Algebra & Number Theory

Volume 14
2020
No. 5

Roots of L-functions of characters over function fields, generic linear independence and biases

Corentin Perret-Gentil

msp

ALGEBRA AND NUMBER THEORY 14:5 (2020)
https://doi.org/10.2140/ant.2020.14.1291

Roots of L-functions of characters over function fields, generic linear independence and biases

Corentin Perret-Gentil

We first show joint uniform distribution of values of Kloosterman sums or Birch sums among all extensions of a finite field $\mathbb{F}_q$, for almost all couples of arguments in $\mathbb{F}_q^\times$, as well as lower bounds on differences. Using similar ideas, we then study the biases in the distribution of generalized angles of Gaussian primes over function fields and primes in short intervals over function fields, following recent works of Rudnick and Waxman, and Keating and Rudnick, building on cohomological interpretations and determinations of monodromy groups by Katz. Our results are based on generic linear independence of Frobenius eigenvalues of ℓ-adic representations, that we obtain from integral monodromy information via the strategy of Kowalski, which combines his large sieve for Frobenius with a method of Girstmair. An extension of the large sieve is given to handle wild ramification of sheaves on varieties.

1. Introduction and statement of the results

Throughout, p will denote a prime larger than 5 and q a power of p.

1A. ***Kloosterman and Birch sums.*** For an integer $n \geq 1$, and $a \in \mathbb{F}_{q^n}^\times$, we consider the Kloosterman sums

$$\mathrm{Kl}_{r,q^n}(a) = \frac{1}{q^{n(r-1)/2}} \sum_{\substack{x_1,\dots,x_r \in \mathbb{F}_{q^n}^\times \\ x_1 \dots x_r = a}} e\left(\frac{\mathrm{tr}(x_1 + \cdots + x_r)}{p}\right) \tag{1}$$

of integer rank $r \geq 2$, as well as the Birch sums

$$\mathrm{Bi}_{q^n}(a) = \frac{1}{q^{n/2}} \sum_{x \in \mathbb{F}_{q^n}^\times} e\left(\frac{\mathrm{tr}(ax + x^3)}{p}\right). \tag{2}$$

MSC2010: primary 14G10; secondary 11J72, 11N36, 11R58, 11T23.
Keywords: exponential sums, linear independence, L-functions, large sieve, characters, function fields, Kloosterman sums.

Here, we adopt the usual notation $e(z) = \exp(2\pi i z)$ for any $z \in \mathbb{C}$, and $\mathrm{tr} : \mathbb{F}_{q^n} \to \mathbb{F}_p$ is the field trace.

For convenience, let us define the rank of Bi_{q^n} to be $r = 2$, and for $r \geq 2$, we let

$$f_{q^n} = \mathrm{Kl}_{r,q^n} \ (r \geq 2) \qquad \text{or} \qquad \mathrm{Bi}_{q^n} \ (r = 2) \tag{3}$$

for every integer $n \geq 1$. By the Deligne–Katz equidistribution theorem [Katz 1988] for Kloosterman sums and Livné's work [1987] for Birch sums (see also [Katz 1990]), as $q^n \to \infty$ the values

$$\{f_{q^n}(a) : a \in \mathbb{F}_{q^n}^\times\}$$

equidistribute in

$$\Omega_r = \begin{cases} [-r, r] \subset \mathbb{R} & \text{for } r \text{ even}, \\ \{z \in \mathbb{C} : |z| \leq r\} & \text{for } r \text{ odd}, \end{cases}$$

with respect to the pushforward $\mathrm{tr}_* \mu_r$ of the Haar measure μ_r on the compact group

$$G_r(\mathbb{C}), \qquad \text{where } G_r := \begin{cases} \mathrm{SU}_r & \text{for } r \text{ odd}, \\ \mathrm{USp}_r & \text{for } r \text{ even} \end{cases}$$

(e.g., the Sato–Tate measure when $r = 2$). These statements encompass bounds on f_{q^n} (e.g., Deligne's bound for hyper-Kloosterman sums), and the fact that f_{q^n} is real-valued whenever r is even. Moreover, they can alternatively be phrased as properties of the "angles" of Kloosterman and Birch sums, i.e., the

$$\theta_{1,f,q}(x), \dots, \theta_{r,f,q}(x) \in [0, 1],$$

such that

$$f_{q^n}(x) = \sum_{i=1}^{r} e(n\theta_{i,f,q}(x)) \qquad \text{for all } n \geq 1, \ x \in \mathbb{F}_q^\times \tag{4}$$

(whose existence follows from profound work of Grothendieck, Deligne, Katz and others, and will be recalled in due time): they are distributed like the eigenvalues of a Haar-random matrix in $G_r(\mathbb{C})$.

Our first main result is the following generic linear independence statement:

Theorem 1.1 (generic pairwise linear independence). *For $r \geq 2$ fixed, let f be as in* (3)*, and let*

$$E_r := \dim G_r + \tfrac{1}{2} \operatorname{rank} G_r = \begin{cases} \frac{1}{2}(2r^2 + r - 3) & \text{for } r \text{ odd}, \\ \frac{1}{4}(2r^2 + 3r) & \text{for } r \text{ even}. \end{cases}$$

For almost all $a, b \in \mathbb{F}_q^\times$, that is for

$$(q-1)^2 \left[1 + O_{r,p}\left(\frac{\log q}{q^{1/(2E_r)}}\right)\right] = (q-1)^2(1 + o_{r,p}(1)) \tag{5}$$

of them, the angles

$$1, \quad \theta_{j,f,q}(a), \quad \theta_{j,f,q}(b) \quad \text{with} \quad \begin{cases} 1 \leq j \leq r-1 & \text{for } r \text{ odd}, \\ 1 \leq j \leq r/2 & \text{for } r \text{ even}, \end{cases} \tag{6}$$

are $\mathbb{Q}$-linearly independent. The implied constants depend only on r, p, and only on r in the case of Kloosterman sums.

$$\mathbb{F}_p^\times \text{ (fixed)} \longrightarrow \mathbb{F}_q^\times \longrightarrow \mathbb{F}_{q^n}^\times \longrightarrow \bigcup_{m\geq 1} \mathbb{F}_{q^m}^\times = \overline{\mathbb{F}}_q^\times$$
$$\ni$$
$$a, b$$

Figure 1. The asymptotic setting for Section 1A.

Remark 1.2. The restriction on j in (6) is necessary since $\sum_{j=1}^r \theta_{j,f,q}(x) = 0$, and if r is even, the angles come by pairs: $\theta_{r/2+j,f,q}(x) = -\theta_{j,f,q}(x)$ $(1 \leq j \leq r/2)$.

Remark 1.3. Actually, we will more generally prove Theorem 1.1 for almost all tuples of $t \geq 1$ arguments, when $t = o(\sqrt{\log q})$ (e.g., t fixed), with (5) replaced by

$$(q-1)^t \left(1 + O_{r,p}\left(\frac{(r^{\delta_{r \text{ odd}}} C)^t \log q}{q^{1/(tE_r)}}\right)\right) \tag{7}$$

for an absolute constant $C \geq 1$. The implied constants depends again only on r in the case of Kloosterman sums.[1]

This has several interesting consequences. First, we obtain the *joint distribution* of almost all pairs of values of f in extensions of a fixed base field:

Corollary 1.4. *For $r \geq 2$, let f be as in* (3)*, a Kloosterman or Birch sum. For all but*

$$O_{r,p}\big((q-1)^2 (\log q) q^{-1/(2E_r)}\big)$$

couples $a, b \in \mathbb{F}_q^\times$, the random vector

$$X_{a,b} = \big((f_{q^n}(a),\, f_{q^n}(b))\big)_{1\leq n\leq N}$$

(*with the uniform measure on* $[1, N] \cap \mathbb{N}$) *converges in law as $N \to \infty$ to*

$$(\mathrm{tr}(g_1), \mathrm{tr}(g_2)),$$

with g_1, g_2 independent uniformly distributed in a maximal torus of $G_r(\mathbb{C})$. Explicitly, $\mathrm{tr}(g_i)$ *is distributed like*

$$\begin{cases} \sum_{j=1}^{r/2} 2\cos(2\pi\theta_j) & \text{for } r \text{ even}, \\ \sum_{j=1}^{r-1} e(\theta_j) + e\Big(-\sum_{j=1}^{r-1} \theta_j\Big) & \text{for } r \text{ odd}, \end{cases} \tag{8}$$

with θ_j independent uniform in $[0, 1]$. *Equivalently, the distribution of* $\mathrm{tr}(g_i)$ *is that of* $\mathrm{tr}(h_i^m)$ *for any $m \geq r$ and h_i uniform in $G_r(\mathbb{C})$ with respect to the Haar measure. The implied constant in Landau's notation depends only on r in the case of Kloosterman sums.*

[1] Here and from now on, δ_B will denote the Kronecker symbol with respect to a binary variable B, i.e., $\delta_B = 1$ if B is true, 0 otherwise. In particular, $r^{\delta_{r \text{ odd}}}$ is equal to r if the latter is odd, and to 1 otherwise.

Remark 1.5. Applying Deligne's equidistribution theorem and [Katz 1988; 1990] would show that $\big(f_{q^n}(a+b_1),\dots,f_{q^n}(a+b_t)\big)_{a\in\mathbb{F}_{q^n},\ a+b_i\neq 0}$ converges in law (with respect to the uniform measure), as $q^n\to\infty$, to a random vector in Ω_r^t distributed with respect to the product measure $(\mathrm{tr}_*\,\mu_r)^{\otimes t}$, when $b_i\in\mathbb{F}_{q^n}$ are $t=o(\log(q^n))$ distinct shifts (see, e.g., [Perret-Gentil 2017], where the dependencies of the errors from [Fouvry et al. 2015] with respect to t are made explicit). However, this only gives information among values that are explicitly related, by fixed shifts.

Remark 1.6 (discrepancy). For the distribution of a single Kloosterman sum of rank 2, conditionally on a linear independence hypothesis, Ahmadi and Shparlinski [2010] also obtained bounds on the discrepancy, using lower bounds arising from Baker's theorem. Their results are stated for curves, but the last paragraph of [Ahmadi and Shparlinski 2010, Section 5.2] explains how they readily extend to Kloosterman sums. Our Theorem 1.1 shows that their discrepancy bounds hold for almost all arguments, and using the same technique, a bound on the discrepancy in Corollary 1.4 could as well be given.

Another corollary is the following absence of bias among values of Birch sums and Kloosterman sums in extensions:

Corollary 1.7. *Let f_{q^n} be either* Kl_{r,q^n} *($r\geq 2$ even),* Bi_{q^n}*, or — if $r\geq 3$ is odd —* $\mathrm{Re}\,\mathrm{Kl}_{r,q^n}$ *or* $\mathrm{Im}\,\mathrm{Kl}_{r,q^n}$*. For all but $O_{r,p}\big((q-1)^2(\log q)q^{-1/(2E_r)}\big)$ couples $a,b\in\mathbb{F}_q^\times$, we have*

$$\mathbb{P}_{n\leq N}(f_{q^n}(a)<f_{q^n}(b)):=\frac{|\{1\leq n\leq N: f_{q^n}(a)<f_{q^n}(b)\}|}{N}\to 1/2\qquad as\quad N\to\infty.$$

The implied constant in Landau's notation depends only on r in the case of Kloosterman sums.

Finally, Theorem 1.1 also yields the following lower bounds, through the method of Bombieri and Katz [2010]. The first is not explicit and the value of n is not effective, while the second is weaker but does not suffer from these issues.

Corollary 1.8. *For $r\geq 2$, let f be as in* (3)*. For every $\varepsilon>0$ and all but $O_{r,p}\big((q-1)^2(\log q)q^{-1/(2E_r)}\big)$ couples $a,b\in\mathbb{F}_q^\times$, we have*:

(1) *For every n large enough* (*with respect to q,r,ε,a,b*),

$$|f_{q^n}(a)-f_{q^n}(b)|\geq q^{-\varepsilon n(r-1)}.$$

(2) *When $r=2$, for every $n\geq 1$ large enough with respect to p,*

$$|f_{q^n}(a)-f_{q^n}(b)|\geq (2/\pi^2)\begin{cases} q^{-2^{26}3^3\pi p^3\log(4p)\log(2n+1/2)}\\ q^{-C_p\log\left(\frac{n}{e}+\frac{2n+1/2}{q}\right)\frac{\log q}{\max(\log q,2)}}\end{cases}$$

with $C_p=1175\big(5.205+0.946\log\big(\frac{1}{2}(p-1)\big)\big)(p-1)^4$.

Remark 1.9. The second bound in (2) uses Gouillon's improvement [2006] on the Baker–Wüstholz theorem [1993] instead of the latter. The condition on n is only to simplify the expression above: the

bound in the proof is fully explicit. Moreover, the first inequality in (2) is valid for any $n \geq 1$. We can also update the lower bound of [Bombieri and Katz 2010, Corollary 4.3(ii)] to (assuming $p \geq 5$):

$$|\operatorname{Kl}_{r,p^n}(a)| \geq (2/\pi)q^{-2C_p \log\left(\frac{n}{e}+\frac{4n+1}{q}\right)\frac{\log q}{\max(\log q,2)}},$$

with C_p as above.

1B. ***Angles of Gaussian primes over function fields.*** Recently, Rudnick and Waxman [2019] studied refined statistics of angles of Gaussian primes $p = a + ib \in \mathbb{Z}[i]$, after Hecke's equidistribution result and the works that ensued. To give motivation for a conjecture they proposed, they developed a function field model where an analogue holds unconditionally.

Explicitly (see [Rudnick and Waxman 2019, Section 1.3, Section 6]), consider the quadratic extension $\mathbb{F}_q(S)$ of the function field $\mathbb{F}_p(T)$, $S = \sqrt{-T}$, with the norm $N(f(S)) = f(S)f(-S)$. The analogue of the unit circle is

$$\mathbb{S}_q^1 := \{u \in \mathbb{F}_q[[S]]^\times : u(0) = 1,\ N(u) = 1\},$$

and we have a well-defined map $U : \mathbb{F}_q[S]\backslash\{0\} \to \mathbb{S}_q^1,\ f \mapsto f/\sqrt{N(f)}$, that actually only depends on the ideal (f). For an integer $k \geq 1$, the "circle" $\mathbb{S}_q^1$ can be divided into q^κ sectors ($\kappa = \lfloor k/2 \rfloor$), $\operatorname{Sec}(u,k) := \{v \in \mathbb{S}_q^1 : v \equiv u \pmod{S^k}\}$, which are parametrized by

$$u \in \mathbb{S}_{k,q}^1 := \{u \in R_{k,q} : u(0) = 1,\ N(u) = 1\}, \quad R_{k,q} := (\mathbb{F}_q[S]/(S^k))^\times. \tag{9}$$

Rudnick and Waxman started by showing that if $k \leq n$ and

$$N_{k,n}(u) := |\{\mathfrak{p} \trianglelefteq \mathbb{F}_q[S] \text{ prime} : \deg(\mathfrak{p}) = n,\ U(\mathfrak{p}) \in \operatorname{Sec}(u,k)\}|$$

is the number of primes of fixed degree lying in a sector given by $u \in \mathbb{S}_{k,q}^1$, then there is equidistribution in the sectors whenever $\kappa < n/2$:

$$N_{k,n}(u) = \frac{|\{\mathfrak{p} \trianglelefteq \mathbb{F}_q[S] \text{ prime} : \deg(\mathfrak{p}) = n\}|}{|\mathbb{S}_{k,q}^1|} + O(q^{n/2}) = \frac{q^n/n}{q^\kappa} + O(q^{n/2}),$$

with an absolute implied constant.[2] Using a deep result of Katz [2017] (based on Deligne's equidistribution theorem and the computation of a monodromy group), they then got an unconditional analogue [Rudnick and Waxman 2019, Theorem 1.3] of their conjecture for $\mathbb{Z}[i]$ [Rudnick and Waxman 2019, Conjecture 1.2] on the variance of $N_{k,n}$ among all sectors.

The notion of Chebyshev bias for primes in arithmetic progressions, studied in depth by Rubinstein and Sarnak [1994], was extended to function fields by Cha [2008]. Further cases of biases in function fields have been considered recently [Cha and Kim 2010; Cha et al. 2016; 2017; Devin and Meng 2018], particularly in families of curves.

[2]The dependencies of the error with respect to k are not explicit in [Rudnick and Waxman 2019], but keeping track of them during the arguments shows that the error in the expression for $N_{k,n}(u)$ above is $O\big(q^{n/2}\kappa/n + \tau(n)^{1/2}q^{n/2}/n\big)$ (recall that we assume that $p \geq 7$), where τ is the number of divisors function.

Similarly, one may ask whether there is a bias in the distribution of prime ideals among different sectors as above. To do so, for $u_1, \dots, u_R \in \mathbb{S}^1_{k,q}$ distinct, we may look at the $\mathbb{R}^R$-valued random vector

$$X_{k,N}(\boldsymbol{u}) := \big(X_{k,N}(u_1), \dots, X_{k,N}(u_R)\big), \quad \text{where } X_{k,N}(u_r) := \left(\frac{q^\kappa n}{q^{n/2}}\left(N_{k,n}(u_r) - \frac{q^n/n}{q^\kappa}\right)\right)_{1\le n\le N}$$

(with the uniform measure on $[1, N]\cap\mathbb{N}$). The normalization is chosen so that $X_{k,N}(u_r)$ is bounded as $N \to \infty$ (with q, k fixed), which will be clear later on.

We recall that key inputs in [Rubinstein and Sarnak 1994; Cha 2008] to study biases finely are hypotheses about linear independence of roots of L-functions, also known as grand simplicity hypotheses (GSH). These are very strong statements and wide open conjectures.

Our second main result is a generic linear independence statement in the setting above, in the same spirit as Theorem 1.1. It concerns roots

$$e(\pm\theta_{\Xi,j}) \quad (1 \le j \le d'(\Xi)), \quad \theta_{\Xi,j} \in [0, 1], \tag{10}$$

of (normalized) L-functions associated to characters Ξ of $\mathbb{S}^1_{k,q}$ with conductor $3 \le d(\Xi) \le 2\kappa - 1$, where $d'(\Xi) := (d(\Xi) - 1)/2$ (these will be defined more precisely in Section 3). The analogue of GSH is:

Hypothesis 1.10. The angles $\theta_{\Xi,j}$, for $\Xi \in \widehat{\mathbb{S}}^1_{k,q}$, $1 \le j \le d'(\Xi)$, are $\mathbb{Q}$-linearly independent.

Towards Hypothesis 1.10, we show:

Theorem 1.11 (generic linear independence). *Assume that $p > k$ and let $t = o(\log|\mathbb{S}^1_{k,q}|)$ (e.g., t fixed). For almost all subsets $S \subset \widehat{\mathbb{S}}^1_{k,q}$ of size t, that is for*

$$\binom{q^\kappa}{t}\left(1 + O_{k,p}\left(\frac{C_{k,p}^t \log q}{q^{1/(2t(2\kappa^2-3\kappa+1))}}\right)\right) = \binom{q^\kappa}{t}(1 + o_{k,p}(1))$$

of them, with $C_{k,p} \ge 1$ depending only on k, p, the elements

$$1, \quad \theta_{\Xi,j} \qquad (\Xi \in S,\ 1 \le j \le d'(\Xi))$$

are $\mathbb{Q}$-linearly independent.

Remark 1.12. Hypothesis 1.10 would be Theorem 1.11 with $S = \mathbb{S}^1_{k,q}$. This is a very strong statement, whose validity may be delicate depending on the relative size of the parameters. Indeed, unlike in the number field situation, there are examples of families of L-functions over function fields where linear independence is not satisfied (although with q fixed, and eventually growing genus); see, e.g., [Kowalski 2008b, Section 6; Cha 2008, Section 5; Li 2018].

Remark 1.13. One can get the explicit dependency of the base $C_{k,p}$ with respect to k, p in Theorem 1.11, at the cost of a weaker error, replacing the latter by

$$O_{k,p}\left(\frac{(C(k+1)^{k+1})^t \log\log q}{\log q}\right)$$

with C absolute. Under a group theoretic conjecture, one could do so while keeping the strength of Theorem 1.11; see Remark 5.18.

Let us now explain how this relates to biases and the random vectors $X_{k,N}(\boldsymbol{u})$ defined above. We adapt classical arguments [Rubinstein and Sarnak 1994; Martin and Ng 2017; Devin 2019] to the function field setting, as in [Cha 2008; Devin and Meng 2018], to show:

Theorem 1.14 (limiting distribution, expected value). *The random vector $X_{k,N}(\boldsymbol{u})$ admits a compactly supported limiting distribution as $N \to \infty$ with $\kappa < N/2$ fixed. Namely, it converges in law to a $\mathbb{R}^R$-valued random variable $X_k(\boldsymbol{u})$. Moreover, the expected value of the latter is*

$$\mathbb{E}(X_k(\boldsymbol{u})) = \big(-\big|\{b \in \mathbb{S}^1_{k,q} : b^2 = u_r\}\big|/2\big)_{1\le r\le R} \subset \big\{-\tfrac{1}{2}, 0\big\}^R,$$

which means that there should be a bias towards sectors parametrized by nonsquares.

Theorem 1.15 (continuity, symmetry, bias). *If Hypothesis 1.10 holds and $R < \frac{1}{2}(\kappa - 1)$ is an integer, the distribution of $X_k(\boldsymbol{u})$ is*

(1) *absolutely continuous: there exists a Lebesgue integrable function f on $\mathbb{R}^R$ such that $\mathbb{P}(X_k(\boldsymbol{u}) \in A) = \int_A f\, d\boldsymbol{x}$ for all Borel subsets $A \subset \mathbb{R}^R$;*

(2) *symmetric with exchangeable components around its mean: for $X_k^0(\boldsymbol{u}) := X_k(\boldsymbol{u}) - \mathbb{E}(X_k(\boldsymbol{u}))$, we have*

$$X_k^0(\boldsymbol{u}) \sim -X_k^0(\boldsymbol{u}),\ \sigma(X_k^0(\boldsymbol{u}))$$

for any permutation $\sigma \in \mathfrak{S}_R$ of the coordinates.

Hence,

$$\lim_{N\to\infty} \mathbb{P}\big(X_{k,N}(u_1) < \cdots < X_{k,N}(u_R)\big) = \mathbb{P}\big(X_k(\boldsymbol{u})_1 < \cdots < X_k(\boldsymbol{u})_R\big),$$

which is $1/R!$ if the u_i are all squares or all nonsquares. If u_2 is a square while u_1 is not, and $\kappa > 5$, then $\lim_{N\to\infty} \mathbb{P}\big(X_{k,N}(u_1) < X_{k,N}(u_2)\big) < \frac{1}{2}$.

Remark 1.16. The restriction $R < \frac{1}{2}(\kappa - 1)$, rather strong with respect to the maximum $R = q^\kappa$, comes from the fact that the L-functions have finitely many zeros, in contrast with the number field case.

Hence, our generic linear independence statement, Theorem 1.11, implies the following towards an unconditional Theorem 1.15:

Corollary 1.17 (of Theorem 1.11). *Assuming that $p > k$, the limiting distribution $X_k(\boldsymbol{u})$ of Theorem 1.14 is*

(1) *continuous: $\mathbb{P}(X_k(\boldsymbol{u}) = \boldsymbol{a}) = 0$ for any $\boldsymbol{a} \in \mathbb{R}^R$. In particular, for $u \in \mathbb{S}^1_{k,q}$, $\lim_{N\to\infty} \mathbb{P}(X_{k,N}(u) > 0) = \mathbb{P}(X_k(u) > 0)$;*

(2) *a pushforward of the Lebesgue measure on a torus of dimension*

$$\gg_{\varepsilon,k} (\log|\mathbb{S}^1_{k,q}|)^{1-\varepsilon}, \quad \text{for any } \varepsilon > 0.$$

Remark 1.18. Concerning the stronger properties of Theorem 1.15 (absolute continuity, symmetry), Devin [2019] and Martin and Ng [2017] have shown that they hold under weaker conditions than full linear independence. However, we cannot exploit these here since their statements always involve all the roots/eigenvalues, while results obtained from the large sieve will be limited to a small subset.

1C. ***Prime polynomials in short intervals.*** Some of the techniques in [Rudnick and Waxman 2019] actually originate from [Keating and Rudnick 2014], which showed function field analogues of a conditional result of Goldston–Montgomery on primes in short intervals and of a conjecture of Hooley on the variance of primes in arithmetic progressions with fixed modulus.

For $A \in \mathbb{F}_q[T]$ of degree $n \geq 1$ and $1 \leq h \leq n$,

$$\nu_h(A) := \sum_{\substack{f \in \mathbb{F}_q[T] \\ \deg(f-A) \leq h}} \Lambda(f)$$

counts prime polynomials in a "short interval" around A, weighted by the function field von Mangoldt function Λ (defined by $\Lambda(f) = \deg(P)$ if $f = P^k$, $P \in \mathbb{F}_q[T]$ prime, $\Lambda(f) = 0$ otherwise). The mean value over the centers A having degree n is

$$\mathbb{E}_{q,n}(\nu_h) := \frac{1}{q^n} \sum_{\substack{A \in \mathbb{F}_q[T] \text{ monic} \\ \deg(A)=n}} \nu_h(A) = q^{h+1}\left(1 - \frac{1}{q^n}\right) \tag{11}$$

(see [Keating and Rudnick 2014, (2.7), Lemma 4.3]). Keating and Rudnick, [2014, Theorem 2.1], using another equidistribution result of Katz [2013b] when $h < n-3$, computed the corresponding variance explicitly, obtaining an unconditional analogue of the Goldston–Montgomery result mentioned above.

Any monic $A \in \mathbb{F}_q[T]$ of degree n can be written uniquely as

$$A = T^{h+1}B + C \quad \text{with} \quad \begin{cases} B \text{ monic, } \deg(B) = n-h-1 \\ \deg(C) \leq h, \end{cases}$$

and $\nu_h(A) = \nu_h(T^{h+1}B)$ only depends on B. This observation allows us to fix $n-h =: m$ and take $n \to \infty$. For $B_1, \ldots, B_R \in \mathbb{F}_q[T]$ distinct and monic of degree $m-1$, we can study the $\mathbb{R}^R$-valued random vector of biases

$$X_{m,N}(\boldsymbol{B}) := \big(X_{m,N}(B_1), \ldots, X_{m,N}(B_R)\big),$$

where

$$X_{m,N}(B_r) := \left(\frac{q^m}{q^{n/2+1}}\big(\nu_{n-m}(T^{n-m+1}B_r) - \mathbb{E}_{q,n}(\nu_{n-m})\big)\right)_{1 \leq n \leq N}$$

(with the uniform measure on $[1, N] \cap \mathbb{N}$), the expected values being those in (11). Again, the normalization is chosen so that $X_{m,N}(u_r)$ is bounded as $N \to \infty$ (with q, m fixed), which will be clear later on.

In this setting, we obtain results analogous to those exposed in Section 1B. Let

$$e(\theta_{\chi,j}) \quad (1 \leq j \leq d-1), \quad \theta_{\chi,j} \in [0,1], \tag{12}$$

be the roots associated to the L-function associated to an even Dirichlet character χ modulo $T^m \in \mathbb{F}_q[T]$ (see Section 3 for the precise definitions), for $2 \leq d \leq m$.

Hypothesis 1.19. The angles $\theta_{\chi,j}$, for $\chi \pmod{T^m}$ even, $1 \leq j \leq \operatorname{cond}(\chi)-2$, are $\mathbb{Q}$-linearly independent.

Theorem 1.20 (generic linear independence). *Assume that m is odd, $p > m$ and $t = o(\log(q^{m-1}))$ (e.g., t fixed). For almost all subsets S of size t of even Dirichlet characters mod T^m, that is for*

$$\binom{q^{m-1}}{t}\left(1 + O_{p,m}\left(\frac{C_{m,p}^t \log q}{q^{1/(2t(m-2)^2)}}\right)\right) = \binom{q^{m-1}}{t}(1 + o_{p,m}(1))$$

of them, with $C_{m,p} \geq 1$ depending only on p, m, the elements

$$1, \quad \theta_{\chi,j} \qquad (\chi \in S,\ 1 \leq j \leq \operatorname{cond}(\chi) - 2)$$

are $\mathbb{Q}$-linearly independent.

Theorem 1.21 (limiting distribution, expected value). *The random vector $X_{m,N}(\boldsymbol{B})$ admits a compactly supported limiting distribution as $N \to \infty$ with $m > 3$ fixed. Namely, it converges in law to a $\mathbb{R}^R$-valued random variable $X_m(\boldsymbol{B})$. Moreover, the latter has mean zero.*

Remark 1.22. There is no bias here, unlike in Theorem 1.14, simply because the von Mangoldt weight was kept.

Theorem 1.23 (continuity, symmetry). *If Hypothesis 1.19 holds and $R < m/2 - 1$, the distribution of $X_m(\boldsymbol{B})$ is absolutely continuous, and symmetric with exchangeable components. In particular,*

$$\lim_{N\to\infty} \mathbb{P}\big(X_{m,N}(B_1) < \cdots < X_{m,N}(B_R)\big) = \frac{1}{R!}.$$

Towards an unconditional Theorem 1.23, we obtain:

Corollary 1.24 (of Theorem 1.21). *Assuming m odd and $p > m$, the limiting distribution $X_m(\boldsymbol{B})$ from Theorem 1.21 is*

(1) *continuous*: $\mathbb{P}(X_m(\boldsymbol{B}) = \boldsymbol{a}) = 0$ *for any $\boldsymbol{a} \in \mathbb{R}^R$. In particular, for $B \in \mathbb{F}_q[T]$ of degree $m-1$,*

$$\lim_{N\to\infty} \mathbb{P}(X_{m,N}(B) > 0) = \mathbb{P}(X_m(B) > 0);$$

(2) *a pushforward of the Lebesgue measure on a torus of dimension*

$$\gg_{\varepsilon,m} (\log(q^{m-1}))^{1-\varepsilon}, \quad \text{for any } \varepsilon > 0.$$

Remark 1.25. The assumption that m is odd is technical, to get the integral monodromy in Theorem 5.12. It is anyway mild, since if m is even, one may as well look at shorter intervals of odd size $m-1$.

Remark 1.26. Again, if one wants explicit dependency of m, p in the base of t in Theorem 1.20, at the price of a weaker error, one may replace the latter by

$$O_{p,m}\left(\frac{(C(m+1)^{m+3})^t \log\log q}{\log q}\right)$$

with C absolute.

1D. ***Outline of the strategy, previous works, and organization of the paper.*** The existence and properties of the limiting distribution under linear independence hypotheses (Theorems 1.14, 1.15, 1.21 and 1.23) follow the methods developed in [Rubinstein and Sarnak 1994; Cha 2008; Martin and Ng 2017]. The continuity statement in Corollary 1.17, under weaker results than full linear independence, is obtained through an idea of Devin [Devin 2019; Devin and Meng 2018].

The main results are then Theorems 1.1, 1.11 and 1.20 on generic linear independence. Combining his large sieve for Frobenius over finite fields [Kowalski 2006; 2008a] with a method of Girstmair [1982; 1999], Kowalski [2008b] proved that a linear independence condition holds generically in some families of L-functions of curves over finite fields. This was recently extended by Cha, Fiorilli and Jouve [Cha et al. 2017] to certain families of elliptic curves over function fields, where the underlying symmetry is orthogonal instead of being symplectic.

We use similar ideas to prove Theorems 1.1 and 1.11, with the families of curves replaced by families of exponential sums or characters. More precisely, by work of Deligne [SGA $4\frac{1}{2}$ 1977] and Katz [2017], there are families of ℓ-adic sheaves on $\mathbb{G}_m$ (resp. on a variety parametrizing primitive characters Ξ or χ as above) such that the (reversed) characteristic polynomial of the Frobenius acting on a stalk yields the roots (resp. L-function) of the corresponding exponential sums (resp. characters).

Unlike in [Kowalski 2008b; Cha et al. 2017], these are not sheaves of $\mathbb{Z}_\ell$-modules, but of $\mathcal{O}_\lambda$-modules, for λ a valuation on the ring of integers $\mathcal{O}$ of a number field. In [Kowalski 2008b; Cha et al. 2017] the monodromy structure is symplectic or orthogonal (the latter being the source of complications handled by Jouve); here, it is either special linear, symplectic or projective general linear.

Another difficulty arises in bounding sums of Betti numbers appearing in the large sieve for Frobenius, because certain sheaves are not defined on curves nor have tame ramification, as assumed by Kowalski and Cha, Fiorilli and Jouve. This yields Theorem 5.14, and answers in this case a question of Kowalski [2006, Remark 4.8].

To apply this variant of the large sieve for Frobenius, we also need information on integral monodromy groups of the sheaves, whereas only information about the monodromy groups over $\mathbb{C}$ (i.e., after taking a Zariski closure) is a priori available from Katz's work [1988; 1990; 2013b; 2017]. This is overcome using deep results of Larsen and Pink through ideas of Katz (or more precise results in the case of Kloosterman sums). Unlike in [Cha et al. 2017], strong approximation for arithmetic groups cannot be used.

Remark 1.27 (Frobenius tori). As explained in [Kowalski 2008b, Section 7], another way to get generic linear independence results is by applying an effective version of Chebotarev's density theorem with Serre's theory of Frobenius tori. However, as explained in [Kowalski 2008b, p. 54], controlling the uniformity with respect to the size of the subsets/tuples considered (crucial for the questions we consider) is more subtle.

Remark 1.28 (prime polynomials in arithmetic progressions). Keating and Rudnick [2014] also studied the variance of prime polynomials in arithmetic progressions, and obtained as well an asymptotic expression (see [Keating and Rudnick 2014, Theorem 2.2]). In one of the ranges, this uses another

equidistribution result of Katz [2013a]. The latter is more complicated, relying on the ideas developed in [Katz 2012a], because the family involved is not parametrized by an algebraic variety. While results similar to those of Section 1C could probably be obtained (see also [Cha 2008]), we leave that to future work for this reason.

In Sections 2, 3 and 4, respectively for Kloosterman/Birch sums, Gaussian prime polynomials, and prime polynomials in short intervals, we:

(1) Give the cohomological interpretations due to Katz, which gives rise to the eigenvalues from (4), (10) and (12) respectively.

(2) For Gaussian prime polynomials and prime polynomials in short intervals:
   (a) Show the existence of the limiting distributions (Theorems 1.14 and 1.21).
   (b) Prove the additional properties of the distributions under Hypotheses 1.10 and 1.19 (Theorems 1.15 and 1.23).

(3) Prove Corollaries 1.4 and 1.8, 1.7 and Corollaries 1.17, 1.24, from the generic linear independence Theorems 1.1, 1.11 and 1.20 respectively.

Finally, Sections 5, 6 and 7 are dedicated to proving these generic linear independence statements.

1E. ***Notations.*** For a prime $p \geq 7$ and a field E with ring of integers $\mathcal{O}$, we let $\mathrm{Spec}_1(\mathcal{O})$ (resp. $\mathrm{Spec}_p(\mathcal{O})$) be the set of all nonzero prime ideals (equivalently, valuations on $\mathcal{O}$) having degree 1 (resp. not lying above p), and $\mathrm{Spec}_{1,p}(\mathcal{O}) = \mathrm{Spec}_1(\mathcal{O}) \cap \mathrm{Spec}_p(\mathcal{O})$. If $\lambda \in \mathrm{Spec}_{1,p}(\mathcal{O})$, we denote by $E_\lambda, \mathcal{O}_\lambda$ the completions, and $\mathbb{F}_\lambda \cong \mathcal{O}/\lambda$ the residue field. Note that $\mathbb{F}_\lambda \cong \mathbb{F}_\ell$, where ℓ is the prime above which λ lies.

2. Kloosterman sums and Birch sums

2A. *Cohomological interpretation.*

Theorem 2.1 (Deligne, Katz). *Let $E = \mathbb{Q}(\zeta_{4p})$, with ring of integers $\mathcal{O}$. For every $\lambda \in \Lambda := \mathrm{Spec}_p(\mathcal{O})$, there exists*

(1) *for every integer $r \geq 2$, a lisse sheaf $\mathcal{K}l_{r,\lambda}$ on $\mathbb{G}_{m,\mathbb{F}_p}$ of free $\mathcal{O}_\lambda$-modules, of rank r, pure of weight 0, such that for every finite field $\mathbb{F}_q$ of characteristic p and $x \in \mathbb{F}_q^\times$,*

$$\mathrm{tr}(\mathrm{Frob}_{\mathbb{F}_q} \mid (\mathcal{K}l_{r,\lambda})_x) = \mathrm{Kl}_{r,q}(x),$$

the normalized hyper-Kloosterman sum of rank r defined in (1)*. Moreover, the family $(\mathcal{K}l_{r,\lambda})_{\lambda\in\Lambda}$ forms a compatible system.*[3]

[3]We recall that this means that for every $\lambda \in \Lambda$, every finite field $\mathbb{F}_q$ of characteristic p and every $x \in \mathbb{F}_q^\times$, the reverse characteristic polynomial $\det(1 - T\,\mathrm{Frob}_{\mathbb{F}_q} \mid (\mathcal{K}l_{r,\lambda})_x) \in \mathcal{O}_\lambda[T]$ has coefficients in E that moreover do not depend on λ; see [Katz 2001, Section II].

(2) *a lisse sheaf* $\mathcal{B}i_\lambda$ *on* $\mathbb{G}_{m,\mathbb{F}_p}$ *of free* $\mathcal{O}_\lambda$*-modules, of rank* 2*, pure of weight* 0*, such that for every field* $\mathbb{F}_q$ *of characteristic* p *and* $x \in \mathbb{F}_q^\times$,

$$\mathrm{tr}(\mathrm{Frob}_{\mathbb{F}_q} \mid (\mathcal{B}i_\lambda)_x) = \mathrm{Bi}_q(x),$$

the normalized Birch sum defined in (2)*. Moreover, the family* $(\mathcal{B}i_\lambda)_{\lambda\in\Lambda}$ *forms a compatible system.*

Proof. (1) This is [Katz 1988, Theorem 4.1.1/Section 8.9]. To normalize by a Tate twist, we enlarge the ring of definition to $\mathbb{Z}[\zeta_{4p}]$, which is enough since $\sqrt{p} \in \mathbb{Z}[\zeta_{4p}]$ by the evaluation of quadratic Gauss sums (see [Katz 1988, 11.0]).

(2) This is contained in [Katz 1990, 7.12] (see also [Katz 1987, Part 3]), along with [Katz 1988] for the definition over $\mathcal{O}_\lambda$ of the ℓ-adic Fourier transform. □

The roots of the characteristic polynomial of $\mathrm{Frob}_{\mathbb{F}_q}$ acting on the stalks at $x \in \mathbb{F}_q^\times$ of any of the sheaves in the system $(\mathcal{K}l_{r,\lambda})_{\lambda\in\Lambda}$, resp. $(\mathcal{B}i_\lambda)_{\lambda\in\Lambda}$, are then the $e(\theta_{i,f,q}(x)) \in \mathbb{C}$ $(1 \le i \le r)$ giving (4), when $f = \mathrm{Kl}_{r,q}$, resp. $f = \mathrm{Bi}_q$ $(r = 2)$.

We now prove the three corollaries of Theorem 1.1 (generic linear independence of the roots) stated in Section 1A.

2B. ***Joint uniform distribution: Corollaries 1.4 and 1.7.*** Let $a, b \in \mathbb{F}_q^\times$ be such that the conclusion of Theorem 1.1 holds. By the Kronecker–Weyl equidistribution theorem (see, e.g., [Devin 2019, Section 4.1] or [Martin and Ng 2017, Appendix B]), the random vector

$$\big(n\theta_{i,f,q}(a),\ n\theta_{j,f,q}(b) : 1 \le i, j \le r\big)_{n\le N}$$

equidistributes in $[0, 1]^{2r}$ as $N \to \infty$. It follows at once by (4) that $X_{a,b}$ converges in law to a pair of independent random variables distributed like (8) as $N \to \infty$.

Finally, the equivalence of the distribution of (8) and traces of large enough powers of matrices in $G_r(\mathbb{C})$ is the content of [Rains 1997, Theorem 2.1].

Corollary 1.7 is then an immediate consequence, by applying the portmanteau theorem to the random variable $\mathrm{tr}(g_1) - \mathrm{tr}(g_2)$ (or its real/imaginary parts), which is symmetric around its mean 0. □

2C. ***Lower bounds: Corollary 1.8.*** We follow the method of Bombieri and Katz [2010, Sections 3–4], based on the subspace theorem from [Evertse 1984; van der Poorten and Schlickewei 1991] and the Baker–Wüstholz theorem [1993].

Let $a, b \in \mathbb{F}_q^\times$ be such that the conclusion of Theorem 1.1 holds. By (4), we have

$$F(n) := f_{q^n}(a) - f_{q^n}(b) = \sum_{i=1}^{r} \big(e(n\theta_{i,f,q}(a)) - e(n\theta_{i,f,q}(b))\big).$$

The Skolem–Mahler–Lech theorem (see [Bombieri and Katz 2010, Theorem 2.1(i)]) shows that if none of

$$e\left(\frac{\theta_{i,f,q}(x)}{\theta_{j,f,q}(x)}\right) \quad (x \in \{a, b\},\ 1 \le i < j \le r), \qquad e\left(\frac{\theta_{i,f,q}(a)}{\theta_{j,f,q}(b)}\right) \quad (1 \le i, j \le r)$$

are roots of unity, which holds by linear independence, then there are only finitely many n (with a, b, r, q fixed) such that $F(n) = 0$.

The subspace theorem [Evertse 1984; van der Poorten and Schlickewei 1991] (see [Bombieri and Katz 2010, Theorem 3.1]) shows that, after multiplying by $q^{n(r-1)/2}$ (i.e., de-normalizing), for every $n \geq 1$ large enough (with respect to the roots $\theta_{i,f,q}$, i.e., with respect to a, b, r, q, ε), either $F(n) = 0$, or $F(n)$ satisfies the lower bound of Corollary 1.8(1). With the above, this proves the first part of the corollary.

For the second part, we assume that $r = 2$. For any integers $k_0, k_1 \in \mathbb{Z}$ and $\theta_0, \theta_1 \in [0, 1]$, we have

$$\begin{aligned}|\cos(2n\pi\theta_0) - \cos(2n\pi\theta_1)| &= 2|\sin(n\pi(\theta_0+\theta_1))\sin(n\pi(\theta_0-\theta_1))| \\ &= 2\prod_{j=0}^{1}|\sin(n\pi\tau_j - k_j\pi)| \qquad (\tau_j = \theta_0 + (-1)^j\theta_1) \\ &\geq 2\prod_{j=0}^{1}\frac{2|n\pi\tau_j - k_j\pi|}{\pi} \\ &= \frac{2}{\pi^2}\prod_{j=0}^{1}|n\log(e(\tau_j)) - k_j\log(-1)|,\end{aligned}$$

where the inequality holds if k_j is chosen to minimize $|n\tau_j - k_j|$.

We can now apply the Baker–Wüstholz theorem [1993, Theorem, p. 20] as in [Bombieri and Katz 2010, Section 4], or its improvement with respect to the numerical constants by Gouillon [2006], giving the first and second expressions in Corollary 1.8(2). As the arguments are essentially the same, we only give the second one. If $1, \theta_0, \theta_1$ are linearly independent, then [Gouillon 2006, Corollary 2.2] shows that this is

$$\geq \frac{2}{\pi^2}\prod_{j=0}^{1}\exp\left(-9400\left(3.317 + \frac{1.888}{d} + 0.946\log d\right)d^4 h_j A_j\right), \tag{13}$$

where A_j is any real number satisfying $\log A_j \geq \max(1, h(e(\tau_j)), |\tau_j|/d, 1/d)$,

$$\begin{aligned}h_j &= \max\left(\log\left(\frac{n}{ed} + \frac{k_j}{dA_1}\right), \frac{1000}{d}, 498 + \frac{284}{d} + 142\log d\right), \\ d &= [\mathbb{Q}(e(\tau_0), e(\tau_1)) : \mathbb{Q}]/2,\end{aligned}$$

for h_0 the absolute logarithmic Weil height. We have $h_0(e(\tau_j)) \leq h_0(e(\theta_0)) + h_0(e(\theta_1))$.

Let us now assume that $(\theta_0, \theta_1) = (\theta_{i,f,q}(a), \theta_{i,f,q}(b))$ are moreover angles of exponential sums (4). Then $q^{1/2}e(\pm\theta_j)$ is an algebraic integer, so $h_0(e(\tau_j)) \leq \log q$. Regarding the degree, we have that $1 \leq d \leq (p-1)/2$ as in [Bombieri and Katz 2010, Proof of Corollary 4.3], because Kloosterman/Birch sums are sums of p-th roots of unity. Thus, we may take $A_j = \max(q, e^2)$ and

$$h_j \leq \max\left(\log\left(\frac{n}{e} + \frac{2n + \frac{1}{2}}{A_j}\right), 1000, 782 + 142\log\frac{p-1}{2}\right).$$

Then, (13) is

$$\geq \frac{2}{\pi^2}\exp\left(-1175\left(5.205+0.946\log\frac{p-1}{2}\right)(p-1)^4 h\max(\log q,2)\right),$$

where

$$h=\max\left(\log\left(\frac{n}{e}+\frac{2n+\frac{1}{2}}{q}\right),1000,782+142\log\frac{p-1}{2}\right).$$

If p is fixed and n is large enough with respect to it, this gives the expression in Corollary 1.8. This yields the result by Theorem 1.1. The argument is essentially the same to lower bound a single Kloosterman sum with Gouillon's result, with the analogue of (13) having a leading factor of $2/\pi$, no product, and $A_0=\max(q/2,e)$. □

3. Angles of Gaussian primes

3A. *Definitions and cohomological interpretation.*

Definition 3.1. Let q be an odd prime power and $k\geq 2$ be an integer. A *super-even character* Ξ *modulo* S^k *over* $\mathbb{F}_q$ is a character of

$$\mathbb{S}^1_{k,q}\cong R_{k,q}/H_k,\qquad H_k:=(\mathbb{F}_q[S^2]/(S^k))^\times$$

(see (9)). The *Swan conductor* of a nontrivial Ξ is the maximal (odd) integer $d(\Xi)$ such that Ξ is nontrivial on $(1+(S^{d(\Xi)}))/(S^k)\leq R_{k,q}$. The character Ξ is *primitive* if $d(\Xi)=2\kappa-1$, with $\kappa:=\lfloor k/2\rfloor$. The *L-function* of a nontrivial Ξ is

$$L(\Xi,T)=\prod_{\substack{P\text{ prime}\\ \text{monic}\\ P(0)\neq 0}}(1-\Xi(P)T^{\deg P})^{-1}. \tag{14}$$

Theorem 3.2 (Katz). *Let $\mathbb{F}_q$ be a finite field of odd characteristic p, $k\geq 2$ be an even integer,*

$$E=\mathbb{Q}\left(\zeta_{4p^r}:1\leq r\leq 1+\frac{\log k}{\log p}\right)\subset\mathbb{Q}(\zeta_{p^\infty})$$

with ring of integers $\mathcal{O}$, and let $\lambda\in\Lambda:=\mathrm{Spec}_p(\mathcal{O})$.

(1) *There exists a unipotent group $\mathbb{W}_{k,\mathrm{odd}}$ over $\mathbb{F}_p$ such that $\mathbb{W}_{k,\mathrm{odd}}(\mathbb{F}_q)=\mathbb{S}^1_{k,q}$ (the group of super-even characters, by duality), as well as an open set $\mathrm{Prim}_{k,\mathrm{odd}}\subset\mathbb{W}_{k,\mathrm{odd}}$ such that $\mathrm{Prim}_{k,\mathrm{odd}}(\mathbb{F}_q)$ is in bijection with primitive super-even characters modulo S^k over $\mathbb{F}_q$.*

(2) *There exists a lisse sheaf $\mathcal{G}_{k,\lambda}$ on $\mathrm{Prim}_{k,\mathrm{odd}}$ of free $\mathcal{O}_\lambda$-modules, of rank $r=2\kappa-2$, pure of weight 1, such that for every $\Xi\in\mathrm{Prim}_{k,\mathrm{odd}}(\mathbb{F}_q)$, we have*

$$\det(1-T\,\mathrm{Frob}_{q,\Xi}\mid\mathcal{G}_{k,\lambda})=\frac{L(\Xi,T)}{1-T},$$

which is a polynomial of degree $d(\Xi)=r+1$. In particular, the family $(\mathcal{G}_{k,\lambda})_{\lambda\in\Lambda}$ forms a compatible system.

(3) *The Tate twist* $\mathcal{F}_{k,\lambda} = \mathcal{G}_{k,\lambda}\left(\frac{1}{2}\right)$ *is a lisse sheaf of free* $\mathcal{O}_\lambda$*-modules on* $\mathrm{Prim}_{k,\,\mathrm{odd}}$*, pure of weight zero, of rank* $d(\Xi) - 1$*, with symplectic auto-duality.*

Proof. These are the contents of [Katz 2017, Section 2] (see also the constructions in [Katz 2013b, Sections 1–4]). □

In particular, the eigenvalues of $\mathrm{Frob}_{\mathbb{F}_q}$ acting on the stalks of $\mathcal{F}_{k,\lambda}$ at super-even primitive Ξ, which are free $\mathcal{O}_\lambda$-modules of rank $2\kappa - 2$, yield the eigenvalues $e(\pm\theta_{\Xi,j}) \in \mathbb{C}$ from (10), such that

$$\begin{aligned} L(\Xi, T) &= (1-T)\prod_{j=1}^{\kappa-1}\big(1-\sqrt{q}e(\theta_{\Xi,j})T\big)\big(1-\sqrt{q}e(-\theta_{\Xi,j})T\big) \\ &= (1-T)\det(1-\sqrt{q}T\Theta_\Xi), \quad \text{with } \Theta_\Xi \in \mathrm{Sp}_{d(\Xi)-1}(\mathbb{C}). \end{aligned}$$

3B. ***Existence of the limiting distribution.*** We start with an explicit formula for $X_{k,N}(\boldsymbol{u})$.

Proposition 3.3. *For all* $u \in \mathbb{S}^1_{k,q}$ *and* $n \le N$*, we have*

$$X_{k,N}(u)_n = -2\sum_{f=2}^{\kappa}\sum_{j=1}^{f-1}\sum_{\substack{\Xi\in\widehat{\mathbb{S}}^1_{k,q}\\ d(\Xi)=2f-1}} \overline{\Xi}(u)\cos(2\pi n\theta_{\Xi,j}) - \delta_{n\ \mathrm{even}}|\{b\in\mathbb{S}^1_{k,q} : b^2 = u\}| + O\left(\frac{q^{k/2}\tau(n)}{q^{n/6}n} + \frac{kq^k}{q^{n/4}}\right),$$

with an absolute implied constant. Moreover, $|\{b \in \mathbb{S}^1_{k,q} : b^2 = u\}| \in \{0, 1\}$ *and in the expression above,* $\overline{\Xi}(u)\cos(2\pi n\theta_{\Xi,j})$ *may be replaced by* $\mathrm{Re}(e(\theta_{\Xi,j})\Xi(u))$.

Remark 3.4. Almost all (i.e., a density $1 + O(1/q)$) super even $\Xi \in \widehat{\mathbb{S}}^1_{k,q}$ have conductor $2\kappa - 1$, but since we look at the $N \to \infty$ limit, we cannot restrict the sum in Proposition 3.3 to those characters only as in [Rudnick and Waxman 2019, Proof of Theorem 6.7] (with a $q \to \infty$ limit).

Proof. By [Rudnick and Waxman 2019, Lemma 6.4, Section 6.6], we have

$$X_{k,N}(u)_n = -\sum_{\Xi\neq 1}\overline{\Xi}(u)\,\mathrm{tr}\,\Theta_\Xi^n - \frac{R_{k,n}(u)q^\kappa}{q^{n/2}} - \frac{\delta_{u=1}q^\kappa}{q^{n/2}},$$

where, by the prime polynomial theorem [Rosen 2002, Theorem 2.2],

$$R_{k,n}(u) := \sum_{\substack{f\in\mathbb{F}_q[S]\ \text{monic}\\ \text{not prime}\\ \deg(f)=n}} \Lambda(f)\delta_{U(f)\in\mathrm{Sec}(u,k)} = \delta_{n\ \mathrm{even}}\,\frac{n}{2}\sum_{\substack{P\ \text{monic}\\ \text{prime}\\ \deg(P)=n/2}} \delta_{U(P^2)\in\mathrm{Sec}(u,k)} + O\left(\frac{q^{n/3}\tau(n)}{n}\right).$$

By the function field analogue of Dirichlet's theorem on primes in arithmetic progressions [Rosen 2002, Theorem 4.8], if n is even,

$$\begin{aligned}
-\frac{q^\kappa n}{2q^{n/2}} \sum_{\substack{P \text{ monic} \\ \text{prime} \\ \deg(P)=n/2}} \delta_{U(P^2)\in \mathrm{Sec}(u,k)} &= -\frac{q^\kappa n}{2q^{n/2}} \sum_{\substack{a\in R_{k,q} \\ a^2\equiv u \pmod * H_k}} \sum_{\substack{P \text{ monic} \\ \text{prime} \\ \deg(P)=n/2}} \delta_{P\equiv a \pmod * S^k} \\
&= -\frac{q^\kappa n}{2q^{n/2}} \sum_{\substack{a\in R_{k,q} \\ a^2\equiv u \pmod * H_k}} \left(\frac{1}{|R_{k,q}|}\frac{q^{n/2}}{n/2} + O\left(\frac{q^{n/4}k}{n}\right)\right) \\
&= -|\{a\in R_{k,q} : a^2 \equiv u \pmod * H_k\}| \left(\frac{1}{|H_k|} + O\left(\frac{q^\kappa k}{q^{n/4}}\right)\right) \\
&= -|\{b\in \mathbb{S}^1_{k,q} : b^2 = u\}| \left(1 + O\left(\frac{k|R_{k,q}|}{q^{n/4}}\right)\right).
\end{aligned}$$

Note that in odd characteristic, the cardinality $|\mathbb{S}^1_{k,q}| = q^\kappa$ is odd, so the function $(x \in \mathbb{S}^1_{k,q}) \mapsto x^2$ is injective, and $|\{b \in \mathbb{S}^1_{k,q} : b^2 = u\}| \in \{0, 1\}$.

Hence,

$$X_{k,N}(u)_n = -\sum_{\Xi\neq 1} \overline{\Xi}(u) \operatorname{tr} \Theta^n_\Xi - \frac{\delta_{u=1}q^\kappa}{q^{n/2}} + O\left(\frac{q^\kappa \tau(n)}{q^{n/6}n}\right) - \delta_{n \text{ even}} |\{b\in \mathbb{S}^1_{k,q} : b^2 = u\}| \left(1 + O\left(\frac{kq^k}{q^{n/4}}\right)\right),$$

which gives the result after splitting the sum over characters Ξ depending on the conductors $d(\Xi)$, which are odd integers. The last assertion follows from the invariance of the sum under $\Xi \mapsto \overline{\Xi}$. □

Proof of Theorem 1.14. The existence of the limiting distribution goes almost exactly as in [Cha 2008, Lemma 3.1, Theorem 3.2] (based on [Rubinstein and Sarnak 1994]). Let $\tilde{X}_{k,N}(\boldsymbol{u})$ be the random variable on $[1, N]$ defined by the right-hand side of the expression in Proposition 3.3, but without the error term. Let moreover

$$V := \big\{(\Xi, j) : \Xi \in \widehat{\mathbb{S}}^1_{k,q},\ \Xi \neq 1,\ 1 \le j \le d'(\Xi)\big\}. \tag{15}$$

There exists an explicit continuous function $g_{k,\boldsymbol{u}} : (\mathbb{R}/\mathbb{Z})^V \to \mathbb{R}^R$ such that

$$\tilde{X}_{k,N}(\boldsymbol{u}) = \big(g_{k,\boldsymbol{u}}(n\theta_{\Xi,j} : (\Xi, j) \in V)\big)_{n\le N.}$$

Note that $g_{k,\boldsymbol{u}}$ is bounded is (when k, q are fixed): each component is bounded by $2\kappa q^\kappa$.

By the Kronecker–Weyl equidistribution theorem, $\big(n\theta_{\Xi,j} : (\Xi, j) \in V\big)_{n\le N}$ converges in law (as $N \to \infty$) to a random vector equidistributed in the closure $\overline{\Gamma}$ of the torus

$$\Gamma = \{n(\theta_{\Xi,j})_{(\Xi,j)\in V} : n \in \mathbb{Z}\} \subset (\mathbb{R}/\mathbb{Z})^V. \tag{16}$$

It then follows from Helly's selection theorem [Billingsley 1986, Theorems 25.9–10] that $X_{k,N}(\boldsymbol{u})$ converges in law to a random vector $X_k(\boldsymbol{u})$ which corresponds to a measure $\mu_{k,\boldsymbol{u}}$ satisfying

$$\int_{\mathbb{R}^R} f(\boldsymbol{x})\, d\mu_{k,\boldsymbol{u}}(\boldsymbol{x}) = \int_{\overline{\Gamma}} (f \circ g_{k,\boldsymbol{u}})(\boldsymbol{x})\, d\boldsymbol{x} \tag{17}$$

for every bounded continuous $f : \mathbb{R}^R \to \mathbb{R}$. The limiting measure $\mu_{k,\boldsymbol{u}}$ is compactly supported from the boundedness of $g_{k,\boldsymbol{u}}$ (k, q fixed).

In particular, there is convergence of the moments, which allows us to compute the expected value by noting that

$$\left| \frac{1}{N} \sum_{f=2}^{\kappa} \sum_{j=1}^{f-1} \sum_{\substack{\Xi \in \widehat{\mathbb{S}}^1_{k,q} \\ d(\Xi)=2f-1}} \overline{\Xi}(u) \sum_{n=1}^{N} \cos(2\pi n \theta_{\Xi,j}) \right| \ll \frac{\kappa q^{\kappa}}{N} \xrightarrow{N\to\infty} 0. \qquad \square$$

3C. ***Properties of the limiting distribution under (generic) linear independence.*** For the next properties, we continue to use the methods of Rubinstein and Sarnak [1994] and others, in particular by studying characteristic functions.

Lemma 3.5 (Fourier transform). *For $u_1, \dots, u_R \in \mathbb{S}^1_{k,q}$ distinct, let $\mu_{k,\boldsymbol{u}}$ be the measure associated with the R-dimensional random vector $X_k(\boldsymbol{u})$. Its Fourier transform*

$$\hat{\mu}_{k,\boldsymbol{u}}(\boldsymbol{t}) := \int_{\mathbb{R}^R} e^{-i\boldsymbol{t}\cdot\boldsymbol{x}}\, d\mu_{k,\boldsymbol{u}}(\boldsymbol{x}) \qquad (\boldsymbol{t} \in \mathbb{R}^R)$$

is given by

$$\exp(i\boldsymbol{t}\cdot\boldsymbol{b}_k(\boldsymbol{u})) \int_{\overline{\Gamma}} \prod_{f=1}^{\kappa} \prod_{j=1}^{f-1} \prod_{\substack{\Xi \in \widehat{\mathbb{S}}^1_{k,q} \\ d(\Xi)=2f-1}} \exp\big(2i \operatorname{Re}(e(x_j)\boldsymbol{t}\cdot\Xi(\boldsymbol{u}))\big)\, d\boldsymbol{x},$$

where Γ is the torus (16) *and $\boldsymbol{b}_k(\boldsymbol{u}) := (|\{b \in \mathbb{S}^1_{k,q} : b^2 = u_r\}|/2)_{1\le r\le R}$, $\Xi(\boldsymbol{u}) := (\Xi(u_r))_{1\le r\le R}$. If Hypothesis 1.10 holds, then*

$$\hat{\mu}_{k,\boldsymbol{u}}(\boldsymbol{t}) = \exp(i\boldsymbol{t}\cdot\boldsymbol{b}_k(\boldsymbol{u})) \prod_{f=2}^{\kappa} \prod_{j=1}^{f-1} \prod_{\substack{\Xi \in \widehat{\mathbb{S}}^1_{k,q} \\ d(\Xi)=2f-1}} J_0(2|\boldsymbol{t}\cdot\Xi(\boldsymbol{u})|), \tag{18}$$

where $J_0(z) = \frac{1}{\pi}\int_0^{\pi} \cos(z\sin t)\, dt$ is the 0-th Bessel function of the first kind.

Proof. The first statement is a direct consequence of Proposition 3.3 and (17). For (18), under Hypothesis 1.10 the torus $\overline{\Gamma}$ is maximal and the integral splits as a product of integrals of the form

$$\int_{\mathbb{R}/\mathbb{Z}} \exp\big(2i \operatorname{Re}(e(x_j)\boldsymbol{t}\cdot\Xi(\boldsymbol{u}))\big)\, dx_j = J_0(2|\boldsymbol{t}\cdot\Xi(\boldsymbol{u})|)$$

by [Martin and Ng 2017, Lemma C.1]. $\square$

We now prove Theorem 1.15 about properties of the limiting distribution under Hypothesis 1.10.

Proof of Theorem 1.15. To show that $X_k(\boldsymbol{u})$ is absolutely continuous, it is enough to show that $\int_{\mathbb{R}^R} |\hat{\mu}_{k,\boldsymbol{u}}(\boldsymbol{t})|\, d\boldsymbol{t} < \infty$; see [Martin and Ng 2017, Lemma A.8(b)]. To do so, we partly follow the method of [Martin and Ng 2017, Section 4]. Since we assume Hypothesis 1.10, we may use (18) from Lemma 3.5:

$$|\hat{\mu}_{k,\boldsymbol{u}}(\boldsymbol{t})| \le \prod_{f=2}^{\kappa} \prod_{j=1}^{f-1} \prod_{\substack{\Xi \in \widehat{\mathbb{S}}^1_{k,q} \\ d(\Xi)=2f-1}} |\boldsymbol{t}\cdot\Xi(\boldsymbol{u})|^{-1/2} \le \Big[\prod_{\Xi\in S} |\boldsymbol{t}\cdot\Xi(\boldsymbol{u})|^2 \Big]^{-\frac{\kappa-1}{4}}$$

$$\le \Big[\frac{1}{|S_1(\boldsymbol{t})|} \sum_{\Xi\in S_1(\boldsymbol{t})} |\boldsymbol{t}\cdot\Xi(\boldsymbol{u})|^2 \Big]^{-\frac{\kappa-1}{4}}$$

where

$$S_1(\boldsymbol{t}) := \{\Xi \in \widehat{\mathbb{S}}^1_{2\kappa,q} \text{ primitive} : |\boldsymbol{t}\cdot\Xi(\boldsymbol{u})| > 1\} \subset S := \{\Xi \in \widehat{\mathbb{S}}^1_{2\kappa,q} \text{ primitive}\},$$

since $|J_0(z)| \le \min(1, \sqrt{2/(\pi|z|)})$ for all $z \in \mathbb{R}$ (see [Martin and Ng 2017, Lemma C.2]). If $\boldsymbol{t} \in \boldsymbol{T} := \{\boldsymbol{t} \in \mathbb{R}^R : |S_1(\boldsymbol{t})| \ge 1\}$, we get

$$\frac{1}{|S_1(\boldsymbol{t})|} \sum_{\Xi\in S_1(\boldsymbol{t})} |t\cdot\Xi(\boldsymbol{u})|^2 \ge \frac{1}{|S|} \sum_{\Xi\in S} |t\cdot\Xi(\boldsymbol{u})|^2 = \sum_{r,r'=1}^{R} t_r \overline{t_{r'}} \frac{1}{|S|} \sum_{\Xi\in S} \Xi(u_r)\overline{\Xi}(u_{r'}).$$

By the orthogonality relations and Möbius inversion,

$$\frac{1}{|S|} \sum_{\Xi\in S} \Xi(u_r)\overline{\Xi}(u_{r'}) = \frac{1}{|S|} \sum_{f=2}^{\kappa} \mu(S^{2(\kappa-f)}) \sum_{\Xi\in\widehat{\mathbb{S}}^1_{2f,q}} \Xi(u_r)\overline{\Xi}(u_{r'}) = \frac{q^\kappa \delta_{u_r=u_{r'}}}{|S|} = \frac{\delta_{u_r=u_{r'}}}{1-1/q}.$$

Since the u_i are distinct, it follows that

$$\frac{1}{|S_1(\boldsymbol{t})|} \sum_{\Xi\in S_1(\boldsymbol{t})} |\boldsymbol{t}\cdot\Xi(\boldsymbol{u})|^2 \ge \|\boldsymbol{t}\|^2 \qquad \text{if } |S_1(\boldsymbol{t})| \ge 1.$$

Therefore, if $\boldsymbol{t} \in \boldsymbol{T}$, then $|\hat{\mu}_{k,\boldsymbol{u}}(\boldsymbol{t})| \le \|\boldsymbol{t}\|^{-(\kappa-1)/2}$. On the other hand, if $\boldsymbol{t} \notin \boldsymbol{T}$, the same argument shows that

$$1 \ge \frac{1}{|S|} \sum_{\Xi\in S} |\boldsymbol{t}\cdot\Xi(\boldsymbol{u})| \ge \|\boldsymbol{t}\|^2,$$

i.e., $\mathbb{R}^R \backslash \boldsymbol{T}$ is bounded. It also contains a neighborhood of $\mathbf{0}$ since it contains the finite intersection $\bigcap_{\Xi\in S}\{\boldsymbol{t} \in \mathbb{R}^R : |\boldsymbol{t}\cdot\Xi(\boldsymbol{u})| < 1\}$ of open sets containing $\mathbf{0}$.

Thus, there exists $\varepsilon > 0$ such that

$$\int_{\mathbb{R}^R} |\hat{\mu}_{k,\boldsymbol{u}}(\boldsymbol{t})|\, d\boldsymbol{t} \ll \int_{\|\boldsymbol{t}\|\le 1} |\hat{\mu}_{k,\boldsymbol{u}}(\boldsymbol{t})|\, d\boldsymbol{t} + \int_{\mathbb{R}^R \backslash B_\varepsilon(\mathbf{0})} \|\boldsymbol{t}\|^{-(\kappa-1)/2}\, d\boldsymbol{t},$$

and the second integral converges when $\kappa - 1 > 2R$; see [Martin and Ng 2017, p. 22]. This concludes the proof of (1).

Concerning (2), the symmetry/exchangeability follow from the expression (18) for $\hat{\mu}_{k,\boldsymbol{u}}$.

The last statements of the theorem follow from the previous ones: since $\mu_{k,\boldsymbol{u}}$ is absolutely continuous, $A = \{\boldsymbol{x} \in \mathbb{R}^R : x_1 < \cdots < x_R\}$ is a continuity set, so that by the portmanteau theorem,

$$\lim_{N\to\infty} \mathbb{P}\big(X_{k,N}(u_1) < \cdots < X_{k,N}(u_R)\big) = \mu_{k,\boldsymbol{u}}(A). \qquad \square$$

Finally, we prove Corollary 1.17 (unconditional properties of the limiting distribution) assuming Theorem 1.11 on generic linear independence.

Proof of Corollary 1.17. (1) It suffices to show it when $R = 1$, i.e., that the random variable $X_k(u)$ is continuous for every $u \in \mathbb{S}^1_{k,q}$. We follow the argument in [Devin 2019, Proof of Theorem 2.2]; see also [Devin and Meng 2018, Proposition 2.1]. By Wiener's lemma, it suffices to show that

$$\lim_{S\to\infty} \frac{1}{S} \int_{-S}^{S} |\hat{\mu}_{k,u}(t)|^2 \, dt = 0. \tag{19}$$

By Lemma 3.5, $|\hat{\mu}_{k,u}(t)| \le |\int_{\overline{\Gamma}} \exp(it\phi(\boldsymbol{x}))\, d\boldsymbol{x}|$, where

$$\phi(\boldsymbol{x}) := 2 \sum_{f=1}^{\kappa} \sum_{j=1}^{f-1} \sum_{\substack{\Xi \in \widehat{\mathbb{S}}^1_{k,q} \\ d(\Xi)=2f-1}} \cos(2\pi x_j)\, \Xi(u).$$

By Theorem 1.11, there exists $\Xi \in \widehat{\mathbb{S}}^1_{k,q}$ and $1 \le j \le d'(\Xi)$ such that $\theta_{\Xi,j} \notin \mathbb{Q}$. It follows that the function $\phi : \overline{\Gamma} \to \mathbb{R}$ is analytic and nonconstant, since $\Xi(u) \ne 0$ (being a root of unity). Thus, the scaling principle [Stein 1993, VIII.2, Proposition 5] shows that $|\hat{\mu}_{k,u}(t)| \ll |t|^{-\alpha}$ for some constant $\alpha > 0$, where α and the implied constant can depend on all parameters but t. Thus, (19) holds, using the trivial bound $|\hat{\mu}_{k,u}(t)| \le 1$ around 0.

(2) This is a consequence of the proof of Theorem 1.14: $\overline{\Gamma}$ is a subtorus of $(\mathbb{R}/\mathbb{Z})^V$, with V as in (15), and if the set of the $\theta_{\Xi,j}$ ($(\Xi, j) \in V$) contains at least t linearly independent elements, then $\dim \overline{\Gamma} \ge t$. By Theorem 1.11, the latter holds whenever $t = o(\log |\mathbb{S}^1_{k,q}|)$. $\square$

4. Prime polynomials in short intervals

4A. *Definitions and cohomological interpretation.*

Definition 4.1. Let $Q \in \mathbb{F}_q[T]$ be nonconstant.

- A Dirichlet character χ modulo Q is a character of $(\mathbb{F}_q[T]/(Q))^\times$.
- The character χ is *even* if it is trivial on $\mathbb{F}_q^\times$.
- It is *primitive* if it is not induced from a character modulo a proper divisor $Q' \mid Q$ through the natural map $(\mathbb{F}_q[T]/(Q))^\times \to (\mathbb{F}_q[T]/(Q'))^\times$. The *conductor* of χ is the monic divisor $Q' \mid Q$ of smallest degree such that χ is primitive modulo Q'.
- As usual, we may extend χ as $\chi : \mathbb{F}_q[T] \to \mathbb{C}$ by defining $\chi(f) = \chi(f \pmod{*Q})$ if $(f, Q) = 1$, $\chi(f) = 0$ otherwise.

- The number of Dirichlet characters modulo Q is denoted by $\varphi(Q)$. The number of even (resp. primitive, even primitive) such characters is $\varphi^{\mathrm{ev}}(Q) = \varphi(Q)/(q-1)$ (resp. $\varphi_{\mathrm{prim}}(Q)$, $\varphi^{\mathrm{ev}}_{\mathrm{prim}}(Q)$).
- The *L-function* of χ is
$$L(\chi, T) = \prod_{\substack{P \text{ prime} \\ \text{monic} \\ P \nmid Q}} (1 - \chi(P) T^{\deg P})^{-1}.$$

We recall that if $\deg(Q) \geq 2$ and $\chi \neq 1$, then $L(\chi, T)$ is a polynomial (rather than a formal power series) of degree $\deg(Q) - 1$; see [Rosen 2002, Proposition 4.3 and p. 130].

If χ is even, then $L(\chi, T)$ has a "trivial" zero at $T = 1$. As in [Keating and Rudnick 2014, (3.34)], we define $\lambda_\chi = \delta_{\chi \text{ even}}$, which allows to factor

$$L(\chi, T) = (1 - \lambda_\chi T) L^*(\chi, T), \quad L^*(\chi, T) \in \mathbb{F}_q[T].$$

If χ is primitive, Weil's work on the Riemann hypothesis over finite fields (see [Rosen 2002, Chapters 4, 5]) shows that

$$L^*(\chi, T) = \det(1 - \sqrt{q} T \Theta_\chi), \quad \Theta_\chi \in U_{\deg(Q)-1-\lambda_\chi}(\mathbb{C}), \tag{20}$$

and we let

$$e(\theta_{\chi,j}), \quad (1 \leq j \leq \deg(Q) - 1 - \lambda_\chi), \quad \theta_{\chi,j} \in [0, 1],$$

be the eigenvalues of Θ_χ^{-1}. This is also reflected in the following result:

Theorem 4.2 (Katz). *Let $\mathbb{F}_q$ be a finite field of odd characteristic p, $m \geq 2$ be an integer,*

$$E = \mathbb{Q}\left(\zeta_{m-2}, \zeta_{4p^r} : 1 \leq r \leq 1 + \frac{\log m}{\log p}\right) \subset \mathbb{Q}(\zeta_{p^\infty}, \zeta_n)$$

with ring of integers $\mathcal{O}$, and let $\lambda \in \Lambda := \mathrm{Spec}_p(\mathcal{O})$.

(1) *There exists a unipotent group $\mathbb{W}_m$ over $\mathbb{F}_p$ such that $\mathbb{W}_m(\mathbb{F}_q)$ is the group of even characters modulo $T^m \in \mathbb{F}_q[T]$, as well as an open set $\mathrm{Prim}_m \subset \mathbb{W}_m$ such that $\mathrm{Prim}_m(\mathbb{F}_q)$ is the set of primitive even characters modulo T^m.*

(2) *There exists a lisse sheaf $\mathcal{G}_{m,\lambda}$ on Prim_m of free $\mathcal{O}_\lambda$-modules, of rank $m-2$, pure of weight 1, such that for every $\chi \in \mathrm{Prim}_m(\mathbb{F}_q)$,*

$$\det(1 - T \operatorname{Frob}_{q,\chi} \mid \mathcal{G}_{m,\lambda}) = L^*(\chi, T),$$

which is a polynomial of degree $m-2$. In particular, the family $(\mathcal{G}_{m,\lambda})_{\lambda \in \Lambda}$ forms a compatible system.

(3) *The Tate twist $\mathcal{F}_{m,\lambda} = \mathcal{G}_{m,\lambda}\left(\frac{1}{2}\right)$ is a lisse sheaf of free $\mathcal{O}_\lambda$-modules on Prim_m, pure of weight zero, of rank $m-2$.*

In other words, the eigenvalues of $\sqrt{q}\Theta_\chi$ (the zeros of $L^*(\chi, T)$) are the eigenvalues of $\mathrm{Frob}_{\mathbb{F}_q}$ acting on the stalk of $\mathcal{G}_{m,\lambda}$ at χ.

Proof. This is essentially the contents of [Katz 2013b, Sections 1–4]. The addition of ζ_{m-2} is not necessary at this point, but will be useful in Theorem 5.12. □

4B. ***Existence of the limiting distribution.*** We start with an explicit formula for $X_{m,N}(\boldsymbol{B})$, and proceed as in Section 3B.

Proposition 4.3. *Under the notations of Section 1C, we have, for $B \in \mathbb{F}_q[T]$ monic of degree $m-1$,*

$$X_{m,N}(B)_n = -\sum_{f=3}^{m} \sum_{\substack{\chi \pmod * T^m \text{ even} \\ \mathrm{cond}(\chi)=T^f}} \sum_{j=1}^{f-2} \overline{\chi}(B^*) e(\theta_{\chi,j}) + \frac{1}{q^{n/2}},$$

where $B^* \in \mathbb{F}_q[T]$ is the reflected polynomial defined by $B^*(T) = T^{\deg B} B(1/T)$.

Proof. By [Keating and Rudnick 2014, (4.22)],

$$X_{m,N}(B)_n = \frac{1}{q^{n/2}} \sum_{\substack{\chi \pmod * T^m \\ \text{even}}} \overline{\chi}(B^*)\psi(n,\chi), \qquad \psi(n,\chi) := \sum_{\substack{f \in \mathbb{F}_q[T] \\ \deg(f)=n}} \Lambda(f)\chi(f) = -q^{n/2}\,\mathrm{tr}(\Theta_\chi^n) - 1,$$

where the last equality is the explicit formula for ψ (see [Keating and Rudnick 2014, (3.38)]), obtained by taking the logarithmic derivative on both sides of (20). Thus,

$$X_{m,N}(B)_n = \frac{1}{q^{n/2}} \sum_{\substack{\chi \pmod * T^m \\ \text{even}}} \overline{\chi}(B^*)\,\mathrm{tr}(\Theta_\chi^n) - \frac{1}{q^{n/2}} \sum_{\substack{\chi \pmod * T^m \\ \text{even}}} \overline{\chi}(B^*).$$

The result follows after splitting the first sum according to the conductor of χ and applying the orthogonality relations in $(\mathbb{F}_q[T]/(T^m))^\times/\mathbb{F}_q^\times$ to the second sum. □

Then, the proof of Theorem 1.21 is exactly like the proof of Theorem 1.14 (see Section 3B). As in Proposition 3.3, one may replace the $e(\theta_{\chi,j})$ in Proposition 4.3 by $\cos(2\pi\theta_{\chi,j})$ since $X_{m,N}(B)_n \in \mathbb{R}$.

4C. ***Properties of the limiting distribution under (generic) linear independence.*** Again, the proofs of Theorem 1.23 and Corollary 1.24 are exactly like the proofs of Theorem 1.15 and Corollary 1.17 respectively, in Section 3C.

5. An extension of the large sieve for Frobenius

In the next two sections, we set up the tools to prove the main Theorems 1.1, 1.11 and 1.20 on generic linear independence. As outlined in Section 1D, the strategy follows that of previous works and is the following:

(1) Obtain information about integral monodromy groups of reductions of sheaves of $\mathcal{O}_\lambda$-modules from Theorem 2.1 and 3.2, for a set of ideals/valuations $\lambda \in \mathrm{Spec}_{1,p}(\mathcal{O})$ of positive density.

(2) Use a variant of the large sieve for Frobenius to show that for all such λ, the (splitting) fields generated by the roots ($\alpha_{i,f,p}(x)$, $e(\theta_{\Xi,j})$ or $e(\theta_{\chi,j})$) are maximal for almost all tuples of arguments x (resp. Ξ, χ) for exponential sums (resp. (super-)even characters).

(3) Apply Girstmair's work to show that (2) implies the desired linear independence.

The first two points and the variant of the large sieve for Frobenius are implemented in this section, and the third point in Section 6.

Remark 5.1. Note that [Kowalski 2008b; Cha et al. 2017] dealt with symplectic and orthogonal monodromy types. Here, we need to consider special linear and symplectic ones, which will correspond to splitting fields with Galois groups $\mathfrak{S}_n$ (the full symmetric group), or $W_{2n} \leq \mathfrak{S}_{2n}$, the subgroup with order $2^n n!$ of permutations of n pairs (the Coxeter group B_n).

Remark 5.2. We consider ideals of degree 1 so that $\mathbb{F}_\lambda = \mathbb{F}_\ell$ and considerations on the sheaves mod λ can be reduced as much as possible to existing arguments, for the large sieve or computations of integral monodromy groups. This is actually not a restriction because $\mathrm{Spec}_{1,p}(\mathcal{O})$ has natural density 1 in $\mathrm{Spec}(\mathcal{O})$ [Narkiewicz 2004, Corollary 2, p. 345, Proposition 7.17].

Remark 5.3. Since we considered Tate-twisted/normalized sheaves of $\mathcal{O}_\lambda$-modules from the beginning (which also forces the determinant to be trivial and the arithmetic/geometric monodromy groups to coincide, for exponential sums and super-even characters), we will not encounter the difficulty observed in [Kowalski 2008b; Cha et al. 2017] that the normalized characteristic polynomials may be defined over a quadratic extension of the base field, with the possibility of a different Galois group. This was overcome in ibid. by looking at squares of the roots, and showing that their Galois group was still maximal from a study of additive relations, in addition to the multiplicative ones.

5A. ***Integral monodromy groups.*** The lisse sheaves $\mathcal{F}_\lambda$ of free modules on a variety X given by Theorems 2.1, 3.2 and 4.2 correspond to continuous representations $\rho_\lambda : \pi_1(X, \bar{\eta}) \to \mathrm{GL}_r(\mathcal{O}_\lambda)$, for $\bar{\eta}$ a geometric generic point, such that, for every $x \in X(\mathbb{F}_q)$, if $\mathrm{Frob}_{x,q} \in \pi_1(X, \bar{\eta})^\sharp$ is the geometric Frobenius conjugacy class at x, then $\rho_\lambda(\mathrm{Frob}_{x,q}) \in \mathrm{GL}_r(\mathcal{O}_\lambda)^\sharp$ gives the action of Frob_q on $(\mathcal{F}_\lambda)_x$.

Definition 5.4 (monodromy groups). The *geometric and arithmetic monodromy groups* of ρ_λ are respectively

$$G_\lambda^{\mathrm{geom}} := \overline{\rho_\lambda(\pi_1^{\mathrm{geom}}(X, \bar{\eta}))}^{\mathrm{Zar}} \leq G_\lambda := \overline{\rho_\lambda(\pi_1(X, \bar{\eta}))}^{\mathrm{Zar}} \leq \mathrm{GL}_r(\overline{E_\lambda}),$$

where $\overline{\cdot}^{\mathrm{Zar}}$ denotes Zariski closure in $\mathrm{GL}_r(\overline{E_\lambda})$. By reducing modulo λ, we also obtain representations $\tilde{\rho}_\lambda : \pi_1(X, \bar{\eta}) \to \mathrm{GL}_r(\mathbb{F}_\lambda)$, and we define the *geometric and arithmetic integral monodromy groups* of ρ_λ as the monodromy groups

$$\widetilde{G}_\lambda^{\mathrm{geom}} := \tilde{\rho}_\lambda(\pi_1^{\mathrm{geom}}(X, \bar{\eta})) \leq \widetilde{G}_\lambda := \tilde{\rho}_\lambda(\pi_1(X, \bar{\eta})) \leq \mathrm{GL}_r(\mathbb{F}_\lambda)$$

of $\tilde{\rho}_\lambda$. If the adjective "projective" is added to those groups, one refers to their image with respect to the projections $\mathrm{GL}_r \to \mathrm{PGL}_r$ (over $\overline{E_\lambda}$ or $\mathbb{F}_\lambda$ respectively).

5A1. *From monodromy to integral monodromy.* The determination of integral monodromy groups may be more challenging that their counterparts over $\overline{E_\lambda}$, since they have less structure (under purity assumption, the connected component at the identity of $G_\lambda^{\mathrm{geom}}$ is a semisimple algebraic group).

Fortunately, as explained by [Katz 2012b, Section 7], one may use deep results of [Larsen and Pink 1992; Larsen 1995] to conclude (roughly) that if the monodromy over $\overline{E_\lambda}$ is as large as possible, then the same holds for a density 1 of the integral monodromy groups.

Katz's argument is given for sheaves of $\mathbb{Z}_\ell$-modules, but carries over more generally to sheaves of $\mathcal{O}_\lambda$-modules: we spelled out the details in [Perret-Gentil 2018a, Section 5.2], and the conclusion reads as:

Theorem 5.5. *Let X be a smooth affine geometrically connected variety over $\mathbb{F}_p$, let $E \subset \mathbb{C}$ be a Galois number field with ring of integers $\mathcal{O}$, and let Λ be a set of valuations on $\mathcal{O}$ of natural density* 1. *Let $(\mathcal{F}_\lambda)_{\lambda\in\Lambda}$ be a compatible system with $\mathcal{F}_\lambda$ a lisse sheaf of free $\mathcal{O}_\lambda$-modules on X. We assume that*

> *there exists $G \in \{\mathrm{SL}_n, \mathrm{Sp}_{2n}\}$ such that for every $\lambda \in \Lambda$, the arithmetic monodromy group of $\mathcal{F}_\lambda$ is conjugate to $G(\overline{E_\lambda})$.*

Then there exists a subset $\Lambda_p \subset \Lambda \cap \mathrm{Spec}_{1,p}(\mathcal{O})$ of natural density 1, *depending on p and on the family, such that $\mathcal{F}_\lambda$ has geometric and arithmetic integral monodromy groups conjugate to $G(\mathbb{F}_\lambda)$ for all $\lambda \in \Lambda_p$.*

Remark 5.6 (implied constants). The dependency of the sets of valuations on some of the variables p, k, m in Theorems 5.10, 5.11 and 5.12 will give dependencies on those of the implied constants in the final results.

Remark 5.7 (strong approximation). Another method to get information on integral monodromy groups from the transcendental ones is through strong approximation results for arithmetic groups, as explained in [Katz 2012b, Section 9] (see also [Jouve et al. 2013, Section 5]); this is for example used in [Cha et al. 2017]. In those cases, [Pink 2000] (a generalization of [Matthews et al. 1984; Weisfeiler 1984]) allows to show that the integral monodromy is large for all but finitely many primes. Moreover, by also using results of [Larsen and Pink 1992], it avoids the classification of finite simple groups, unlike [Matthews et al. 1984; Weisfeiler 1984].

However, this requires that the sheaves $\mathcal{F}_\lambda$ on X may be formed over the analytification X^{an}: a sheaf $\mathcal{F}^{\mathrm{an}}$ of finitely generated $\mathcal{O}$-modules is constructed on X^{an}, whose extension of scalars to $\mathcal{O}_\lambda$ corresponds to the analytification of $\mathcal{F}_\lambda$, and strong approximation can then be applied to the monodromy of $\mathcal{F}^{\mathrm{an}}$ in $G(\mathcal{O})$ to yield the result. This can be done in the case of families of L-functions considered in [Katz 2012b; Cha et al. 2017], but a priori not for the sheaves from Theorems 2.1 and 3.2 (one may think about Artin–Schreier sheaves, i.e., Kloosterman sheaves of rank 1, as a first example).

5A2. *Kloosterman and Birch sheaves.* Combining Theorem 5.5 with the determination of monodromy groups over $\bar{E}_\lambda$ by Katz, we obtain the following:

Theorem 5.8 (Kloosterman sheaves). *In the setting of Theorem 2.1, there exists a subset $\Lambda_{r,p}$ of $\mathrm{Spec}_{1,p}(\mathcal{O})$, of natural density* 1, *such that for every $\lambda \in \Lambda_{r,p}$, the arithmetic and geometric integral monodromy groups of $\mathcal{K}l_{r,\lambda}$ are equal and conjugate to $\mathrm{SL}_r(\mathbb{F}_\lambda)$ if r is odd, $\mathrm{Sp}_r(\mathbb{F}_\lambda)$ if r is even.*

Proof. This follows from Theorem 5.5 and the determination of monodromy groups over $\bar{E}_\lambda$ contained in [Katz 1988, Chapter 11]. □

Remark 5.9. By work of Hall [2008] or J-K. Yu (unpublished) when $r = 2$, and the author [Perret-Gentil 2018b] for any $r \geq 2$, one may actually take

$$\Lambda_{r,p} = \{\lambda \in \mathrm{Spec}_{1,p}(\mathcal{O}) \text{ above } \ell : \ell \gg_r 1\}. \tag{21}$$

In particular, the densities of elements $\Lambda_{r,p}$ with bounded norm are bounded from below independently of p.

Theorem 5.10 (Birch sheaves). *In the setting of Theorem 2.1*(2), *there exists a subset* Λ_p *of* $\mathrm{Spec}_{1,p}(\mathcal{O})$, *of natural density* 1, *such that for every* $\lambda \in \Lambda_p$, *the arithmetic and geometric integral monodromy groups of* $\mathcal{B}i_\lambda$ *are equal to* $\mathrm{SL}_2(\mathbb{F}_\lambda)$.

Proof. This follows from Theorem 5.5 and the determination of monodromy groups over E_λ in [Katz 1990, 7.12]. □

5A3. *Primitive super-even characters.*

Theorem 5.11. *In the setting of Theorem 3.2* (3), *assuming that* $k \geq 4$, *there exists a subset* $\Lambda_{k,p} \subset \mathrm{Spec}_{1,p}(\mathcal{O})$ *of natural density* 1 *such that for every* $\lambda \in \Lambda_{k,p}$, *the arithmetic and geometric integral monodromy groups of* $\mathcal{G}_{k,\lambda}$ *are equal and conjugate to* $\mathrm{Sp}_{2\kappa-2}(\mathbb{F}_\lambda)$.

Proof. This follows from Theorem 5.5 and the determination of monodromy groups over E_λ in [Katz 2017, Theorem 2.5] (using results from [Katz 2005, 3.10]). □

5A4. *Primitive even characters mod* T^m.

Theorem 5.12. *In the setting of Theorem 4.2* (3), *assuming that* $m \geq 5$ *is odd*, *there exists a subset* $\Lambda_{m,p} \subset \mathrm{Spec}_{1,p}(\mathcal{O})$ *of natural density* 1 *such that for every* $\lambda \in \Lambda_{m,p}$, *the projective arithmetic and geometric integral monodromy groups of* $\mathcal{G}_{m,\lambda}$ *are conjugate to* $\mathrm{PSL}_{m-2}(\mathbb{F}_\lambda)$.

Proof. By, [Katz 2013b, Theorem 5.1],

$$\mathrm{SL}_{m-2}(\mathbb{C}) \leq G_{\mathrm{geom}}(\mathcal{G}_{m,\lambda}) \leq G_{\mathrm{arith}}(\mathcal{G}_{m,\lambda}) \leq \mathrm{GL}_{m-2}(\mathbb{C}),$$

whence $PG_{\mathrm{geom}}(\mathcal{G}_{m,\lambda}) = PG_{\mathrm{arith}}(\mathcal{G}_{m,\lambda}) = \mathrm{PGL}_{m-2}(\mathbb{C})$.

However, projective representations are not directly handled in Theorem 5.5. Instead, we note that if $\lambda \in \mathrm{Spec}_{1,p}(\mathcal{O})$ is above $\ell \nmid m-2$, then $\ell \equiv 1 \pmod{m-2}$ (by the characterization of ideals of degree 1 in cyclotomic extensions), so Hensel's lemma implies that every element of $\mathcal{O}_\lambda$ has an $(m-2)$-th root, whence $\mathrm{PGL}_{m-2}(\mathcal{O}_\lambda) \cong \mathrm{SL}_{m-2}(\mathcal{O}_\lambda)$.

If $\mathcal{G}_{m,\lambda}$ corresponds to a representation $\rho_\lambda : \pi_1(X, \bar{\eta}) \to \mathrm{GL}_{m-2}(\mathcal{O}_\lambda)$ and $\pi : \mathrm{GL}_{m-2} \to \mathrm{PGL}_{m-2}$ is the projection, we get in this case a continuous representation $\pi \circ \rho_\lambda : \pi_1(X, \bar{\eta}) \to \mathrm{SL}_{m-2}(\mathcal{O}_\lambda)$ with transcendental arithmetic and geometric monodromy groups isomorphic to $\mathrm{SL}_{m-2}(\mathbb{C})$. We may then apply Theorem 5.5 to get that the arithmetic and geometric integral monodromy of $\pi \circ \rho_\lambda$ are

$\mathrm{SL}_{m-2}(\mathbb{F}_\lambda) \cong \mathrm{PGL}_{m-2}(\mathbb{F}_\lambda)$ for a subset of density 1 of $\mathrm{Spec}_{1,p}(\mathcal{O})$. Since $\mathrm{im}(\pi \circ \rho_\lambda \pmod *\lambda) = \pi(\mathrm{im}\,\rho_\lambda \pmod *\lambda)$, this proves the assertion on the projective monodromy groups of $(\mathcal{G}_{m,\lambda})_\lambda$. □

5B. ***Large sieve for Frobenius, with wild ramification.*** Next, we need a version of the large sieve for Frobenius, originally developed in [Kowalski 2006]; see also [Kowalski 2008a; 2008b].

In these works as well as in [Cha et al. 2017], the sieve applies to sheaves of $\mathbb{F}_\ell$-modules on a variety X over $\mathbb{F}_p$, that either

(1) are compatible systems, with X a curve;

(2) are tamely ramified;

(3) have monodromy group of cardinality prime to p, a stronger condition than the previous one.

For Kloosterman and Birch sums, (1) applies. However, for super-even characters, the variety is not a curve, and the sheaves are a priori not tamely ramified, which rules out (2). Concerning (3), note that for $E = \mathbb{Q}(\zeta_{p^N})$ and $\lambda \in \mathrm{Spec}(\mathcal{O})$, the prime p always divides $|\mathrm{SL}_r(\mathbb{F}_\lambda)|$ and $|\mathrm{Sp}_r(\mathbb{F}_\lambda)|$ (if r is even).

5B1. *Extension of the large sieve for Frobenius.* Instead, we give an extension of [Kowalski 2006, Theorem 3.1; 2008b, Theorems 4.1, 4.3] that works in this case and answers the question in [Kowalski 2006, Remark 4.8]. To bound the sums of Betti numbers that appear, we give two arguments:

(1) Theorem 5.14(b), involving sums of Betti numbers associated to tensor powers of the sheaves, inspired by [Kowalski 2006, Section 4; Katz and Sarnak 1999, Theorem 9.2.6; Katz 2017, Lemma 5.2] and an effective/modular version of a theorem of Burnside on irreducible representations contained in tensor powers of faithful representations.

(2) Theorem 5.14(c), provided by Will Sawin, reducing to the tame case (where a result of Deligne [Illusie 1981] on the Euler characteristic of tamely ramified sheaves can be applied) by exploiting the presence of a compatible system. This gives a much stronger bound, but with less explicit constants.

Definition 5.13. Let X be a smooth affine geometrically connected algebraic variety over $\mathbb{F}_p$, E be a number field with ring of integers $\mathcal{O}$, let $\lambda, \lambda' \in \mathrm{Spec}_{1,p}(\mathcal{O})$, and let $\mathcal{F}$ be a lisse sheaf of R-modules on X, where $R = \overline{\mathbb{Q}}_\ell$, $\mathcal{O}_\lambda$, $\mathcal{O}_\lambda \otimes \mathcal{O}_{\lambda'}$, $\mathbb{F}_\lambda$, or $\mathbb{F}_\lambda \otimes \mathbb{F}_{\lambda'}$. We define the sum of Betti numbers

$$\sigma_c(X, \mathcal{F}) = \sum_{i=0}^{2\dim X} \mathrm{rank}\, H_c^i(X, \mathcal{F}),$$

where the rank of an R-module is defined as its dimension over the total ring of fractions of R (recall that these cohomology groups are finitely generated by [SGA 4½ 1977, Exposé 1, Théorème 4.6.2]).

G	$\dim G$	$\mathrm{rank}\, G$	E_G	Type	Weyl group
SL_r	r^2-1	$r-1$	$\frac{1}{2}(2r^2+r-3)$	A_{r-1}	$\mathfrak{S}_r$
Sp_r	$\frac{1}{2}(r(r+1))$	$r/2$	$\frac{1}{4}(r(2r+3))$	$C_{r/2}$	$W_r \leq \mathfrak{S}_r$

Table 1. Reminder of certain invariants for the groups considered.

If X is a curve and $R = \mathcal{O}_\lambda$, we moreover define

$$\mathrm{cond}(\mathcal{F}_\lambda) = 1 - \chi_c(X, \mathbb{Q}_\ell) + 2\sum_x \mathrm{Swan}_x(\mathcal{F}_\lambda)$$

to be the quantity in [Kowalski 2006, (4.1)] (see also [Katz 1988, Chapters 1–2]), where the sum is over "points at infinity" of X.

Theorem 5.14. *Let X be a smooth affine geometrically connected algebraic variety of dimension d over $\mathbb{F}_p$. For E a number field with ring of integers $\mathcal{O}$, let $\Lambda \subset \mathrm{Spec}_{1,p}(\mathcal{O})$ with lower density*

$$\delta_\Lambda := \liminf_{L\to\infty} \frac{|\{\lambda \in \Lambda : N(\lambda) \le L\}|}{L/\log L} > 0.$$

For every $\lambda \in \Lambda$, let $\mathcal{F}_\lambda$ be a rank r lisse sheaf of $\mathbb{F}_\lambda$-modules on X, corresponding to a representation

$$\rho_\lambda : \pi_1(X, \bar\eta) \to \mathrm{GL}_r(\mathbb{F}_\lambda), \tag{22}$$

for $\bar\eta$ a geometric generic point. We assume that there exists $G \in \{\mathrm{SL}_r, \mathrm{Sp}_r\}$ such that either

(i) *the arithmetic and geometric monodromy groups of ρ_λ are equal and conjugate to $G(\mathbb{F}_\lambda)$ for all $\lambda \in \Lambda$; or*

(ii) *the **projective** arithmetic and geometric monodromy group of ρ_λ are equal and conjugate to $\mathrm{PGL}_r(\mathbb{F}_\lambda)$ for all $\lambda \in \Lambda$, and $\zeta_r \in E$, so that $\mathrm{PGL}_r(\mathbb{F}_\lambda) = \mathrm{SL}_r(\mathbb{F}_\lambda) = G(\mathbb{F}_\lambda)$.*[4]

Let $t \ge 1$ be an integer. For every $\lambda \in \Lambda$, let $\mathbf{\Omega}_\lambda \subset G(\mathbb{F}_\lambda)^t$ be a conjugacy-invariant subset, such that

$$\delta_{\mathbf{\Omega}} := \sup_{\lambda\in\Lambda} \frac{|\mathbf{\Omega}_\lambda|}{|G(\mathbb{F}_\lambda)|^t} < 1.$$

Then, for any field $\mathbb{F}_q$ of characteristic p and any $L \ge 1$,

$$\begin{aligned} P\big(q, (\mathcal{F}_\lambda, \mathbf{\Omega}_\lambda)_{\lambda\in\Lambda}\big) &:= \frac{|\{\boldsymbol{x} \in X(\mathbb{F}_q)^t : (\rho_\lambda(\mathrm{Frob}_{x_i,q}))_i \in \mathbf{\Omega}_\lambda \text{ for all } \lambda \in \Lambda\}|}{|X(\mathbb{F}_q)|^t} \\ &\ll \frac{1}{(1-\delta_{\mathbf{\Omega}})\delta_\Lambda} \frac{\log L}{L}\left(1 + \frac{tC(L, (\mathcal{F}_\lambda)_{\lambda\in\Lambda})^t}{q^{1/2}}\right), \end{aligned}$$

where

(a) *if $d = 1$, $C(L, (\mathcal{F}_\lambda)_{\lambda\in\Lambda}) \ll r^{\delta_{G=\mathrm{SL}_r}} L^{\dim G + ((\mathrm{rank}\, G)/2)} \max_{N(\lambda)\le L} \mathrm{cond}(\mathcal{F}_\lambda)$;*

(b) *if $d \ge 1$, $C(L, (\mathcal{F}_\lambda)_{\lambda\in\Lambda}) \ll d L^{\dim G} \max_{N(\lambda)\le L} \max_{M \le N(\lambda)^{M_G}} \sigma_c(X, \mathcal{F}_\lambda^{\otimes M})^2$, with $M_G = \mathrm{rank}(G)(\mathrm{rank}(G)+1)/2$;*

(c) *if the representations (22) arise from a compatible system $\rho : \pi_1(X, \bar\eta) \to \mathrm{GL}_r\big(\prod_{\lambda\in\Lambda} \mathcal{O}_\lambda\big)$, and X has a compactification where it is the complement of a divisor with normal crossing, then*

$$C(L, (\mathcal{F}_\lambda)_{\lambda\in\Lambda}) \ll L^{\dim G + 1} r^{\delta_{G=\mathrm{SL}_r}} (r + C(X, \rho_{\lambda_0})),$$

where $C(X, \rho_{\lambda_0})$ only depends on X and ρ_{λ_0} for an arbitrary fixed $\lambda_0 \in \Lambda$.

[4] See the proof of Theorem 5.12, recalling that λ has degree 1.

Remarks 5.15. (1) In the case of curves ($d = 1$) with $E = \mathbb{Q}$ and (i), this is [Kowalski 2006, Theorem 3.1, Proposition 3.3]; see also [Kowalski 2008b, Section 5, Remark 5.4].

(2) We handle the weaker (ii) on projective monodromy groups to treat L-function attached to even Dirichlet characters over function fields (Section 4).

(3) The constant $C(L, (\mathcal{F}_\lambda)_{\lambda\in\Lambda})$ may depend on the characteristic p, but crucially not on the index $[\mathbb{F}_q : \mathbb{F}_p]$.

(4) The last part of [Kowalski 2006, Remark 5.2] does not seem quite correct: one crucially has to control the dependency of C with respect to L (that is, the Betti numbers) if one wants to take $L \to \infty$.

In practice, we will use the following consequence of Theorem 5.14:

Corollary 5.16. *In the setting of Theorem 5.14*:

(a) *If X is a curve, then*

$$P\big(q, (\mathcal{F}_\lambda, \boldsymbol{\Omega}_\lambda)_{\lambda\in\Lambda}\big) \ll \frac{t \sup_{\lambda\in\Lambda} \operatorname{cond}(\mathcal{F}_\lambda)^t}{(1-\delta_{\boldsymbol{\Omega}})\delta_\Lambda} \frac{\log q}{q^{1/(tE_G)}},$$

where the implied constant is absolute and $E_G = \dim G + (\operatorname{rank} G)/2$.

(b) *If there are constants $B_1 > 0$ and $B_2 > 1$ such that*

$$\sup_{\lambda\in\Lambda} \sigma_c(X, \mathcal{F}_\lambda^{\otimes N}) \le B_1 B_2^N \qquad \text{for all } N \ge 1,$$

then

$$P\big(q, (\mathcal{F}_\lambda, \boldsymbol{\Omega}_\lambda)_{\lambda\in\Lambda}\big) \ll \frac{t^2 (B_1^2 d r^{\delta_{G=\mathrm{SL}_r}})^t (\log(B_2) M_G + \dim G)}{(1-\delta_{\boldsymbol{\Omega}})\delta_\Lambda} \frac{\log\log q}{\log q},$$

with an absolute implied constant.

(c) *If hypothesis (c) of Theorem 5.14 holds, then*

$$P\big(q, (\mathcal{F}_\lambda, \boldsymbol{\Omega}_\lambda)_{\lambda\in\Lambda}\big) \ll \frac{t (r^{\delta_{G=\mathrm{SL}_r}+1} C(X, \rho_{\lambda_0}))^t}{(1-\delta_{\boldsymbol{\Omega}})\delta_\Lambda} \frac{\log q}{q^{1/(2t(\dim G+1))}}.$$

We prove the theorem and its corollary in the next sections.

5C. *Preliminaries to the proof of Theorem 5.14(b).*

5C1. *Irreducibles in tensor powers of faithful representations.* A classical theorem of Burnside asserts that

> if G is a finite group with a faithful (complex) representation ρ, then any irreducible representation of G appears as a direct summand of $\rho^{\otimes M}$ for some integer $M \ge 1$

(see, e.g., [Steinberg 1962; Brauer 1964; Bryant and Kovács 1972]). The same result holds for compact groups, and is the key to get bounds on Betti numbers in [Katz 2017]. For classical groups, this can actually directly be seen from Weyl's constructions of the irreducible modules.

A key input to the proof of Theorem 5.14(b) is the following modular version of Burnside's result, for classical finite groups in defining characteristic.

Proposition 5.17. *Let k be a field of characteristic ℓ and $G = \mathrm{SL}_n(\mathbb{F}_\ell)$ or $\mathrm{Sp}_n(\mathbb{F}_\ell)$ with its standard k-representation* $\mathrm{Std} : G \to \mathrm{GL}_n(k)$. *Any irreducible k-representation of G appears as a composition factor*[5] *of* $\mathrm{Std}^{\otimes M}$ *for some $M \leq \ell M_G$, $M_G = \mathrm{rank}(G)(\mathrm{rank}(G)+1)/2$. Therefore, for any k-representation π of G, the semisimplification π^{ss} appears as a direct summand of* $(\dim \pi)(\mathrm{Std}^{\otimes M})^{\mathrm{ss}}$.

Proof. Since G is defined over $\mathbb{F}_\ell$, any irreducible k-representation of G is absolutely irreducible, because $\mathbb{F}_\ell$ is the splitting field of G by a 1968 result of Steinberg [Humphreys 2006, Section 5.2].

By a 1963 lifting theorem of Steinberg (see [Humphreys 2006, Section 2.11]), the absolutely irreducible representations of G in characteristic ℓ are given by the modules $L(\lambda)$ with λ an ℓ-restricted highest weight, i.e., $0 \leq \langle \lambda, \alpha^\vee \rangle < q$ for all $\alpha \in \Delta$. For ω_i $(1 \leq i \leq \mathrm{rank}(G))$ the fundamental dominant weights, that means that $\lambda = \sum_{i=1}^{\mathrm{rank}(G)} a_i \omega_i$ with $0 \leq a_i < \ell$.

In Bourbaki numbering [2005, Tables], ω_i is $\Lambda^i(\mathrm{Std})$ (see [ibid., VIII.13.1.IV]) (resp. $\ker(\Lambda^i(\mathrm{Std}) \to \Lambda^{i-2}(\mathrm{Std}))$; see [ibid, VIII.13.3.IV]) for SL_n (resp. Sp_n). These are simple quotients or subrepresentations of $\mathrm{Std}^{\otimes i}$, so they appear in the composition series. □

Remark 5.18. For complex representations, combining David Speyer's proof of Burnside's theorem [Speyer 2011] with character bounds [Gluck 1993] shows that $M \ll \dim G$ is enough, as $\ell \to \infty$. Such an improvement (or even $M \ll \log |\mathbb{F}_\ell|$) to Proposition 5.17 would lead to bounds of the quality of Corollary 5.16(c) in Corollary 5.16(b). However, while Brauer characters control composition factors, they do not satisfy (in defining characteristic) good bounds, to extend this characteristic 0 idea.

5C2. *Betti numbers of reductions modulo λ and semisimplifications.*

Lemma 5.19. *In the setting of Theorem 5.14, if $\mathcal{F}_\lambda$ is the sheaf of $\mathbb{F}_\lambda$-modules on X obtained by reduction of a lisse sheaf of $\mathcal{O}_\lambda$-modules $\widehat{\mathcal{F}}_\lambda$ on X, then*

$$\sigma_c(X, \widehat{\mathcal{F}}_\lambda^{\otimes M}) \leq \sigma_c(X, \mathcal{F}_\lambda^{\otimes M}) \leq 2\sigma_c(X, \widehat{\mathcal{F}}_\lambda^{\otimes M})$$

for any $M \geq 1$.

Proof. Let $\mathcal{G} = \mathcal{F}_\lambda^{\otimes M}$ and $\widehat{\mathcal{G}}_\lambda = \widehat{\mathcal{F}}_\lambda^{\otimes M}$. The lower bound appears in [Katz and Sarnak 1999, p. 279], and the same argument yields the upper bound: we have the universal coefficients short exact sequence

$$0 \to H_c^i(X, \widehat{\mathcal{G}}_\lambda) \otimes_{\mathcal{O}_\lambda} \mathbb{F}_\lambda \to H_c^i(X, \mathcal{G}_\lambda) \otimes_{\mathcal{O}_\lambda} \mathbb{F}_\lambda \to H_c^{i+1}(X, \widehat{\mathcal{G}}_\lambda)[\lambda] \to 0,$$

obtained after truncating the long exact sequence in cohomology [SGA 4½ 1977, 1.6.5] associated to the short exact sequence $0 \to \widehat{\mathcal{F}}_\lambda \xrightarrow{\cdot\lambda} \widehat{\mathcal{F}}_\lambda \to \mathcal{F}_\lambda \to 0$. Taking dimensions, this implies that

$$\sigma_c(X, \widehat{\mathcal{G}}_\lambda) \leq \sigma_c(X, \mathcal{G}_\lambda) \leq \sum_{i \geq 0} \big(\dim H_c^i(X, \hat{\mathcal{G}}_\lambda) + \dim H_c^{i+1}(X, \widehat{\mathcal{G}}_\lambda)\big). \qquad \square$$

[5] We need to look at composition factors instead of summands, since we consider modular representations, which are not completely reducible.

Remark 5.20. If the sheaves $\mathcal{F}_\lambda$ in Theorem 5.14 are obtained by reduction of sheaves of $\mathcal{O}_\lambda$-modules $\widehat{\mathcal{F}}_\lambda$, Lemma 5.19 shows that it suffices to check hypothesis in (b) of Corollary 5.16 for $\mathcal{F}_\lambda$, up to replacing B_1 by $2B_1$.

To deal with noncompletely reducible representations, we observe the following:

Lemma 5.21. *Let $\mathcal{F}$ be a sheaf of $\mathbb{F}_\ell$-modules on X with composition series*

$$0 = \mathcal{F}_0 \subset \cdots \subset \mathcal{F}_n = \mathcal{F}, \quad \mathcal{G}_i := \mathcal{F}_{i+1}/\mathcal{F}_i \text{ simple} \quad (0 \le i \le n-1).$$

Then $\sigma_c(X, \mathcal{F}^{\mathrm{ss}}) = \sum_{i=0}^{n-1} \sigma_c(X, \mathcal{G}_i) = \sigma_c(X, \mathcal{F})$.

Proof. For all $0 \le i \le n-1$, we have a short exact sequence $0 \to \mathcal{F}_i \to \mathcal{F}_{i+1} \to \mathcal{G}_i \to 0$, which gives for all $a \ge 0$ a long exact sequence in cohomology

$$\cdots \to H_c^a(X, \mathcal{F}_i) \to H_c^a(X, \mathcal{F}_{i+1}) \to H_c^a(X, \mathcal{G}_i) \to H_c^{a+1}(X, \mathcal{F}_i) \to \cdots$$

that yields $\sigma_c(X, \mathcal{F}_{i+1}) = \sigma_c(X, \mathcal{G}_i) + \sigma_c(X, \mathcal{F}_i)$, whence $\sigma_c(X, \mathcal{F}) = \sigma_c(X, \mathcal{F}_n) = \sum_{i=0}^{n-1} \sigma_c(X, \mathcal{G}_i) = \sigma_c(X, \mathcal{F}^{\mathrm{ss}})$. □

5D. ***Proof of Theorem 5.14.*** We first give the proof under (i), before indicating the changes required in the projective case (ii).

For $\lambda, \lambda' \in \Lambda$, we will denote by ℓ, ℓ' the primes above which they respectively lie. Since $\Lambda \subset \mathrm{Spec}_{1,p}(\mathcal{O})$, note that $\mathbb{F}_\lambda = \mathbb{F}_\ell$, $\mathbb{F}_{\lambda'} = \mathbb{F}_{\ell'}$. We also let $\widehat{G(\mathbb{F}_\ell)}$ be the set of irreducible (complex) representations of $G(\mathbb{F}_\ell)$.

For every $\lambda \in \Lambda$, we consider the lisse sheaf $\mathcal{G}_\lambda = \mathcal{F}_\lambda^{\boxtimes t}$ on X^t. By [Kowalski 2008b, Lemma 5.1], the natural map $\pi_1(X^t, (\bar\eta, \dots, \bar\eta)) \to \pi_1(X, \bar\eta)^t$ is surjective, so that the arithmetic and geometric monodromy groups of $\mathcal{G}_\lambda$ are equal and conjugate to $G(\mathbb{F}_\lambda)^t$.

Exactly as in [Kowalski 2006, Theorem 3.1, Proposition 3.3, Section 5], we get that

$$P\big(q, (\mathcal{F}_\lambda, \boldsymbol{\Omega}_\lambda)_{\lambda\in\Lambda}\big) \ll \Delta\Bigg[\sum_{\substack{\lambda\in\Lambda\\ N(\lambda)\le L}} \left(1 - \frac{|\boldsymbol{\Omega}_\lambda|}{|G(\mathbb{F}_\lambda)|}\right)\Bigg]^{-1} \ll \frac{\Delta \log L}{\delta_\Lambda(1-\delta_{\boldsymbol{\Omega}})L},$$

where $\Delta \ll 1 + q^{-1/2}\tilde{C}(L, (\mathcal{F}_\lambda)_{\lambda\in\Lambda})$, and $\tilde{C}(L, (\mathcal{F}_\lambda)_{\lambda\in\Lambda})$ is defined by

$$\max_{\substack{\lambda\in\Lambda\\ N(\lambda)\le L}} \max_{\substack{\boldsymbol{\pi}\in\widehat{G(\mathbb{F}_\lambda)^t}\\ \boldsymbol{\pi}\ne 1}} \Bigg[\sum_{\substack{\boldsymbol{\pi}'\in\widehat{G(\mathbb{F}_\lambda)^t}\\ \boldsymbol{\pi}'\ne 1}} \sigma_c(X^t, \mathcal{F}_{\boldsymbol{\pi},\boldsymbol{\pi}'}) + \sum_{\substack{\lambda'\in\Lambda\\ N(\lambda')\le L\\ \ell'\ne\ell}} \sum_{\substack{\boldsymbol{\pi}'\in\widehat{G(\mathbb{F}_{\lambda'})^t}\\ \boldsymbol{\pi}'\ne 1}} \sigma_c(X^t, \mathcal{F}_{\boldsymbol{\pi},\boldsymbol{\pi}'})\Bigg],$$

with (see [Kowalski 2006, Proof of Proposition 5.1])

$$\mathcal{F}_{\boldsymbol{\pi},\boldsymbol{\pi}'} = \tau_{\boldsymbol{\pi},\boldsymbol{\pi}'} \circ \begin{cases} \rho_\lambda^{\boxtimes t} & \text{for } \ell = \ell', \\ (\rho_\lambda^{\boxtimes t}, \rho_{\lambda'}^{\boxtimes t}) & \text{for } \ell \ne \ell', \end{cases} \qquad \tau_{\boldsymbol{\pi},\boldsymbol{\pi}'} = \begin{cases} \boldsymbol{\pi} \otimes D(\boldsymbol{\pi}') & \text{for } \ell = \ell', \\ \boldsymbol{\pi} \boxtimes D(\boldsymbol{\pi}') & \text{for } \ell \ne \ell', \end{cases}$$

identifying lisse sheaves of $\overline{\mathbb{Q}}_\ell$-modules on X^t and continuous representations $\pi_1(X^t, \bar\eta) \to \mathrm{GL}_m(\overline{\mathbb{Q}}_\ell)$. Note that ρ_λ and $(\rho_\lambda, \rho_{\lambda'})$ respectively correspond to sheaves of $\mathbb{F}_\ell$- and $\mathbb{Z}/\ell\ell'$-modules (if $\ell \ne \ell'$).

Hence, we need to show that

$$\widetilde{C}(L, (\mathcal{F}_\lambda)_{\lambda\in\Lambda}) \ll tC(L, (\mathcal{F}_\lambda)_{\lambda\in\Lambda})^t,$$

with C defined in the statement of the theorem. Künneth's formula [SGA 4½ 1977, Exposé 6, 2.4] reduces this to the case $t = 1$.

5D1. *Case (a): curves.* The first bound on $C(L, (\mathcal{F}_\lambda)_{\lambda\in\Lambda})$ in Theorem 5.14, when $d = 1$, is contained in [Kowalski 2006] (with a power of L smaller by one here, because we assume that the arithmetic and geometric monodromy groups coincide).

5D2. *Case (c): compatible systems on varieties by reduction to the tame case.* Let $\lambda_0 \in \Lambda$ be fixed and let $\varphi : Y \to X$ be the étale covering corresponding to $f \pmod{\lambda_0}$. As in [Kowalski 2006, Proposition 4.7], by the Hochschild–Serre sequence,

$$\sigma_c(X, \mathcal{F}_{\pi,\pi'}) \le \sigma_c(Y, \varphi^*\mathcal{F}_{\pi,\pi'}).$$

It then suffices to show that the compatible system ρ is tame when restricted to Y. Indeed, a result of Deligne [Illusie 1981, Corollaire 2.8] shows that the Euler characteristic of a lisse tame sheaf is equal to its rank times the Euler characteristic of the variety, so by [Katz 2001, $\sigma - \chi$ inequality, p. 40], we have in this case

$$\begin{aligned}\sigma_c(Y, \varphi^*\mathcal{F}_{\pi,\pi'}) &\ll r + |\chi_c(Y, \varphi^*\mathcal{F}_{\pi,\pi'})| + \sum_{j=1}^{\dim X} |\chi_c(\text{codim } j \text{ in } Y, \varphi^*\mathcal{F}_{\pi,\pi'})| \\ &\le r + \dim(\pi)\dim(\pi')C(X, \rho_{\lambda_0}),\end{aligned}$$

where $C(X, \rho_{\lambda_0})$ is a constant depending only on the Euler characteristics χ_c of Y and its subvarieties, hence only on X and $\mathcal{F}_{\lambda_0}$. Therefore,

$$\begin{aligned}\widetilde{C}(L, (\mathcal{F}_\lambda)_{\lambda\in\Lambda}) &\ll C(X, \rho_{\lambda_0}) \cdot r \max_{\substack{\lambda\in\Lambda\\ N(\lambda)\le L}} \max_{\substack{\pi\in\widehat{G(\mathbb{F}_\lambda)}\\ \pi\ne 1}} d_\pi \Bigg[\sum_{\substack{\pi'\in\widehat{G(\mathbb{F}_\lambda)}\\ \pi'\ne 1}} d_{\pi'} + \sum_{\substack{\lambda'\in\Lambda\\ N(\lambda')\le L\\ \ell'\ne\ell}} \sum_{\substack{\pi'\in\widehat{G(\mathbb{F}_{\lambda'})}\\ \pi'\ne 1}} d_{\pi'} \Bigg] \\ &\ll C(X, \rho_{\lambda_0}) \cdot r^{\delta_{G=\mathrm{SL}_r}+1} L^{\dim G+1},\end{aligned}$$

where $d_\pi := \dim \pi$. Indeed, the number (complex) of irreducible representations of $G(\mathbb{F}_\ell)$ is given by $|G(\mathbb{F}_\ell)^\sharp| \ll |Z(G(\mathbb{F}_\ell))|\ell^{\operatorname{rank} G} \le r^{\delta_{G=\mathrm{SL}_r}}\ell^{\operatorname{rank} G}$ (see [Malle and Testerman 2011, Corollary 26.10]), and the maximal dimension of such a representation is $\ll \ell^{\frac{1}{2}(\dim G - \operatorname{rank} G)}$; see [Kowalski 2008a, Proposition 5.4].

To show the tameness of the compatible system restricted to Y, first note that it is tame at λ_0, since it factors by construction through the pro-ℓ_0-group $\{g \in \mathrm{GL}_n(\mathcal{O}_{\lambda_0}) : g \equiv 1 \pmod{\lambda_0}\}$, where ℓ_0 is the prime above which λ_0 lies. By purity, it suffices to look at restriction to curves; see [Illusie 1981, Section 2.6; Kerz and Schmidt 2010]. In this case, [Katz 2002, 7.5.1] shows, from a compatibility result of Deligne, that tameness at one prime implies tameness of the whole system.

5D3. *Case (b): varieties through modular representations.* Given $\pi \in \widehat{G(\mathbb{F}_\lambda)}$, $\pi' \in \widehat{G(\mathbb{F}_{\lambda'})}$, we need to bound the sums of Betti numbers $\sigma_c(X, \mathcal{F}_{\pi,\pi'})$. By [Curtis and Reiner 1962, Corollary 75.4], π (resp. π') is defined over the ring of integers of a finite extension F_λ/E_λ (resp. $F_{\lambda'}/E_{\lambda'}$), say

$$\pi : G(\mathbb{F}_\lambda) \to \mathrm{GL}_m(\mathcal{O}_{F_\lambda}), \qquad \pi' : G(\mathbb{F}_{\lambda'}) \to \mathrm{GL}_{m'}(\mathcal{O}_{F_{\lambda'}}).$$

By reduction, we obtain

$$\widetilde{\pi} : G(\mathbb{F}_\lambda) \to \mathrm{GL}_m(k), \qquad \widetilde{\pi}' : G(\mathbb{F}_{\lambda'}) \to \mathrm{GL}_{m'}(k'),$$

for the residue field $k/\mathbb{F}_\lambda$, (resp. $k'/\mathbb{F}_{\lambda'}$). Let $\mathrm{Std}_\lambda : G(\mathbb{F}_\lambda) \to \mathrm{GL}_r(\mathbb{F}_\lambda)$ be the standard representation by inclusion.

We start with the case $\ell = \ell'$, which is easier. We may then assume that $\mathbb{F}_\lambda = \mathbb{F}_{\lambda'}$. By Lemmas 5.19 and 5.21, along with the fact that $\rho_\lambda : \pi_1(X, \bar{\eta}) \to G(\mathbb{F}_\lambda)$ is surjective,

$$\sigma_c(X, \mathcal{F}_{\pi,\pi'}) \le \sigma_c(X, \mathcal{F}_{\widetilde{\pi},\widetilde{\pi}'}) \le \sigma_c(X, \tau^{\mathrm{ss}}_{\widetilde{\pi},\widetilde{\pi}'} \circ \rho_\lambda).$$

By Proposition 5.17, every simple summand of $\tau^{\mathrm{ss}}_{\widetilde{\pi},\widetilde{\pi}'}$ appears as a composition factor of $(\mathrm{Std}_\lambda \otimes \overline{\mathbb{F}}_\ell)^{\otimes M}$ for some $M \le \ell M_G$. It follows that

$$\sigma_c(X, \mathcal{F}_{\pi,\pi'}) \le (\dim \pi)(\dim \pi') \max_{M \le \ell M_G} \sigma_c(X, \mathcal{F}_\lambda^{\otimes M}). \tag{23}$$

Let us now assume that $\ell \ne \ell'$, and note that $(\rho_\lambda, \rho_{\lambda'})$ corresponds to the sheaf of $\mathbb{Z}/\ell\ell'$-modules on X given by $\Delta^*(\mathcal{F}_\lambda \boxtimes \mathcal{F}_{\lambda'})$, for $\Delta : X \to X \times X$ the diagonal immersion. We may view $\mathcal{F}_{\pi,\pi'}$ as sheaf of $(\mathcal{O}_{F_\lambda} \otimes \mathcal{O}_{F_{\lambda'}})$-modules, and $\sigma_c(X, \mathcal{F}_{\pi,\pi'})$ is equal to the sum of the ranks (under Definition 5.13) of the corresponding étale cohomology groups with compact support. Then $\mathcal{F}_{\widetilde{\pi},\widetilde{\pi}'}$ is a sheaf of $(k \otimes k')$-modules, and by Lemma 5.21 and the same argument as in Lemma 5.19,

$$\sigma_c(X, \mathcal{F}_{\pi,\pi'}) \le \sigma_c(X, \mathcal{F}_{\widetilde{\pi},\widetilde{\pi}'}) = \sigma_c\big(X, \tau^{\mathrm{ss}}_{\widetilde{\pi},\widetilde{\pi}'} \circ \Delta^*(\mathcal{F}_\lambda \boxtimes \mathcal{F}_{\lambda'})\big).$$

As above, we get that every simple summand in $\tau^{\mathrm{ss}}_{\widetilde{\pi},\widetilde{\pi}'}$ appears as a composition factor of the $(k \otimes k')$-module $\mathrm{Std}^{\otimes M} \boxtimes \mathrm{Std}^{\otimes M'}$ for some $M \le \ell M_G$ and $M' \le \ell' M_G$. This implies that

$$\sigma_c(X, \mathcal{F}_{\widetilde{\pi},\widetilde{\pi}'}) \le (\dim \pi + \dim \pi') \max_{M \le \ell M_G} \max_{M' \le \ell' M_G} \sigma_c(X, \Delta^* \mathcal{G}_{M,M'}),$$

where $\mathcal{G}_{M,M'} = (\mathcal{F}_\lambda \otimes k)^{\otimes M} \boxtimes (\mathcal{F}_{\lambda'} \otimes k')^{\otimes M'}$.

By purity [Fu 2011, Corollary 8.5.6] and the localization sequence [Fu 2011, Proposition 5.6.11], this implies that $\sigma_c(X, \Delta^* \mathcal{G}_{M,M'}) \le \sigma_c(X \times X, \mathcal{G}_{M,M'})$. By Künneth's formula [SGA 4½ 1977, Exposé 6, 2.4],

$$\operatorname{rank} H^i_c(X \times X, \mathcal{G}_{M,M'}) = \sum_{a+b=i} \operatorname{rank} H^a_c(X, \mathcal{F}_\lambda^{\otimes M}) \operatorname{rank} H^b_c(X, \mathcal{F}_{\lambda'}^{\otimes M'}) \le \sigma_c(X, \mathcal{F}_\lambda^{\otimes M}) \sigma_c(X, \mathcal{F}_{\lambda'}^{\otimes M'}),$$

hence

$$\sigma_c(X, \mathcal{F}_{\pi,\pi'}) \ll d(\dim \pi + \dim \pi') S(\lambda) S(\lambda') \tag{24}$$

where $S(\lambda) := \max_{M \le N(\lambda) M_G} \sigma_c(X, \mathcal{F}_\lambda^{\otimes M})$.

Thus, (23) and (24) yield that, as in Section 5D2,

$$\widetilde{C}(L,(\mathcal{F}_\lambda)_{\lambda\in\Lambda}) \ll \max_{\substack{\lambda\in\Lambda\\ N(\lambda)\le L}} S(\lambda) \max_{\substack{\pi\in\widehat{G(\mathbb{F}_\ell)}\\ \pi\neq 1}} \Bigg[d_\pi \sum_{\substack{\pi'\in\widehat{G(\mathbb{F}_\ell)}\\ \pi'\neq 1}} d_{\pi'} + d \sum_{\substack{\lambda'\in\Lambda\\ N(\lambda')\le L\\ \ell'\neq\ell}} \sum_{\substack{\pi'\in\widehat{G(\mathbb{F}_{\ell'})}\\ \pi'\neq 1}} (d_\pi + d_{\pi'}) S(\lambda') \Bigg]$$

$$\ll d r^{\delta_{G=\mathrm{SL}_r}} L^{\dim G} \max_{N(\lambda)\le L} S(\lambda)^2.$$

5D4. *Projective monodromy groups.* Let us now suppose that only (ii) holds. For $\eta : G \to PG$ the projection, we have

$$P\big(q,(\mathcal{F}_\lambda,\boldsymbol{\Omega}_\lambda)_{\lambda\in\Lambda}\big) \le \frac{|\{\boldsymbol{x}\in X(\mathbb{F}_q)^t : (\eta\rho_\lambda(\mathrm{Frob}_{x_i,q}))_i \in \eta(\boldsymbol{\Omega}_\lambda) \text{ for all } \lambda\in\Lambda\}|}{|X(\mathbb{F}_q)|^t},$$

and for any $\Omega \subset G(\mathbb{F}_\lambda)$,

$$\frac{|\eta(\Omega)|}{|PG(\mathbb{F}_\lambda)|} = \frac{|\eta(\Omega)||Z(G(\mathbb{F}_\lambda))|}{|G(\mathbb{F}_\lambda)|} \le \frac{|\Omega|}{|G(\mathbb{F}_\lambda)|} = \delta_\Omega.$$

Thus, it is enough to repeat the arguments above with G replaced by PG. Indeed, since $(r, |\mathbb{F}_\lambda|-1) = r$ for all $\lambda\in\Lambda$, we have $\mathrm{SL}_r(\mathbb{F}_\lambda) \cong \mathrm{PGL}_r(\mathbb{F}_\lambda)$, so this can be done mutatis mutandis (in particular, the "standard representation" $PG(\mathbb{F}_\lambda) \to \mathrm{GL}_r(\mathbb{F}_\lambda)$ on page 1321 is well-defined). □

6. Generic maximality of splitting fields and linear independence

This section mostly recalls some results from [Kowalski 2008b] and gives their analogues for SL when necessary.

6A. *Generic maximality of splitting fields.*

Definition 6.1. For R a ring and $r \ge 2$ an integer, we let

$$\mathcal{P}_{\mathrm{SL}_r}(R) := \{P\in R[T] \text{ monic} : \deg(P) = r,\ P(0) = 1\} \qquad (r\ge 2),$$

$$\mathcal{P}_{\mathrm{Sp}_r}(R) := \{P\in \mathcal{P}_{\mathrm{SL}_r}(R) : P(T) = T^r P(1/T)\} \qquad (r\ge 2 \text{ even}).$$

Note that for $G\in\{\mathrm{SL}_r, \mathrm{Sp}_r\}$, the set of (reversed) characteristic polynomials of elements of $G(R)$ is included in $\mathcal{P}_G(R)$, with equality at least when R is a finite field; see the reference to Chavdarov's proof in [Kowalski 2008a, Lemma B.5(2)].

Let E be a Galois number field with ring of integers $\mathcal{O}$. Note that the Galois group of a polynomial $P\in\mathcal{P}_G(\bar{E})$ of degree n is contained in

- $\mathfrak{S}_r$ if $G = \mathrm{SL}_r$.
- $W_r \le \mathfrak{S}_r$ (the Coxeter group $B_{r/2}$) if $G = \mathrm{Sp}_r$ (r even).

We will say that the Galois group is *nonmaximal* if this inclusion is strict.

6A1. *Detecting nonmaximal Galois groups.*

Proposition 6.2. *Let $G = \mathrm{SL}_r$ ($r \geq 2$) or $G = \mathrm{Sp}_r$ ($r \geq 2$ even). For every $t \geq 1$ and $\lambda \in \mathrm{Spec}_1(\mathcal{O})$, there exist conjugacy-invariant sets $\boldsymbol{\Omega}_{\boldsymbol{i},\lambda,G^t} \subset G(\mathbb{F}_\lambda)^t$ ($\boldsymbol{i} \in \boldsymbol{I}$, with $\boldsymbol{I}$ an index set of size $4t$) such that*:

- *$\boldsymbol{\Omega}_{i,\lambda,G^t}$ has density $\leq \delta_{r,t} := ((1-(1/r!))(1+(r/\ell)))^t(1-(1/2r))$.*
- *If $\boldsymbol{g} = (g_1, \dots, g_t) \in \mathcal{P}_G(\mathcal{O}_\lambda)^t$ is such that $\prod_{i=1}^t \det(1 - Tg_i) \in \mathcal{P}_G(\mathcal{O}_\lambda) \subset \mathcal{O}_\lambda[T]$ has nonmaximal Galois group, that is, strictly contained in $\mathfrak{S}_r^t$ (resp. W_r^t) if $G = \mathrm{SL}_r$ (resp. Sp_r), then there exists $\boldsymbol{i} \in \boldsymbol{I}$ such that $\boldsymbol{g} \pmod{*}\lambda \in \boldsymbol{\Omega}_{\boldsymbol{i},\lambda,G^t}$.*

Proof. The case $G = \mathrm{Sp}_r$ is contained in [Kowalski 2008b, Proof of Theorem 4.3] (see also [Kowalski 2008a, Proof of Theorem 8.13]), using [Kowalski 2008a, Lemma B.5] to switch between densities of matrices and characteristic polynomials, and up to replacing $\mathbb{Z}$ by $\mathcal{O}_\lambda$.

The case $G = \mathrm{SL}_r$ is simpler, and we also apply the lemma of Bauer quoted by Gallagher [1973, p. 98]: if $H \leq \mathfrak{S}_r$ is transitive, contains a transposition and a m-cycle with $m > r/2$ prime, then $H = \mathfrak{S}_r$. We define

$$\begin{aligned}
\widetilde{\Omega}_{0,\lambda} &= \{P \in \mathcal{P}_{\mathrm{SL}_r}(\mathbb{F}_\lambda) : \text{product of linear factors}\}^c,\\
\widetilde{\Omega}_{1,\lambda} &= \{P \in \mathcal{P}_{\mathrm{SL}_r}(\mathbb{F}_\lambda) : P \text{ reducible}\},\\
\widetilde{\Omega}_{2,\lambda} &= \{P \in \mathcal{P}_{\mathrm{SL}_r}(\mathbb{F}_\lambda) : P = QQ_1\cdots Q_s,\ Q, Q_i \text{ irreducible},\ \deg(Q) = 2,\ \deg(Q_i) \text{ odd}\}\\
\widetilde{\Omega}_{3,\lambda} &= \{P \in \mathcal{P}_{\mathrm{SL}_r}(\mathbb{F}_\lambda) : P \text{ has an irreducible factor of prime degree} > r/2\}^c,\\
\Omega_{j,\lambda} &= \{g \in \mathrm{SL}_r(\mathbb{F}_\lambda) : \det(1-Tg) \in \widetilde{\Omega}_{j,\lambda}\} \qquad (0 \leq j \leq 3),\\
\boldsymbol{\Omega}_{\boldsymbol{i},\lambda,G^t} &= \Omega_{0,\lambda}^{k-1} \times \Omega_{j,\lambda} \times \Omega_{0,\lambda}^{t-k}, \quad \boldsymbol{i} = (k, j) \in \boldsymbol{I} := \{1, \dots, t\} \times \{1, 2, 3\},
\end{aligned}$$

(we make the reader attentive to the fact that some of the sets above are defined using complements) and the same arguments as in the Sp_r case give the conclusion. □

6A2. *Application of the large sieve.*

Corollary 6.3. *Let X, E, $\mathcal{O}$ and Λ be as in Theorem 5.14. For every $\lambda \in \mathcal{O}$, let $\widehat{\mathcal{F}}_\lambda$ be a rank r lisse sheaf of free $\mathcal{O}_\lambda$-modules on X, corresponding to a representation $\hat{\rho}_\lambda : \pi_1(X, \bar{\eta}) \to \mathrm{GL}_r(\mathcal{O}_\lambda)$. We assume (i) or (ii) of Theorem 5.14, and hypothesis (a), (b) or (c) of Corollary 5.16, hold for $\hat{\rho}_\lambda$. For $\boldsymbol{x} \in X(\mathbb{F}_q)^t$, let*

$$P_\lambda(\boldsymbol{x}) := \prod_{i=1}^t P_\lambda(x_i), \qquad P_\lambda(x_i) = \det(1 - T\rho_\lambda(\mathrm{Frob}_{x_i,q})).$$

Then, for every $t \geq 1$ and every finite field $\mathbb{F}_q$ of characteristic p, we have

$$\begin{aligned}
&\frac{|\{\boldsymbol{x} \in X(\mathbb{F}_q)^t : P_\lambda(\boldsymbol{x}) \in \mathcal{O}_\lambda[T] \text{ has nonmaximal Galois group for all } \lambda \in \Lambda\}|}{|X(\mathbb{F}_q)|^t} \qquad (25)\\
&\ll \frac{t^2}{(1-\delta_{r,t})\delta_\Lambda} \begin{cases} \sup_{\lambda\in\Lambda} \mathrm{cond}(\mathcal{F}_\lambda)^t \dfrac{\log q}{q^{1/(tE_G)}} & \text{under (a)},\\ t(B_1^2 d r^{\delta_{G=\mathrm{SL}_r}})^t(\log(B_2)M_G + \dim G)\dfrac{\log\log q}{\log q} & \text{under (b)},\\ \left(r^{\delta_{G=\mathrm{SL}_r}+1}C(X, \rho_{\lambda_0})\right)^t \dfrac{\log q}{q^{1/(2t(\dim G+1))}} & \text{under (c)}, \end{cases}
\end{aligned}$$

with an absolute implied constant.

Proof. By Proposition 6.2, the density on the left-hand side is less than or equal to

$$\sum_{\boldsymbol{i}\in\boldsymbol{I}} \frac{|\{\boldsymbol{x}\in X(\mathbb{F}_q)^t : (\rho_\lambda(\mathrm{Frob}_{x_i,q}))_{1\le i\le t}\in \boldsymbol{\Omega}_{\boldsymbol{i},\lambda,G^t} \text{ for all } \lambda\in\Lambda\}|}{|X(\mathbb{F}_q)|^t},$$

and it suffices to apply Corollary 5.16 to each summand. □

6B. ***Girstmair's method.*** Below, we recall the following forms of Girstmair's results [1982; 1999], as exposed in [Kowalski 2008b] (with some changes in the symmetric case).

Definition 6.4. For a set M of complex numbers, let

$$\mathrm{Rel}_m(M)=\left\{(n_\alpha)\in\mathbb{Z}^M : \prod_{\alpha\in M}\alpha^{n_\alpha}=1\right\}.$$

Proposition 6.5. *Let E be a number field, $t\ge 1$ an integer, and for $1\le i\le t$, let $P_i\in E[X]$ be a polynomial with splitting field K_i, set of roots $M_i\subset K_i$, and Galois group $G_i:=\mathrm{Gal}(K_i/E)$. We assume that the fields K_i are linearly disjoint, and we let $M=\bigcup_{i=1}^t M_i$, $K=K_1\cdots K_t$. Then $\mathrm{Rel}_m(M)\otimes\mathbb{Q}=\bigoplus_{i=1}^t \mathrm{Rel}_m(M_i)\otimes\mathbb{Q}$. Moreover*:

(1) (*W case*) *Assume that $G_i\cong W_r$ for some $r\ge 4$ even, acting by permutation on M_i. If $|\alpha|=1$ for every $\alpha\in M_i$, then*

$$\mathrm{Rel}_m(M_i)\otimes\mathbb{Q}=\{(n_\alpha)\in\mathbb{Q}^{M_i} : n_\alpha=n_{\bar\alpha}\}.$$

(2) (*$\mathfrak{S}$ case*) *Assume that $G_i\cong\mathfrak{S}_r$ for some $r\ge 2$, acting by permutation on M_i. Then $\mathrm{Rel}_m(M_i)\otimes\mathbb{Q}$ is either*:

(a) *if $r=2$:* 0, $\mathbb{Q}\mathbf{1}$, *or* $\mathbb{Q}(-1,1)$.

(b) *if $r\ge 3$:* 0 *or* $\mathbb{Q}\mathbf{1}$.

Proof. The W case is [Kowalski 2008b, Proposition 2.4, (2.5)]. However, $\mathbb{Q}$ in the paragraph after the second display of [Kowalski 2008b, p. 13] should probably be replaced by E, and the contradiction comes from the fact that the splitting field of K/E would be a 2-group.

For the $\mathfrak{S}$ case, note that the permutation representation $F(M_i)$ of $\mathfrak{S}_r$ decomposes as the sum of two irreducible representations

$$F(M_i)=\mathbb{Q}\mathbf{1}\oplus G(M_i),\qquad \text{where } G(M_i)=\left\{(n_\alpha)\in\mathbb{Q}^{M_i} : \sum_{\alpha\in M_i} n_\alpha=0\right\}.$$

If $G(M_i)$ is contained in the subrepresentation $\mathrm{Rel}_m(M_i)\otimes\mathbb{Q}$ of $F(M_i)$, then there exists $m\ge 1$ such that $(\alpha_j/\alpha_1)^m=1$ for $1\le j\le r$, if $M_i=\{\alpha_1,\dots,\alpha_r\}$, so that $\alpha_1^{nm}=N_{M_i/E}(\alpha_1)^m\in E$. Hence, K_i/E is a Kummer extension and $\mathrm{Gal}(K_i/E)$ is abelian, which implies that $r=|M_i|=2$. If $r=2$, note that $\mathrm{Rel}_m(M_i)\otimes\mathbb{Q}=\mathbb{Q}^2$ would imply that $\mathrm{Rel}_m(M_i)=\mathbb{Z}^2$, which is a contradiction. □

6C. *Conclusion.*

Corollary 6.6. *Under the hypotheses of Corollary 6.3, assume moreover that* $(\mathcal{F}_\lambda)_{\lambda\in\Lambda}$ *forms a* ***compatible system****, i.e., that for all* $x \in X(\mathbb{F}_q)$, $P_\lambda(x) = P(x) \in E[T]$ *does not depend on* λ. *For every* $\boldsymbol{x} \in X(\mathbb{F}_q)^t$ *and* $1 \le i \le t$, *let* $M(x_i) \subset \mathbb{C}$ *be the set of zeros of* $\det(1 - T\rho_\lambda(\mathrm{Frob}_{x_i,q}))$, *so that the set of zeros of* $P_\lambda(\boldsymbol{x})$ *is* $\bigcup_{i=1}^t M(x_i)$. *Then, for all but at most a proportion* (25) *of* $\boldsymbol{x} \in X(\mathbb{F}_q)^t$, *we have*

$$\mathrm{Rel}_m(M(\boldsymbol{x})) = \begin{cases} \bigotimes_{i=1}^t \mathbb{Z}\mathbf{1} & \text{for } G = \mathrm{SL}_r \ (r \ge 2), \\ \bigotimes_{i=1}^t \{(n_\alpha) \in \mathbb{Z}^{M(x_i)} : n_\alpha = n_{\bar\alpha}\} & \text{for } G = \mathrm{Sp}_r \ (r \ge 4 \text{ even}). \end{cases}$$

In other words, the only multiplicative relations among the roots are the trivial ones. If we write the roots of $P(x_i)$ *as*

$$\begin{cases} e(\theta_j(x_i)) & \text{for } G = \mathrm{SL}_r \quad (1 \le j \le r), \\ e(\pm\theta_j(x_i)) & \text{for } G = \mathrm{Sp}_r \quad (1 \le j \le r/2), \end{cases}$$

then the angles

$$\begin{cases} 1,\ \theta_j(x_i) & \text{for } G = \mathrm{SL}_r \quad (1 \le i \le t,\ 1 \le j \le r-1), \\ 1,\ \theta_j(x_i) & \text{for } G = \mathrm{Sp}_r \quad (1 \le i \le t,\ 1 \le j \le r/2) \end{cases}$$

are $\mathbb{Q}$*-linearly independent for all but at most a proportion* (25) *of* $\boldsymbol{x} \in X(\mathbb{F}_q)^t$.

Proof. By the compatibility assumption and Corollary 6.3, $P_\lambda(\boldsymbol{x})$ has maximal Galois group $\mathfrak{S}_r^t$ or W_r^t for all but at most a proportion (25) elements $\boldsymbol{x} \in X(\mathbb{F}_q)^t$. Let us assume this maximality condition holds, in which case the hypotheses of Proposition 6.5 hold. Since the product of the zeros of $P_\lambda(x_i)$ is equal to 1, we have $\mathbb{Z}\mathbf{1} \subset \mathrm{Rel}_m(M(x_i))$ for all $x_i \in X(\mathbb{F}_q)$. By Proposition 6.5 and the fact that $\mathrm{Rel}_m(M(x_i))$ is a lattice, this implies that $\mathrm{Rel}_m(M(\boldsymbol{x}))$ is as given in the statement. □

7. Proof of the generic linear independence theorems

In this section, we finally prove Theorems 1.1, 1.11 and 1.20, by applying Corollary 6.6. That basically means checking that assumptions (i) or (ii) of Theorem 5.14 (on monodromy groups) apply, as well as hypothesis (a) or (c) of Corollary 5.16.

7A. *Proof of Theorem 1.1 (exponential sums).*

Theorem 5.14(i) holds by Theorems 5.8 and 5.10 for Kloosterman sums and Birch sums respectively, with the set of valuations $\Lambda_{r,p}$, Λ_p given therein. For Kloosterman sums, the dependency with respect to p can be removed by Remark 5.9.

Since the sheaves are on curves, Corollary 5.16(a) holds. By [Katz 1988, Theorem 4.1.1(3,4)], $\mathrm{cond}(\mathrm{Kl}_{r,\lambda})$ is bounded by a constant depending only on r (and not on p), and the same holds true for Birch sheaves by the bounds on Swan conductors and ramification points in [Katz 1990, Chapter 7]. □

7B. *Proof of Theorem 1.11 (super-even primitive characters).*

Theorem 5.14(i) applies by Theorem 5.12, with the set of valuations $\Lambda_{k,p}$ given by the latter.

If $p > k$, we see (as in [Katz 2017, Lemma 5.2]) that $\mathbb{W}_{2\kappa,\,\mathrm{odd}} = \prod_{1\le a\le 2\kappa,\,a\ \mathrm{odd}} W_1$ is the space of odd polynomials of degree $\le 2\kappa - 1$ and $\mathrm{Prim}_{2\kappa,\,\mathrm{odd}}$ the subspace of those polynomials with degree exactly $2\kappa - 1$. One can then apply Corollary 5.16(c), which gives the theorem.

To obtain the weaker error (but with explicit base of t) in Remark 1.13, one applies Corollary 5.16(b) instead, using the bounds for Betti numbers in [Katz 2017, Lemma 5.2], giving $B_1 = 3(2\kappa+1)^{2\kappa}$, $B_2 = 2\kappa + 1$. □

7C. ***Proof of Theorem 1.20 (even primitive characters).*** In this case, hypothesis (ii) of Theorem 5.14 (projective monodromy groups) applies by Theorem 5.12.

If $p > m$, then as in [Katz 2017], we see that $\mathbb{W}_m = \prod_{1\le a\le m} W_1$ is the space of polynomials of degree $\le m$ with constant term 1 and Prim_m is the subspace of those polynomials with degree exactly m. One can then apply Corollary 5.16(c), which gives the theorem.

To obtain the weaker error (but with explicit base of t) in Remark 1.26, one applies Corollary 5.16(c) instead, proceeding from [Katz 2013b] as in [Katz 2017, Lemma 5.2] to bound the Betti numbers. Let us indeed show that Hypothesis (b) of Corollary 5.16 holds with $B_1 = 3(m+1)^{m+1}$ and $B_2 = m+1$. Let $M \ge 1$ be an integer. With coordinates $(t_1, \dots, t_M, f)$ on $\mathbb{A}^M \times \mathrm{Prim}_m$,

$$H_c^i(\mathrm{Prim}_m, \mathcal{L}_{\mathrm{univ}}^{\otimes M}) = H_c^{i+M}(\mathbb{A}^M \times \mathrm{Prim}_m, \mathcal{L}_{\psi(f(t_1)+\cdots+f(t_M))}).$$

Note that $\mathbb{A}^M \times \mathrm{Prim}_m$ is defined in $\mathbb{A}^{M+1+m}$ (an additional coordinate is needed for the condition that $a_m \ne 0$) and $f(t_1)+\cdots+f(t_M)$ is a polynomial in t_i, a_i of degree $m+1$. By [Katz 2001, Theorem 12] (with $(\delta, N, r, d, s, e_j) = (m+1, M+1+m, 1, 2, 0, 0)$), we have

$$\sigma_c(\mathrm{Prim}_m, \mathcal{L}_{\mathrm{univ}}^{\otimes M}) \le 3(1+\max(m+1,3))^{M+m+1} = 3(m+1)^{M+m+1}.$$ □

Acknowledgements

The author thanks Lucile Devin, Michele Fornea, Javier Fresán, Florent Jouve and Will Sawin for helpful discussions and comments. Will Sawin in particular provided a better way to bound the sums of Betti numbers in the large sieve, leading to stronger results; the idea and proof of Theorem 5.14(c) are due to him. We thank the organizers of the 2019 Shaoul fund IAS Function field arithmetic workshop in Tel-Aviv for providing the opportunity for some of these exchanges. We are grateful to the anonymous referees who provided helpful and detailed comments to improve the manuscript. The author was partially supported by Koukoulopoulos' Discovery Grant 435272-2013 of the Natural Sciences and Engineering Research Council of Canada, and by Radziwiłł's NSERC DG grant and the CRC program.

References

[Ahmadi and Shparlinski 2010] O. Ahmadi and I. E. Shparlinski, "On the distribution of the number of points on algebraic curves in extensions of finite fields", *Math. Res. Lett.* **17**:4 (2010), 689–699. MR Zbl

[Baker and Wüstholz 1993] A. Baker and G. Wüstholz, "Logarithmic forms and group varieties", *J. Reine Angew. Math.* **442** (1993), 19–62. MR Zbl

[Billingsley 1986] P. Billingsley, *Probability and measure*, 2nd ed., Wiley, New York, 1986. MR Zbl

[Bombieri and Katz 2010] E. Bombieri and N. M. Katz, "A note on lower bounds for Frobenius traces", *Enseign. Math.* (2) **56**:3-4 (2010), 203–227. MR Zbl

[Bourbaki 2005] N. Bourbaki, *Lie groups and Lie algebras: Chapters 7–9*, Springer, 2005. MR Zbl

[Brauer 1964] R. Brauer, "A note on theorems of Burnside and Blichfeldt", *Proc. Amer. Math. Soc.* **15** (1964), 31–34. MR Zbl

[Bryant and Kovács 1972] R. M. Bryant and L. G. Kovács, "Tensor products of representations of finite groups", *Bull. London Math. Soc.* **4** (1972), 133–135. MR Zbl

[Cha 2008] B. Cha, "Chebyshev's bias in function fields", *Compos. Math.* **144**:6 (2008), 1351–1374. MR Zbl

[Cha and Kim 2010] B. Cha and S. Kim, "Biases in the prime number race of function fields", *J. Number Theory* **130**:4 (2010), 1048–1055. MR Zbl

[Cha et al. 2016] B. Cha, D. Fiorilli, and F. Jouve, "Prime number races for elliptic curves over function fields", *Ann. Sci. Éc. Norm. Supér.* (4) **49**:5 (2016), 1239–1277. MR Zbl

[Cha et al. 2017] B. Cha, D. Fiorilli, and F. Jouve, "Independence of the zeros of elliptic curve L-functions over function fields", *Int. Math. Res. Not.* **2017**:9 (2017), 2614–2661. MR Zbl

[Curtis and Reiner 1962] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics **XI**, Interscience, New York, 1962. MR Zbl

[Devin 2019] L. Devin, "Chebyshev's bias for analytic L-functions", *Math. Proc. Cambridge Philos. Soc.* (online publication March 2019).

[Devin and Meng 2018] L. Devin and X. Meng, "Chebyshev's bias for products of irreducible polynomials", preprint, 2018. arXiv

[Evertse 1984] J.-H. Evertse, "On sums of S-units and linear recurrences", *Compositio Math.* **53**:2 (1984), 225–244. MR Zbl

[Fouvry et al. 2015] E. Fouvry, E. Kowalski, and P. Michel, "A study in sums of products", *Philos. Trans. Roy. Soc. A* **373**:2040 (2015), art. id. 20140309, 26 pp. MR Zbl

[Fu 2011] L. Fu, *Etale cohomology theory*, Nankai Tracts in Mathematics **13**, World Scientific, Hackensack, NJ, 2011. MR Zbl

[Gallagher 1973] P. X. Gallagher, "The large sieve and probabilistic Galois theory", pp. 91–101 in *Analytic number theory* (St. Louis, MO, 1972), edited by H. G. Diamond, Proc. Sympos. Pure Math. **XXIV**, Amer. Math. Soc., Providence, RI, 1973. MR Zbl

[Girstmair 1982] K. Girstmair, "Linear dependence of zeros of polynomials and construction of primitive elements", *Manuscripta Math.* **39**:1 (1982), 81–97. MR Zbl

[Girstmair 1999] K. Girstmair, "Linear relations between roots of polynomials", *Acta Arith.* **89**:1 (1999), 53–96. MR Zbl

[Gluck 1993] D. Gluck, "Character value estimates for nonsemisimple elements", *J. Algebra* **155**:1 (1993), 221–237. MR Zbl

[Gouillon 2006] N. Gouillon, "Explicit lower bounds for linear forms in two logarithms", *J. Théor. Nombres Bordeaux* **18**:1 (2006), 125–146. MR Zbl

[Hall 2008] C. Hall, "Big symplectic or orthogonal monodromy modulo l", *Duke Math. J.* **141**:1 (2008), 179–203. MR Zbl

[Humphreys 2006] J. E. Humphreys, *Modular representations of finite groups of Lie type*, London Mathematical Society Lecture Note Series **326**, Cambridge University Press, 2006. MR Zbl

[Illusie 1981] L. Illusie, "Théorie de Brauer et caractéristique d'Euler–Poincaré (d'après P. Deligne)", pp. 161–172 in *The Euler–Poincaré characteristic*, Astérisque **82**, Soc. Math. France, Paris, 1981. MR Zbl

[Jouve et al. 2013] F. Jouve, E. Kowalski, and D. Zywina, "Splitting fields of characteristic polynomials of random elements in arithmetic groups", *Israel J. Math.* **193**:1 (2013), 263–307. MR Zbl

[Katz 1987] N. M. Katz, "On the monodromy groups attached to certain families of exponential sums", *Duke Math. J.* **54**:1 (1987), 41–56. MR Zbl

[Katz 1988] N. M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Annals of Mathematics Studies **116**, Princeton University Press, 1988. MR Zbl

[Katz 1990] N. M. Katz, *Exponential sums and differential equations*, Annals of Mathematics Studies **124**, Princeton University Press, 1990. MR Zbl

[Katz 2001] N. M. Katz, "Sums of Betti numbers in arbitrary characteristic", *Finite Fields Appl.* **7**:1 (2001), 29–44. MR Zbl

[Katz 2002] N. M. Katz, *Twisted L-functions and monodromy*, Annals of Mathematics Studies **150**, Princeton University Press, 2002. MR Zbl

[Katz 2005] N. M. Katz, *Moments, monodromy, and perversity: a Diophantine perspective*, Annals of Mathematics Studies **159**, Princeton University Press, 2005. MR Zbl

[Katz 2012a] N. M. Katz, *Convolution and equidistribution: Sato-Tate theorems for finite-field Mellin transforms*, Annals of Mathematics Studies **180**, Princeton University Press, 2012. MR Zbl

[Katz 2012b] N. M. Katz, "Report on the irreducibility of L-functions", pp. 321–353 in *Number theory, analysis and geometry*, edited by D. Goldfeld et al., Springer, 2012. MR Zbl

[Katz 2013a] N. M. Katz, "On a question of Keating and Rudnick about primitive Dirichlet characters with squarefree conductor", *Int. Math. Res. Not.* **2013**:14 (2013), 3221–3249. MR Zbl

[Katz 2013b] N. M. Katz, "Witt vectors and a question of Keating and Rudnick", *Int. Math. Res. Not.* **2013**:16 (2013), 3613–3638. MR Zbl

[Katz 2017] N. M. Katz, "Witt vectors and a question of Rudnick and Waxman", *Int. Math. Res. Not.* **2017**:11 (2017), 3377–3412. MR Zbl

[Katz and Sarnak 1999] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications **45**, Amer. Math. Soc., Providence, RI, 1999. MR Zbl

[Keating and Rudnick 2014] J. P. Keating and Z. Rudnick, "The variance of the number of prime polynomials in short intervals and in residue classes", *Int. Math. Res. Not.* **2014**:1 (2014), 259–288. MR Zbl

[Kerz and Schmidt 2010] M. Kerz and A. Schmidt, "On different notions of tameness in arithmetic geometry", *Math. Ann.* **346**:3 (2010), 641–668. MR Zbl

[Kowalski 2006] E. Kowalski, "The large sieve, monodromy and zeta functions of curves", *J. Reine Angew. Math.* **601** (2006), 29–69. MR Zbl

[Kowalski 2008a] E. Kowalski, *The large sieve and its applications: arithmetic geometry, random walks and discrete groups*, Cambridge Tracts in Mathematics **175**, Cambridge University Press, 2008. MR Zbl

[Kowalski 2008b] E. Kowalski, "The large sieve, monodromy, and zeta functions of algebraic curves, II: Independence of the zeros", *Int. Math. Res. Not.* **2008** (2008), art. id. rnn091, 57 pp. MR Zbl

[Larsen 1995] M. Larsen, "Maximality of Galois actions for compatible systems", *Duke Math. J.* **80**:3 (1995), 601–630. MR Zbl

[Larsen and Pink 1992] M. Larsen and R. Pink, "On l-independence of algebraic monodromy groups in compatible systems of representations", *Invent. Math.* **107**:3 (1992), 603–636. MR Zbl

[Li 2018] W. Li, "Vanishing of hyperelliptic L-functions at the central point", *J. Number Theory* **191** (2018), 85–103. MR Zbl

[Livné 1987] R. Livné, "The average distribution of cubic exponential sums", *J. Reine Angew. Math.* **375/376** (1987), 362–379. MR Zbl

[Malle and Testerman 2011] G. Malle and D. Testerman, *Linear algebraic groups and finite groups of Lie type*, Cambridge Studies in Advanced Mathematics **133**, Cambridge University Press, 2011. MR Zbl

[Martin and Ng 2017] G. Martin and N. Ng, "Inclusive prime number races", preprint, 2017. arXiv

[Matthews et al. 1984] C. R. Matthews, L. N. Vaserstein, and B. Weisfeiler, "Congruence properties of Zariski-dense subgroups, I", *Proc. London Math. Soc.* (3) **48**:3 (1984), 514–532. MR Zbl

[Narkiewicz 2004] W. a. a. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 3rd ed., Springer, 2004. MR Zbl

[Perret-Gentil 2017] C. Perret-Gentil, "Gaussian distribution of short sums of trace functions over finite fields", *Math. Proc. Cambridge Philos. Soc.* **163**:3 (2017), 385–422. MR Zbl

[Perret-Gentil 2018a] C. Perret-Gentil, "Exponential sums over finite fields and the large sieve", *Int. Math. Res. Not.* (online publication August 2018), art. id. rny202, 36 pp.

[Perret-Gentil 2018b] C. Perret-Gentil, "Integral monodromy groups of Kloosterman sheaves", *Mathematika* **64**:3 (2018), 652–678. MR Zbl

[Pink 2000] R. Pink, "Strong approximation for Zariski dense subgroups over arbitrary global fields", *Comment. Math. Helv.* **75**:4 (2000), 608–643. MR Zbl

[van der Poorten and Schlickewei 1991] A. J. van der Poorten and H. P. Schlickewei, "Additive relations in fields", *J. Austral. Math. Soc. Ser. A* **51**:1 (1991), 154–170. MR Zbl

[Rains 1997] E. M. Rains, "High powers of random elements of compact Lie groups", *Probab. Theory Related Fields* **107**:2 (1997), 219–241. MR Zbl

[Rosen 2002] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics **210**, Springer, 2002. MR Zbl

[Rubinstein and Sarnak 1994] M. Rubinstein and P. Sarnak, "Chebyshev's bias", *Experiment. Math.* **3**:3 (1994), 173–197. MR Zbl

[Rudnick and Waxman 2019] Z. Rudnick and E. Waxman, "Angles of Gaussian primes", *Israel J. Math.* **232**:1 (2019), 159–199. MR Zbl

[SGA $4\frac{1}{2}$ 1977] P. Deligne, *Cohomologie étale* (Séminaire de Géométrie Algébrique du Bois Marie), Lecture Notes in Math. **569**, Springer, 1977. MR Zbl

[Speyer 2011] D. E. Speyer, "Faithful representations and tensor powers", answer on MathOverflow, 2011, available at https://mathoverflow.net/q/63043.

[Stein 1993] E. M. Stein, *Harmonic analysis: real-variable methods, orthogonality, and oscillatory integrals*, Princeton Mathematical Series **43**, Princeton University Press, 1993. MR Zbl

[Steinberg 1962] R. Steinberg, "Complete sets of representations of algebras", *Proc. Amer. Math. Soc.* **13** (1962), 746–747. MR Zbl

[Weisfeiler 1984] B. Weisfeiler, "Strong approximation for Zariski-dense subgroups of semisimple algebraic groups", *Ann. of Math.* (2) **120**:2 (1984), 271–315. MR Zbl

Communicated by Melanie Matchett Wood
Received 2019-05-09 Revised 2019-09-14 Accepted 2019-12-16

corentin.perretgentil@gmail.com *Zürich, Switzerland*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2020 is US $415/year for the electronic version, and $620/year (+$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 14 No. 5 2020

1937-0652(2020)14:5;1-X