\rightsquigarrow$ $(x_1, x_2) = (x_3, x_4)$

$= (x_4, x_3)$

so there are $\leq 2|I|^2$ solutions.

Conclusion:

$$M_4 \leq \frac{3|I|^2}{(p-1)^2} + C|t-s|^2$$

$$\leq (3+C)|t-s|^2$$

□

8. Remarks on Katz's Theorem

Recall:

Th. (Katz)

As $p \to \infty$, the vector

$$(a,b) \mapsto \left(Kl_2(a-h, b; p)\right)_{h \in \mathbb{Z}}$$

converges in law to a vector $(ST_h)_{h \in \mathbb{Z}}$ of i.i.d. Sato-Tate random variables.

(1) This is an extremely deep result (much deeper than anything else we've used), relying on the most general forms of the Riemann Hypothesis over finite fields (as proved by Deligne in 1971).

(2) The starting point goes back to Weil, who proved $|Kl_2(a,b;p)| \leq 2$, by showing that there exists a matrix

$$\Theta_{a,b}(p) \in SU_2(\mathbb{C})$$

such that

$$Kl_2(a,b;p) = Tr(\Theta_{a,b}(p)).$$

($SU_2(\mathbb{C})$ — unitary matrix of determinant 1)

(Then $|Tr| = |$ sum of eigenvalues$| \leq 2$)

③ The work of Deligne and Katz (building on all the foundations of algebraic geometry, due to Grothendieck and his collaborators) allows to understand the distribution of the matrices

$\theta_{a,b}(p)$ as a, b vary in $\Omega_p = (\mathbb{F}_p^\times)^2$

(or more precisely the distribution of the conjugacy classes in $SU_2(\mathbb{C})$).

It turns out that any matrix

$$g \in SU_2(\mathbb{C})$$

is conjugate to a unique diagonal matrix

$$g \sim \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$$

where $\theta \in [0, \pi]$.

In terms of this parameter, we

have $\mathrm{Tr}(g) = 2\cos\Theta \in [-2, 2]$

and one can check that the Sato-Tate measure $\frac{1}{\pi}\sqrt{1 - \frac{x^2}{4}}\,dx$ on $[-2, 2]$ is the image by the trace of the Haar measure on the group $SU_2(\mathbb{C})$.

(probability)

Katz really proved (using work of Deligne):

Th. (Katz) ~1988 As $p \to \infty$, the $\Theta_{a,b}(p)$ become uniformly distributed in (the space of conjugacy classes of) $SU_2(\mathbb{C})$.

[$\Longrightarrow$ $(a,b) \longmapsto Kl_2(a,b;p)$ converge in law to a Sato-Tate r.v.]

For a single $(a,b) \longmapsto Kl_2(a-h, b; p)$

we get the same result.

(4) Quite remarkably, uniform r.v. on $SU_2(\mathbb{C})$ satisfy a very strong independence criterion

special case of

Prop. (Katz; "Goursat-Kolchin-Ribet criterion")

Let $(X_i)_{i \in I}$ be finite family of r.v, each uniform on $SU_2(\mathbb{C})$ (conj. classes of).

Then the X_i are (fully) independent if there is no $i \neq j$ s.t.

$$(\mathrm{Tr}\ X_i) = (\mathrm{Tr}\ X_j) \cdot \xi$$

with $|\xi| = 1$.

(Somewhat comparable to independance criteria for gaussians)

In our case, it is at least easy to check that $Kl_2(a,b;p) \neq Kl_2(a-h,b;p)$ for all (a,b) if $\underline{h \neq 0}$, by checking that

$$\frac{1}{(p-1)^2} \sum_{a,b} Kl_2(ab;p)\, Kl_2(a-h,b;p) \longrightarrow_{p\to\infty} 0$$

(suggests $\mathbb{E}(ST_0\, ST_h) = 0$).

9. Final remarks

Open Problem: can we get the same convergence in law for $Kl_2(a,1;p)$

[i.e $\Omega'_p = \mathbb{F}_p^\times$, $a \longmapsto \underline{K}_p(t)(a)$ as $C([0,1])$ - r.v.]

(natural because $Kl_2(a,b;p) = Kl_2(ab,1;p)$)

The theorem of Katz holds in this context: the $\left(a \longmapsto Kl_2(a-h, 1; p)\right)_{h \in \mathbb{Z}}$ converges to (ST_h), as $p \to \infty$.

However, we can't prove tightness!

This amounts to bounding

$$\frac{1}{p-1} \sum_{a \in \mathbb{F}_p^*} \left| \frac{1}{\sqrt{p}} \sum_{x \in I} e\left(\frac{ax + \bar{x}}{p}\right) \right|^4$$

and one can show that it suffices to do so if

$$p^{\frac{1}{2} - \eta} \leq |I| \leq p^{1/2 + \eta}$$

for some fixed $\eta > 0$ (arbitrarily small).

Opening as before, you get the main term is

$$\frac{1}{p(p-1)} \sum_{x_1, \dots, x_4 \in I} \cdots \sum_{\substack{x_1 + x_2 = x_3 + x_4}} e\left(\frac{\bar{x_1} + \bar{x_2} - \bar{x_3} - \bar{x_4}}{p}\right)$$

Issue is: nb. of solutions of

$$x_1 + x_2 = x_3 + x_4, \qquad x_i \in I$$

is $\simeq |I|^3$, which turns out to be too big. So we need cancellation from the exponential!

This is as yet unknown...