EXCEPTIONAL BIASES IN COUNTING PRIMES OVER FUNCTION FIELDS

ALEXANDRE BAILLEUL, LUCILE DEVIN, DANIEL KELIHER, AND WANLIN LI

Abstract. We study how often exceptional configurations of irreducible polynomials over finite fields occur in the context of prime number races and Chebyshev's bias. In particular, we show that three types of biases, which we call "complete bias", "lower order bias" and "reversed bias", occur with probability going to zero among the family of all squarefree monic polynomials of a given degree in $\mathbb{F}_q[x]$ as q, a power of a fixed prime, goes to infinity. The bounds given extend a previous result of Kowalski, who studied a similar question along particular 1-parameter families of reducible polynomials. The tools used are the large sieve for Frobenius developed by Kowalski, an improvement of it due to Perret-Gentil and considerations from the theory of linear recurrence sequences and arithmetic geometry.

1. Introduction

Chebyshev's bias is the phenomenon that there are more prime numbers of the form $4n + 3$ than of the form $4n + 1$ in initial intervals $[\![2, x]\!]$ of $\mathbb{N}$ for most values of x (more precisely, the set of such x admits a logarithmic density of around 99.59%). More generally, primes which are congruent to a fixed non-square residue class modulo an integer q are more numerous than those which are congruent to a given square residue class modulo q in initial intervals of $\mathbb{N}$. The origin of this phenomenon was explained by Rubinstein and Sarnak in [RS94].

The analogue of Chebyshev's bias over function fields was first considered by Cha in [Cha08] to study inequities in the distribution of irreducible polynomials in residue classes of $\mathbb{F}_q[x]$, and later by Cha and Im in [CI11] in function field extensions. As in the classical archimedean case of [RS94], a central hypothesis is a linear independence hypothesis which will be noted LI throughout. If the arguments of the non-trivial inverse zeros (of non-negative imaginary parts) of the underlying L-functions are of the form $\sqrt{q}e^{i\theta}$, then LI claims that the θ's, together with π, are linearly independent over $\mathbb{Q}$. A consequence of LI is that Chebyshev's bias favours non-square residue classes rather than square residue classes in the distribution of primes. See [RS94, page 185] (where it is called GSH) for the archimedean case, and [Cha08, page 1366] for the function field case. For surveys on prime number races over $\mathbb{Q}$, see [FK02a] and [GM06].

Over $\mathbb{Q}$ and number fields, exceptional biases have been studied in the literature, notably in a series of papers by Ford and Konyagin [FK02b, FK03] and [FKL13] using particular configurations of zeros of L-functions. Fiorilli and Martin [FM13], under both the Generalized Riemann Hypothesis and LI, list the largest possible biases in the prime number race between quadratic residues and non-quadratic residues. In number field extensions, Bailleul produced infinite families of examples for which the bias is reversed, favouring squares over non-squares, conditional on a suitable linear independence hypothesis [Bai21]. As for unconditional results, Fiorilli and Jouve constructed infinite families exhibiting a complete bias in [FJ22].

The state of affairs in the function field setting is rather different. For instance, over $\mathbb{F}_q[x]$, there are a few known counterexamples to LI (see [Cha08, Section 5], [DM21, Section 3], [DKRV21, Section 7], [Sed22, Section 10]), which can lead to what we call "exceptional biases". In [CFJ16], Cha, Fiorilli and Jouve give examples of exceptional biases in Mazur's race related to counting points on elliptic curves. They prove also the genericity of LI for certain families in this context in [CFJ17].

In this paper, we investigate three types of exceptional biases. Namely, we call "complete bias" the situation where there are more primes in non-square residue classes than in square residue classes 100% of the time. We call "lower order bias" the situation in which there could often be exactly as many primes that are square residues as non-square residues. Finally, we call "reversed bias" the situation in which square residue classes are favored over non-square residue classes. See Definitions 2.2, 2.4, and 2.6 for rigorous definitions of these terms. For those types of biases, we establish more precise necessary conditions than negation of LI for them to hold, and we show that they happen very rarely.

In order to state our results more precisely, we need to introduce some notation. When q is a power of a prime p and $d \geq 1$, we let

$$\mathcal{H}_d(\mathbb{F}_q) = \{f \in \mathbb{F}_q[x] \mid f \text{ is monic, squarefree}, \deg f = d\}.$$

For $f \in \mathcal{H}_d(\mathbb{F}_q)$, let χ_f denote the unique primitive quadratic character modulo f, and

$$\Pi(n;\chi_f) := \frac{n}{q^{n/2}}\Big(\#\{h \in \mathbb{F}_q[x] \mid h \text{ is irreducible}, \ \deg h = n \text{ and } \chi_f(h) = 1\} \\ - \#\{h \in \mathbb{F}_q[x] \mid h \text{ is irreducible}, \ \deg h = n \text{ and } \chi_f(h) = -1\}\Big).$$

Note that when f is irreducible then this is, up to a positive factor, the difference between the number of irreducible square residues modulo f of degree n and those which are non-square residues. We also denote by $\mathcal{C}_f$ the hyperelliptic curve defined over $\mathbb{F}_q$ as the smooth projective model of the curve with affine equation $y^2 = f(x)$.

In [Kow08b], Kowalski showed that, in a precise quantitative sense (see formula (1.1) below), as $q \to \infty$, the LI hypothesis is generically true for the zeta functions of hyperelliptic curves of the form $\mathcal{C}_{h(x)(x-t)}$, where $h \in \mathcal{H}_d(\mathbb{F}_q)$ of even degree is fixed and $t \in \mathbb{F}_q$ is a parameter such that $h(t) \neq 0$. This implies that for most of the parameters t, the counting function $\Pi(n;\chi_{h(x)(x-t)})$ is biased towards negative values and changes sign infinitely many times. This behavior is expected to hold for $\Pi(n;\chi_f)$ generically among $f \in \mathcal{H}_d(\mathbb{F}_q)$ because of LI.

Our main results are the following four bounds, which extend Kowalski's result to the full family of square free polynomials. We also improve the upper bound with more restrictive conditions. Recall that the terms "complete bias", "lower order bias", and "reversed bias" used in the statement are rigorously defined, respectively, in Definitions 2.2, 2.4, and 2.6. Each of these three notions correspond to a natural refinement of the condition that the LI hypothesis is not satisfied.

Theorem 1.1. *Let p be an odd prime number, q a power of p and $d \geq 1$. We write $g = \lfloor \frac{d-1}{2} \rfloor$ and $A = 2g^2 + g + 2$.*

(1) *We have*

$$\frac{1}{|\mathcal{H}_d(\mathbb{F}_q)|}\#\{f \in \mathcal{H}_d(\mathbb{F}_q) \mid \text{ The zeta function of } \mathcal{C}_f \text{ does not satisfy LI}\} \ll_{p,g} q^{-\frac{1}{2A}}(\log q)^{1-\delta}$$

where $\delta \leq 1$ satisfies $\delta \underset{g\to+\infty}{\sim} \frac{1}{8g}$.

(2) *If q is a square then, we have*

$$\frac{1}{|\mathcal{H}_d(\mathbb{F}_q)|}\#\{f \in \mathcal{H}_d(\mathbb{F}_q) \mid \Pi(n;\chi_f) \text{ exhibits a complete bias}\} \ll_{p,g} q^{-\frac{1}{A}}\log q,$$

and $\#\{f \in \mathcal{H}_d(\mathbb{F}_q) \mid \Pi(n;\chi_f)$ exhibits a complete bias$\} = 0$ otherwise.

(3) *We have*

$$\frac{1}{|\mathcal{H}_d(\mathbb{F}_q)|}\#\{f \in \mathcal{H}_d(\mathbb{F}_q) \mid \Pi(n;\chi_f) \text{ exhibits a lower order bias}\} \ll_{p,g} q^{-\frac{1}{A}}\log q.$$

(4) *We have*

$$\frac{1}{|\mathcal{H}_d(\mathbb{F}_q)|}\#\{f \in \mathcal{H}_d(\mathbb{F}_q) \mid \Pi(n;\chi_f) \text{ exhibits a reversed bias}\} \ll_{p,g} q^{-\frac{1}{2A}}(\log q)^{1-\delta'},$$

where $\delta' \leq 1$ satisfies $\delta' \underset{g\to+\infty}{\sim} \frac{7}{24g}$.

To prove this theorem, we follow closely Kowalski's method based on the large sieve for Frobenius developed in [Kow08a] (and improved by Perret-Gentil [PG20]). The theorem above should be compared to Kowalski's bound (1.1), which we now state.

Theorem 1.2 ([Kow08b, Proposition 1.1])**.** *Let $g \geq 1$ be an integer, and let $f \in \mathbb{Z}[x]$ be a squarefree monic polynomial of degree $2g$. Let p be an odd prime such that p does not divide the discriminant of f, and let $U/\mathbb{F}_p$ be the open subset of the affine t-line where $f(t) \neq 0$. Consider the algebraic family $\mathcal{C}_f \to U$ of smooth* *projective hyperelliptic curves of genus g given as the smooth projective models of the curves with affine equations*

$$C_t : y^2 = f(x)(x-t), \quad \text{for } t \in U.$$

Then for any extension $\mathbb{F}_q/\mathbb{F}_p$ we have

$$\frac{1}{|U(\mathbb{F}_q)|}\#\{t \in U(\mathbb{F}_q) \mid \text{ The zeta function of } C_t \text{ does not satisfy LI}\} \ll_g q^{-\frac{1}{2A}}(\log q)^{1-\delta}, \tag{1.1}$$

where $A = 2g^2 + g + 2$, and $\delta \leq 1$ satisfies $\delta \underset{g\to+\infty}{\sim} \frac{1}{8g}$.

Remark 1.3. The bound stated in [Kow08b] is a bit larger, the exponent of $\log q$ is simply 1, but Kowalski gave this better exponent in [Kow08a, Theorem 8.15], for the more general condition that the Galois group of the zeta function of C_t is not maximal. It is indeed more general since if there exists a non-trivial linear relation between π and the arguments of the roots of the zeta function, hence a multiplicative relation between those roots, then its Galois group is not maximal since this relation cannot be preserved by every allowed permutations of the roots. However, note there is a typo in the bound stated in [Kow08a, Theorem 8.15]: the exponent there reads $1-\delta$ with $\delta \underset{g\to+\infty}{\sim} \frac{1}{4g}$, coming from the larger contribution of $\delta_2 \geq \frac{1}{4g}$ in p.181 of loc. cit., but we can actually only get $\delta_2 \geq \frac{1}{8g}$. The count is detailed in [Kow06, Lemma 7.3 iii)] but the author is counting each symplectic polynomial with a given factorization twice, hence a missing $\frac{1}{2}$ factor. The proof of Lemma 7.7 fixes this.

It should be noted that our method would allow us to prove the same bounds as in Theorem 1.1 along Kowalski's family of curves in Theorem 1.2, independently of p, by using the large sieve estimate [Kow08a, Corollary 8.10] instead of Proposition 2.22 of this paper. Observe however that by passing to a multidimensional space of parameters, we lose the uniformity in p in the bounds. Such a phenomenon was already present in [Kow08a, Corollary 8.10] where it results in a larger exponent of q in the multidimensional case. In our case, we keep the small q exponent, but the uniformity in p is lost when applying the improved bound [PG20, Theorem 5.14.(ii).(c)].

Moreover, note that in the case of a complete bias (Theorem 1.1.2) and in the case of a lower order bias (Theorem 1.1.3), we improve the exponents for q in the upper bounds by a factor 2 compared to the bound for LI. In our last bound, which is the case of a reversed bias (Theorem 1.1.4), we improve the exponent for $\log q$.

For the first two properties considered in Theorem 1.1, inputs from arithmetic geometry give us better bounds for some restricted genera. Our first improvement is for genus 1 or 2 concerning the failure of LI.

Theorem 1.4. *Let $p \neq 2, 3$ be a prime number, q a power of p and $3 \leq d \leq 6$. We write $g = \lfloor \frac{d-1}{2} \rfloor$, so that $1 \leq g \leq 2$. When $g = 1$, we have*

$$\frac{1}{|\mathcal{H}_d(\mathbb{F}_q)|}\#\{f \in \mathcal{H}_d(\mathbb{F}_q) \mid \text{ The zeta function of } \mathcal{C}_f \text{ does not satisfy LI}\} \ll \frac{p}{q}.$$

When $g = 2$, then we have

$$\frac{1}{|\mathcal{H}_d(\mathbb{F}_q)|}\#\{f \in \mathcal{H}_d(\mathbb{F}_q) \mid \text{ The zeta function of } \mathcal{C}_f \text{ does not satisfy LI}\} \ll_p q^{-\frac{1}{12}} \log q.$$

In particular, in this more restricted setting, these bounds improve on Theorem 1.1 1 and *a fortiori* on Theorem 1.1 4. Note that the result for genus at most two comes from the fact that we completely understand the Frobenius eigenvalues for genus 1 and 2 hyperelliptic curves over $\overline{\mathbb{F}}_p$. The reason is that all smooth projective curves of genus at most two are hyperelliptic, and the Torelli image of the moduli space of smooth projective genus 2 curves $\mathcal{M}_2$ is dense in the moduli space of abelian surfaces $\mathcal{A}_2$. Neither of these facts holds for higher genus.

Our last result is a bound for the bias dealt with in Theorem 1.1 2 which is uniform in the degree, at the expense of being worse in terms of q for small g.

Theorem 1.5. *If $q = p^e$ is a fixed prime power with $2 \mid e$. Then,*

$$\sup_{d\geq 3} \frac{1}{|\mathcal{H}_d(\mathbb{F}_q)|}\#\{f \in \mathcal{H}_d(\mathbb{F}_q) \mid \Pi(n;\chi_f) \text{ exhibits a complete bias}\} \ll \frac{1}{q^{1/276}}.$$

In particular, this bound is better than the second bound of Theorem 1.1 in terms of q as soon as $g \geq 12$. The underlying method coming from arithmetic geometry cannot deal with the conditions in Theorem 1.1 3 and 4 because they are concerned with multiple zeros of the zeta function of $\mathcal{C}_f$ at once.

Outline of the paper. In Section 2 we set the notation and give preliminary results used in the rest of the paper. In particular, section 2.3 states some results about linear recurrent sequences, and section 2.4 is devoted to the proof of a large sieve statement, which is one important step in the proof of Theorem 1.1. In Section 3 we give a proof of the first item of Theorem 1.1 following Kowalski's method and Theorem 1.4 by elementary methods. In Section 4 we derive conditions for a complete bias and prove the second item of Theorem 1.1 with the large sieve for Frobenius and Theorem 1.5 with arithmetic geometry. In Section 5 and 6 we derive conditions for a lower order bias and a reversed bias respectively and we prove the last two items of Theorem 1.1. Finally, in Section 7 we gather counting lemmas obtained using our large sieve result Proposition 2.22 that are used in the proofs of the different parts of Theorem 1.1.

Acknowledgements. This work was partially supported by the grant KAW 2019.0517 from the Knut and Alice Wallenberg Foundation (for LD). Part of this work was conducted while WL was in residence at the Mathematical Sciences Research Institute in Berkeley, California, during the Spring 2023 semester. The aim of this work is to answer a question asked by Kannan Soundararajan to the second author as she was visiting Stanford, she is very grateful for the invitation and the discussion. The authors thank Byungchul Cha, Florent Jouve, Jordan Ellenberg and Emmanuel Kowalski for helpful discussions. They also thank Régis de la Bretèche for organizing the elementary and analytic number theory seminar in IHP, Paris, where ideas used in this paper were born.

2. Preliminary results and notations

2.1. **Notations and Definitions.** We first provide notations for the rest of the paper. When $f \in \mathcal{H}_d(\mathbb{F}_q)$, the projective curve with affine model $y^2 = f(x)$ is denoted by $\mathcal{C}_f$. Recall that $\mathcal{C}_f$ has genus $g = \lfloor \frac{d-1}{2} \rfloor$.

For $f \in \mathcal{H}_d(\mathbb{F}_q)$, let χ_f be the primitive quadratic character modulo f. We want to compare the number of degree n irreducible polynomials P over $\mathbb{F}_q$ such that $\chi_f(P) = 1$ and those such that $\chi_f(P) = -1$ for varying n. Define the Dirichlet L-function associated to a Dirichlet character χ modulo f as

$$L(s, \chi) = \sum_{a \text{ monic}} \frac{\chi(a)}{|a|^s} = \prod_{P \text{ irreducible}} \left(1 - \frac{\chi(P)}{|P|^s}\right)^{-1},$$

where $|a| = q^{\deg a}$ and the sum and product above range over monic (resp. irreducible) polynomials of $\mathbb{F}_q[x]$.

We now recall some properties of the L-functions under consideration; see e.g. [Ros02, Proposition 4.3, Theorem 5.9] for details. For a non-principal Dirichlet character χ, the Dirichlet L-function $L(s, \chi)$ is a polynomial $\mathcal{L}(u, \chi)$ in $u := q^{-s}$ with integer coefficients and the zeta function of $\mathcal{C}_f$ is a rational function in u, which we denote by $\zeta(\mathcal{C}_f, u) = \frac{Z_f(u)}{(1-u)(1-qu)}$. Thanks to the deep work of Weil [Wei48], we know the analogue of the Riemann Hypothesis is satisfied for these zeta functions, that is their inverse zeros have absolute value $\sqrt{q}$. When d is odd, then $\mathcal{L}(u, \chi_f) = Z_f(u)$, and when d is even, we have $\mathcal{L}(u, \chi_f) = Z_f(u)(1-u)$. In the following, we will mostly use the reciprocal polynomial

$$P_f(T) = T^{2g} Z_f(T^{-1}), \tag{2.1}$$

which is monic, and its roots are the inverse zeros of Z_f.

We denote by $\alpha_j(\chi) = \sqrt{q} e^{i\theta_j(\chi)}$ the distinct inverse zeros of $\mathcal{L}(u, \chi)$ of norm $\sqrt{q}$, with multiplicity $m_{\theta_j}(\chi)$. We might forget the dependency in the character χ when only one character is considered and the notation stays clear from the context. We let r be the number of distinct pairs of conjugate non-real zeros of $\mathcal{L}(u, \chi_f)$. Since $\mathcal{L}(u, \chi_f)$ has real coefficients, after reordering, we can assume $\theta_{j+r}(\chi_f) = -\theta_j(\chi_f)$ and we have $m_{\theta_j}(\chi_f) = m_{-\theta_j}(\chi_f)$ for $1 \leq j \leq r$. Since χ_f is primitive, we have

$$m_0(\chi_f) + m_\pi(\chi_f) + 2\sum_{j=1}^{r} m_{\theta_j}(\chi_f) = 2g.$$

Using the explicit formula in [Cha08, Proposition 4.2], our object of study is the function

$$\begin{aligned}\Pi(n;\chi_f) :=\ & \frac{n}{q^{n/2}}\Big(\#\{h\in\mathbb{F}_q[x]\mid h \text{ is irreducible },\ \deg h=n \text{ and } \chi_f(h)=1\}\\ & -\#\{h\in\mathbb{F}_q[x]\mid h \text{ is irreducible },\ \deg h=n \text{ and } \chi_f(h)=-1\}\Big)\\ =\ & \frac{n}{q^{n/2}}\sum_{\substack{\deg h=n\\ h \text{ irreducible}}}\chi_f(h)\\ =\ & -\left(m_0(\chi_f)+\tfrac12\right)-\left(m_\pi(\chi_f)+\tfrac12\right)(-1)^n-\sum_{\theta_j\neq0,\pi}m_{\theta_j}(\chi_f)e^{in\theta_j(\chi_f)}+O_f\left(q^{-\frac{n}{6}}\right).\end{aligned}\tag{2.2}$$

Let $\Delta_f(n)$ be the opposite of the main sum of $\Pi(n;\chi_f)$ in (2.2); that is

$$\Delta_f(n)=\left(m_0(\chi_f)+\tfrac12\right)+\left(m_\pi(\chi_f)+\tfrac12\right)(-1)^n+\sum_{\theta_j\neq0,\pi}m_{\theta_j}(\chi_f)e^{in\theta_j(\chi_f)}.\tag{2.3}$$

In the case the set $\{\theta_1(\chi_f),\dots,\theta_r(\chi_f)\}\cup\{\pi\}$ is linearly independent over $\mathbb{Q}$, which is expected to be the generic case, then $\Delta_f(n)-\left(m_0(\chi_f)+\frac12\right)$ oscillates around zero and takes positive (resp. negative) values half of the time (i.e., for 50% of positive integers n). Thus, Δ_f is larger (resp. smaller) than its mean value $m_0(\chi_f)+\frac12$ for half of the positive integers n. One deduces (see [Cha08, page 1366]) that there is a bias in the distribution of the values of Δ_f in the direction of positive values, *i.e.* coming back to $\Pi(n;\chi_f)$ we expect a bias towards negative values. Or in other terms, there are in general more irreducible polynomials P of degree n with $\chi_f(P)=-1$ than with $\chi_f(P)=1$.

Now, it can happen that the oscillating part does not distribute so well between positive and negative values. This is the case in the examples given in [Cha08, Section 5] and also for the different kinds of behaviors we consider in this paper.

Remark 2.1. In this paper, we are studying the summatory function of a quadratic character over irreducible polynomials. Another "prime number race" of interest is the one between quadratic residues and non-quadratic residues. Observe that these are the same in the case f is irreducible. In the case f is not irreducible, one has to take into account the contribution of all quadratic (non-necessarily primitive) characters modulo f, which makes the study more difficult. The general formula proved in [DM21, Proposition 5.2] is

$$\begin{aligned}\Pi(n;f,\square,\boxtimes) :=\ & \frac{n}{q^{n/2}}\Big(\frac{1}{|\square|}|\{h\in\mathbb{F}_q[x]\mid h \text{ monic irreducible},\ \deg h=n, h \bmod f\in\square\}|\\ & -\frac{1}{|\boxtimes|}|\{h\in\mathbb{F}_q[x]\mid h \text{ monic irreducible},\ \deg h=n, h \bmod f\in\boxtimes\}|\Big)\\ =\ & \frac{-1}{|\boxtimes|}\Bigg\{\sum_{\chi\in X_f^{\text{quad}}}\Bigg(\left(m_0(\chi)+\tfrac12\right)+\left(m_\pi(\chi)+\tfrac12\right)(-1)^n+\sum_{\theta_j\neq0,\pi}m_{\theta_j}(\chi)e^{in\theta_j(\chi)}\Bigg)\\ & +O_f\left(q^{-\frac{n}{6}}\right)\Bigg\},\end{aligned}$$

where $\square$ denotes the set of quadratic residues modulo f, $\boxtimes$ denotes the set of non-quadratic residues modulo f and X_f^{quad} is the set of quadratic characters modulo f.

For a given $f\in\mathcal{H}_d(\mathbb{F}_q)$, we define three kinds of "exceptional biases" as follows.

Definition 2.2. [Complete bias] We say that $\Pi(n,\chi_f)$ exhibits a *complete bias* if $\Delta_f(n)>0$ for almost all n, that is when

$$\operatorname{dens}(\Delta_f(n)>0):=\lim_{X\to+\infty}\frac1X\sum_{n\le X}\mathbf{1}_{\Delta_f(n)>0}=1.$$

Remark 2.3. [$\Pi(n,\chi_f)$ vs. $\Delta(n,\chi_f)$] In particular, if $\Pi(n,\chi_f)$ exhibits a complete bias, then $\operatorname{dens}(\Pi(n,\chi_f)<0)$ exists and is equal to 1, but the converse need not hold. Note that the above definition may not cover all the cases for which $\overline{\operatorname{dens}}(\Pi(n,\chi_f)<0)=1$: it may happen that $\Delta_f(n)=0$ for a positive proportion of n and then for those n, the sign of $\Pi(n,\chi_f)$ is determined by the sign of the error term $O_f\left(q^{-\frac{n}{6}}\right)$ and necessitate further study. In the next definition, we define the case of "lower order bias" below to characterize this possibility.

Definition 2.4. [Lower order bias] We say that $\Pi(n,\chi_f)$ exhibits a *lower order bias* if $\Delta_f(n)=0$ for a positive proportion of n. That is,

$$\mathrm{dens}(\Delta_f(n)=0) := \lim_{X\to+\infty}\frac{1}{X}\sum_{n\le X}\mathbf{1}_{\Delta_f(n)=0} > 0.$$

Remark 2.5. The condition of having a lower order bias is close to the condition "ties have positive density", as introduced by Martin and Ng in [MN20] in the context of prime number races.

Finally, the last type of exceptional bias we are going to study is a direct incompatibility with the expectation that $\Pi(n,\chi_f)$ is negative for more than 50% of integers n.

Definition 2.6. [Reversed bias] We say that $\Pi(n,\chi_f)$ exhibits a *reversed bias* if $\Delta_f(n)<0$ for more than half of the n. That is,

$$\mathrm{dens}(\Delta_f(n)<0) := \lim_{X\to+\infty}\frac{1}{X}\sum_{n\le X}\mathbf{1}_{\Delta_f(n)<0} > \frac{1}{2}.$$

Remark 2.7.

(1) In Section 2.3, we will show the three densities in Definitions 2.2,2.4,2.6 exist, see Corollaries 2.15 and 2.17.
(2) Note that both a lower order bias and a reversed bias may occur simultaneously, but that is the only possible combination of two exceptional biases.

Remark 2.8. Observe that we could also (as in [Cha08, DM21]) count irreducible polynomials of degree $\le n$ instead of degree $=n$. In this case, the functions replacing $\Pi(n;f,\square,\boxtimes)$ and $\Pi(n,\chi_f)$ take the following more complicated forms:

$$\begin{aligned}
\Pi(\le n;f,\square,\boxtimes) :=\ & \frac{n}{q^{n/2}}\Big(\frac{1}{|\square|}|\{h\in\mathbb{F}_q[x]\mid h \text{ monic irreducible, } \deg h\le n, h \bmod f\in\square\}| \\
& -\frac{1}{|\boxtimes|}|\{h\in\mathbb{F}_q[x]\mid h \text{ monic irreducible, } \deg h\le n, h \bmod f\in\boxtimes\}|\Big) \\
=\ & \frac{-1}{|\boxtimes|}\Bigg\{\sum_{\chi\in X_f^{\mathrm{quad}}}\Bigg(\left(m_0(\chi)+\tfrac12\right)\frac{\sqrt{q}}{\sqrt{q}-1}+\left(m_\pi(\chi)+\tfrac12\right)\frac{\sqrt{q}}{\sqrt{q}+1}(-1)^n \\
& +\sum_{\theta_j\ne0,\pi} m_{\theta_j}(\chi)\frac{\sqrt{q}e^{i\theta_j(\chi)}}{\sqrt{q}e^{i\theta_j(\chi)}-1}e^{in\theta_j(\chi)}\Bigg)+O_f\left(q^{-\frac{n}{6}}\right)\Bigg\}; \\
\Pi(\le n;\chi_f) :=\ & \frac{n}{q^{n/2}}\sum_{\substack{\deg h\le n\\ h\text{ irreducible}}}\chi_f(h) \\
=\ & -\left(m_0(\chi_f)+\tfrac12\right)\frac{\sqrt{q}}{\sqrt{q}-1}-\left(m_\pi(\chi_f)+\tfrac12\right)\frac{\sqrt{q}}{\sqrt{q}+1}(-1)^n \\
& -\sum_{\theta_j\ne0,\pi} m_{\theta_j}(\chi_f)\frac{\sqrt{q}e^{i\theta_j(\chi_f)}}{\sqrt{q}e^{i\theta_j(\chi_f)}-1}e^{in\theta_j(\chi_f)}+O_f\left(q^{-\frac{n}{6}}\right),
\end{aligned}$$

where the sums are over $\{h\in\mathbb{F}_q[x]\mid h \text{ monic irreducible, } \deg h\le n\}$.

We cannot adapt most of our proofs for those quantities. For instance, the maximal value of such a sum is not easy to determine, and we'll make frequent use of the maximum values in Section 4.1 (e.g. the proof of Proposition 4.2 to see why maximal values are relevant to us). However, we have for example $\Delta(\le n;f,\square,\boxtimes)=\Delta(n;f,\square,\boxtimes)+O\left(\frac{\sum_\theta m_\theta(\chi_f)}{\sqrt{q}}\right)$, where $\Delta(\le n;f,\square,\boxtimes)$ represents the main sum in $\Pi(\le n;f,\square,\boxtimes)$ above, and so if q is large enough compared to $\sum_\theta m_\theta(\chi_f)$, the sign of $\Delta(\le n;f,\square,\boxtimes)$ is the sign of $\Delta(n;f,\square,\boxtimes)$. In particular, under the right conditions, a complete bias and a reversed bias in the "degree $=n$" setting one gets from studying $\Pi(n;\chi_f)$, implies a similar bias in the "degree $\le n$" setting one gets from studying $\Pi(\leq n; \chi_f)$. Note also that the difference between counting irreducible polynomials of degree equal to n and counting those of degree at most n is analogous to the difference between counting prime number in intervals of the form $[X, 2X]$ and those in intervals of the form $[2, X]$.

2.2. **Properties of limiting distributions.** To study the densities involved in the definitions 2.2, 2.4, and 2.6, we will use the notion of limiting distribution, which we define as follows.

Definition 2.9. Let $D : \mathbb{N} \to \mathbb{R}$ be a real function, we say that D admits a limiting distribution if there exists a probability measure μ on Borel sets in $\mathbb{R}$ such that for any bounded continuous function h on $\mathbb{R}$, we have

$$\lim_{Y\to\infty} \frac{1}{Y} \sum_{n\leq Y} h(D(n)) = \int_{\mathbb{R}} h(t)\,\mathrm{d}\mu(t).$$

We call μ the limiting distribution of the function D.

The function Δ_f defined as Equation 2.3 is quasi-periodic, and we can apply the Kronecker-Weyl equidistribution theorem (see e.g. [Hum12, Lemma 2.7] and [Bai22, Theorem 2.2]) to prove the following proposition ([DM21, Proposition 2.1]).

Proposition 2.10. *The function Δ_f admits a limiting distribution μ_{Δ_f} with mean value $m_0(\chi_f) + \frac{1}{2}$ and variance*

$$(m_\pi(\chi_f) + \tfrac{1}{2})^2 + \frac{1}{2} \sum_{j=1}^{r} m_{\theta_j}(\chi_f)^2.$$

Moreover, the measure μ_{Δ_f} has support in

$$\left[m_0(\chi_f) - m_\pi(\chi_f) - 2\sum_{j=1}^{r} m_{\theta_j}(\chi_f),\ m_0(\chi_f) + m_\pi(f) + 1 + 2\sum_{j=1}^{r} m_{\theta_j}(\chi_f) \right].$$

The next lemma will be used to study reversed biases.

Lemma 2.11. *The distribution μ_{Δ_f} in Proposition 2.10 is symmetric with respect to $m_0(\chi_f) + \frac{1}{2}$ if and only if there is no relation*

$$k_0\pi + \sum_{j=1}^{r} k_j\theta_j \equiv 0 \mod 2\pi$$

with $k_0, \ldots, k_r \in \mathbb{Z}$ and $k_0 + \sum_{j=1}^{r} k_j \equiv 1 \mod 2$.

Proof. Denote by $A(\Delta_f)$ the closure of the 1-parameter group $H := \{n(\pi, \theta_1, \ldots, \theta_r) : n \in \mathbb{Z}\}/(2\pi\mathbb{Z})^{r+1}$ in the $(r+1)$-dimensional torus $\mathbb{T}^{r+1} := (\mathbb{R}/2\pi\mathbb{Z})^{r+1}$. We first remark that by Pontryagin duality, for any $\underline{z} \in \mathbb{T}^{r+1}$, $\underline{z} \in A(\Delta_f)$ if and only if for every character $\underline{k} = (k_0, \ldots, k_r) \in H^{\perp} \subset \mathbb{Z}^{r+1}$, one has $\underline{k}(\underline{z}) = k_0z_0 + \cdots + k_rz_r = 0$. Therefore, we just need to show that μ_{Δ_f} is symmetric with respect to $m_0(\chi_f) + \frac{1}{2}$ if and only if $(\pi, \ldots, \pi) \in A(\Delta_f)$, since $\underline{k}(\pi, \ldots, \pi) = 0$ if and only if $\sum_{i=0}^{r} k_i$ is even.

By the Kronecker–Weyl Equidistribution Theorem (see for example [DM21, Lemma 2.2]), $A(\Delta_f)$ is a subtorus of $\mathbb{T}^r$ and we have, for any continuous function $h : \mathbb{T}^r \to \mathbb{C}$,

$$\lim_{Y\to\infty} \frac{1}{Y} \sum_{n=0}^{Y} h(n\pi, n\theta_1, \ldots, n\theta_r) = \int_{A(\Delta_f)} h(a)\,\mathrm{d}\omega_{A(\Delta_f)}(a)$$

where $\omega_{A(\Delta_f)}$ is the normalized Haar measure on $A(\Delta_f)$. Then μ_{Δ_f} is the push-forward measure of $\omega_{A(\Delta_f)}$ through

$$\int_{\mathbb{R}} h(t)\,\mathrm{d}\mu_{\Delta_f}(t) = \int_{A(\Delta_f)} h\Big(m_0(\chi_f) + \tfrac{1}{2} + (m_\pi(\chi_f) + \tfrac{1}{2})e^{ia_0} + 2\sum_{j=1}^{r} m_{\theta_j}(\chi_f)\cos(a_j)\Big)\,\mathrm{d}\omega_{A(\Delta_f)}(a)$$

for any bounded continuous functions $h : \mathbb{R} \to \mathbb{R}$.

Now, μ_{Δ_f} is symmetric with respect to $m_0(\chi_f) + \frac{1}{2}$ if and only if, for every continuous function h, one has

$$\int_{\mathbb{R}} h(2m_0(\chi_f) + 1 - t)\,\mathrm{d}\mu_{\Delta_f}(t) = \int_{\mathbb{R}} h(t)\,\mathrm{d}\mu_{\Delta_f}(t).$$

Observe that

$$\int_{\mathbb{R}} h(2m_0(\chi_f)+1-t)\,\mathrm{d}\mu_{\Delta_f}(t) = \int_{A(\Delta_f)} h\Big(m_0(\chi_f)+\tfrac{1}{2}-(m_\pi(\chi_f)+\tfrac{1}{2})e^{ia_0}-2\sum_{j=1}^{r} m_{\theta_j}(\chi_f)\cos(a_j)\Big)\,\mathrm{d}\omega_{A(\Delta_f)}(a)$$
$$= \int_{A(\Delta_f)} h\Big(m_0(\chi_f)+\tfrac{1}{2}+(m_\pi(\chi_f)+\tfrac{1}{2})e^{i(a_0+\pi)}+2\sum_{j=1}^{r} m_{\theta_j}(\chi_f)\cos(a_j+\pi)\Big)\,\mathrm{d}\omega_{A(\Delta_f)}(a).$$

So, if $(\pi,\dots,\pi)\in A(\Delta_f)$, using the fact that the Haar measure is translation-invariant, we deduce that μ_{Δ_f} is symmetric with respect to $m_0(\chi_f)+\frac{1}{2}$.

On the other hand, assume $(\pi,\dots,\pi)\notin A(\Delta_f)$. Then as $A(\Delta_f)$ is closed, and $m_\pi(\chi_f), m_{\theta_j}(\chi_f)\geq 0$ there exists $\epsilon>0$ such that for each $a\in A(\Delta_f)$ one has[1]

$$(m_\pi(\chi_f)+\tfrac{1}{2})e^{ia_0}+2\sum_{j=1}^{r} m_{\theta_j}(\chi_f)\cos(a_j) \geq \epsilon - m_\pi(\chi_f)-\tfrac{1}{2}-2\sum_{j=1}^{r} m_{\theta_j}(\chi_f).$$

Let h_ϵ be a non-zero, non-negative function, supported in an interval of length ϵ around $m_0(\chi_f)-m_\pi(\chi_f)-2\sum_{j=1}^{r} m_{\theta_j}(\chi_f)$. Then

$$\int_{\mathbb{R}} h_\epsilon(t)\,\mathrm{d}\mu_{\Delta_f}(t)=0$$

while

$$\int_{\mathbb{R}} h_\epsilon(2m_0(\chi_f)+1-t)\,\mathrm{d}\mu_{\Delta_f}(t)>0.$$

In particular, we deduce that μ_{Δ_f} is not symmetric with respect to $m_0(\chi_f)+\frac{1}{2}$. This concludes the proof. □

2.3. **Results about linear recurrence sequences.** We are interested in the positivity and zero-sets of the quantities $\Delta_f(n)$ defined in 2.3. One of the key insight is that those quantities are linear recurrence sequences which will imply the limits in Definitions 2.2, 2.4, and 2.6 exist as shown in Corollaries 2.15, 2.17.

Definition 2.12. A linear recurrence sequence of order $k\in\mathbb{Z}_{>0}$ is a sequence $(a_n)_{n\in\mathbb{N}}$ such that there exist $u_0,\dots,u_{k-1}\in\mathbb{C}$ satisfying

$$a_{n+k}=u_{k-1}a_{n+k-1}+\cdots+u_0a_n$$

for all $n\in\mathbb{N}$. We define its zero-set as $\{n\in\mathbb{Z}_{>0}\mid a_n=0\}$.

It is classical that any linear recurrence sequence can be expressed in a generalized power sum form and that, conversely, any generalized power sum satisfies a linear recurrence relation.

Lemma 2.13. *Let $f\in\mathcal{H}_d(\mathbb{F}_q)$, then the sequence Δ_f is a linear recurrence sequence.*

Proof. Let P_f be the reversed zeta function of the curve $\mathcal{C}_f : y^2=f(x)$ with $f\in\mathcal{H}_d(\mathbb{F}_q)$, and let χ_f be the primitive quadratic character modulo f and g be the genus of $\mathcal{C}_f$. The roots of P_f are $\alpha_1,\dots,\alpha_{2g}$ which are of the form $\sqrt{q}e^{i\theta_i(\chi_f)}$ with some of them possibly $\pm\sqrt{q}$. Then, the conclusion follows from [EvdPSW03, page 3]. □

Note that Lemma 2.13 is a well-known fact that follows directly from the rationality of the L-function. It is not a particularity of hyperelliptic curves. We stated and proved the result here, as this is the first time it is used in the context of studying Chebyshev's bias.

It turns out one can characterize the zero-set of such a linear recurrence sequence following the Skolem-Mahler-Lech theorem, which is stated below. A very short proof over $\mathbb{Q}$ (the Skolem case), which is the case of interest for us, using p-adic analysis, is given in [EvdPSW03, Theorem 2.1].

Theorem 2.14 (Skolem-Mahler-Lech, [EvdPSW03, Theorem 2.1])**.** *Assume $(a_n)_{n\in\mathbb{N}}$ is a linear recurrence sequence over a field of characteristic zero. Then its zero-set is the union of a finite set and a finite number of arithmetic progressions.*

This allows us to show that the density in the Definition 2.4 of a lower order bias always exists.

Corollary 2.15. *The density* $\mathrm{dens}(\Delta_f(n)=0)$ *in Definition 2.4 for lower order bias exists.*

[1] See Lemma 4.8 for an explicit bound.

Proof. By Lemma 2.13, Δ_f is a linear recurrence sequence. Its zero-set is a finite union of arithmetic progressions and a finite set following Theorem 2.14, therefore it admits a natural density. □

Another useful fact is the following result, showing that the densities considered for complete biases and reversed biases exist.

Theorem 2.16 ([BG07, Theorem 1])**.** *Let $(a_n)_{n\in\mathbb{N}}$ be a linear recurrence sequence of real numbers. Then its positivity set $\{n \in \mathbb{N} \mid a_n > 0\}$ admits a natural density.*

Corollary 2.17. *The densities* $\mathrm{dens}(\Delta_f > 0)$ *and* $\mathrm{dens}(\Delta_f < 0)$ *in Definitions 2.2 and 2.6 exist.*

For certain kinds of linear recurrence sequences, called non-degenerate linear recurrence sequences, we know their zero-sets are finite. We introduce the following more general terminology for the character χ_f inspired by [EvdPSW03, Section 1.1.9] because it will be an important condition to study in the proofs of (3) and (4) in Theorem 1.1.

Definition 2.18. We say that χ_f is *non-degenerate* when none of $\frac{\alpha_i}{\alpha_j}$, for $1 \le i \ne j \le r$, and none of $\frac{\overline{\alpha_i}}{\alpha_j}$, for $1 \le i, j \le r$, is a root of unity.

Using Definition 2.18, we prove the following Lemma which will be of important use in the study of lower order bias in Section 5.

Lemma 2.19. *Assume χ_f is non-degenerate as in Definition 2.18. Then the zero-set of $\Delta_f(n)$ is finite.*

Proof. By [EvdPSW03, page 25], a non-degenerate linear recurrence sequence, that is, a sequence whose characteristic roots $\beta_1, \dots, \beta_d$ satisfy that no $\frac{\beta_i}{\beta_j}$ is a root of unity for $i \ne j$, is equal to zero only finitely many times. In our case however, the characteristic roots are $\frac{\alpha_1}{\sqrt{q}}, \dots, \frac{\alpha_r}{\sqrt{q}}, \frac{\overline{\alpha_1}}{\sqrt{q}}, \dots, \frac{\overline{\alpha_r}}{\sqrt{q}}$, but also 1 and -1 because of the terms $m_0(\chi_f) + \frac{1}{2}$ and $\left(m_\pi(\chi_f) + \frac{1}{2}\right)(-1)^n$ in $\Delta_f(n)$, and obviously $\frac{1}{-1}$ is a root of unity. But it is easily seen that the subsequence $\Big(\Delta_f(2n)\Big)_{n\ge 0}$ is a linear recurrence sequence ([EvdPSW03, Theorem 1.1] and [EvdPSW03, Theorem 1.3]) with characteristic roots $\frac{\alpha_1^2}{q}, \dots, \frac{\alpha_r^2}{q}, \frac{\overline{\alpha_1}^2}{q}, \dots, \frac{\overline{\alpha_r}^2}{q}$, and 1. When χ_f is non-degenerate according to Definition 2.18, then $\Big(\Delta_f(2n)\Big)_{n\ge 0}$ is non-degenerate as a linear recurrence sequence. In particular, its zero-set is finite. The same argument applies to $\Delta_f(2n+1)$ with the same characteristic roots, and this proves that $\Delta_f(n)$ vanishes a finite number of times. □

Remark 2.20. In the non-degenerate case, we could replace the densities in Definitions 2.2 and 2.6 by the corresponding densities for $\Pi(n; \chi_f)$ since they exist and coincide with the ones about Δ_f in that case following the fact that the density $\mathrm{dens}(\Delta_f(n) = 0)$ in Definition 2.4 is zero.

2.4. **A large sieve statement.** Let $\mathrm{CSp}_{2g}(\mathbb{F}_\ell)$ be the group of symplectic similitudes[2] in $\mathrm{GL}_{2g}(\mathbb{F}_\ell)$. It contains matrices $M \in \mathrm{GL}_{2g}(\mathbb{F}_\ell)$ such that there exists a scalar $m \in \mathbb{F}_\ell^*$, called the multiplicator of M, satisfying $M^\top J M = mJ$ with $J = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$. When M is a symplectic similitude with multiplicator m, we say that M is m-symplectic. In this paper, following [Kow08a, page 158] but with a reversed convention, we call m-symplectic, any monic polynomial P of even degree $2g$ satisfying

$$P(T) = m^{-g} T^{2g} P\left(\frac{m}{T}\right).$$

In particular, for $f \in \mathcal{H}_d(\mathbb{F}_q)$ the polynomial P_f as defined in (2.1) is q-symplectic.

Let us first state the large sieve bound in Theorem 2.21 for a general setting, using Perret-Gentil's improvement of Kowalski's large sieve for Frobenius [PG20, Theorem 5.14.(ii).(c)] and later apply it to our setting in Proposition 2.22.

The theorem is given for a general $U/\mathbb{F}_p$ smooth affine geometrically connected algebraic variety of dimension $d \ge 1$ over $\mathbb{F}_p$. We assume that U has a compactification where it is the complement of a divisor with normal crossing. We denote by $\bar\eta$ a geometric generic point of U.

Let us fix Λ a set of primes different from 2 and p of density 1. We study a family $\mathcal{F}_\ell$ of lisse sheaves of $\mathbb{F}_\ell$-vector spaces on U, corresponding to continuous homomorphisms $\rho_\ell : \pi_1(U, \bar\eta) \to \mathrm{GL}_r(\mathbb{F}_\ell)$, for $\ell \in \Lambda$ that

[2] This is sometimes called the general symplectic group and denoted as GSp

arise from a compatible system (as in [Kow08a, Definition 8.7]). Then for $\ell \in \Lambda$, we denote $G_\ell = \rho_\ell(\pi_1(U, \overline{\eta}))$ and $G_\ell^{\mathrm{geo}} = \rho_\ell(\pi_1(U_{\overline{\mathbb{F}}_q}, \overline{\eta}))$.

Theorem 2.21. *Let p be a prime number and $q > 1$ be a power of p. For each $\ell \in \Lambda$, fix $\Omega_\ell \subset G_\ell$ a conjugacy invariant subset in the coset $\rho_\ell(\mathrm{Frob}_{f,q})G_\ell^{\mathrm{geo}}$.*

Then, for any $L \geq 1$ and for any q which is a power of p, one has

$$\frac{|\{f \in U(\mathbb{F}_q) \mid \rho_\ell(\mathrm{Frob}_{f,q}) \notin \Omega_\ell \text{ for all } \ell \leq L, \ell \in \Lambda\}|}{|U(\mathbb{F}_q)|} \leq \Big(1 + \frac{(L+1)^A C}{q^{\frac{1}{2}}}\Big) H^{-1},$$

with $C = C(U_{\overline{\mathbb{F}}_q}, \{\rho_\ell\}_{\ell \in \Lambda})$ a constant that depends only on $U_{\overline{\mathbb{F}}_q}$ and on the family $\{\rho_\ell\}_{\ell\in\Lambda}$ (in particular not on q, but certainly on d),

$$H = \sum_{\substack{m \in \mathcal{L} \\ \psi(m) \leq L+1}} \prod_{\ell \mid m} \frac{|\Omega_\ell|}{|G_\ell^{\mathrm{geo}}| - |\Omega_\ell|}, \tag{2.4}$$

where $\mathcal{L}$ is the set of squarefree integers whose prime factors are all in Λ, $\psi(m) := \prod_{\ell \mid m}(\ell + 1)$, and when $G_\ell^{\mathrm{geo}} = \mathrm{Sp}(2g, \mathbb{F}_\ell)$ one can take $A = 2g^2 + g + 2$.

Proof. We are in the setting of [Kow08a, Chapter 8], following the ideas and notations of loc. cit. It follows from [Kow08a, Proposition 2.9] as in [Kow08a, Corollary 8.10] that

$$\#\{f \in U(\mathbb{F}_q) \mid \rho_\ell(\mathrm{Frob}_{f,q}) \notin \Omega_\ell \text{ for all } \ell \leq L, \ell \in \Lambda\} \leq \Delta H^{-1},$$

where H is as defined in (2.4) and Δ is the large sieve constant. As in the proof of [Kow08a, Proposition 8.8] we obtain that

$$\Delta \leq \max_{\substack{m \in \mathcal{L} \\ \psi(m) \leq L+1}} \max_{\pi \in \Pi_m^*} \sum_{\substack{n \in \mathcal{L} \\ \psi(n) \leq L+1}} \sum_{\tau \in \Pi_n^*} |W(\pi, \tau)|$$

with

$$W(\pi, \tau) = \delta((m, \pi), (n, \tau)) q^d + O(\sigma_c'(\bar{U}, \mathcal{W}(\pi, \tau)) q^{d - \frac{1}{2}})$$

where $\mathcal{W}(\pi, \tau)$ is the lisse sheaf corresponding to the representation $[\pi, \bar{\tau}]$ as defined in [Kow08a, (3.8)], and σ_c' is the sum of all except the largest Betti numbers as defined in [Kow08a, page 166]. In [PG20, Section 5D2], Perret-Gentil improves the bound on $\sigma_c'(U_{\overline{\mathbb{F}}_q}, \mathcal{W}(\pi, \tau))$ compared to the bound of [Kow08a, Proposition 8.8] in the case of the complement of a divisor with normal crossing. He obtains

$$\sigma_c'(U_{\overline{\mathbb{F}}_q}, \mathcal{W}(\pi, \tau)) \ll_{U,\rho} \dim[\pi, \bar{\tau}] = \dim \pi \dim \tau,$$

where the implicit constant depends on $U_{\overline{\mathbb{F}}_q}$ and on the family $\{\rho_\ell\}_{\ell\in\Lambda}$ (in particular not on q, but certainly on d and on p). Thus, we have

$$\Delta \leq q^d + q^{d - \frac{1}{2}} C(U, \rho) \max_{\substack{m \in \mathcal{L} \\ \psi(m) \leq L+1}} \max_{\pi \in \Pi_m^*} \sum_{\substack{n \in \mathcal{L} \\ \psi(n) \leq L+1}} \sum_{\tau \in \Pi_n^*} \dim \pi \dim \tau.$$

To conclude, we use [Kow08a, (8.13)], and multiplicativity. In particular, representations of $\mathrm{Sp}(2g, \mathbb{F}_\ell)$ satisfy $\dim \pi \leq (\ell + 1)^{g^2}$ and $\sum_{\pi \in \Pi_\ell^*} \dim \pi \leq (\ell + 1)^{g^2 + g + 1}$. □

To extend Kowalski's bound (1.1) in Theorem 1.2, we are going to use the following large sieve result which follows from Theorem 2.21 applied to the variety of configurations, with the compatible system given by the action of the Frobenius.

Proposition 2.22. *Let p be a prime number and $q > 1$ be a power of p. Let $d \geq 2$, $\mathscr{H}_d$ be the configuration space of monic squarefree polynomials of degree n and Λ be the set of primes different from 2 and p.*

For each $\ell \in \Lambda$, the action of the Frobenius endomorphism $\mathrm{Frob}_{f,q}$ on $\mathrm{H}^1_{\acute{e}t}(\mathcal{C}_f, \mathbb{Z}_\ell)$ gives a representation $\rho_\ell : \pi_1(\mathscr{H}_d, \overline{\eta}) \to \mathrm{GL}_{2g}(\mathbb{F}_\ell)$ for $\overline{\eta}$ a geometric generic point and for all $\ell \in \Lambda$ they form a compatible system (as in [Kow08a, Definition 8.7]*), with image equal to the set of q-symplectic similitudes following the work of Hall* [Hal08]*.*

For every $\ell \in \Lambda$, let $\Omega_\ell \subset \mathrm{CSp}_{2g}(\mathbb{F}_\ell)$ be a conjugacy invariant subset such that the multiplicator of every element of Ω_ℓ is q.

Then, one has

$$\frac{\#\{f \in \mathcal{H}_d(\mathbb{F}_q) \mid \rho_\ell(\mathrm{Frob}_{f,q}) \notin \Omega_\ell \text{ for all } \ell < q^{\frac{1}{2A}}, \ell \in \Lambda\}}{|\mathcal{H}_d(\mathbb{F}_q)|} \ll_{p,d} \Big(\sum_{\substack{\psi(m) \leq q^{\frac{1}{2A}} \\ m \in \mathcal{L}}} \prod_{\ell \mid m} \frac{|\Omega_\ell|}{|\mathrm{Sp}_{2g}(\mathbb{F}_\ell)| - |\Omega_\ell|} \Big)^{-1},$$

where the implicit constant depends only on d and p, we can take $A = 2g^2 + g + 2$, $\mathcal{L}$ is the set of squarefree integers whose prime factors are all in Λ, and $\psi(m) = \prod_{\ell \mid m}(\ell + 1)$.

Proof. We are in the setting of Theorem 2.21 with $U = \mathscr{H}_d$ of dimension $d - 1 \geq 1$. The variety $\mathscr{H}_d \subset \mathbb{A}^d$ is defined by the non-vanishing of the discriminant, it is thus a smooth affine geometrically connected algebraic variety which is the complement of a divisor with normal crossing ([EVW16, Lemma 7.6]).

As in [Kow08a, Section 8.6] for each $\ell \neq 2, p$, the sheaf $\mathcal{F}_\ell$ corresponding to ρ_ℓ is a rank $2g$ lisse sheaf of $\mathbb{F}_\ell$-modules on $\mathscr{H}_d$. Since the action of the Frobenius on $H^1(C, \mathbb{Z}_\ell)$ is independent of ℓ, the representations ρ_ℓ arise from a compatible system. By [Hal08, Theorem 1.2] (attributed to Yu), the images of $\pi_1(\mathscr{H}_d, \bar{\eta})$ and of $\pi_1(\overline{\mathscr{H}}_d, \bar{\eta})$ (arithmetic and geometric monodromy groups) are conjugate to $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ for all $\ell \neq 2, p$.

Hence, the bound follows from Theorem 2.21, where we chose $L + 1 = q^{\frac{1}{2A}}$. □

Remark 2.23. Note that for any finite set of primes S, the result of Proposition 2.22 holds with the set Λ replaced by $\Lambda' = \Lambda \setminus S$, and the set $\mathcal{L}$ replaced by the set $\mathcal{L}'$ of squarefree integers with prime factors in Λ'. This is used in the proof of Lemma 7.5.

3. Linear dependence

Kowalski's Theorem 1.2 is concerned with one-parameter families of reducible squarefree polynomials. The large sieve result Proposition 2.22 above allows us, following Kowalski's proof in [Kow08a], to get the exact same bound, but for the larger space of parameters $\mathcal{H}_d(\mathbb{F}_q)$.

Proof of Theorem 1.1.1. We follow exactly the proof of [Kow08a, Theorem 8.15] but instead of using [Kow08a, Corollary 8.10], we use Proposition 2.22. Thus, we obtain

$$\frac{1}{|\mathcal{H}_d(\mathbb{F}_q)|} \#\{f \in \mathcal{H}_d(\mathbb{F}_q) \mid \text{ The zeta function of } \mathcal{C}_f \text{ does not satisfy LI}\} \ll_{p,g} H_1^{-1} + H_2^{-1} + H_3^{-1} + H_4^{-1},$$

where for $i = 1, \dots 4$,

$$H_i = \sum_{\substack{\psi(m) \leq q^{\frac{1}{2A}} \\ m \in \mathcal{L}}} \prod_{\ell \mid m} \frac{|\Omega_{i,\ell}|}{|\mathrm{Sp}_{2g}(\mathbb{F}_\ell)| - |\Omega_{i,\ell}|},$$

and the sets $\Omega_{i,\ell}$ are defined as in [Kow08a, pages 179–180]. In particular,

1. $\Omega_{1,\ell}$ is the set of matrices $M \in \mathrm{CSp}_{2g}(\mathbb{F}_\ell)$ with multiplicator q such that $\chi_M(X)$ is irreducible, and [Kow08a, page 181] gives $\frac{|\Omega_{1,\ell}|}{|\mathrm{Sp}(\mathbb{F}_\ell)|} \geq \frac{1}{2g}$.
2. $\Omega_{2,\ell}$ is the set of matrices $M \in \mathrm{CSp}_{2g}(\mathbb{F}_\ell)$ with multiplicator q such that $\chi_M(X)$ factors as a product of an irreducible quadratic polynomial and a product of irreducible polynomials of odd degree, which satisfy[3] $\frac{|\Omega_{2,\ell}|}{|\mathrm{Sp}(\mathbb{F}_\ell)|} \geq \frac{1}{8g}$ by Lemma 7.7 (with $k = 1$, $n_0 = 1$, $n_{\frac{g-3}{2}} = 1$ in the case g is odd) and [Kow08a, Lemma B.5].
3. $\Omega_{3,\ell}$ is the set of matrices $M \in \mathrm{CSp}_{2g}(\mathbb{F}_\ell)$ with multiplicator q such that the polynomial h defined by $\chi_M(X) = X^g h(X + qX^{-1})$ factors as a product of an irreducible quadratic polynomial and a product of irreducible polynomials of odd degree, and [Kow08a, page 181] gives $\frac{|\Omega_{3,\ell}|}{|\mathrm{Sp}(\mathbb{F}_\ell)|} \underset{g \to +\infty}{\sim} \frac{\log 2}{\log g}$.
4. $\Omega_{4,\ell}$ is the set of matrices $M \in \mathrm{CSp}_{2g}(\mathbb{F}_\ell)$ with multiplicator q such that the polynomial h defined by $\chi_M(X) = X^g h(X + qX^{-1})$ has an irreducible factor of prime degree $> \frac{g}{2}$, and [Kow08a, page 181] gives $\frac{|\Omega_{4,\ell}|}{|\mathrm{Sp}(\mathbb{F}_\ell)|} \underset{g \to +\infty}{\sim} \frac{1}{\sqrt{2\pi g}}$.

The final bound is the same (correcting $\delta_2 \geq (4g)^{-1}$ into $\delta_2 \geq (8g)^{-1}$), but the space of parameters $\mathcal{H}_d(\mathbb{F}_q)$ is larger. The dependency on p is lost in the proof of Theorem 2.21. □

[3] a factor $\frac{1}{2}$ was forgotten in [Kow08a, page 181].

To prove Theorem 1.4 for the genus 2 case, we will use the following result of Ahmadi and Shparlinski.

Theorem 3.1 ([AS10, Theorem 2])**.** *Let $\mathcal{C}$ be a smooth projective curve of genus* 2*. If the Jacobian of $\mathcal{C}$ is absolutely simple, then the zeta function of $\mathcal{C}$ satisfies* LI.

Proof of Theorem 1.4. Let us first prove the bound when $g = 1$ and assume for now that $\deg f = 3$. Then $\mathcal{C}_f$ is an elliptic curve, with two conjugate (possibly equal) Frobenius eigenvalues. The only way for LI to fail is that those eigenvalues are of the form $\sqrt{q}\zeta$ with ζ a root of unity, that is, $\mathcal{C}_f$ has to be a supersingular elliptic curve. By [Sil09, V Theorem 4.1.(c)], there are $\ll p$ such curves over $\mathbb{F}_q$, up to $\overline{\mathbb{F}}_q$-isomorphism (recall that q is a power of the prime number p). But two elliptic curves are isomorphic over $\overline{\mathbb{F}}_q$ if and only if they have the same j-invariant ([Sil09, III Proposition 1.4.(b)] which holds in every characteristic). Let E be a fixed supersingular elliptic curve defined over $\mathbb{F}_q$ with j-invariant j, and let us write $j(f)$ the j-invariant of the elliptic curve $\mathcal{C}_f$. Then clearly $j(f) = j$ is a non-zero polynomial equation in the $\deg f$ coefficients of f by the definition of the j-invariant [Sil09, page 42]. It is indeed non-zero since there always exist a non-supersingular elliptic curve over $\mathbb{F}_q$ ([Wat69, Theorem 4.1]). In particular, one has

$$\#\{(a, b, c) \in \mathbb{F}_q^3 \mid f = x^3 + ax^2 + bx + c, \mathcal{C}_f \text{ is isomorphic to } E \text{ over } \overline{\mathbb{F}}_q\} \ll q^2.$$

This yields

$$\#\{f \in \mathcal{H}_3(\mathbb{F}_q) \mid \mathcal{C}_f \text{ is supersingular }\} \ll pq^2$$

and the result follows since in general $|\mathcal{H}_d(\mathbb{F}_q)| = q^d - q^{d-1}$. In the case where $\deg f = 4$ we assume that $p \neq 2, 3$. Then $\mathcal{C}_f$ is isomorphic to its Jacobian J_f, and by [Cre01, page 82], J_f is given as the smooth projective model of the curve defined by the equation $y^2 = x^3 - 27Ix - 27J$, and I and J are the quartic invariants defined in [Cre01, pages 72–73]. The j-invariant of J_f is then clearly a non-constant rational function in the coefficients of f, and we conclude as in the case $\deg f = 3$.

Assume now that $g = 2$. By Theorem 3.1, if LI fails for the zeta function of $\mathcal{C}_f$, then its Jacobian J_f is not absolutely simple, *i.e.* it splits over a finite extension $\mathbb{K}$ of $\mathbb{F}_q$. In particular, the Weil polynomial $W_{f,\mathbb{K}}$ of $J_f/\mathbb{K}$ is reducible. Calling n the degree $[\mathbb{K} : \mathbb{F}_q]$, one has $W_{f,\mathbb{K}}(X^n) = \prod_{k=0}^{n-1} W_f(\zeta_n^k X) = \prod_{k=0}^{n-1} P_f(\zeta_n^k X)$, where W_f is the Weil polynomial of $J_f/\mathbb{F}_q$, which is equal to P_f ([CS86, VII. Corollary 11.4]), and ζ_n is a primitive n-th root of unity. It easily implies that $W_{f,\mathbb{K}}$ has roots $\alpha_j(\chi_f)^n$, $j \in \{1, \ldots, 4\}$. Now, there are two possible cases. Either one of $\alpha_i(\chi_f)^n$ is a rational number (necessarily $\pm q^{n/2}$), or there are two indices $i \neq j \in \{1, \ldots, 4\}$ such that $\alpha_i(\chi_f)^n \alpha_j(\chi_f)^n$ is a rational number (necessarily $\pm q^n$). In particular, χ_f is degenerate according to Definition 2.18. We conclude by Lemma 7.3. □

4. Complete biases

4.1. **Upper bounds for complete biases.** To derive a necessary condition for exhibiting a complete bias, we will use the following simple inequality of Bhatia and Davis [BD00, Theorem 1] (the proof in [BD00] is done for discrete random variables, but the general case works exactly the same).

Theorem 4.1 (Bhatia-Davis Inequality)**.** *Let X be a bounded random variable such that $a \leq X \leq b$ almost-surely with mean μ and variance σ^2, then*

$$\sigma^2 \leq (b - \mu)(\mu - a). \tag{4.1}$$

Proposition 4.2 (Necessary condition for complete bias)**.** *Let $f \in \mathbb{F}_q[x]$ and assume that $\Pi(n; \chi_f)$ admits a complete bias. Then one of the following assertions is true.*

1. *The distribution μ_{Δ_f} is symmetric with respect to its mean value and $m_0(\chi_f) \geq m_\pi(\chi_f) + 2\sum_{j=1}^{r} m_j(\chi_f)$ and in the case $r = 0$, the inequality is strict with more than half of the zeros equal to $\sqrt{q}$.*
2. *The distribution μ_{Δ_f} is not symmetric with respect to its mean value and $m_0(\chi_f) > m_\pi(\chi_f)$.*

In particular, this implies the following condition.

Corollary 4.3. *If $\Pi(n; \chi_f)$ admits a complete bias for $f \in \mathbb{F}_q[x]$, then q is a square and $L(\frac{1}{2}, \chi_f) = 0$.*

Remark 4.4. In the case of Dirichlet L-functions over $\mathbb{Q}$, it is a famous conjecture of Chowla[Cho65] that no such L-function can vanish at $\frac{1}{2}$. It is known that Artin L-functions corresponding to number fields extensions can vanish at $\frac{1}{2}$. Incidentally, this was used in [Bai21] to provide examples of reversed bias in this context. In the function field case, it was shown in [Li18, Theorem 1.3] that for any q there are infinitely many Dirichlet L-functions over $\mathbb{F}_q(x)$ vanishing at $\frac{1}{2}$, that is such that the corresponding Weil polynomial vanishes at $\sqrt{q}$. However it is expected that 100% of those L-functions do not vanish at $\frac{1}{2}$ for a fixed q ([Li18, Remark 1.4]). If this were true, we would obtain the following result instead of Theorem 1.5: for every q a power of an odd prime,

$$\lim_{d\to+\infty} \frac{\#\{f \in \mathcal{H}_d(\mathbb{F}_q) \mid \Pi(n;\chi_f) \text{ exhibits a complete bias}\}}{|\mathcal{H}_d(\mathbb{F}_q)|} = 0.$$

Note also that by [ELS20, Corollary 1.6] there is no complete bias when f is irreducible and 4 does not divide the degree of f. Indeed, in this case $L(\frac{1}{2},\chi_f) \neq 0$.

We can now prove our main results concerning upper bounds for complete bias using the necessary condition in Corollary 4.3.

Proof of Theorem 1.1.2. The proof follows from applying Corollary 4.3 and Lemma 7.1. □

Proof of Theorem 1.5. By [ELS20, Theorem 3.2], one has

$$\sup_d \frac{\#\{f \in \mathcal{H}_d(\mathbb{F}_q) \mid \mathcal{L}(\sqrt{q},\chi_f) = 0\}}{|\mathcal{H}_d(\mathbb{F}_q)|} \ll q^{-\frac{1}{276}},$$

and so the bound follows from Corollary 4.3. □

We finally give the proof of our necessary condition for complete bias.

Proof of Proposition 4.2. Suppose that the distribution μ_{Δ_f} is symmetric with respect to its mean value $m_0(\chi_f) + \frac{1}{2}$. We have $\Delta_f(0) = m_0(\chi_f) + m_\pi(\chi_f) + 1 + 2\sum_{j=1}^{r} m_j(\chi_f)$, so this value is in $\operatorname{supp}\mu_{\Delta_f}$. Indeed, let $\varepsilon > 0$ and $h : \mathbb{R} \to \mathbb{R}$ be non-negative continuous and supported on $[\Delta_f(0) - \varepsilon, \Delta_f(0) + \varepsilon]$, with $h(\Delta_f(0)) > 0$. Then

$$\int_{\mathbb{R}} h(t)\,\mathrm{d}\mu_{\Delta_f}(t) = \int_{A(\Delta_f)} \tilde{h}(a_0,\dots,a_r)\,\mathrm{d}\omega_{A(\Delta_f)}(a)$$

where $\tilde{h}(a_0,\dots,a_r) = h\Big(m_0(\chi_f) + \frac{1}{2} + (m_\pi(\chi_f) + \frac{1}{2})e^{ia_0} + 2\sum_{j=1}^{r} m_{\theta_j}(\chi_f)\cos(a_j)\Big)$ and $\mathrm{d}\omega_{A(\Delta_f)}$ is the Haar measure on the subtorus $A(\Delta_f)$ of $\mathbb{T}^{r+1}$ generated by $(\pi,\theta_1,\dots,\theta_r)$. Since $h(\Delta_f(0)) = \tilde{h}(0,\dots,0) > 0$, we get $\int_{\mathbb{R}} h(t)\,\mathrm{d}\mu_{\Delta_f}(t) > 0$, which implies $\Delta_f(0) \in \operatorname{supp}\mu_{\Delta_f}$.

By symmetry, $2(m_0(\chi_f) + \frac{1}{2}) - (m_0(\chi_f) + m_\pi(\chi_f) + 1 + 2\sum_{j=1}^{r} m_j(\chi_f))$ is also in $\operatorname{supp}\mu_{\Delta_f}$, so it is non-negative.

In the case μ_{Δ_f} is not symmetric with respect to its mean value, we are interested in the behavior of

$$\Delta_f : n \mapsto m_0(\chi_f) + \frac{1}{2} + (-1)^n\left(m_\pi(\chi_f) + \frac{1}{2}\right) + 2\sum_{j=1}^{r} m_j(\chi_f)\cos(n\theta_j).$$

By [Bai22, Theorem 3.1], we have $\operatorname{dens}(\Delta_f > 0) \le \frac{1}{2}\mathbb{P}(Y_0 \ge 0) + \frac{1}{2}\mathbb{P}(Y_1 \ge 0)$ where Y_0, Y_1 are random variables whose distributions are the limiting distributions of $\Delta_f(2\cdot)$ and $\Delta_f(2\cdot+1)$ respectively. Since we are assuming complete bias, then $\operatorname{dens}(\Delta_f > 0) = 1$ yields $\mathbb{P}(Y_0 \ge 0) = \mathbb{P}(Y_1 \ge 0) = 1$.

We apply the Bhatia-Davis Inequality, Theorem 4.1, to the random variable Y_1. To do so, we need the maximum, minimum, mean, and variance of Y_1. To understand these, we simplify the sum by grouping terms corresponding to pairs $(\theta_j, \theta_{j'})$ where $\theta_{j'} = \pi - \theta_j$ and removing the term corresponding to $\frac{\pi}{2}$ if necessary. We have

$$\begin{aligned}\Delta_f(2n+1) &= m_0(\chi_f) - m_\pi(\chi_f) + 2\sum_{j=1}^{r} m_j(\chi_f)\cos(\theta_j(2n+1))\\ &= m_0(\chi_f) - m_\pi(\chi_f) + 2\sum_{j=1}^{r'} m'_j(\chi_f)\cos(\theta_j(2n+1)),\end{aligned}$$

where we sum on $\{\theta_1,\dots,\theta_{r'}\} = \{\theta_1,\dots,\theta_r\} \setminus \{\theta_j \mid \exists k \le j, \theta_j = \pi - \theta_k\}$ (in particular $\frac{\pi}{2} \notin \{\theta_1,\dots,\theta_{r'}\}$), and we define $m'_j(\chi_f) = m_j(\chi_f) - m_{k(j)}(\chi_f)$ where $\theta_{k(j)} = \pi - \theta_j$ (and $m_{k(j)}(\chi_f) = 0$ if such a $\theta_{k(j)}$ does not exist). This grouping of terms was made to simplify the computation of the variance below. From this expression we deduce

$$\mathbb{E}(Y_1) = m_0(\chi_f) - m_\pi(\chi_f).$$

By the assumption of complete bias, we have $Y_1 \geq 0$ almost-surely. By the definition of Y_1, we have

$$Y_1 \leq m_0(\chi_f) - m_\pi(\chi_f) + 2\sum_{j=1}^{r'} |m_j'(\chi_f)| \text{ almost-surely}$$

and

$$\begin{aligned}\mathrm{Var}(Y_1) &= \lim_{K\to\infty} \frac{1}{K}\sum_{x=0}^{K-1}\Big(2\sum_{j=1}^{r'} m_j'(\chi_f)\cos(\theta_j(2x+1))\Big)^2 \\ &= \lim_{K\to\infty} \frac{4}{K}\sum_{x=0}^{K-1}\Big[\sum_{j=1}^{r'}\big(m_j'(\chi_f)\cos(\theta_j(2x+1))\big)^2 + \sum_{1\leq j\neq k\leq r'} m_j'(\chi_f)m_k'(\chi_f)\cos(\theta_j(2x+1))\cos(\theta_k(2x+1))\Big] \\ &= 2\sum_{j=1}^{r'} m_j'(\chi_f)^2.\end{aligned}$$

By the Bhatia-Davis inequality (Theorem 4.1), we obtain

$$\mathrm{Var}(Y_1) \leq \big(m_0(\chi_f) - m_\pi(\chi_f) + 2\sum_{j=1}^{r'} |m_j'(\chi_f)| - \mathbb{E}(Y_1)\big)\big(\mathbb{E}(Y_1) - 0\big).$$

This yields

$$\sum_{j=1}^{r'} m_j'(\chi_f)^2 \leq 2\sum_{j=1}^{r'} |m_j'(\chi_f)|\left(m_0(\chi_f) - m_\pi(\chi_f)\right). \tag{4.2}$$

If every $m_j'(\chi_f)$ is zero, this means that for every integer n, one has $\Delta_f(2n+1) = m_0(\chi_f) - m_\pi(\chi_f)$. Since $\Pi(n;\chi_f)$ exhibits a complete bias, this has to be positive, *i.e.* $m_0(\chi_f) > m_\pi(\chi_f)$. If there is at least one non-zero $m_j'(\chi_f)$, the inequality (4.2) also implies $m_0(\chi_f) > m_\pi(\chi_f)$.

Finally, since $\sqrt{q}$ and $-\sqrt{q}$ have distinct multiplicities as roots of $P_f \in \mathbb{Z}[T]$, they must be rational, hence integers, and so q must be a square. □

4.2. **Examples of complete biases.** In this section, we first give a sufficient condition for a complete bias, in the hope to use it to find examples of instances of such an exceptional behavior.

Lemma 4.5 (Sufficient condition for complete bias)**.** *Let $f \in \mathbb{F}_q[x]$. Write*

$$P_f(u) = (u-\sqrt{q})^{m_0}(u+\sqrt{q})^{m_\pi}L_1(u)L_2(u)$$

with $L_2(-u) = L_2(u)$ of maximal degree, $\deg L_i = d_i$. Assume that one of the following assertions holds,

1. *we have $m_0 > m_\pi + d_1$ and $m_0 + m_\pi + 1 > d_1 + d_2$, or*
2. *we have $m_0 \geq m_\pi + d_1$ and $m_0 + m_\pi + 1 \geq d_1 + d_2$, and*
   - (a) *L_1 admits a root whose angle is not in $\mathbb{Q}\pi$, or*
   - (b) *there exists $k_1, \dots, k_{d_1} \in \mathbb{Z}$ satisfying $\sum_{i=1}^{d_1} k_i\theta_i \equiv 0 \pmod{2\pi}$ and $\sum_{i=1}^{d_1} k_i$ is odd, where $\theta_1, \dots, \theta_{d_1}$ are the angles of the roots of L_1.*

Then there is a complete bias with modulus f.

One such example is $f = t^4+2t^3+2t+a^7 \in \mathbb{F}_9[t]$ where a is a generator of $\mathbb{F}_9$ over $\mathbb{F}_3$, in [DM21, Example 3] the authors show that $P_f(u) = (u-3)^2$.

Remark 4.6. More generally, in [DM21, Proposition 3.1], based on Honda–Tate ideas (citing [Wat69, Theorem 4.1]), one can see that for each q square, there exist $f \in \mathbb{F}_q[x]$ of degree 3 such that the L-function of χ_f is $(1-\sqrt{q}u)^2$. This gives one example satisfying Lemma 4.5 for each q square.

Remark 4.7. Note however that our sufficient condition for a complete bias Lemma 4.5 is more restrictive than simply vanishing at $\frac{1}{2}$ so we cannot use the lower bound from [Li18, Theorem 1.3] to give infinitely many examples of complete bias for a fixed q.

Proof of Lemma 4.5. It suffices to prove that under these conditions, we have $\Delta_f(n) > 0$ for almost all n, where Δ_f is defined in (2.3). We order the zeros of P_f so that the first ones correspond to the zeros of L_1, with multiplicities. Then, for all n we have

$$\Delta_f(2n+1) = m_0(\chi_f) - m_\pi(\chi_f) + \sum_{j=1}^{d_1} \cos(\theta_j(2n+1))$$

and

$$\Delta_f(2n) = 1 + m_0(\chi_f) + m_\pi(\chi_f) + \sum_{j=1}^{d_1+d_2} \cos(2\theta_j n).$$

Since $\cos(\theta_j n) \geq -1$ for all j and n, the conditions in case 1 imply that $\Delta_f(n) > 0$ for all n. In the case the conditions of 2a are satisfied, we have $\sum_{j=1}^{d_1} \cos(\theta_j n) > -d_1$ for almost all n, since, up to reordering, we can assume that $\theta_1 \notin \mathbb{Q}\pi$ which yields $\cos(\theta_1 n) > -1$ for almost all n. This concludes the proof in the case 2a. In the case 2b, it follows from Lemma 4.8 that $\sum_{j=1}^{d_1} \cos(\theta_j n) \geq -d_1 + 1 + \cos(\pi(1 - \frac{1}{\kappa})) > -d_1$ for all n, where $\kappa = \sum_{i=1}^{d_1} |k_i|$ and this concludes the proof. □

We conclude this section by proving a technical lemma that was used in the proof of the sufficient condition (Lemma 4.5).

Lemma 4.8. *Let $\gamma_1, \ldots, \gamma_N \in (0, \pi)$ and assume that there exists $k_1, \ldots, k_N \in \mathbb{Z}$ satisfying $\sum_{i=1}^N k_i\gamma_i \equiv 0 \pmod{2\pi}$ and $\sum_{i=1}^N k_i$ is odd. Then, for all $\ell \in \mathbb{Z}$, we have $\max_{1\leq i\leq N} \|\ell\gamma_i - \pi\|_{2\pi} \geq \frac{\pi}{\sum_{i=1}^N |k_i|}$. In particular,*

$$\sum_{1\leq i\leq N} \cos(\ell\gamma_i) \geq -N + 1 + \cos\left(\pi\Big(1 - \frac{1}{\sum_{i=1}^N |k_i|}\Big)\right).$$

Proof. Recall that $\|\ell\gamma_i - \pi\|_{2\pi} = \min_{n\in\mathbb{Z}} |\ell\gamma_i - (2n+1)\pi|$. For each i, let $n_i \in \mathbb{Z}$ be an integer that satisfies this minimum. We have

$$\begin{aligned}\max_{1\leq i\leq N} \|\ell\gamma_i - \pi\|_{2\pi} &= \max_{1\leq i\leq N} \left|\ell\gamma_i - (2n_i+1)\pi\right| \\ &\geq \frac{1}{\sum_{i=1}^N |k_i|} \Big|\ell \sum_{i=1}^N k_i\gamma_i - \sum_{i=1}^N k_i(2n_i+1)\pi\Big| \\ &\geq \frac{\pi}{\sum_{i=1}^N |k_i|}.\end{aligned}$$

Now, suppose that $\|\gamma - \pi\|_{2\pi} \geq \frac{\pi}{\kappa}$, then we have

$$\cos(\gamma) \geq \cos(\pi(1 - \tfrac{1}{\kappa})).$$

This concludes the proof. □

5. Lower order biases

5.1. **Upper bound.** Our reflections on linear recurrence sequences from Section 2.3 give a good understanding on lower order bias. In particular, the contraposition of Lemma 2.19 yields the following necessary condition for a lower order bias.

Proposition 5.1 (Necessary condition for lower order bias)**.** *If $\Pi(n; \chi_f)$ admits a lower order bias, then χ_f is degenerate (see Definition 2.18).*

This lemma implies that for $\Pi(n; \chi_f)$ to admit a lower order bias, the Jacobian of the curve $C_f : y^2 = f(x)$ is either non-ordinary or geometrically admitting an isogenous factor of order at least 2.

Using this lemma and an application of the large sieve from Proposition 2.22, we obtain the proof of Theorem 1.1.3.

Proof of Theorem 1.1.3. The proof follows from applying Proposition 5.1 and Lemma 7.3. □

5.2. **A sufficient condition for lower order bias and examples.**

Lemma 5.2 (Sufficient condition for lower order bias)**.** *Let $f \in \mathbb{F}_q[x]$. Suppose that $P_f(u) = P_f(-u)$, then $\Delta_f(2n+1) = 0$ for all n, in particular, there is a lower order bias with modulus f.*

Proof. Assume that the roots of P_f with positive imaginary parts are labelled so that their arguments are $\theta_1, ..., \theta_t, \pi - \theta_1, ..., \pi - \theta_t$. Since $P_f(u) = P_f(-u)$, the multiplicity of θ_i equals to that of $\pi - \theta_i$. For $n \in \mathbb{N}$ and $1 \le j \le t$, one has $\cos((\pi - \theta_j)(2n+1)) = -\cos(\theta_j(2n+1))$, whence

$$\sum_{j=1}^{t} 2m_{\theta_j}(\chi_f)\cos(\theta_j(2n+1)) + \sum_{j=1}^{t} 2m_{\pi-\theta_j}(\chi_f)\cos((\pi-\theta_j)(2n+1)) = 0.$$

Further,

$$\left(\frac{1}{2} + m_0(\chi_f)\right) + \left(\frac{1}{2} + m_\pi(\chi_f)\right)(-1)^{2n+1} = 0.$$

The above together give $\Delta_f(2n+1) = 0$ for all $n \in \mathbb{N}$. This is sufficient to deduce that there is a lower order bias with modulus f. ☐

One such example is $f = t^6 + 2t^3 + 5 \in \mathbb{F}_{23}[t]$ which is irreducible and the L-function of χ_f is $1 - 29u^2 + 23^2u^4$ which is even with 4 inverse roots $\pm\alpha$, $\pm\overline{\alpha}$, where

$$\alpha = \sqrt{23}\exp\left(\frac{i}{2}\arctan\left(\left(\frac{5\sqrt{51}}{29}\right)\right)\right).$$

Moreover, using [Cal06, page 17], we see that the argument of α and π are linearly independent over $\mathbb{Q}$.

Remark 5.3. Using [HNR09, Table 1.2] and the sufficient condition, we can give several examples for each q that present a lower order bias. Namely, the authors show that the polynomial $X^4 - bX^2 + q^2$ with $b = 2q\cos(2\theta)$ is the Weil polynomial of the Jacobian of a hyperelliptic curve of genus 2 if $b \in \mathbb{Z}$, $b \neq q, 2q, 2q-1, 2q-2$ and $b + 2q$ is not a square. Since the Weil polynomial of the Jacobian of such a curve is equal to the corresponding P_f ([CS86, VII. Corollary 11.4]), for such f, $\Pi(n, \chi_f)$ exhibits lower order bias.

Remark 5.4. The condition of Lemma 5.2 gives rise to the following question: Fix a finite field $\mathbb{F}_q$, how many hyperelliptic curves admit even Frobenius characteristic polynomials? If C is such a curve, then $C \otimes \mathbb{F}_{q^2}$ has its Frobenius characteristic polynomial being a perfect square. This question is thus closely related to counting curves/characters whose L-functions are perfect squares.

6. Reversed biases

6.1. **Upper bound.** Let us first give a necessary condition for a reversed bias.

Proposition 6.1 (Necessary condition for a reversed bias)**.** *If there is a reversed bias with modulus f then*

- *either there exist $k_1, \dots, k_g \in \mathbf{Z}$ satisfying $\sum_{i=1}^{g} k_i\theta_i \equiv 0 \pmod{2\pi}$ and $\sum_{i=1}^{g} k_i$ is odd, where the θ_i are angles of zeros of P_f.*
- *or $m_0 < m_\pi$ (in particular, q is a square).*

Proof. Suppose $\Pi(n, \chi_f)$ admits a reversed bias. Then the distribution μ_f is not symmetric with respect to its mean value $m_0 + \frac{1}{2} \ge 0$. So, from Lemma 2.11, there exists $k_0, k_1, \dots, k_r$ such that $k_0 + \sum_{j=1}^{r} k_j \equiv 1 \pmod 2$ and $k_0\pi + \sum_{j=1}^{r} k_j\theta_j \equiv 0 \pmod{2\pi}$.

If k_0 is even, we get the first condition. Otherwise, assume that all relation between the θ_j's, $\sum_{i=1}^{g} k_i\theta_i \equiv 0 \pmod{2\pi}$ satisfy $\sum_{i=1}^{g} k_i$ is even. Then we deduce from Lemma 2.11, that the limiting distribution of the functions $\Delta(2\cdot)$ and $\Delta(2\cdot +1)$ are symmetric with respect to their mean values, which are $m_0 + m_\pi + 1$ and $m_0 - m_\pi$. If the probability that one of the two functions is negative is larger than $\frac{1}{2}$, then at least one of the mean values has to be negative. ☐

Here is a translation of our necessary condition in terms of the Galois group of P_f over $\mathbb{Q}$, which is more convenient to use in the large sieve. Recall that for $f \in \mathcal{H}_d(\mathbb{F}_q)$, $\mathrm{Gal}_{\mathbb{Q}}(P_f)$ is a subgroup of $W_{2g} = \mathfrak{S}_g \ltimes (\mathbb{Z}/2\mathbb{Z})^g$, itself a subgroup of $\mathfrak{S}_{2g}$ (see [Kow08a, page 249]). In the following, we will consider that $\mathrm{Gal}(P_f) \subset \mathfrak{S}_{2g}$ acts on $\{-g, \dots, -1, 1, \dots, g\}$, the set of indices of the roots $\alpha_1, \dots, \alpha_g, \alpha_{-1} = \overline{\alpha_1}, \dots, \alpha_{-g} = \overline{\alpha_g}$. The fact that $\mathrm{Gal}(P_f) \subset W_{2g}$ means that if $\sigma \in \mathrm{Gal}(P_f)$ then $\sigma(-i) = -\sigma(i)$ for all $i \in \{-g, \dots, -1, 1, \dots, g\}$.

Lemma 6.2. *Let $f \in \mathcal{H}_d(\mathbb{F}_q)$. Assume that there exist $k_1, \ldots, k_g \in \mathbb{Z}$ such that $k_1\theta_1 + \cdots + k_g\theta_g \equiv 0$ mod 2π and $k_1 + \cdots + k_g \equiv 1 \pmod 2$. Then at least one of the following conditions hold:*

1. *P_f is not separable.*
2. *χ_f is degenerate (in the sense of Definition 2.18).*
3. *$\mathrm{Gal}_{\mathbb{Q}}(P_f)$ does not act transitively on the set of pairs $\{\{1,-1\}, \ldots, \{g,-g\}\}$;*
4. *For every $i \in \{1, \ldots, g\}$, $\mathrm{Gal}(P_f)$ does not contain the transposition $(i\ -i)$, and for every pair $\{i,j\}$, with $i \neq j \in \{1, \ldots, g\}$, $\mathrm{Gal}_{\mathbb{Q}}(P_f)$ does not contain the 4-cycle $(i\,j\ -i\ -j)$.*

Proof. Assume that none of the first three items are satisfied. Let us fix $i \in \{1, \ldots, g\}$, then for every $j \in \{1, \ldots, g\} \setminus \{i\}$, there exist $\sigma_j \in \mathrm{Gal}(P_f)$ such that $\sigma_j(j) \in \pm i$. From the multiplicative relation

$$\left(\frac{\alpha_1}{\sqrt{q}}\right)^{k_1} \times \cdots \times \left(\frac{\alpha_g}{\sqrt{q}}\right)^{k_g} = 1$$

with $\sum_{j=1}^{g} k_j \equiv 1 \pmod 2$, we apply σ_j and taking the product over all j's we obtain another multiplicative relation of the form

$$\left(\frac{\alpha_1}{\sqrt{q}}\right)^{S_{i,1}} \times \cdots \times \left(\frac{\alpha_g}{\sqrt{q}}\right)^{S_{i,g}} = 1 \tag{6.1}$$

where $S_{i,i} = \sum \pm k_j \equiv 1 \pmod 2$. In particular $S_{i,i} \neq 0$. This being true for each $i \in \{1, \ldots, g\}$, by taking a suitable product of large powers of expressions of the form 6.1, we deduce that there exists $S_1, \ldots, S_g \in \mathbb{Z}\backslash\{0\}$ such that

$$\left(\frac{\alpha_1}{\sqrt{q}}\right)^{S_1} \times \cdots \times \left(\frac{\alpha_g}{\sqrt{q}}\right)^{S_g} = 1. \tag{6.2}$$

Let $i \in \{1, \ldots, g\}$. If $(i\ -i) \in \mathrm{Gal}_{\mathbb{Q}}(P_f)$, then we apply it to the relation 6.2 and taking a quotient we get $\left(\frac{\alpha_i}{\sqrt{q}}\right)^{2S_i} = 1$. This is a contradiction because $S_i \neq 0$ and $\frac{\alpha_i}{\sqrt{q}}$ is not a root of unity since χ_f is non-degenerate.

Now, let $i \neq j \in \{1, \ldots, g\}$. If $(i\,j\ -i\ -j) \in \mathrm{Gal}_{\mathbb{Q}}(P_f)$ we get $\left(\frac{\alpha_i}{\sqrt{q}}\right)^{S_i+S_j}\left(\frac{\alpha_j}{\sqrt{q}}\right)^{S_j-S_i} = 1$, and similarly by applying its inverse $(i\ -j\ -i\,j) = (i\,j\ -i\ -j)^3$, we get $\left(\frac{\alpha_i}{\sqrt{q}}\right)^{S_i-S_j}\left(\frac{\alpha_j}{\sqrt{q}}\right)^{S_j+S_i} = 1$. Combining the two relations, we obtain $\left(\frac{\alpha_j}{\sqrt{q}}\right)^{(S_j+S_i)^2+(S_j-S_i)^2} = 1$. But at least one among $S_i + S_j$ and $S_i - S_j$ is non-zero, since the S_i's are non-zero, and as before, this shows that we cannot have $(i\,j\ -i\ -j) \in \mathrm{Gal}_{\mathbb{Q}}(P_f)$. □

Lemma 6.3. *Let $P \in \mathbb{Q}[T]$ be a q-symplectic polynomial of degree $2g$ with roots $\alpha_1, \overline{\alpha_1}, \ldots, \alpha_g, \overline{\alpha_g}$. If $\mathrm{Gal}_{\mathbb{Q}}(P)$ does not act transitively on the pairs $\{\alpha_1, \overline{\alpha_1}\}, \ldots, \{\alpha_g, \overline{\alpha_g}\}$ then h_P defined by $P(T) = T^g h_P(T + qT^{-1})$ is reducible.*

Proof. Notice the roots of h_P are the $\alpha_i + \overline{\alpha_i}$. Every element of $\mathrm{Gal}_{\mathbb{Q}}(h_P)$ are restrictions of elements of $\mathrm{Gal}_{\mathbb{Q}}(P)$ to the splitting field of h_P. Now if h_P is irreducible over $\mathbb{Q}$, then $\mathrm{Gal}(h_P)$ acts transitively on the set $\{\alpha_i + \overline{\alpha_i} \mid i = 1, \ldots, g\}$. Thus, if $i \neq j \in \{1, \ldots, g\}$, there exists $\sigma \in \mathrm{Gal}(P)$ such that $\sigma(\alpha_i + \overline{\alpha_i}) = \alpha_j + \overline{\alpha_j}$. But $\sigma(\alpha_i) = \alpha_k$ for some $k \in \{1, \ldots, 2g\}$ so we have $\sqrt{q}\cos(\theta_k) = \sqrt{q}\cos(\theta_j)$ which implies $\theta_k = \pm\theta_j$, which means $\sigma(\alpha_i) = \alpha_j$ or $\sigma(\alpha_i) = \overline{\alpha_j}$, and $\mathrm{Gal}_{\mathbb{Q}}(P)$ acts transitively on the set of pairs $\{\alpha_i, \overline{\alpha_i}\}$. □

We can finally prove the last part of our main theorem.

Proof of Theorem 1.1.4. The proof follows by using the necessary conditions of Proposition 6.1. We obtain a bound for the second condition by the same argument as in Lemma 7.1. For the first condition of Proposition 6.1, we use Lemma 6.2 and bound the conditions 1. and 2. by Lemma 7.3. The third item is bounded by using Lemma 6.3 and Lemma 7.4. Finally, the bound obtained with the condition on the Galois group, which is the largest contribution, is dealt with by Lemma 7.5. □

6.2. **Examples.** In the hope of finding examples of reversed biases in the sense of Definition 2.6 we estimated

$$\Delta_f(n) = \left(m_0(\chi_f) + \tfrac{1}{2}\right) + \left(m_\pi(\chi_f) + \tfrac{1}{2}\right)(-1)^n + \sum_{\theta_j \neq 0,\pi} m_{\theta_j}(\chi_f) e^{in\theta_j(\chi_f)},$$

where χ_f is the primitive quadratic character modulo $f \in \mathcal{H}_d(\mathbb{F}_q)$ for small genera $g = \left\lfloor \frac{d-1}{2} \right\rfloor$ and small finite fields $\mathbb{F}_q$. In particular, for fixed $f(x) \in \mathbb{F}_q[x]$ we computed $\Delta_f(n)$ for many values of n, e.g. all $0 \leq n \leq 1000$. We found no clear candidate curves which exhibited a "strong" reversed bias amongst $\mathcal{C}_f/\mathbb{F}_q$ with q a prime less than 11 and $\deg f(x) \leq 6$ as well as among those curves with $\deg f(x) \leq 8$ and $q = 3$.

Remark 6.4. We can still provide an infinite family of examples exhibiting a reversed bias. Indeed, when q is a square the polynomial $(1 - u\sqrt{q} + u^2 q)^2$ is the L-function of a hyperelliptic curve of genus 2 according to [HNR09]. For such a curve $\mathcal{C}_f$, we have $\Delta_f(n) = \frac{1}{2} + \frac{(-1)^n}{2} + 4\cos(\frac{2\pi}{3}n)$ which is 6-periodic and takes 2 positive values and 4 negative values; explicitly, it takes the values $5, -2, -1, 4, -1, -2$.

Cha's example ([Cha08, Example 5.3]) corresponds to a reversed bias, however Cha is counting polynomials with degree less than n instead of polynomials of degree equal to n (see Remark 2.8). We verified that this example does not meet our criterion of being a reversed bias with our way of counting polynomials, but it exhibits a lower order bias because $\Delta_f(n)$ is 10-periodic, takes 3 positive values (at $n \in \{0, 1, 9\}$), 2 negative values (at $n \in \{3, 7\}$) and is zero otherwise.

7. A few counting lemmas

Using the large sieve statement Proposition 2.22, we will now prove important intermediate counting lemmas that are used to establish our upper bounds for exceptional biases. Recall that q is a power of the prime p, and for any $d \geq 2$, $g = \left\lfloor \frac{d-1}{2} \right\rfloor$ is the genus of the curve $\mathcal{C}_f$ for any $f \in \mathcal{H}_d(\mathbb{F}_q)$ the set of monic squarefree polynomials in $\mathbb{F}_q[x]$ of degree d.

Lemma 7.1. *We have*

$$\frac{1}{|\mathcal{H}_d(\mathbb{F}_q)|} \#\left\{ f \in \mathcal{H}_d(\mathbb{F}_q) \mid m_0(\chi_f) > m_\pi(\chi_f) \right\} = \begin{cases} 0 & \text{if } q \text{ is not a square} \\ O_{p,g}\left(q^{-\frac{1}{A}} \log q\right) & \text{otherwise,} \end{cases}$$

where $A = 2g^2 + g + 2$.

Proof. We first remark that the set $\{f \in \mathcal{H}_d(\mathbb{F}_q) \mid m_0(\chi_f) > m_\pi(\chi_f)\}$ is empty when q is not a square, because in that case, $\sqrt{q}$ and $-\sqrt{q}$ are conjugate algebraic numbers, so they must have the same multiplicity as roots of a polynomial with integer coefficients such as P_f. We will prove our bound by showing that when q is a square, we have

$$\frac{1}{|\mathcal{H}_d(\mathbb{F}_q)|} \#\left\{ f \in \mathcal{H}_d(\mathbb{F}_q) \mid m_0(\chi_f) > m_\pi(\chi_f) \right\} \leq \frac{1}{|\mathcal{H}_d(\mathbb{F}_q)|} \#\left\{ f \in \mathcal{H}_d(\mathbb{F}_q) \mid m_0(\chi_f) \geq 1 \right\} \ll_{p,g} q^{-\frac{1}{A}} \log q.$$

For every $\ell \in \Lambda$ (recall that Λ is simply the set of primes different from 2 and p), we introduce the set $\Omega_{5,\ell} \subset \mathrm{CSp}_{2g}(\mathbb{F}_\ell)$ of q-symplectic matrices for which $\sqrt{q}$ is not an eigenvalue. From [Kow08a, Lemma B.5] (due to Chavdarov) we have

$$\frac{|\Omega_{5,\ell}|}{|\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|} \geq 1 - \frac{1}{\ell^g} \left(\frac{\ell}{\ell-1}\right)^{2g^2+g+1} \#\{P \in \mathbb{F}_\ell[T],\ q\text{-symplectic},\ \deg P = 2g, P(\sqrt{q}) = 0\}.$$

Since the set of symplectic q-polynomials of degree $2g$ in $\mathbb{F}_\ell[T]$ has dimension g, and that the condition of vanishing at one point is a linear equation of the coefficients, we have

$$\#\{P \in \mathbb{F}_\ell[T],\ q\text{-symplectic},\ \deg P = 2g, P(\sqrt{q}) = 0\} = \ell^{g-1}.$$

We deduce that there exist a constant C_g depending on g such that

$$\frac{|\Omega_{5,\ell}|}{|\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|} \geq 1 - \frac{C_g}{\ell}.$$

Therefore, for $A = 2g^2 + g + 2$, we have

$$\sum_{\substack{\ell \le q^{\frac{1}{2A}} - 1 \\ \ell \in \Lambda}} \frac{|\Omega_{5,\ell}|}{|\operatorname{Sp}_{2g}(\mathbb{F}_\ell)| - |\Omega_{5,\ell}|} \ge \sum_{\substack{\ell \le q^{\frac{1}{2A}} - 1 \\ \ell \in \Lambda}} \frac{1 - \frac{C_g}{\ell}}{\frac{C_g}{\ell}} \gg_g \sum_{\substack{\ell \le q^{\frac{1}{2A}} - 1 \\ \ell \in \Lambda}} \ell \gg_g q^{\frac{1}{A}} (\log q)^{-1}.$$

The desired bound then follows from Proposition 2.22 by summing only over primes in Λ. □

Remark 7.2. We could improve the bound above by not restricting to the sum over primes, but we decided not to pursue this here, as we expect the improvement will only be on the power of $\log q$.

The following lemma will allow us to reduce our counting to the case of non-degenerate characters χ_f (as in Definition 2.18) and simple roots of P_f.

Lemma 7.3. *We have*

$$\frac{1}{|\mathcal{H}_d(\mathbb{F}_q)|} \# \{ f \in \mathcal{H}_d(\mathbb{F}_q) \mid \chi_f \text{ is degenerate or } P_f \text{ has a multiple root in } \mathbb{C} \} \ll_{p,g} q^{-\frac{1}{A}} \log q,$$

where $A = 2g^2 + g + 2$.

Proof. Let f satisfy the above condition, that is χ_f is degenerate or P_f has a multiple root in $\mathbb{C}$. Then there exist $1 \le i \ne j \le 2g$ such that $\frac{\alpha_i}{\alpha_j}$ is a root of unity, we denote n its order (one can take $n = 1$ in the case of a multiple root $\alpha_i = \alpha_j$). We first remark that α_i and α_j are algebraic integers of degree at most $2g$, so clearly $\frac{\alpha_i}{\alpha_j}$ is an algebraic number of degree at most $4g^2$, and so $\varphi(n) \le 4g^2$.

Since $\alpha_i^n = \alpha_j^n$, it means that the polynomial $P_{f,n} = \prod_{i=1}^{2g} (X - \alpha_i^n)$ has a multiple root. This implies that its discriminant is 0. Now, $\operatorname{disc}(P_{f,n})$ is a polynomial with integer coefficients in the coefficients of $P_{f,n}$ since it is the resultant of $P_{f,n}$ and its derivative. Moreover, those coefficients are symmetric polynomials in the α_k^n's, and in particular in the α_k's. By the fundamental theorem of symmetric polynomials, this is a polynomial expression in the elementary symmetric polynomials in the α_k's, which are precisely the coefficients of P_f.

We have shown that P_f satisfies a certain integral polynomial equation, *i.e.* there exists a polynomial $Q_{g,n} \in \mathbb{Z}[X_1, \dots, X_{2g}]$ such that, if $a_0, \dots, a_{2g-1}$ are the coefficients of P_f, then one has $Q_{g,n}(a_0, \dots, a_{2g-1}) = 0$. Since there are at most finitely many n such that $\varphi(n) \le 4g^2$, we get a universal relation

$$Q_g = \prod_{n, \varphi(n) \le 4g^2} Q_{g,n} \in \mathbb{Z}[X_1, \dots, X_{2g}]$$

such that if χ_f is degenerate or P_f has a multiple root, then $Q_g(a_0, \dots, a_{2g-1}) = 0$.

Moreover, when q is large enough, we know that Q_g is non-zero since by Kowalski's result (Theorem 1.2), there exists a polynomial $h \in \mathbb{F}_q[x]$ monic of degree d such that $P_h(T) = T^{2g} + \cdots + b_1 T + b_0$ satisfies LI, and in particular, none of its quotients of roots is a root of unity, and for that polynomial, one has $Q(b_0, \dots, b_{2g-1}) \ne 0$.

So the equation $Q_g = 0$ defines a hypersurface in the set of q-symplectic polynomials of fixed degree, and we have

$$\#\{P \in \mathbb{F}_\ell[T] \mid q\text{-symplectic}, \ \deg P = 2g, Q(P) = 0\} \ll_g \ell^{g-1}.$$

See also [Kow08a, Theorem B.6]. The end of the proof is completely similar to the end of the proof of Lemma 7.1. □

In the next lemma, h_{P_f} denotes the "real Weil polynomial" attached to $\mathcal{C}_f$, defined by the relation

$$P_f(T) = T^g h_{P_f}(T + qT^{-1}).$$

Lemma 7.4. *We have*

$$\frac{1}{|\mathcal{H}_d(\mathbb{F}_q)|} \# \left\{ f \in \mathcal{H}_d(\mathbb{F}_q) \mid h_{P_f} \text{ is reducible} \right\} \ll_{p,g} q^{-\frac{1}{2A}} (\log q)^{1 - \frac{1}{g-1}},$$

where $A = 2g^2 + g + 2$.

Proof. We use Proposition 2.22 with the set

$$\Omega_{6,\ell} = \{M \in \mathrm{CSp}_{2g}(\mathbb{F}_\ell) \mid \exists h \in \mathbb{F}_\ell[T], h \text{ is monic irreducible and } \chi_M(T) = T^g h(T + qT^{-1})\}.$$

Since if a monic polynomial is reducible, none of its reduction modulo a prime can be irreducible, we have

$$\#\left\{f \in \mathcal{H}_d(\mathbb{F}_q) \mid h_{P_f} \text{ is reducible}\right\} \leq \#\left\{f \in \mathcal{H}_d(\mathbb{F}_q) \mid \rho_\ell(\mathrm{Frob}_{f,q}) \notin \Omega_{6,\ell} \text{ for all } \ell < q^{\frac{1}{2A}}, \ell \in \Lambda\right\}$$
$$\ll_{p,d} |\mathcal{H}_d(\mathbb{F}_q)| \Big(\sum_{\substack{\psi(m) \leq q^{\frac{1}{2A}} \\ m \in \mathcal{L}}} \prod_{\ell \mid m} \frac{\delta_{6,\ell}}{1-\delta_{6,\ell}} \Big)^{-1}.$$

where $\delta_{6,\ell} = \frac{|\Omega_{6,\ell}|}{|\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|}$. There are $\frac{1}{g}\ell^g(1+O_g(\frac{1}{\ell}))$ monic irreducible polynomials of degree g with coefficients in $\mathbb{F}_\ell$. As $P \mapsto h_P$ is a bijection from the set of q-symplectic polynomials in $\mathbb{F}_\ell[T]$ of degree $2g$ to the set of monic polynomials of degree g in $\mathbb{F}_\ell[T]$, we deduce from [Kow08a, Lemma B.5] (similarly to Lemma 7.1) that

$$\delta_{6,\ell} \geq \frac{1}{g} + O_g(\tfrac{1}{\ell}) =: \delta_\ell.$$

We conclude using the estimation of the sum from a theorem of Lau and Wu [Kow08a, Theorem G.2] applied the same way as Kowalski in [Kow08a, (8.24)]:

$$\sum_{\substack{\psi(m) \leq q^{\frac{1}{2A}} \\ m \in \mathcal{L}}} \prod_{\ell \mid m} \frac{\delta_{6,\ell}}{1-\delta_{6,\ell}} \geq \sum_{\substack{\psi(m) \leq q^{\frac{1}{2A}} \\ m \in \mathcal{L}}} \prod_{\ell \mid m} \frac{\delta_\ell}{1-\delta_\ell} \gg q^{\frac{1}{2A}} (\log q)^{-1+\frac{1/g}{1-1/g}},$$

from which we deduce the stated bound. □

The last counting lemma is about polynomials $f \in \mathcal{H}_d(\mathbb{F}_q)$ such that $\mathrm{Gal}_{\mathbb{Q}}(P_f)$ does not contain certain permutations. Recall from the discussion above Lemma 6.2 that $\mathrm{Gal}_{\mathbf{Q}}(P_f)$ acts on $\{-g, \ldots, -1, 1, \ldots, g\}$.

Lemma 7.5. *We have*

$$\#\Big\{f \in \mathcal{H}_d(\mathbb{F}_q) \mid \forall i \neq j \in \{1, \ldots, g\}, (i\ -i) \notin \mathrm{Gal}(P_f) \text{ and } (i\, j\ -i\ -j) \notin \mathrm{Gal}(P_f)\Big\}$$
$$\ll_{p,g} q^{-\frac{1}{2A}} (\log q)^{1-\frac{1}{\frac{24}{7}g-1}},$$

where $A = 2g^2 + g + 2$.

Proof. First, we may assume that P_f is separable, since the announced bound is worse than that of 7.3.

We are once again going to use the large sieve bound coming from Proposition 2.22 but the set Λ of prime numbers used in the large sieve has to be modified a bit here because of Lemma 7.7: we take Λ to be the set of prime numbers different from 2 and p and larger than $4g^2$ (see Remark 2.23). This only induces a further dependency on g in the implied constants, but doesn't modify the final bound.

For every $\ell \in \Lambda$, we consider $\Omega_{7,\ell}$ be the set of q-symplectic matrices $M \in \mathrm{CSp}_{2g}(\mathbb{F}_\ell)$ such that the characteristic polynomial χ_M admits a factorization either as a quadratic irreducible polynomial multiplied by distinct irreducible polynomials of odd degree, or as a quartic irreducible polynomial multiplied by distinct irreducible polynomials of odd degree. Indeed, if P_f is separable but the Galois group $\mathrm{Gal}(P_f)$ does not contain a transposition nor a 4-cycle (when seen as a subgroup of $\mathfrak{S}_{2g}$), then $\rho_\ell(\mathrm{Frob}_{f,q}) \notin \Omega_{7,\ell}$ for any ℓ (see [Jac85, Theorem 4.37]).

Therefore, we need to count the symplectic polynomials with such factorizations to be able to conclude as above. For $\ell \in \Lambda$, we let $\delta_{7,\ell} = \frac{|\Omega_{7,\ell}|}{|\mathrm{Sp}_{2g}(\mathbb{F}_\ell)|}$.

In the case g is even, we use Lemma 7.7 with ($k = 1$, $n_{\frac{g-2}{2}} = 1$) and with ($k = 2$, $n_{\frac{g-4}{2}} = 1$, $n_0 = 1$) to get

$$\delta_{7,\ell} \geq \frac{1}{4(g-1)} + \frac{1}{16(g-3)} + O(\ell^{-1/2}) \geq \frac{5}{16g} + O(\ell^{-\frac{1}{2}}).$$

In the case g is odd we use Lemma 7.7 with ($k = 1$, $n_{\frac{g-3}{2}} = 1$, $n_0 = 1$) with ($k = 1$, $n_{\frac{g-5}{2}} = 1$, $n_1 = 1$), and with ($k = 2$, $n_{\frac{g-3}{2}} = 1$) to get

$$\delta_{7,\ell} \geq \frac{1}{8(g-2)} + \frac{1}{24(g-4)} + \frac{1}{8(g-2)} + O(\ell^{-\frac{1}{2}}) \geq \frac{7}{24g} + O(\ell^{-\frac{1}{2}}).$$

In both cases we have $\delta_{7,\ell} \geq \frac{7}{24g} + O(\ell^{-\frac{1}{2}})$, so we obtain the announced bound in the same way as in the proof of Proposition 7.4. $\square$

Remark 7.6. In the proof above of Lemma 7.5 one could expand the application of Lemma 7.7 to add more terms to the lower bound of $\delta_{7,\ell}$ to gain marginal improvements. The additional condition in the lemma and its application above with $k = 2$ delivers our refinement over Kowalski's bound (1.1).

Lemma 7.7. *Let $0 \leq k \leq g$ be two integers, and let $\ell > 4g^2$ be a prime number. Write $r = \lfloor \frac{g-k-1}{2} \rfloor$ and let n_i, $1 \leq i \leq r$, be integers such that $g = k + n_0 + 3n_1 + 5n_2 + \cdots + (2r+1)n_r$. Let $\omega_{k,\ell}(\underline{n})$ be the set of q-symplectic squarefree polynomials $P \in \mathbb{F}_\ell[T]$ which factor as a product $P = Q_{2k} R_0 \tilde{R}_0 R_1 \tilde{R}_1 \ldots R_r \tilde{R}_r$, where Q_{2k} is an irreducible q-symplectic polynomial of degree $2k$, each R_i is a product of n_i distinct irreducible monic polynomials of degree $2i+1$, and $\tilde{R}_i = \frac{T^{(2i+1)n_i}}{R_i(0)} R_i\left(\frac{q}{T}\right)$ is the q-reciprocal of R_i. Then, we have*

$$|\omega_{k,\ell}(\underline{n})| \geq \left(\prod_{i=0}^{r} \frac{1}{2^{n_i}(2i+1)^{n_i} n_i!} \right) \frac{1}{2k} \ell^g - O(\ell^{g-\frac{1}{2}}).$$

Proof. First observe that for any q-symplectic polynomial $P \in \mathbb{F}_\ell[T]$, one has $P(0) = q^{\deg P/2} \neq 0$, in particular, for all $R \mid P$, one has $R(0) \neq 0$. We appeal to [Kow06, Lemma 7.3 (ii)], which gives that the count of irreducible symplectic polynomials of degree $2k$ is larger than $\frac{1}{2k}\ell^k - O(\ell^{k-1})$ (see also [DDS98, Lemma 3] which can be adapted to the case of q-symplectic polynomials). The irreducible factors of odd degree of a symplectic polynomial come in pairs $\{R(T), \tilde{R}(T) = \frac{T^{\deg R}}{R(0)} R\left(\frac{q}{T}\right)\}$, uniquely determined by either of its elements. So it suffices to count polynomials of degree $g - k$ that are products of distinct odd degree irreducible polynomials. By [Kow08a, Lemma B.1] there are $\prod_{i=0}^{r} \frac{1}{(2i+1)^{n_i} n_i!} \ell^{g-k} - O(\ell^{g-k-\frac{1}{2}})$ polynomials with given factorization $R_0 R_1 \ldots R_r$ (as in the statement of the lemma).

For each polynomial with factorization type $R_0 R_1 \ldots R_r$, for each factor R_i, $0 \leq i \leq r$, we have made a choice of which element of the pair $\{R(T), \tilde{R}(T)\}$ to include. There are 2^{n_i} such choices for each i.

We just need to remove from the final count the monic q-symplectic polynomials that have multiple roots, as counted in the proof of Lemma 7.3, there are at most $O(\ell^{g-1})$ such polynomials, so this does not change the main term. $\square$

References

[AS10] Omran Ahmadi and Igor E Shparlinski, *On the distribution of the number of points on algebraic curves in extensions of finite fields*, Mathematical Research Letters **17** (2010), no. 4, 689–699.

[Bai21] Alexandre Bailleul, *Chebyshev's bias in dihedral and generalized quaternion Galois groups*, Algebra Number Theory **15** (2021), no. 4, 999–1041.

[Bai22] ———, *Explicit Kronecker-Weyl theorems and applications to prime number races*, Research in Number Theory **8** (2022), no. 3, Paper No. 43, 34.

[BG07] Jason P. Bell and Stefan Gerhold, *On the positivity set of a linear recurrence sequence*, Israel J. Math. **157** (2007), 333–345.

[BD00] Rajendra Bhatia and Chandler Davis, *A Better Bound on the Variance*, American Mathematical Monthly **107** (2000), no. 4, 353–357.

[Cal06] Jack S. Calcut, *Rationality and the Tangent Function*, 2006. preprint available at https://www2.oberlin.edu/faculty/jcalcut/tanpap.pdf.

[Cha08] Byungchul Cha, *Chebyshev's bias in function fields*, Compositio Mathematica **144** (2008), no. 6, 1351–1374.

[CI11] Byungchul Cha and Bo-Hae Im, *Chebyshev's bias in Galois extensions of global function fields*, Journal of Number Theory **131** (2011), no. 10, 1875–1886.

[CFJ16] Byungchul Cha, Daniel Fiorilli, and Florent Jouve, *Prime number races for elliptic curves over function fields*, Annales Scientifiques de l'École Normale Supérieure. Quatrième Série **49** (2016), no. 5, 1239–1277.

[CFJ17] ———, *Independence of the zeros of elliptic curve L-functions over function fields*, Int. Math. Res. Not. IMRN **9** (2017), 2614–2661.

[Cho65] Sarvadaman Chowla, *The Riemann hypothesis and Hilbert's tenth problem*, Norske Vid. Selsk. Forh. (Trondheim) **38** (1965), 62–64.

[CS86] Gary Cornell and Joseph H. Silverman (eds.), *Arithmetic geometry*, Springer-Verlag, New York, 1986. Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984.

[Cre01] John E. Cremona, *Classical invariants and 2-descent on elliptic curves*, J. Symbolic Comput. **31** (2001), no. 1-2, 71–87. Computational algebra and number theory (Milwaukee, WI, 1996).

[DDS98] Sandra Davis, William Duke, and Xiaodong Sun, *Probabilistic Galois theory of reciprocal polynomials*, Expositiones Mathematicae. International Journal **16** (1998), no. 3, 263–270.

[DM21] Lucile Devin and Xianchang Meng, *Chebyshev's bias for products of irreducible polynomials*, Advances in Mathematics **392** (2021), Paper No. 108040, 45.

[DKRV21] Taylor Dupuy, Kiran Kedlaya, David Roe, and Christelle Vincent, *Counterexamples to a Conjecture of Ahmadi and Shparlinski*, Experimental Mathematics (2021), 1–5.

[ELS20] Jordan S. Ellenberg, Wanlin Li, and Mark Shusterman, *Nonvanishing of hyperelliptic zeta functions over finite fields*, Algebra Number Theory **14** (2020), no. 7, 1895–1909.

[EVW16] Jordan S. Ellenberg, Akshay Venkatesh, and Craig Westerland, *Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields*, Ann. of Math. (2) **183** (2016), no. 3, 729–786.

[EvdPSW03] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward, *Recurrence sequences*, Vol. 104, American Mathematical Society Providence, RI, 2003.

[FJ22] Daniel Fiorilli and Florent Jouve, *Unconditional Chebyshev biases in number fields*, Journal de l'École polytechnique. Mathématiques **9** (2022), 671–679.

[FM13] Daniel Fiorilli and Greg Martin, *Inequities in the Shanks-Rényi prime number race: an asymptotic formula for the densities*, Journal für die Reine und Angewandte Mathematik. [Crelle's Journal] **676** (2013), 121–212.

[FK02a] Kevin Ford and Sergei Konyagin, *Chebyshev's conjecture and the prime number race*, IV International Conference "Modern Problems of Number Theory and its Applications": Current Problems, Part II (Russian) (Tula, 2001), 2002, pp. 67–91.

[FK02b] ———, *The prime number race and zeros of L -functions off the critical line*, Duke Mathematical Journal **113** (2002), no. 2, 313–330.

[FK03] ———, *The prime number race and zeros of L-functions off the critical line. II*, Bonner Math. Schriften, vol. 360, Univ. Bonn, Bonn, 2003.

[FKL13] Kevin Ford, Sergei Konyagin, and Youness Lamzouri, *The prime number race and zeros of Dirichlet L-functions off the critical line: Part III*, The Quarterly Journal of Mathematics **64** (2013), no. 4, 1091–1098.

[GM06] Andrew Granville and Greg Martin, *Prime Number Races*, The American Mathematical Monthly **113** (2006), 1-33.

[Hal08] Chris Hall, *Big symplectic or orthogonal monodromy modulo ℓ*, Duke Mathematical Journal **141** (2008), no. 1, 179–203.

[HNR09] Everett W. Howe, Enric Nart, and Christophe Ritzenthaler, *Jacobians in isogeny classes of abelian surfaces over finite fields*, Université de Grenoble. Annales de l'Institut Fourier **59** (2009), no. 1, 239–289.

[Hum12] Peter Humphries, *The Mertens and Pólya conjectures in function fields*, Australian National University, 2012.

[Jac85] Nathan Jacobson, *Basic algebra. I*, 2nd ed., W. H. Freeman and Company, New York, 1985.

[Kow06] Emmanuel Kowalski, *The large sieve, monodromy and zeta functions of curves*, J. Reine Angew. Math. **601** (2006), 29–69.

[Kow08a] ———, *The Large Sieve and its Applications: Arithmetic Geometry, Random Walks and Discrete Groups*, Cambridge Tracts in Mathematics, vol. 175, Cambridge University Press, Cambridge, 2008.

[Kow08b] ———, *The large sieve, monodromy, and zeta functions of algebraic curves. II. Independence of the zeros*, International Mathematics Research Notices. IMRN (2008), Art. ID rnn 091, 57.

[Li18] Wanlin Li, *Vanishing of hyperelliptic L-functions at the central point*, Journal of Number Theory **191** (2018), 85-103.

[MN20] Greg Martin and Nathan Ng, *Inclusive prime number races*, Transactions of the American Mathematical Society **373** (2020), no. 5, 3561-3607.

[PG20] Corentin Perret-Gentil, *Roots of L-functions of characters over function fields, generic linear independence and biases*, Algebra & Number Theory **14** (2020), no. 5, 1291–1329.

[Ros02] Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.

[RS94] Michael Rubinstein and Peter Sarnak, *Chebyshev's bias*, Experimental Mathematics **3** (1994), no. 3, 173–197.

[Sed22] Youssef Sedrati, *Inequities in the Shanks-Renyi prime number race over function fields*, Mathematika **68** (2022), no. 3, 840–895.

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, Second, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[Wat69] William C. Waterhouse, *Abelian varieties over finite fields*, Annales Scientifiques de l'École Normale Supérieure. Quatrième Série **2** (1969), 521–560.

[Wei48] André Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041, Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann et Cie., Paris, 1948.

ENS Paris-Saclay, Centre Borelli, UMR 9010, 91190 Gif-sur-Yvette, France
Email address: alexandre.bailleul@ens-paris-saclay.fr

Univ. Littoral Côte d'Opale, UR 2597 LMPA, Laboratoire de Mathématiques Pures et Appliquées Joseph Liouville, F-62100 Calais, France
Email address: lucile.devin@univ-littoral.fr

Department of Mathematics, University of Georgia, Athens, GA 30602, USA
Email address: keliher@uga.edu

Washington University in St. Louis, Department of Mathematics and Statistics, One Brookings Drive, St. Louis, MO 63130, USA
Email address: wanlin@wustl.edu