ULTRA-SHORT SUMS OF TRACE FUNCTIONS

E. KOWALSKI AND T. UNTRAU

Abstract. We generalize results of Duke, Garcia, Hyde, Lutz and others on the distribution of sums of roots of unity related to Gaussian periods to obtain equidistribution of similar sums over zeros of arbitrary integral polynomials. We also interpret these results in terms of trace functions, and generalize them to higher rank trace functions.

1. Introduction

The motivation for this work lies in papers of Garcia, Hyde and Lutz [17] and Duke, Garcia and Lutz [10], recently generalized by Untrau [26] in a number of ways, which considered the distribution properties of certain finite sums of roots of unity which are related to Gaussian periods and to "supercharacters" of finite groups.

We interpret these sums as examples of sums of trace functions over certain *bounded* finite sets. From this point of view, this study is a complement to results concerning sums of trace functions with growing length modulo a prime p (for instance, the paper of Perret-Gentil [23] for sums of length roughly up to $\log p$, or that of Fouvry, Kowalski, Michel, Raju, Rivat and Soundararajan [15] for sums of length slightly above $\sqrt{p}$, and that of Kowalski and Sawin [22] for sums of length proportional to p).

The range of summation will be taken to be more general than an interval, and despite the simplicity of the setting, one obtains some interesting equidistribution results.

Here is a simple illustration of our statements. More general versions will be proved in Sections 2, 6 and 7. We recall the definition

$$\mathrm{Kl}_2(a;q) = \frac{1}{\sqrt{q}} \sum_{x\in \mathbf{F}_q^\times} e\Big(\frac{ax+\bar{x}}{q}\Big), \qquad e(z) = e^{2i\pi z},$$

of the normalized Kloosterman sums modulo a prime number q.

Theorem 1.1 (Ultra-short sums of additive characters and Kloosterman sums)**.** *Let $g \in \mathbf{Z}[\mathrm{X}]$ be a fixed monic polynomial of degree $d \geqslant 1$. For any field K, denote by $\mathrm{Z}_g(\mathrm{K})$ the set of zeros of g in K, and put $\mathrm{Z}_g = \mathrm{Z}_g(\mathbf{C})$. Let $\mathrm{K}_g = \mathbf{Q}(\mathrm{Z}_g)$ be the splitting field of g.*

Date: June 24, 2023, 11:56.

2010 *Mathematics Subject Classification.* 11T23, 11L15.

Key words and phrases. Equidistribution, linear relations between algebraic numbers, Weyl sums, roots of polynomial congruences, trace functions.

(1) *As $q \to +\infty$ among prime numbers unramified and totally split in* K_g*, the sums*

$$\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} e\Big(\frac{ax}{q}\Big)$$

parameterized by $a \in \mathbf{F}_q$ become equidistributed in $\mathbf{C}$ with respect to some explicit probability measure μ_g.

(2) *Suppose that $0 \notin \mathrm{Z}_g$. As $q \to +\infty$ among prime numbers unramified and totally split in* K_g*, the sums*

$$\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} \mathrm{Kl}_2(ax; q)$$

parameterized by $a \in \mathbf{F}_q$ become equidistributed in $\mathbf{C}$ with respect to the measure which is the law of the sum of d independent Sato–Tate random variables.

Example 1.2. (1) The case considered in the previous papers that we mentioned is that of $g = \mathrm{X}^d - 1$ for some integer $d \geqslant 1$, in which case Z_g is the set of d-th roots of unity and the primes involved are the prime numbers congruent to 1 modulo d. (In fact, these references consider more generally the sums above for q a power of an odd prime $\equiv 1 \pmod{d}$, and we will also handle this case.)

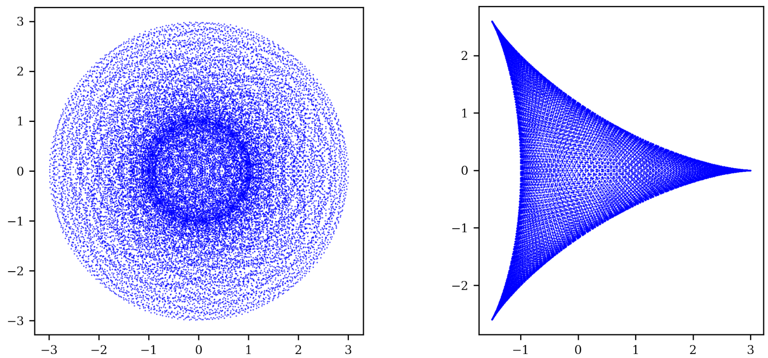
(2) The measure μ_g can be described relatively explicitly, and depends on the additive relations (with integral coefficients) satisfied by the zeros of g. We will discuss this in more detail below, but "generically", we will see that μ_g is just the law of the sum $\mathrm{X}_1 + \cdots + \mathrm{X}_d$ of d independent random variables each uniformly distributed on the unit circle. However, more interesting measures also arise, for instance for $g = \mathrm{X}^\ell - 1$ where ℓ is a prime number, the measure $\mu_{\mathrm{X}^\ell - 1}$ is the image by the map

$$(z_1, \ldots, z_{\ell-1}) \mapsto z_1 + \cdots + z_{\ell-1} + \frac{1}{z_1 \cdots z_{\ell-1}}$$

of the uniform (Haar) probability measure on $(\mathbf{S}^1)^{\ell-1}$. Figure 1 below illustrates two examples. In the case of the polynomial $\mathrm{X}^3 + 2\mathrm{X}^2 + 3$, one can show that there are no non-trivial additive relations between the zeros of g, whereas in the case of the polynomial $\mathrm{X}^3 + \mathrm{X} + 3$, there is clearly the relation given by the sum of the roots which equals zero (because the coefficient of X^2 is zero). We see that this difference between their module of additive relations translates into different limiting measures μ_g for the associated sums of additive characters. Since these two polynomials have Galois group $\mathfrak{S}_3$ over $\mathbf{Q}$, these pictures will be fully explained in Section 3, Example 2.

(3) The second part of the theorem also has precursors: for instance, the result follows from [14, Prop. 3.2] if $g = (\mathrm{X} - 1) \cdots (\mathrm{X} - d)$. We illustrate our generalization in Figure 2 with the example of another polynomial g of degree 3.

Remark 1.3. We assume that g is monic mostly for simplicity to ensure that the roots of g are algebraic integers. However, one can also handle an arbitrary polynomial g by considering an integer $\mathrm{N} \geqslant 1$ such that $\mathrm{N}z$ is integral for all roots z of g, and either reduce to the monic case by using the polynomial $\widetilde{g}$ with roots the $\mathrm{N}z$, or by considering below the ring $\mathbf{O}_g[1/\mathrm{N}]$ of N-integers in K_g instead of the full ring of integers.



(A) $g = X^3 + 2X^2 + 3$ and $q = 30113$.

(B) $g = X^3 + X + 3$ and $q = 30223$.

FIGURE 1. The sums $\sum_{x \in Z_g(\mathbf{F}_q)} e(\frac{ax}{q})$ as a varies in $\mathbf{F}_q$, for two different polynomials g of degree 3.

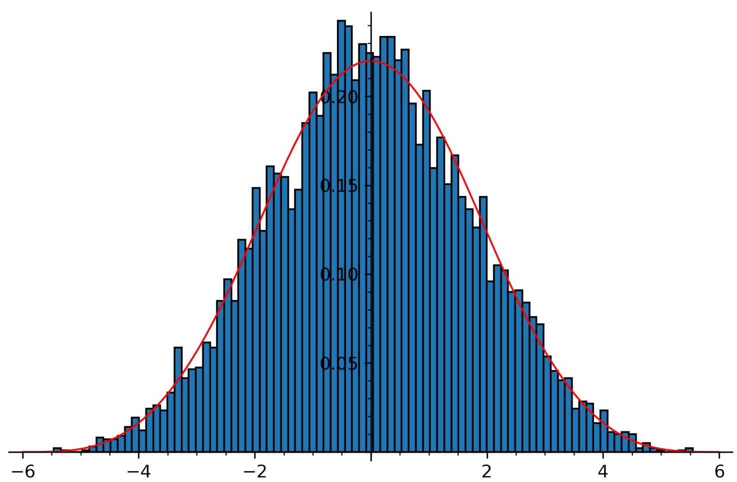


FIGURE 2. Distribution of the values of the sums $\sum_{x \in Z_g(\mathbf{F}_q)} \mathrm{Kl}_2(ax; q)$ as a varies in $\mathbf{F}_q$, for $g = X^3 - 9X - 1$ and $q = 8089$. The red curve is the probability density function of the random variable $X_1 + X_2 + X_3$ defined as the sum of three independent and identically distributed Sato–Tate random variables.

Notation. Let G be a locally compact abelian group, with character group $\widehat{G}$. Let H be a closed subgroup of G. We recall that the restriction homomorphism from $\widehat{G}$ to $\widehat{H}$ is surjective (in other words, any character of H can be extended to a character of G).

The *orthogonal* $H^\perp$ of H is the closed subgroup of $\widehat{G}$ defined by

$$H^\perp = \{\chi \in \widehat{G} \mid \chi(x) = 1 \text{ for all } x \in H\}.$$

If we identify the dual of $\widehat{G}$ with G by Pontryagin duality, then the orthogonal of $H^\perp$ is identified with H, or in other words

$$H = \{x \in G \mid \chi(x) = 1 \text{ for all } \chi \in H^\perp\}.$$

We refer, e.g., to Bourbaki's account [6] of Pontryagin duality for these facts.

Suppose that G is compact. A random variable with values in G is said to be *uniformly distributed on* H if its law μ is the probability Haar measure on H (viewed as a probability measure on G).

Throughout this paper, we will consider a fixed *monic* polynomial $g \in \mathbf{Z}[X]$ of degree $d \geqslant 1$. We denote by Z_g the set of zeros of g in $\mathbf{C}$, and more generally by $Z_g(A)$ the set of zeros of g in any commutative ring A. We further denote by K_g the splitting field of g in $\mathbf{C}$, so that $K_g = \mathbf{Q}(Z_g)$. Since our discussion only depends on Z_g, we will assume, without loss of generality, that g is separable. Since g is monic, the set Z_g is contained in the ring of integers $\mathbf{O}_g$ of K_g.

For any set X, we denote by $C(Z_g; X)$ the set of functions $Z_g \to X$, and in particular we write $C(Z_g) = C(Z_g; \mathbf{C})$ for the vector space of $\mathbf{C}$-valued functions on Z_g. We denote by σ the linear form on $C(Z_g)$ defined by

$$\sigma(f) = \sum_{x \in Z_g} f(x),$$

and by γ the morphism of abelian groups from $C(Z_g; \mathbf{Z})$ to K_g defined by

$$\gamma(f) = \sum_{x \in Z_g} f(x)x. \tag{1}$$

The set $C(Z_g; \mathbf{S}^1)$ is a compact abelian group, isomorphic to $(\mathbf{S}^1)^{|Z_g|}$ by sending α to $(\alpha(z))_{z \in Z_g}$.

Acknowledgements. The second author wishes to thank Florent Jouve and Guillaume Ricotta for many helpful discussions, and Emanuele Tron for giving the key ideas of the proof of the linear independence of j-invariants. Pictures were made using the open-source software `sagemath`.

2. The case of additive characters

We begin with the simple setup of the first part of Theorem 1.1 before considering a much more general situation.

We fix a separable monic polynomial $g \in \mathbf{Z}[X]$ as in the previous discussion. Let p be a non-zero prime ideal in $\mathbf{O}_g$. We denote by $|p| = |\mathbf{O}_g/p|$ the norm of p. For any ideal $I \subset \mathbf{O}_g$, the canonical projection $\mathbf{O}_g \to \mathbf{O}_g/I$ will be denoted ϖ_I, or simply ϖ when the ideal is clear from context.

We denote by $\mathcal{S}_g$ the set of prime ideals $p \subset \mathbf{O}_g$ which do not divide the discriminant of g (so that the reduction map modulo p is injective on Z_g) and have residual degree one (in particular, these are unramified primes). For $p \in \mathcal{S}_g$, the norm $q = |p|$ is a prime number, and for any integer $n \geqslant 1$, the restriction $\mathbf{Z} \to \mathbf{O}_g/p^n$ of ϖ_{p^n} induces a ring isomorphism $\mathbf{Z}/q^n\mathbf{Z} \to \mathbf{O}_g/p^n$. We will usually identify these two rings. Moreover, for $p \in \mathcal{S}_g$ and $n \geqslant 1$, the separable polynomial g has $\deg(g)$ different roots in the completion of K_g at p, hence the reduction map modulo p^n induces a bijection $\mathrm{Z}_g \to \mathrm{Z}_g(\mathbf{O}_g/p^n) = \mathrm{Z}_g(\mathbf{Z}/|p|^n\mathbf{Z})$ for any integer $n \geqslant 1$.

For any prime ideal $p \in \mathcal{S}_g$ and any integer $n \geqslant 1$, we view $\mathbf{O}_g/p^n$ as a finite probability space with the uniform probability measure. We define random variables U_{p^n} on $\mathbf{O}_g/p^n$, taking values in $\mathrm{C}(\mathrm{Z}_g; \mathbf{S}^1)$, by

$$\mathrm{U}_{p^n}(a)(x) = e\Big(\frac{a\varpi(x)}{|p|^n}\Big),$$

where $\varpi = \varpi_{p^n}$ here (according to our convention, $a\varpi(x)$ is an element of $\mathbf{O}_g/p^n$ which is identified to an element of $\mathbf{Z}/|p|^n\mathbf{Z}$).

Remark 2.1. In the earlier references [10], [17] and [26], we have $g = \mathrm{X}^d - 1$ for some integer d, and one considers primes $q \equiv 1 \pmod d$. A primitive d-th root of unity modulo q, say w_q, is fixed for all such q, and one considers the limit as $q \to \infty$ of the tuples $(e(\frac{aw_q^k}{q}))_{0\leqslant k\leqslant d-1}$, for a uniform in $\mathbf{F}_q$. This approach does not generalize in a convenient way to more general polynomials g, where the roots are not as easily parameterized.

Proposition 2.2 (Ultra-short equidistribution)**.** *The random variables U_{p^n} converge in law as $|p|^n \to +\infty$ to a random function $\mathrm{U}\colon \mathrm{Z}_g \to \mathbf{S}^1$ such that U is uniformly distributed on the subgroup $\mathrm{H}_g \subset \mathrm{C}(\mathrm{Z}_g; \mathbf{S}^1)$ which is orthogonal to the abelian group*

$$\mathrm{R}_g = \ker(\gamma) = \{\alpha \in \mathrm{C}(\mathrm{Z}_g; \mathbf{Z}) \mid \sum_{x\in \mathrm{Z}_g} \alpha(x)x = 0\}$$

of (integral) additive relations betweens roots of g, i.e.

$$\mathrm{H}_g = \{f \in \mathrm{C}(\mathrm{Z}_g; \mathbf{S}^1) \mid \text{ for all } \alpha \in \mathrm{R}_g, \text{ we have } \prod_{x\in\mathrm{Z}_g} f(x)^{\alpha(x)} = 1\}.$$

Proof. Since $\mathrm{C}(\mathrm{Z}_g; \mathbf{S}^1)$ is a compact abelian group, we can apply the generalized Weyl Criterion for equidistribution: it is enough to check that, for any character η of $\mathrm{C}(\mathrm{Z}_g; \mathbf{S}^1)$, we have

$$\mathbf{E}(\eta(\mathrm{U}_{p^n})) \to \mathbf{E}(\eta(\mathrm{U}))$$

as $|p|^n \to +\infty$. The right-hand side is either 1 or 0, depending on whether the restriction of η to H_g is trivial or not.

The character η is determined uniquely by a function $\alpha \in \mathrm{C}(\mathrm{Z}_g; \mathbf{Z})$ by the rule

$$\eta(f) = \prod_{x\in\mathrm{Z}_g} f(x)^{\alpha(x)}$$

for any $f \in \mathrm{C}(\mathrm{Z}_g; \mathbf{S}^1)$. We have then by definition

$$\mathbf{E}(\eta(\mathrm{U}_{p^n})) = \frac{1}{|p|^n} \sum_{a\in\mathbf{O}_g/p^n} e\Big(\frac{a}{|p|^n}\varpi\Big(\sum_{x\in\mathrm{Z}_g} \alpha(x)x\Big)\Big).$$

Simply by orthogonality of the characters modulo $|p|^n$, this sum is either 1 or 0, depending on whether

$$\gamma(\alpha) = \sum_{x \in \mathrm{Z}_g} \alpha(x) x$$

is zero modulo p^n or not. As soon as $|p|^n$ is large enough, this condition is equivalent with $\gamma(\alpha)$ being zero or not in K_g. In particular, the limit of $\mathbf{E}(\eta(\mathrm{U}_{p^n}))$ is either 1 or 0 depending on whether $\alpha \in \ker(\gamma) = \mathrm{R}_g$ or not, and this is exactly what we wanted to prove. $\square$

Remark 2.3. The proof shows that in fact the Weyl sums are *stationary*. This somewhat unusual feature[1] explains the very regular aspect of the experimental pictures. We will explore further consequences of this fact in a later work.

Corollary 2.4. *For a taken uniformly at random in $\mathbf{O}_g/p^n$ with $p \in \mathcal{S}_g$, lying above a prime number q which does not divide* $\mathrm{disc}(g)$*, the sums*

$$\sum_{x \in \mathrm{Z}_g(\mathbf{O}_g/p^n)} e\Big(\frac{ax}{|p|^n}\Big)$$

become equidistributed in $\mathbf{C}$ as $|p|^n \to +\infty$ with limiting measure μ_g given by the law of $\sigma(\mathrm{U})$, where U is uniformly distributed on H_g.

Similarly, for a prime number q totally split in K_g and not dividing the discriminant of g, the sums

$$\sum_{\substack{x \in \mathbf{Z}/q^n\mathbf{Z} \\ g(x) \equiv 0 \,(\mathrm{mod}\, q^n)}} e\Big(\frac{ax}{q^n}\Big)$$

for $a \in \mathbf{Z}/q^n\mathbf{Z}$ become equidistributed in $\mathbf{C}$ as $q^n \to +\infty$ with limit $\sigma(\mathrm{U})$.

Proof. Since ϖ_{p^n} induces a bijection between Z_g and $\mathrm{Z}_g(\mathbf{O}_g/p^n)$, the random variables whose limit we are considering coincide with $\sigma(\mathrm{U}_{p^n})$, and since σ is a continuous function from $\mathrm{C}(\mathrm{Z}_g; \mathbf{S}^1)$ to $\mathbf{C}$, we obtain the result from Proposition 2.2 by composition.

For the second part, we note that for any prime number q which is totally split in $\mathbf{O}_g$ and does not divide the discriminant of g, there exists a prime ideal $p \in \mathcal{S}_g$ above q, and for any $n \geqslant 1$, we have then $\mathrm{Z}_g(\mathbf{Z}/q^n\mathbf{Z}) = \mathrm{Z}_g(\mathbf{O}_g/p^n)$, so that

$$\sum_{x \in \mathrm{Z}_g(\mathbf{O}_g/p^n)} e\Big(\frac{ax}{|p|^n}\Big) = \sum_{\substack{x \in \mathbf{Z}/q^n\mathbf{Z} \\ g(x) \equiv 0 \,(\mathrm{mod}\, q^n)}} e\Big(\frac{ax}{q^n}\Big),$$

and the result follows from the first part since we are considering a subsequence of the random variables previously considered. $\square$

Before studying a few examples in the next section, we make a few remarks concerning the limiting measures. Since the random variable $\sigma(\mathrm{U})$ is bounded, one can compute all its moments using the equidistribution. This leads straightforwardly to the formulas

$$\mathbf{E}(\sigma(\mathrm{U})) = \begin{cases} 0 & \text{if } 0 \notin \mathrm{Z}_g \\ 1 & \text{if } 0 \in \mathrm{Z}_g, \end{cases}$$

[1] Though there are important instances of limit theorems where *moments* are stationary, e.g. in the convergence of the number of fixed points of random permutations to a Poisson distribution.

and

$$\mathbf{E}(|\sigma(\mathrm{U})|^2) = |\mathrm{Z}_g|.$$

The fact that the expectation is zero if g is irreducible of degree at least 2 has some indirect relevance to the well-known conjecture according to which the fractional parts of the roots modulo primes $q \leqslant x$ of an irreducible polynomial g of degree at least 2 should become equidistributed (with respect to the Lebesgue measure) in $\mathbf{R}/\mathbf{Z}$ as $x \to +\infty$ – see, e.g., the paper [9] of Duke, Friedlander and Iwaniec.

Indeed, the Weyl sums for this equidistribution problem are (essentially)

$$\frac{1}{\pi(x)} \sum_{q \leqslant x} \sum_{\substack{y \in \mathbf{F}_q \\ g(y)=0}} e\Big(\frac{ay}{q}\Big)$$

(where q ranges over primes) for some *fixed* non-zero integer a. For each prime q which happens to be totally split in K_g, the inner sum is of the form $\sigma(\mathrm{U}_p(a))$ for some prime ideal $p \in \mathcal{S}_g$. Thus, Proposition 2.2 tells us about the asymptotic distribution of these terms *when a varies modulo q*. Intuitively, we may hope that the average over q should lead to a limit which coincides with $\mathbf{E}(\sigma(\mathrm{U})) = 0$, and this would translate to the equidistribution conjecture.

In fact, we may even ask whether these inner parts of the Weyl sums for equidistribution are *themselves* equidistributed. More precisely, fix a non-zero integer a, and consider the random variables of the type

$$\mathrm{U}'_{\mathrm{T}}(p)(x) = e\Big(\frac{a\varpi_p(x)}{|p|}\Big)$$

defined on the probability spaces $\mathcal{S}_g(\mathrm{T})$ of primes p in $\mathcal{S}_g$ with $|p| \leqslant \mathrm{T}$ (with uniform probability measure), and with values in $\mathrm{C}(\mathrm{Z}_g; \mathbf{S}^1)$.

Question. Do the random functions U'_{T} converge in law as $\mathrm{T} \to +\infty$? If Yes, is the limit the same as in Proposition 2.2?

If the answer to this question is positive, then the equidistribution conjecture holds, at least when averaging only over primes totally split in K_g, since then

$$\frac{1}{|\mathcal{S}_g(\mathrm{T})|} \sum_{p \in \mathcal{S}_g(\mathrm{T})} \sum_{x \in \mathrm{Z}_g} e\Big(\frac{a\varpi_p(x)}{|p|}\Big) \to \int_{\mathbf{C}} z d\mu_g(z) = 0.$$

The answer is indeed positive when g is irreducible of degree 2, by the work of Duke, Friedlander and Iwaniec [9] and Toth [25] (more precisely, in this case the relevant inner Weyl sums are essentially Salié sums, and it is proved – using the equidistribution property for the roots of quadratic congruences, which is the main result of these papers – that the Salié sums become equidistributed in $[-2, 2]$ like the sums $e(x) + e(-x)$ where x is uniformly distributed in $\mathbf{R}/\mathbf{Z}$. Moreover, this question is closely related with recent conjectures of Hrushovski [18, § 5.5], themselves motivated by questions concerning the model theory of finite fields with an additive character.

Numerical experiments also seem to suggest a positive answer at least in many cases. But note also that obtaining the same limiting measure depends on assuming that g is irreducible.

(For instance, if there is an integral root k for g, as is the case with $k = 1$ for $X^d - 1$, then the value $U'_T(p)(k) = e(ak/|p|)$ converges to 1 as $|p| \to +\infty$, which is a different behavior than that provided by Proposition 2.2.)

3. Examples

We now consider a few examples of Proposition 2.2.

(1) Suppose that $g = X^d - 1$ for some $d \geqslant 1$, so that $Z_g = \boldsymbol{\mu}_d$ is the group of d-th roots of unity.

Consider first the case when $d = \ell$ is a prime number. The group of additive relations is generated in this case by the constant function $\alpha = 1$ (indeed, let $\xi \in \boldsymbol{\mu}_\ell$ be a root of unity different from 1; then a relation

$$\sum_{x \in \boldsymbol{\mu}_\ell} \alpha(x)x = 0$$

is equivalent to $f(\xi) = 0$, where f is the polynomial

$$\sum_{i=0}^{\ell-1} \alpha(\xi^i) X^i \in \mathbf{Z}[X],$$

which must therefore be an integral multiple of the minimal polynomial

$$1 + X + \cdots + X^{\ell-1}$$

of ξ). The subgroup $H_{X^\ell - 1}$ which is the support of the limit U in this case is then

$$H_{X^\ell-1} = \{f \colon \boldsymbol{\mu}_\ell \to \mathbf{S}^1 \mid \prod_{x \in \boldsymbol{\mu}_\ell} f(x) = 1\}.$$

which can be identified with $(\mathbf{S}^1)^{\ell-1}$ by the group isomorphism $f \mapsto (f(x))_{x \in \boldsymbol{\mu}_\ell - \{1\}}$. The linear form σ is then identified with the linear form $(\mathbf{S}^1)^{\ell-1} \to \mathbf{C}$ such that

$$(y_1, \ldots, y_{\ell-1}) \mapsto y_1 + \cdots + y_{\ell-1} + \frac{1}{y_1 \cdots y_{\ell-1}}.$$

In the case of a general d, the same argument shows that R_{X^d-1} is the group of functions $\alpha \colon \boldsymbol{\mu}_d \to \mathbf{Z}$ such that the d-th cyclotomic polynomial Φ_d divides

$$\sum_{i=0}^{d-1} \alpha(\xi^i) X^i,$$

where ξ is a primitive d-th root of unity. Thus R_{X^d-1} is a free abelian group of rank $d - \varphi(d)$, generated by the functions α corresponding to the polynomials

$$\Phi_d,\ X\Phi_d,\ \cdots,\ X^{d-\varphi(d)-1}\Phi_d.$$

Although this presentation is more abstract, it coincides with the description of Duke, Garcia and Lutz in [10, Th. 6.3].

(2) The group of additive relations of a polynomial is studied by Berry, Dubickas, Elkies, Poonen and Smyth [2] in some detail (see also [20]). It is known for instance (see e.g. [20,

Prop. 2.8] or [21, Prop. 4.7.12]; this goes back at least to Smyth [24]) that if the Galois group of K_g over $\mathbf{Q}$ is the symmetric group $\mathfrak{S}_d$, then only two cases are possible: either R_g is trivial (in which case the limit measure μ_g is the law of the sum of d independent random variables uniformly distributed on $\mathbf{S}^1$) or R_g is generated by the constant function 1 (in which case the measure μ_g is the same measure described in (1), except that d is not necessarily prime here). This second case corresponds to the situation where the sum of the roots is zero, i.e., to the case when the coefficient of X^{d-1} in g is zero.

(3) More interesting examples arise from polynomials g that are characteristic polynomials of "random" elements of the group of integral matrices in a simple Lie algebra L, where additive relations corresponding to the root system of L will appear. For instance, for the Lie algebra of type G_2, in its 7-dimensional irreducible representation, the roots of a characteristic polynomial have the form of tuples

$$(0, x, y, x+y, -x, -y, -x-y)$$

so that the group of additive relations will be quite large. It would be interesting to determine explicitly the support of the image measure in this case.

(4) Another natural example comes from the *Hilbert class polynomial* $g = H_\Delta$, whose roots are the j-invariants of elliptic curves with CM by an imaginary quadratic order $\mathcal{O}$ of given discriminant Δ (see, e.g., [8, § 13, Prop. 13.2]). This means that we consider sums

$$\sum_{\text{E with CM by } \mathcal{O}} e\Big(\frac{aj(\mathrm{E})}{q}\Big), \tag{2}$$

where the sum runs over isomorphism classes over $\mathbf{C}$ of elliptic curves with CM by $\mathcal{O}$, for prime numbers q totally split in the ring class field corresponding to the order $\mathcal{O}$. For instance, if $\Delta = -4m$ with $m \geqslant 1$ squarefree, these are exactly the primes of the form $x^2 + my^2$ (see the book of Cox [8] for details).

From Proposition 2.2, and Corollary 2.4, we know that the asymptotic distribution of the sums (2), as q tends to infinity and a varies in $\mathbf{F}_q$, is governed by the additive relations between these j-invariants. As it turns out, there are no non-trivial relations, except for $\Delta = -3$. This is essentially due to the fact that there is one j-invariant (for fixed $\mathcal{O}$ with discriminant large enough) which is much larger than the others, combined with the following lemma.

Lemma 3.1. *Let $g \in \mathbf{Z}[X]$ be irreducible over $\mathbf{Q}$ of degree $d \geqslant 2$. If there exists $x_0 \in Z_g$ such that*

$$|x_0| > \sum_{\substack{x \in Z_g \\ x \neq x_0}} |x|,$$

then $R_g = \{0\}$.

Proof. Suppose that there exists $\alpha \in R_g$ non-zero. Let $x_1 \in Z_g$ be such that $|\alpha(x_1)|$ is maximal, hence non-zero. Dividing by $\alpha(x_1)$, we obtain a relation

$$0 = \sum_{x \in Z_g} \beta(x) x$$

where $\beta(x) \in \mathbf{Q}$ with $|\beta(x)| \leqslant 1$ for all x and $\beta(x_1) = 1$. Since g is irreducible, we can find a Galois automorphism ξ such that $\xi(x_1) = x_0$, which means that we may assume that $x_1 = x_0$. Then we obtain

$$|x_0| = \Big|\sum_{x \neq x_0} \beta(x)x\Big| \leqslant \sum_{x \neq x_1} |x|,$$

and we conclude by contraposition. □

This lemma is applicable to the Hilbert class polynomial H_Δ. Indeed, it is irreducible (see, e.g., [8, § 13]). To check the existence of a dominating j-invariant, we use the bound

$$\Big||j(\tau)| - e^{2\pi \operatorname{Im}(\tau)}\Big| \leqslant 2079,$$

for τ in the usual fundamental domain F of $\mathbf{H}$ modulo $\mathrm{SL}_2(\mathbf{Z})$ (see [5, Lemma 1] by Bilu, Masser and Zannier), combined with the fact that there is a unique τ in F such that $j(\tau)$ is a root of H_Δ and $\operatorname{Im}(\tau) \geqslant \sqrt{|\Delta|}/2$, while all other j-invariants for the order $\mathcal{O}$ are of the form $j(\tau')$ where $\tau' \in \mathrm{F}$ has $\operatorname{Im}(\tau') \leqslant \sqrt{|\Delta|}/4$ (see [1, Section 3.3] by Allombert, Bilu and Pizarro-Madariaga). These properties imply that the lemma is applicable as soon as the bound

$$e^{\pi\sqrt{|\Delta|}} - 2079 > \deg(\mathrm{H}_\Delta)(e^{\pi\frac{\sqrt{|\Delta|}}{2}} + 2079)$$

holds. The degree of H_Δ is the Hurwitz class number, and one knows classically that

$$\deg \mathrm{H}_\Delta \leqslant \frac{\sqrt{|\Delta|}}{\pi}(\log|\Delta| + 2),$$

(see, e.g., [3, Lemma 3.6] by Bilu, Habegger and Kühne). One checks easily that the desired bound follows unless $\Delta \geqslant -9$. For the remaining cases, H_Δ has degree 1, and its unique root is a non-zero integer, except that $\mathrm{H}_{-3} = \mathrm{X}$ (see for instance the table [8, § 12.C] in the book of Cox). Therefore, unless $\Delta = -3$, the module of additive relations of H_Δ is trivial. Of course, for $\Delta = -3$, it is isomorphic to $\mathbf{Z}$.

This immediately leads to the following corollary concerning the distribution of sums of type (2):

Corollary 3.2. *Fix a negative discriminant $\Delta \neq -3$ of an imaginary quadratic order $\mathcal{O}$ with class number h. As $q \to \infty$ among the primes totally split in the ring class field corresponding to the order $\mathcal{O}$, the sums*

$$\sum_{\mathrm{E} \text{ with CM by } \mathcal{O}} e\Big(\frac{aj(\mathrm{E})}{q}\Big)$$

parametrized by $a \in \mathbf{F}_q$ become equidistributed in $\mathbf{C}$ with respect to the law of the sum $\mathrm{X}_1 + \cdots + \mathrm{X}_h$ of h independent random variables, each uniformly distributed on the unit circle.

On the other hand, for $\Delta = -3$, we have

$$\sum_{\mathrm{E} \text{ with CM by } \mathcal{O}} e\Big(\frac{aj(\mathrm{E})}{q}\Big) = 1$$

for all q.

4. Conditioning

The basic argument leading to Proposition 2.2 extends in another nice way to the *conditioning* situation, where we restrict the random variables U_{p^n} to suitable subsets of $\mathbf{O}_g/p^n$. This turns out to be closely related to the distribution of the fractional parts of these subsets.

The precise statements require some additional notation. First, we define by $\kappa(g)$ the non-negative integer such that

$$\mathrm{Im}(\gamma)\cap\mathbf{Z}=\kappa(g)\mathbf{Z}$$

(recall the definition (1) of γ; note that it is possible that $\kappa=0$, e.g. for $g=\mathrm{X}^2+d$ with $d\neq 0$).

For a prime ideal $p\in\mathcal{S}_g$ and $n\geqslant 1$, and for any $a\in\mathbf{O}_g/p^n$, we define the "fractional part" of a to be the fractional part in $[0,1]$ of $\bar{a}/|p|^n$ for any lift $\bar{a}\in\mathbf{Z}$ of a identified as an element of $\mathbf{Z}/|p|^n\mathbf{Z}$.

We denote by U the limit in Proposition 2.2.

Proposition 4.1 (Ultra-short equidistribution)**.** *For a subsequence of ideals p^n with $p\in\mathcal{S}_g$ and $n\geqslant 1$, let A_{p^n} be a non-empty subset of $\mathbf{O}_g/p^n$.*

(1) *If the fractional parts of $a\in\mathrm{A}_{p^n}$ are* uniformly equidistributed modulo 1 *as $|p|^n\to+\infty$, in the sense that*

$$\max_{\substack{h\in\mathbf{O}_g/p^n\\ h\neq 0}}\frac{1}{|\mathrm{A}_{p^n}|}\Big|\sum_{a\in\mathrm{A}_{p^n}}e\Big(\frac{ah}{|p|^n}\Big)\Big|\to 0$$

as $|p|^n\to+\infty$, then the restriction of the random variables U_{p^n} to A_{p^n}, viewed as probability space with uniform probability measure, converge in law to U*.*

(2) *Suppose that $\kappa(g)\neq 0$ and that the restriction of the random variables U_{p^n} to A_{p^n}, viewed as probability space with uniform probability measure, converge in law to* U*. Then the fractional parts of elements of $\kappa(g)\mathrm{A}_{p^n}$ are equidistributed modulo* 1*.*

Proof. We denote by U'_{p^n} the restriction of U_{p^n} to A_{p^n}, viewed as probability space with the uniform probability measure.

We expand the characteristic function f_{p^n} of A_{p^n} in discrete Fourier series

$$f_{p^n}(a)=\sum_{h\in\mathbf{O}_g/p^n}\alpha_{p^n}(h)e\Big(\frac{ha}{|p|^n}\Big)$$

where

$$\alpha_{p^n}(h)=\frac{1}{|p|^n}\sum_{a\in\mathrm{A}_{p^n}}e\Big(-\frac{ha}{|p|^n}\Big).$$

Let η be a character of $\mathrm{C}(\mathrm{Z}_g;\mathbf{S}^1)$, determined by $\alpha\in\mathrm{C}(\mathrm{Z}_g;\mathbf{Z})$ as in Proposition 2.2. By definition, we have

$$\begin{aligned}\mathbf{E}(\eta(\mathrm{U}'_{p^n})) &= \frac{1}{|\mathrm{A}_{p^n}|}\sum_{a\in\mathrm{A}_{p^n}} e\Big(\frac{a}{|p|^n}\varpi\Big(\sum_{x\in\mathrm{Z}_g}\alpha(x)x\Big)\Big)\\ &= \frac{1}{|\mathrm{A}_{p^n}|}\sum_{h\in\mathbf{O}_g/p^n}\alpha_{p^n}(h)\sum_{a\in\mathbf{O}_g/p^n} e\Big(\frac{a}{|p|^n}(\varpi(\gamma(\alpha))+h)\Big)\\ &= \frac{|p|^n}{|\mathrm{A}_{p^n}|}\alpha_{p^n}(-\varpi(\gamma(\alpha))) = \frac{1}{|\mathrm{A}_{p^n}|}\sum_{a\in\mathrm{A}_{p^n}} e\Big(\frac{\varpi(\gamma(\alpha))a}{|p|^n}\Big),\end{aligned}$$

an identity between Weyl sums for the equidistribution of U_{p^n} and Weyl sums for the equidistribution of the fractional parts of elements of A_{p^n}.

Suppose first that A_{p^n} is uniformly equidistributed modulo 1. If $\gamma(\alpha)=0$, then we get $\mathbf{E}(\eta(\mathrm{U}'_{p^n}))=1$. Otherwise, for $|p|^n$ large enough, we get $\varpi(\gamma(\alpha))\neq 0\in\mathbf{O}_g/p^n$, and therefore

$$|\mathbf{E}(\eta(\mathrm{U}'_{p^n}))|\leqslant \max_{\substack{h\in\mathbf{O}_g/p^n\\ h\neq 0}}\frac{1}{|\mathrm{A}_{p^n}|}\Big|\sum_{a\in\mathrm{A}_{p^n}} e\Big(\frac{ah}{|p|^n}\Big)\Big|,$$

which tends to 0 by assumption. This proves the first statement.

Conversely, suppose that $\kappa(g)\neq 0$ and that U'_{p^n} converges in law to U. Let $h\in\mathbf{Z}-\{0\}$. Pick $\alpha\in\mathrm{C}(\mathrm{Z}_g;\mathbf{Z})$ such that $\gamma(\alpha)=\kappa(g)h$, which exists by definition of $\kappa(g)$. For all p^n, we get

$$\frac{1}{|\mathrm{A}_{p^n}|}\sum_{a\in\mathrm{A}_{p^n}} e\Big(\frac{h\,\kappa(g)a}{|p|^n}\Big) = \frac{1}{|\mathrm{A}_{p^n}|}\sum_{a\in\mathrm{A}_{p^n}} e\Big(\frac{\varpi(\gamma(\alpha))a}{|p|^n}\Big) = \mathbf{E}(\eta(\mathrm{U}'_{p^n}))$$

where η is the character of $\mathrm{C}(\mathrm{Z}_g;\mathbf{S}^1)$ corresponding to α. This character is not trivial on H_g (because $\gamma(\alpha)\neq 0$), and therefore

$$\lim_{|p|^n\to+\infty}\frac{1}{|\mathrm{A}_{p^n}|}\sum_{a\in\mathrm{A}_{p^n}} e\Big(\frac{h\,\kappa(g)a}{|p|^n}\Big)=0,$$

which proves equidistribution modulo 1 of fractional parts of $\kappa(g)\mathrm{A}_{p^n}$ by the Weyl Criterion.

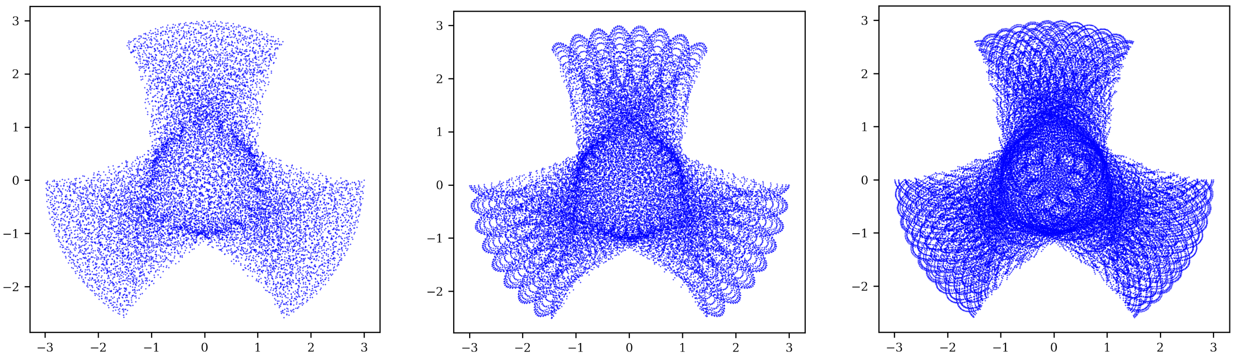
□

Example 4.2. (1) Let $\alpha\in\mathbf{R}$ satisfy $0<\alpha<1$. Let A_{p^n} be the set of classes corresponding to an interval of length $\sim\alpha|p|^n$ in $\mathbf{Z}/|p|^n\mathbf{Z}$. Then equidistribution (and a fortiori uniform equidistribution) of the fractional parts *fails*, hence the second part implies, by contraposition, that if $\kappa(g)=1$, then the random variables U_{p^n} conditioned to have $a\in\mathrm{A}_{p^n}$ *do not* converge to U.

As an illustration, let $g=\mathrm{X}^3+\mathrm{X}^2+2\mathrm{X}+1$. One checks quickly that g is irreducible, with Galois group $\mathfrak{S}_3$, so that Example 2 of Section 3 implies that the sums

$$\sum_{x\in\mathrm{Z}_g(\mathbf{F}_q)} e\Big(\frac{ax}{q}\Big), \tag{3}$$

parametrized by $a\in\mathbf{F}_q$ for q totally split in K_g, become equidistributed with respect to the measure μ_g which is the law of the sum of three independent random variables, each



(A) $q = 30307$ (B) $q = 60383$ (C) $q = 100357$

Figure 3. The sums (3) for a varying in $\{0, \ldots, \frac{q-1}{2}\}$, for three values of q

uniformly distributed on $\mathbf{S}^1$. A plot of the values $\sum_{x \in \mathrm{Z}_g(\mathbf{F}_q)} e(\frac{ax}{q})$ for $a \in \mathbf{F}_q$ would then be very similar to Figure 1, (A).

However, this polynomial g satisfies $\kappa(g) = 1$ (since the coefficient 1 of X^2 shows that the sum of the roots, which is an element of $\mathrm{Im}(\gamma) \cap \mathbf{Z}$, is -1) and hence these sums, parametrized by $a \in \{0, \ldots, \frac{q-1}{2}\}$, do not become equidistributed with respect to the same measure. Numerical experiments confirm this (see Figure 3), but suggest that there is equidistribution with respect to another measure.

(2) Many examples of uniformly equidistributed sets (modulo primes at least) are provided by using the theory of trace functions and the Riemann Hypothesis over finite fields. For instance, if $f \in \mathbf{Z}[\mathrm{X}]$ is a monic polynomial, then the fractional parts of elements of the sets $\mathrm{A}_p = f(\mathbf{O}_p/p) \subset \mathbf{O}_g/p$ are uniformly equidistributed. Indeed, one derives, e.g., from [12, Prop. 6.7], and the Riemann Hypothesis over finite fields that $|\mathrm{A}_p| \gg |p|$ and that

$$\frac{1}{|\mathrm{A}_p|} \sum_{\substack{a \in \mathbf{O}_g/p \\ a = f(b) \text{ for some } b}} e\Big(\frac{ha}{|p|}\Big) \ll \frac{1}{|p|^{1/2}}$$

for all $h \in (\mathbf{O}_g/p)^\times$, where the implied constant depends only on $\deg(f)$. The simplest example is that of quadratic residues.

(3) In the last estimate, since the implied constant depends only on the degree of the polynomial f, one can take f to depend on p. It is natural to ask how large $\deg(f)$ can really be taken. The simplest "test" case is when $f = \mathrm{X}^d$ is a monomial, and the question is then whether Proposition 4.1 applies to small *multiplicative subgroups* $\mathrm{A}_{p^n} \subset (\mathbf{O}_g/p^n)^\times$.

Using a striking result of Bourgain [7], and adapting an argument of Untrau [26, Prop. 1.14] (to show that if $\varpi_{p^n}(\gamma(\alpha)) \neq 0$, then its $|p|$-adic valuation is bounded as p^n varies), one can deduce easily that the first part of Proposition 4.1 does indeed apply if there exists $\delta > 0$ such that A_{p^n} is a subgroup of $(\mathbf{O}_g/p^n)^\times$ with $|\mathrm{A}_{p^n}| \gg |p|^{n\delta}$.

5. Additive characters with more general polynomials

Very simple adaptations of the proof of Proposition 2.2 (which are left to the reader) lead to the following more general statements, the second of which was also studied by Untrau in the case $g = \mathrm{X}^d - 1$.

Proposition 5.1 (Ultra-short equidistribution, 2)**.** *Let $v \in \mathbf{Z}[\mathrm{X}, \mathrm{X}^{-1}]$ be a non-constant Laurent polynomial. Assume that $0 \notin \mathrm{Z}_g$. Define random variables W_{p^n} on $\mathbf{O}_g/p^n$ for $p \in \mathcal{S}_g$ dividing none of the roots of g and $n \geqslant 1$, with values in $\mathrm{C}(\mathrm{Z}_g; \mathbf{S}^1)$, by*

$$\mathrm{W}_{p^n}(a)(x) = e\Big(\frac{av(\varpi(x))}{|p|^n}\Big).$$

The random variables W_{p^n} converge in law as $|p|^n \to +\infty$ to the random function $\mathrm{W}\colon \mathrm{Z}_g \to \mathbf{S}^1$ such that W is uniformly distributed on the subgroup orthogonal to the abelian group $\mathrm{R}_{g,v} \subset \mathrm{C}(\mathrm{Z}_g; \mathbf{Z})$ of additive relations between components of $(v(x))_{x\in\mathrm{Z}_g}$, namely

$$\mathrm{R}_{g,v} = \{\alpha\colon \mathrm{Z}_g \to \mathbf{Z} \mid \sum_{x\in\mathrm{Z}_g} \alpha(x)v(x) = 0\}.$$

Proposition 5.2 (Ultra-short equidistribution, 3)**.** *Let $k \geqslant 1$ be an integer and fix distinct integers $m_1, \ldots, m_k$ in $\mathbf{Z}$. Assume $0 \notin \mathrm{Z}_g$. For $p \in \mathcal{S}_g$ dividing none of the roots of g and $n \geqslant 1$, define random variables Y_{p^n} on the space $(\mathbf{O}_g/p^n)^k$ with uniform probability measure, with values in $\mathrm{C}(\mathrm{Z}_g; \mathbf{S}^1)$, by*

$$\mathrm{Y}_{p^n}(a_1, \ldots, a_k)(x) = e\Big(\frac{1}{|p|^n}\Big(\sum_{i=1}^{k} a_i \varpi(x)^{m_i}\Big)\Big)$$

The random variables Y_{p^n} converge in law as $|p|^n \to +\infty$ to the random function $\mathrm{Y}\colon \mathrm{Z}_g \to \mathbf{S}^1$ such that Y is uniformly distributed on the subgroup orthogonal to the abelian group

$$\{\alpha\colon \mathrm{Z}_g \to \mathbf{Z} \mid \sum_{x\in\mathrm{Z}_g} \alpha(x)x^{m_i} = 0 \text{ for } 1 \leqslant i \leqslant k\}.$$

As corollaries, we have equidistribution for the sums

$$\sum_{x\in\mathrm{Z}_g(\mathbf{F}_q)} e\Big(\frac{av(x)}{q}\Big)$$

as a varies in $\mathbf{F}_q$ for q totally split in K_g and

$$\sum_{x\in\mathrm{Z}_g(\mathbf{F}_q)} e\Big(\frac{a_1x^{m_1} + \cdots + a_kx^{m_k}}{q}\Big),$$

as $a_1, \ldots, a_k$ vary independently and uniformly in $\mathbf{F}_q$ for q totally split in K_g.

Example 5.3. Consider the case of $g = \mathrm{X}^d - 1$ and the sums

$$\sum_{x\in\boldsymbol{\mu}_d(\mathbf{F}_q)} e\Big(\frac{a(x+\bar{x})}{q}\Big) \tag{4}$$

and

$$(5) \qquad \sum_{x\in\boldsymbol{\mu}_d(\mathbf{F}_q)} e\Big(\frac{ax+b\bar{x}}{q}\Big),$$

as a and b vary in $\mathbf{F}_q$ for q totally split in K_g. Both satisfy equidistribution, but in general have different limiting measures. For (4), we need to determine the functions α satisfying the relation

$$\sum_{x\in\boldsymbol{\mu}_d} \alpha(x)(x+x^{-1}) = 0,$$

and for (5), we need to solve

$$\sum_{x\in\boldsymbol{\mu}_d} \alpha(x)x = \sum_{x\in\boldsymbol{\mu}_d} \alpha(x)x^{-1} = 0.$$

This last case boils down to the same relations as in Section 3, Example 1, since the second sum above is the complex-conjugate of the first.

For (4), on the other hand, the relation is equivalent to

$$\sum_{x\in\boldsymbol{\mu}_d} (\alpha(x)+\alpha(x^{-1}))x = 0,$$

which means that $\beta\colon x\mapsto \alpha(x)+\alpha(x^{-1})$ belongs to the group of additive relations of X^d-1.

We now assume that $d=\ell$ is an odd prime number. Then, by the previous examples, the map β must be constant. Let then ξ be a non-trivial ℓ-th root of unity. It is then fairly easy to check that the module $\mathrm{R}_{\mathrm{X}^\ell-1,\mathrm{X}+\mathrm{X}^{-1}}$ is generated by the constant function $\alpha_0=1$ and the functions α_j for $1\leqslant j\leqslant (\ell-1)/2$ such that

$$\alpha_j(\xi^k) = \begin{cases} 0 & \text{if } k\notin\{j,\ell-j\} \\ 1 & \text{if } k=j \\ -1 & \text{if } k=\ell-j. \end{cases}$$

(It is clear that α_0, …, $\alpha_{(\ell-1)/2}$ provide relations; conversely, if β is constant then we check that

$$\alpha = \alpha(1)\alpha_0 + \sum_{j=1}^{(\ell-1)/2} (\alpha(\xi^j)-\alpha(1))\alpha_j,$$

so that these functions generate the group of relations.)

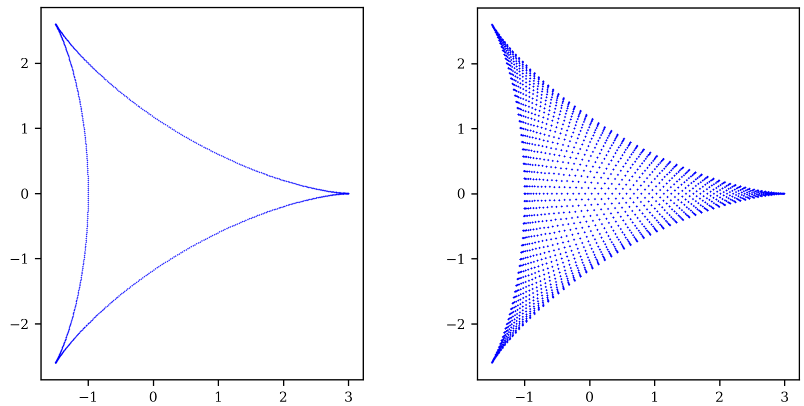
In particular, the module of relations has rank $(\ell+1)/2$, and the limit W, in this case, is uniform on the subgroup $\mathrm{H}_{\mathrm{X}^\ell-1,\mathrm{X}+\mathrm{X}^{-1}}$ characterized by $f\in \mathrm{H}_{\mathrm{X}^\ell-1,\mathrm{X}+\mathrm{X}^{-1}}$ if and only if

$$\prod_{j=0}^{\ell-1} f(\xi^j) = 1,$$

(corresponding to α_0) and

$$f(\xi^j) = f(\xi^{\ell-j})$$

for $1\leqslant j\leqslant (\ell-1)/2$ (corresponding to α_j).



(A) The sums of type (4) for $d = 3$, $q = 811$, and a varying in $\mathbf{F}_q$.

(B) The sums of type (5) for $d = 3$, $q = 109$, and a and b varying in $\mathbf{F}_q$.

FIGURE 4. Comparison between the regions of equidistribution for sums of type (4) and sums of type (5).

Consider for instance the case $\ell = 3$. The sums (5) will become equidistributed with respect to the measure on $\mathbf{C}$ which is the pushforward measure of the uniform measure on $\mathbf{S}^1 \times \mathbf{S}^1$ by $(y_1, y_2) \mapsto y_1 + y_2 + 1/(y_1 y_2)$. This is illustrated in Figure 4 (B), since the image of the above map is the closed region delimited by a 3-cusp hypocycloid.

On the other hand, the sums (4) become equidistributed in this case with respect to the image of the Haar measure on $\mathbf{S}^1$ by the map $y \mapsto 2y + 1/y^2$. Since the image of this map is precisely the 3-cusp hypocycloid, this explains the picture obtained in Figure 4 (A).

In the case $\ell = 5$, the sums (5) are equidistributed with respect to the measure on $\mathbf{C}$ which is the pushforward measure of the uniform measure on $(\mathbf{S}^1)^4$ by $(y_1, \ldots, y_4) \mapsto y_1 + \cdots + y_4 + 1/(y_1 \cdots y_4)$. The sums (4) are equidistributed in this case with respect to the image of the Haar measure on $(\mathbf{S}^1)^2$ by the map $(y_1, y_2) \mapsto 2y_1 + 2y_2 + 1/(y_1 y_2)^2$.

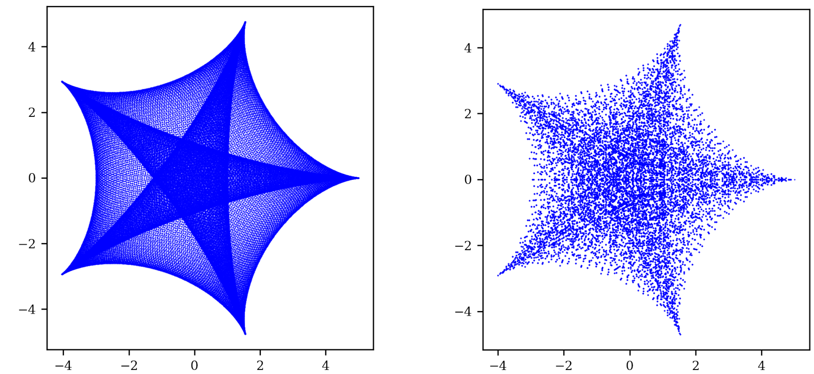
6. A multiplicative analogue

In [20], the group of multiplicative relations between roots of a polynomial also appears naturally. Is it also relevant for the type of questions under consideration here? It turns out that it is, if we change the probability space, and look at the distribution of sums

$$\sum_{x \in \mathrm{Z}_g} \chi(v(x))$$

where χ is a varying multiplicative character of $\mathbf{F}_q$ and v is a fixed polynomial.

More precisely, we continue with the notation from the previous section, but assume moreover that $v(x) \neq 0$ for $x \in \mathrm{Z}_g$ (for instance, $0 \notin \mathrm{Z}_g$ if $v = \mathrm{X}$). For $p \in \mathcal{S}_g$, we now consider the probability space X_p of multiplicative characters $\chi\colon (\mathbf{O}_g/p)^\times \to \mathbf{S}^1$, with the uniform probability measure (we consider only primes instead of prime powers for simplicity here). The random variables are now $\widetilde{\mathrm{U}}_p$, taking values in the group $\mathrm{C}(\mathrm{Z}_g; \mathbf{S}^1)$, and defined



(A) The sums of type (4) for $d = 5$, $q = 96331$, and a varying in $\mathbf{F}_q$.

(B) The sums of type (5) for $d = 5$, $q = 311$, and a and b varying in $\mathbf{F}_q$.

FIGURE 5. Comparison between the equidistribution results for sums of type (4) and sums of type (5) for $d = 5$.

by

$$\widetilde{\mathrm{U}}_p(\chi)(x) = \chi(v(\varpi(x))).$$

Proposition 6.1. *The random variables $\widetilde{\mathrm{U}}_p$ converge in law as $|p| \to +\infty$ to the random function $\widetilde{\mathrm{U}} \colon \mathrm{Z}_g \to \mathbf{S}^1$ such that $\widetilde{\mathrm{U}}$ is uniformly distributed on the subgroup $\widetilde{\mathrm{H}}_{g,v} \subset \mathrm{C}(\mathrm{Z}_g; \mathbf{S}^1)$ which is orthogonal to the abelian group $\widetilde{\mathrm{R}}_{g,v} \subset \mathrm{C}(\mathrm{Z}_g; \mathbf{Z})$ of multiplicative relations between values of v on Z_g, namely we have*

$$\widetilde{\mathrm{R}}_{g,v} = \{\alpha \colon \mathrm{Z}_g \to \mathbf{Z} \mid \prod_{x \in \mathrm{Z}_g} v(x)^{\alpha(x)} = 1\},$$

and

$$\widetilde{\mathrm{H}}_{g,v} = \{f \in \mathrm{C}(\mathrm{Z}_g; \mathbf{S}^1) \mid \text{ for all } \alpha \in \widetilde{\mathrm{R}}_{g,v}, \text{ we have } \prod_{x \in \mathrm{Z}_g} f(x)^{\alpha(x)} = 1\}.$$

In particular, as $q \to +\infty$ among primes totally split in K_g, the sums

$$\sum_{x \in \mathrm{Z}_g} \chi(v(x))$$

converge in law to the image by the linear form σ of the Haar probability measure on $\widetilde{\mathrm{H}}_{g,v}$.

Proof. This is the same as Proposition 2.2, mutatis mutandis, with now

$$\mathbf{E}(\eta(\widetilde{\mathrm{U}}_p)) = \frac{1}{|p| - 1} \sum_{\chi \in \mathrm{X}_p} \prod_{x \in \mathrm{Z}_g} \chi(v(\varpi(x)))^{\alpha(x)}$$

for a character η of $\mathrm{C}(\mathrm{Z}_g; \mathbf{S}^1)$ determined by the function α. This is

$$\mathbf{E}(\eta(\widetilde{\mathrm{U}}_p)) = \frac{1}{|p| - 1} \sum_{\chi \in \mathrm{X}_p} \chi\Big(\varpi\Big(\prod_{x \in \mathrm{Z}_g} v(x)^{\alpha(x)}\Big)\Big)$$

and for the same reasons as before, converges to 1 or 0, depending on whether

$$\prod_{x\in \mathrm{Z}_g} v(x)^{\alpha(x)}$$

is equal to 1 or not. □

Example 6.2. (1) Here also there are some interesting examples in [20] and [21] if we take $v = \mathrm{X}$ (so that $\widetilde{\mathrm{R}}_{g,v}$ corresponds to multiplicative relations between roots of g). In particular, we could take a polynomial g with Galois group the Weyl group of $\mathbf{E}_8$, which is of degree 248 but has all roots obtained multiplicatively from 8 of them (see [19] for examples).

(2) For $v = \mathrm{X}$ again, the case of $g = \mathrm{X}^d - 1$ is quite degenerate. Indeed, for $q \equiv 1 \pmod d$ and a multiplicative character χ of $\mathbf{F}_q$, the sum

$$\sum_{x\in \boldsymbol{\mu}_d(\mathbf{F}_q)} \chi(x)$$

is either d or 0, depending on whether the character χ is trivial on the d-th roots of unity or not. The former means that $\chi^{(|p|-1)/d} = 1$, and there are therefore $(|p|-1)/d$ such characters. Hence the sum is equal to d with probability $1/d$, and to 0 with probability $1 - 1/d$.

(3) If we consider the class polynomial for CM curves (as in Section 3, Example 4), we are led to consider potential multiplicative relations between j-invariants. This is apparently more challenging than the additive case, and we do not have a precise answer at the moment (see, e.g., the papers of Bilu, Luca and Pizarro-Madariaga [4] and Fowler [16] for partial results).

7. Higher rank trace functions

We now elaborate on the setting of Section 2 to involve more general trace functions. Thus the goal is to study the distribution of

$$\sum_{x\in \mathrm{Z}_g(\mathbf{O}_g/p)} t_p(ax), \qquad \text{or} \qquad \sum_{x\in \mathrm{Z}_g(\mathbf{O}_g/p)} t_p(a+x),$$

(or other similar expressions) when t_p is, for each $p \in \mathcal{S}_g$, a trace function over the finite field $\mathbf{O}_g/p$. The cases of Section 2 correspond to $t_p(x) = e(x/|p|)$ or $t_p(x) = e(v(x)/|p|)$, i.e., to the trace functions of Artin–Schreier sheaves.

We thus assume that for each $p \in \mathcal{S}_g$, we are given a middle-extension sheaf $\mathcal{F}_p$ on the affine line over $\mathbf{O}_g/p$. We assume that these sheaves are pure of weight 0, and have the same rank r, and moreover have bounded conductor in the sense of Fouvry, Kowalski and Michel [11, 13].

We denote by $\mathrm{U}_r(\mathbf{C})^\sharp$ the space of conjugacy classes in the unitary group $\mathrm{U}_r(\mathbf{C})$. For any $x \in \mathbf{O}_g/p$ such that $\mathcal{F}_p$ is lisse at x, the action of the geometric Frobenius automorphism at x on the stalk of $\mathcal{F}_p$ at x gives a unique conjugacy class $\Theta_p(x) \in \mathrm{U}_r(\mathbf{C})^\sharp$. We denote

$$\mathrm{A}_p = \{a \in (\mathbf{O}_g/p)^\times \mid \text{ for all } x \in \mathrm{Z}_g(\mathbf{O}_g/p),\ \mathcal{F}_p \text{ is lisse at } ax\},$$
$$\mathrm{B}_p = \{a \in \mathbf{O}_g/p \mid \text{ for all } x \in \mathrm{Z}_g(\mathbf{O}_g/p),\ \mathcal{F}_p \text{ is lisse at } a+x\}.$$

Note that $|\mathrm{A}_p| \gg |p|$ if $0 \notin \mathrm{Z}_g$ and $|\mathrm{B}_p| \gg |p|$ in all cases.

We can define random functions U_p and V_p on A_p and B_p, respectively (with the uniform probability measure), with values in the space $\mathrm{C}(\mathrm{Z}_g; \mathrm{U}_r(\mathbf{C})^\sharp)$ by

$$\mathrm{U}_p(a)(x) = \Theta_p(ax), \qquad \mathrm{V}_p(a)(x) = \Theta_p(a+x).$$

Since the trace function t_p of $\mathcal{F}_p$ satisfies

$$t_p(x) = \mathrm{tr}(\Theta_p(x))$$

when $\mathcal{F}_p$ is lisse at x, we see that if one can prove that (U_p) or (V_p) have a limit, then the corresponding sums

$$(6) \qquad \sum_{x \in \mathrm{Z}_g(\mathbf{O}_g/p)} t_p(ax), \qquad \text{and/or} \qquad \sum_{x \in \mathrm{Z}_g(\mathbf{O}_g/p)} t_p(a+x),$$

for $a \in \mathrm{A}_p$ (resp. B_p) will become equidistributed according to the image of this limit distribution by the map

$$f \mapsto \sum_{x \in \mathrm{Z}_g} \mathrm{tr}(f(x))$$

for $f \colon \mathrm{Z}_g \to \mathrm{U}_r(\mathbf{C})^\sharp$.

Remark 7.1. It happens frequently that $t_p(y) \ll p^{-1/2}$ if $\mathcal{F}_p$ is not lisse at y, where the implied constant depends only on the conductor of $\mathcal{F}_p$. In such a case, the equidistribution for the sums (6) holds when a is taken in all of $(\mathbf{O}_g/p)^\times$ or $\mathbf{O}_g/p$, since the remaining value of a have negligible contributions.

We obtain a large supply of examples from known results on estimates of "sums of products" of trace functions (see [13]). Although the terminology might not be familiar to all readers, examples after the proof will provide concrete illustrations.

Proposition 7.2. *Assume that $\mathcal{F}_p$ is bountiful in the sense of* [13] *for all p in $\mathcal{S}_g$.*

(1) *If $\mathcal{F}_p$ is of Sp_r-type for all p, then (U_p) and (V_p) converge in law as $|p| \to +\infty$, with limit uniform on $\mathrm{C}(\mathrm{Z}_g; \mathrm{USp}_r(\mathbf{C})^\sharp)$.*

(2) *If $\mathcal{F}_p$ is of SL_r-type for all p, and the special involution, if it exists, is not $y \mapsto -y$, then (U_p) and (V_p) converge in law as $|p| \to +\infty$, with limit uniform on $\mathrm{C}(\mathrm{Z}_g; \mathrm{SU}_r(\mathbf{C})^\sharp)$.*

(3) *If $\mathcal{F}_p$ is of SL_r-type for all p with special involution $y \mapsto -y$, then (V_p) converge in law as $|p| \to +\infty$ with limit uniform on $\mathrm{C}(\mathrm{Z}_g; \mathrm{SU}_r(\mathbf{C})^\sharp)$, and (U_p) converges in law with limit uniform on*

$$\{f \colon \mathrm{Z}_g \to \mathrm{SU}_r(\mathbf{C}) \mid f(x) = \overline{f(y)} \text{ if } x = -y\}.$$

In all three cases, we assume that $0 \notin \mathrm{Z}_g$ in the case of (U_p).

Proof. We argue with U_p, as the case of V_p is very similar. By definition, the random variables U_p take values in $\mathrm{C}(\mathrm{Z}_g; \mathrm{USp}_r(\mathbf{C})^\sharp)$. Applying the Weyl Criterion, it suffices to show that if $(\pi_x)_{x\in \mathrm{Z}_g}$ is a family of irreducible representations of $\mathrm{USp}_r(\mathbf{C})$, not all trivial, with characters $\chi_x = \mathrm{tr}(\pi_x)$, we have

$$\lim_{|p|\to+\infty} \frac{1}{|\mathrm{A}_p|}\sum_{a\in\mathrm{A}_p}\prod_{x\in\mathrm{Z}_g(\mathbf{O}_g/p)} \chi_x(\Theta_p(ax)) = 0.$$

The sum is, up to negligible amount coming from points where $\mathcal{F}_p$ is not lisse, the sum of the traces of Frobenius on the sheaf

$$\mathcal{G} = \bigotimes_{x\in\mathrm{Z}_g(\mathbf{O}_g/p)} \pi_x([a\mapsto ax]^*\mathcal{F}_p),$$

and by the Riemann Hypothesis over finite fields of Deligne, we obtain

$$\frac{1}{|p|}\sum_{a\in\mathbf{O}_g/p}\prod_{x\in\mathrm{Z}_g(\mathbf{O}_g/p)} \chi_x(\Theta_p(ax)) \ll |p|^{-1/2}$$

as soon as the geometric monodromy group of this sheaf has no trivial subrepresentation in its standard representation. This is true because the bountiful property of $\mathcal{F}_p$ ensures that the geometric monodromy group of $\mathcal{G}$ is the product group $\prod_x \mathrm{Sp}_r$.

The argument is similar for (2); for (3), we have to take into account the fact that the assumption implies that $[a\mapsto -a]^*\mathcal{F}_p$ is isomorphic to the dual of $\mathcal{F}_p$, so that $\mathrm{tr}(\Theta_p(-ax)) = \overline{\mathrm{tr}(\Theta_p(ax))}$ for all $x\in\mathrm{Z}_g$. ∎

Example 7.3. We illustrate here all three cases with examples.

(1) The classical Kloosterman sums Kl_2 (as in part (2) of Theorem 1.1) are trace functions of a bountiful sheaf of rank $r=2$ of Sp_2-type which is lisse except at 0 and ∞. Thus the first case of the proposition applies (with A_p being the whole multiplicative group $(\mathbf{O}_g/p)^\times$) and in particular this establishes the second part of Theorem 1.1, in view of the fact that the trace of a uniform random matrix in $\mathrm{SU}_2(\mathbf{C})$ is Sato–Tate distributed.

Similarly, for even-rank hyper-Kloosterman sums (for which $\mathcal{F}_p$ is also lisse except at 0 and ∞), we obtain the USp_r case (see [13, § 3.2]).

(2) If r is odd, then the hyper-Kloosterman sum $\mathrm{Kl}_r(a;p)$ arise as trace functions of a bountiful sheaf of SL_r-type with special involution $y\mapsto -y$ (see [13, § 3.3]), which is lisse except at 0 and ∞. So the third case of the proposition applies here. In particular, if the polynomial g is even or odd (so that $\mathrm{Z}_g = -\mathrm{Z}_g$), the support of the limit of U_p is only "half-dimensional".

(3) Examples of trace functions coming from bountiful sheaves of SL_r-type without special involution are given for instance by

$$t_p(x) = \frac{1}{\sqrt{|p|}}\sum_{y\in\mathbf{O}_g/p}\chi(h(y))e\Big(\frac{xy}{|p|}\Big)$$

where $h\in\mathbf{Z}[\mathrm{X}]$ is a "generic" squarefree polynomial of degree $\geqslant 2$. This follows from [13, Prop. 3.7], where the meaning of "generic" is also explained; here also, the sheaf $\mathcal{F}_p$ is lisse except at 0 and ∞.

References

[1] B. Allombert, Y. Bilu, A. Pizarro-Madariaga: CM *points on straight lines*, Analytic number theory, 1–18, Springer, Cham (2015).

[2] C. Berry, A. Dubickas, N.D. Elkies, B. Poonen and C. Smyth: *The conjugate dimension of algebraic numbers*, Quart. J. Math. 55 (2004), 237–252.

[3] Y. Bilu, P. Habegger and L. Kühne: *No singular modulus is a unit*, International Mathematics Research Notices, Volume 2020, Issue 24, 10005–10041.

[4] Y. Bilu, F. Luca and A. Pizarro-Madariaga: *Rational products of singular moduli*, Journal of Number Theory 158 (2016), 397–410.

[5] Y. Bilu, D. Masser, U. Zannier: *An effective "theorem of André" for* CM*-points on a plane curve*, Math. Proc. Cambridge Philos. Soc. 154 (2013),145–152.

[6] N. Bourbaki: *Théories spectrales, Chapitre II*, Springer 2019.

[7] J. Bourgain: *Exponential sum estimates over subgroups of* $\mathbb{Z}_q^*$*, q arbitrary*, Journal d'Analyse Mathématique Vol. 97 (2005), 317–355.

[8] D. Cox: *Primes of the form* $x^2 + ny^2$, Wiley 1989.

[9] W. Duke, J. Friedlander et H. Iwaniec : *Equidistribution of roots of a quadratic congruence to prime moduli*, Ann. of Math. 141 (1995), 423–441.

[10] W. Duke, S.R. Garcia and B. Lutz: *The graphic nature of Gaussian periods*, Proc. Amer. Math. Soc. 143 (2015), 1849–1863.

[11] É. Fouvry, E. Kowalski and Ph. Michel: *Algebraic twists of modular forms and Hecke orbits*, Geom. Funct. Anal. 25 (2015), 580–657.

[12] É. Fouvry, E. Kowalski and Ph. Michel: *Algebraic trace functions over the primes*, Duke Math. Journal 163 (2014), 1683–1736.

[13] É. Fouvry, E. Kowalski and Ph. Michel: *A study in sums of products*, Phil. Trans. R. Soc. A 373:20140309.

[14] É. Fouvry, S. Ganguly, E. Kowalski and Ph. Michel: *Gaussian distribution for the divisor function and Hecke eigenvalues in arithmetic progressions*, Commentarii Math. Helv. 89 (2014), 979–1014.

[15] É. Fouvry, E. Kowalski, Ph. Michel, C. Raju, J. Rivat, and K. Soundararajan: *On short sums of trace functions*, Annales de l'Institut Fourier 67 (2017), 423–449.

[16] G. Fowler: *Triples of singular moduli with rational product*, Int. J. Number Theory 16 (2020), 2149–2166.

[17] S.R. Garcia, T. Hyde and B. Lutz: *Gauss's hidden menagerie: from cyclotomy to supercharacters*, Notices AMS 62 (2015), 878–888.

[18] E. Hrushovski: *Ax's theorem with an additive character*, EMS Surv. Math. Sci. 8 (2021), 179–216.

[19] F. Jouve, E. Kowalski and D. Zywina: *An explicit integral polynomial whose splitting field has Galois group* $\mathrm{W}(\mathrm{E}_8)$, Journal de Théorie des Nombres de Bordeaux 20 (2008), 761–782.

[20] E. Kowalski: *The large sieve, monodromy, and zeta functions of algebraic curves, II: independence of the zeros*, International Math. Res. Notices 2008, doi:10.1093/imrn/rnn091.

[21] E. Kowalski: *An introduction to the representation theory of groups*, Grad. Texts in Math. 155, A.M.S (2014).

[22] E. Kowalski and W. Sawin: *Kloosterman paths and the shape of exponential sums*, Compositio Math. 152 (2016), 1489–1516.

[23] C. Perret-Gentil: *Gaussian distribution of short sums of trace functions over finite fields*, Mathematical Proc. Cambridge Phil. Soc. 163 (2017), 385–422.

[24] C.J. Smyth: *Additive and multiplicative relations connecting conjugate algebraic numbers*, J. Number Theory 23 (1986), 243–254.

[25] A. Tóth: *Roots of quadratic congruences*, Internat. Math. Res. Notices 2000, 719–739.

[26] T. Untrau: *Equidistribution of exponential sums indexed by a subgroup of fixed cardinality*, Math. Proc. Cambridge Phil. Soc., to appear.

ETH Zürich – D-MATH, Rämistrasse 101, 8092 Zürich, Switzerland
Email address: kowalski@math.ethz.ch

Université de Bordeaux, CNRS, Bordeaux INP, IMB, UMR 5251, F-33400, Talence, France
Email address: theo.untrau@math.u-bordeaux.fr