J. w. A. Forey, J. Fresán
(and W. Sawin)

Motivation

arithmetic functions
(in $\mathbb{k}[t]$) in arith.
finite field progressions

$\rightsquigarrow$ Keating - Rudnick

Hall - Keating - Roddity
Gershon

Sawin

Context: $f(n)$ arithmetic function

[ex. $f(n) = \Lambda(n)$]

$q \geq 1$

$$\sum_{\substack{n \le x \\ n \equiv a \, (q)}} f(n)$$

$$V = \frac{1}{\varphi(q)} \sum_{a \bmod q}^{*} \left| \sum_{\substack{n \le x \\ n \equiv a \, (q)}} f(n) - (\,) \right|^2$$

$f = \Lambda$: conj. (Hooley)

Friedlander - Goldston

...

[wrong in some ranges]

$V \sim X \log q$ (in some ranges)

K - R : polynomials in (Katz)

$k[t]$, $|k| \to +\infty$

$q \longleftrightarrow f \in k[t]$, squarefree

$2 \le \deg(f) \le n+1$

where average is over $\deg(g) = n$

H - K - RG : Λ_f for

functions f of "higher degree"

i.e. $-\frac{L'}{L}(f,s) = \sum_{n\geq 1} \Lambda_f(n) n^{-s}$

$\longrightarrow$ conj. "two-step formula"

$\longrightarrow$ prove it over $k[t]$

for typically f "=" elliptic curves parametrized by t,

e.g.

$E_t : y^2 = x(x-1)(x-t)$

$|k| + 1 - a(t) = |E_t(k)|$

Get : asymptotic formula for variance modulo $f = k(t)$ for $g \in k[t]$ of degree n,

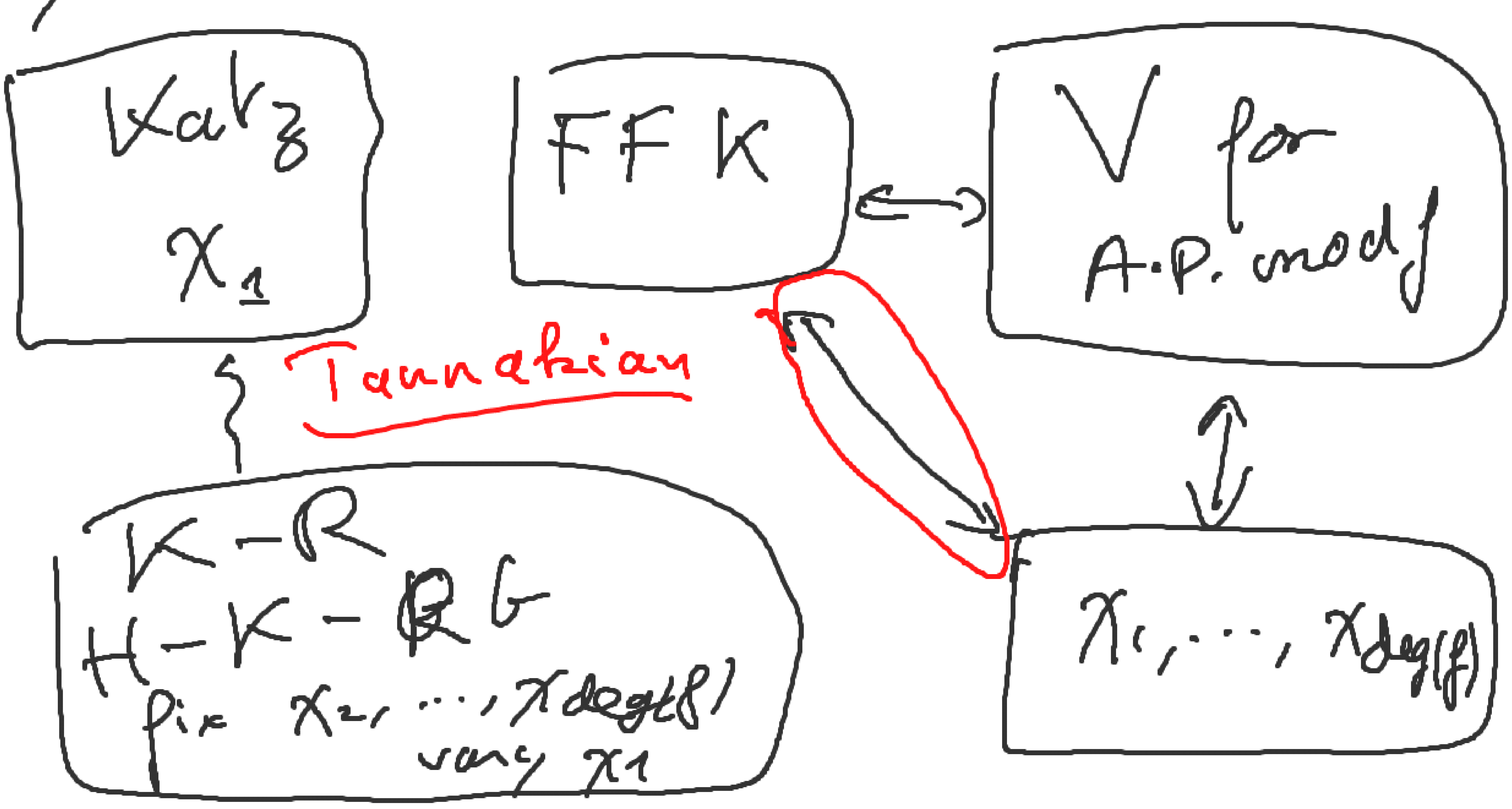
(monic)

provided

$$\begin{cases} \deg(f) > 900 \\ \underbrace{(t(t-1), f) = t}_{\text{artificial}} \end{cases}$$

<u>Method:</u> refine Katz's work

<u>Our goal:</u> improve on this by generalizing Katz's framework for equidistribution of sums parameterized by a multiplicative character.



"Th." (FFK) $E_f : y^2 = x(x-1)(x-f)$

f squarefree

$\deg(f) \geq 4$, $n \geq 1$

$\Longrightarrow$

$$\lim_{v \to \infty} V_{k_v} = \min(n, 2\deg(f) - 1)$$

k_v = extension of degree v of k

Key reason for releasing the hypothesis: by using equidistribution over <u>all</u> characters, we can use the "Larsen Alternative" (Guralnick-Thiep).

(2) Variance → twisted L-functions

Katz / Keating - Rudnick

$$B = k[t]/f\,k[t] \simeq \prod_{z \in Z} k \qquad g \longmapsto (g(z))_{z \in Z}$$

f splits over k

$Z = \{$ zeros of f in $\bar{k}\}$

$$B^\times = \left(k[t]/f\,k[t]\right)^\times \simeq (k^\times)^{\deg f}$$

$$\hat{B}^\times = \text{Dir. characters modulo } f \simeq \left(\widehat{k^\times}\right)^{\deg f}$$

$$\chi \longmapsto (\chi_z)_{z \in Z}$$

$$\chi(g) = \prod_{z \in Z} \chi_z(g(z))$$

E given, or some other "object" over k which has an L-function, say M; then

$$-T\frac{L'}{L}(M,T)=\sum_{g \text{ monic}} \Lambda_M(g)\,T^{\deg(g)}$$

variable

and we assume $L(M,T)$ is a polynomial.

<u>Computation of K-R:</u>

$$V_{k_v} = \frac{1}{|B_v^\times|^2}\sum_{x\in B_v^\times,\ x\neq 1} |V_{M,v}(n;x)|^2$$

$[k_v : k] = v,\ v\to\infty$

$B_v = k_v[t]/f k_v[t]$

$$\boxed{\begin{gathered} L(M,T)=\exp\Big(\sum \frac{S_v}{v}T^v\Big) \\ L(M\otimes x,T)=\exp\Big(\sum_{v\geq 1} V_{M,v}(n;x)/v\ T^v\Big)\end{gathered}}$$

Point:

$L(M \otimes \chi, T)$

$= \det\big(1 - T\,\mathrm{Fr}_k \mid \underbrace{H_c^0(M\otimes\chi)}_{\substack{\text{dim } N \\ \text{independent} \\ \text{of "good" } \chi}}\big)$

for "good" χ;

"most" χ's are good.

$= \det(1 - T\,\underbrace{\Theta_M(\chi)}_{\in U_N(\mathbb{C})})$

(unitary) $\longrightarrow$ Riemann Hypothesis (Deligne)

so understanding variance amounts to ______ distribution of $\Theta_M(\chi)$ in $U_N(\mathbb{C})$.

indeed
$$|V_M(n;x)|^2 = |\mathrm{Tr}(\theta_M(x)^n)|^2$$

"<u>Th.</u>" (FFK) In this setting there exists a compact subgroup
$$G \subset U_N(\mathbb{C})$$
s.t. $(\theta_M(x))_{x \in \widehat{B}^{\times}_{k_\nu}}$ become equidistributed in $G^{\#} = \{\text{conj. classes}\}$ as $\nu \to +\infty$.

(<u>Katz:</u> single character)

<u>Cor.</u>
$$\lim_{\nu \to \infty} V_{k_\nu} = \int_G |\mathrm{Tr}(g^n)|^2 \, dg$$

If $\boxed{G = U_N(\mathbb{C})}$ [proved by H-K-RG]

Then

$$\int_{U_N(\mathbb{C})} |\mathrm{Tr}(g^n)|^2 \, dg$$

$$= \underbrace{\min(n, N)}_{\text{two formulas}}$$

$2\deg(f)-1$
" for E_t

Diaconis-Evans

To show $G \supset SU_N(\mathbb{C})$

one can use:

Th. (Guralnick - Thiep)

$G \subset U_N(\mathbb{C})$ compact. $(N \geq 4)$

$G \supset SU_N(\mathbb{C})$

$$\iff \int_G |\mathrm{Tr}\, g|^8 \, dg = 24 = 4!$$

Why do we get 24?

In the application (to $\mathcal{E}_f$)

$$\mathrm{Tr}(\Theta_M(\chi))$$

$$= \frac{1}{\sqrt{|k|}} \sum_{x \in k} \chi(t-x) \underbrace{t_M(x)}_{a(x)}$$

$$\frac{1}{|B^\times|} \sum_{\chi \in \hat{B}^\times} \left| \frac{1}{\sqrt{|k|}} \sum_{x} \chi(t-x)\, t_M(x) \right|^8$$

$$= \frac{1}{|k|^4} \sum_{\substack{x_1, \dots, x_4 \\ x_5, \dots, x_8}} t_M(x_1) \cdots \overline{t_M(x_8)}$$

$$\cdot \underbrace{\frac{1}{|B^\times|} \sum_{\chi \in \hat{B}^\times} \frac{\chi((t-x_1) \cdots (t-x_4))}{\chi((t-x_5) \cdots (t-x_8))}}_{}$$

$= 0$ unless $(t-x_1) \cdots (t-x_4) = (t-x_5) \cdots (t-x_8) \bmod f$

so if $\deg(f) \geq 4$, this is 0 unless the polynomials are equal:

$$(t-x_1)\cdots(t-x_4) = (t-x_5)\cdots(t-x_8)$$

$$\Longrightarrow \{x_1, \ldots, x_4\} = \{x_5, \ldots, x_8\}$$

so if the roots are distinct then $(x_5, \ldots, x_8)$ is a permutation of $(x_1, \ldots, x_4)$

so

$$\frac{1}{|k|^4} \sum_{\sigma \in S_4} \sum_{x_1, \ldots, x_4} t_M(x_1) \cdots t_M(x_4) \overline{t_M(x_{\sigma(1)})} \cdots \overline{t_M(x_{\sigma(4)})}$$

$$= 24 \left(\frac{1}{|k|} \sum_x |t_M(x)|^2 \right)^4$$

$\to 1$ $u \to \infty$ in ~~many~~ cases