On the Distribution of Rational Functions Along a Curve over $\mathbb{F}_p$ and Residue Races

Andrew Granville
Départment de Mathématiques et Statistique, Université de Montréal
CP 6128 succ Centre-Ville, Montréal, QC H3C 3J7, Canada
andrew@dms.umontreal.ca

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

Alexandru Zaharescu
Department of Mathematics, University of Illinois at Urbana-Champaign
Altgeld Hall, 1409 W. Green Street, Urbana, IL, 61801, USA
zaharesc@math.uiuc.edu

Abstract

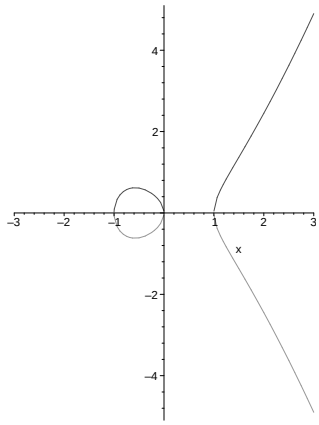
Let p be a prime number, let $\overline{\mathbb{F}}_p$ be the algebraic closure of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, let $\mathcal{C}$ be an absolutely irreducible curve in $\mathbb{A}^r(\overline{\mathbb{F}}_p)$ and $\mathbf{h} = (h_1, \cdots, h_s)$ a rational map defined on the curve $\mathcal{C}$. We investigate the distribution in the s-dimensional unit cube $(\mathbb{R}/\mathbb{Z})^s$ of the images through $\mathbf{h}$ of the $\mathbb{F}_p$-points of $\mathcal{C}$, after a suitable embedding.

Mathematics Subject Classification 2002: 11T99.

Key words and phrases: affine curves, distribution on the torus, discrepancy

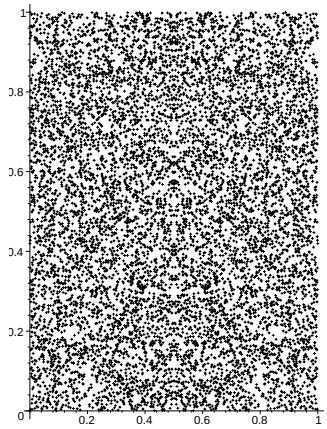
1 Introduction

An arithmetic geometer lecturing on elliptic curves might draw an example like the real locus of $y^2 = x^3 - x$:



The real locus of $y^2 = x^3 - x$

To understand the elliptic curve (for instance in defining its L-function) one often must study it $\pmod p$ for all primes p; and our arithmetic geometer has been known to discuss this "reduction" $\pmod p$ by using the same picture. Although this may be illustrative of geometric concepts, it doesn't seem to reflect the true picture of the curve $\pmod p$. For example, taking $p = 957$ one has the following:



Points $(x/p, y/p)$ *where* $y^2 \equiv x^3 - x \pmod p$ *with* $0 \le x, y < p$

It does not seem as if the points on the curve $\pmod p$ conform to some geometric curve, but rather they seem to be uniformly distributed across the square (and indeed one gets a similar impression looking at the picture for other primes p). In other words, if Ω is a subset of the unit square, it seems as if $\#\{0 \le x, y \le p-1 : \ y^2 \equiv x^3 - x \pmod p \text{ and } (x/p, y/p) \in \Omega\}$ is roughly $\mathrm{Vol}(\Omega)p$. Our goal in this paper is to show that this is so in some generality.

One objection to what we have just suggested is that we have chosen a particular embedding of the points mod p onto the unit square, and it may be that a different embedding will not show such an unclear picture (that is, that the points may then appear to lie along a geometric curve). Thus we will allow *any* embedding given by a rational map, and determine whether the embedded points are then necessarily uniformly distributed.

Sometimes one does get a clear picture: indeed, certain rational maps will embed the points of our curve into a geometrically identifiable object in our range. For example the map $(x, y) \to ((x + y^2)/p, x^3/p + 1/2) \pmod 1$ for integers (x, y) satisfying $y^2 \equiv x^3 - x \pmod p$ maps the points on our curve into the line $v = u + 1/2 \pmod 1$ in our range, and this is easily recognized in $[0, 1)^2$ (or, more precisely, in the two dimensional torus $(\mathbb{R}/\mathbb{Z})^2$). It is not hard to cook up further examples where points on a curve are injected into a translate of a linear subspace of the range (that is, a surface), so that the points could not be uniformly distributed in the unit cube, as we suggested in the previous paragraph. However if one considers the curve to be embedded inside the smallest such surface then one can ask whether the points are uniformly distributed therein, and this is what we prove to be true, as the main result in this paper.

2 Uniform Distribution in the Whole Space

Let p be a prime number, and let $\overline{\mathbb{F}}_p$ be the algebraic closure of $\mathbb{F}_p$. We identify $\mathbb{F}_p$ with the set $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$ and so, given $x \in \mathbb{F}_p$, we can consider the rational number $t(x) = x/p \in \mathbb{T} := \mathbb{R}/\mathbb{Z} = [0, 1)$; thus we associate $\mathbb{F}_p$ with $p\mathbb{T} \cap \mathbb{Z}$. In this way $\mathbb{F}_p^s$ injects into the s-dimensional unit cube $\mathbb{T}^s = [0, 1]^s$, with a point $\mathbf{x} = (x_1, \ldots, x_s) \in \mathbb{F}_p^s$ being sent to $t(\mathbf{x}) = (x_1/p, \ldots, x_s/p) \in \mathbb{T}^s$.

We recall that a curve $\mathcal{C}$, defined over $\mathbb{F}_p$, is called *absolutely irreducible* if it remains irreducible over the algebraic closure $\overline{\mathbb{F}}_p$.

Let $\mathcal{C}$ be an absolutely irreducible curve of degree d, defined over $\mathbb{F}_p$, embedded in affine space $\mathbb{A}^r(\overline{\mathbb{F}}_p)$. We shall call $\mathbf{h} = (h_1, \ldots, h_s)$ a *suitable* rational map $\mathcal{C} \to \mathbb{A}^s(\overline{\mathbb{F}}_p)$, with $h_j = f_j/g_j$, where $f_j, g_j \in \mathbb{F}_p[X_1, \ldots, X_r]$ if $\mathcal{C}$ is not contained in the hypersurface $g_j = 0$, for $1 \le j \le s$. Define the degree, D, of $\mathbf{h}$ to be the maximum of $\max\{\deg f_j, \deg g_j\}$ for $1 \le j \le s$. By the above identification, the set $\mathcal{C}(\mathbb{F}_p)$ of $\mathbb{F}_p-$points on $\mathcal{C}$ becomes a subset of $\mathbb{T}^r$, while its image $t(\mathbf{h}(\mathcal{C}(\mathbb{F}_p)))$ will be a subset of $\mathbb{T}^s$.

Given a domain $\Omega \subseteq \mathbb{T}^s$ let $\mu_{\mathcal{C},\mathbf{h}}(\Omega)$ be the proportion of points $\mathbf{x} \in \mathcal{C}(\mathbb{F}_p)$ for which $t(\mathbf{h}(\mathbf{x})) \in \Omega$, that is,

$$\mu_{\mathcal{C},\mathbf{h}}(\Omega) = \frac{\#\{\mathbf{x} \in \mathcal{C}(\mathbb{F}_p) \mid t(\mathbf{h}(\mathbf{x})) \in \Omega\}}{\#\mathcal{C}(\mathbb{F}_p)}. \tag{1}$$

We shall say that $1, h_1, \ldots, h_s$ are *linearly independent along* $\mathcal{C}$, if $\mathcal{C}$ is not contained in any hyper-surface of the form

$$c_0 + c_1 h_1(X) + \cdots + c_s h_s(X) = 0 \tag{2}$$

with $c_0, c_1, \ldots, c_s \in \mathbb{F}_p$ not all zero. In other words, $c_1 = \ldots = c_s = 0$ whenever $c_1 h_1(X) + \cdots + c_s h_s(X)$ is constant along the curve $\mathcal{C}$. We say that $\mathbf{h}$ is *L-free along* $\mathcal{C}$ if $\mathcal{C}$ is not contained in any hyper-surface (2) with $c_1, \ldots, c_s \in [-L, L]$, and not all zero. In particular $1, h_1, \ldots, h_s$ are linearly independent along $\mathcal{C}$ *exactly* when $\mathbf{h}$ is $(p-1)/2$-free along $\mathcal{C}$.

We begin by improving and generalizing results from [1, 3, 13, 16, 17] which focus on the $\mu_{\mathcal{C},\mathbf{h}}(\Omega)$ without consideration of relations like (2) (which we take into account in the next section).

Theorem 1. *Let $r \ge 2$ and $s, d, D \ge 1$ be integers. For any domain $\Omega \subseteq \mathbb{T}^s$ with piecewise smooth boundary, any absolutely irreducible curve $\mathcal{C}$ of degree d in $\mathbb{A}^r(\overline{\mathbb{F}}_p)$ defined over $\mathbb{F}_p$ and any suitable rational map $\mathbf{h} : \mathcal{C} \to \mathbb{A}^s(\overline{\mathbb{F}}_p)$ of degree D which is L-free along $\mathcal{C}$, one has*

$$\mu_{\mathcal{C},\mathbf{h}}(\Omega) = \mu(\Omega) + O_{r,s,d,D,\Omega}\left(L^{-1/s} + p^{-1/2s} \log L\right),$$

where μ denotes the normalized Haar measure on $\mathbb{T}^r$.

For $L \ge p^{1/2}$ the error term is $O(p^{-1/2s} \log p)$, which improves and extends the result of [13] (obtained under the condition corresponding to $L = (p-1)/2$).

In effect Theorem 1 says that if the image of $\mathcal{C}(\mathbb{F}_p)$ through $(h_1, \ldots, h_s)$ is not contained inside a surface of the form (2), then it is uniformly distributed

(indeed, the discrepancy of this set is very small). Evidently if the image is contained inside a surface of the form (2), then it cannot be uniformly distributed. However in the next section we will show that this image does satisfy a different, but just as natural (when explained), distribution law.

3 Uniform Distribution in a Translate of a Proper Subspace

In this section we investigate the case when the curve $\mathcal{C}$ and the map $\mathbf{h}$ are such that there exist integer numbers $c_0, c_1, \ldots, c_s \in \{\frac{1-p}{2}, \ldots, \frac{p-1}{2}\}$ not all zero for which (2) holds. So in this case $1, h_1, \ldots, h_s$ are no longer linearly independent along the curve $\mathcal{C}$. We first discuss some terminology. We look at the components $h_1, \ldots, h_s$ of $\mathbf{h}$ and select a maximal subset of them which, together with the constant function $h_0(\mathbf{x}) = 1$, form a set which is linearly independent along the curve $\mathcal{C}$. We may assume without any loss of generality that $\{h_1, \ldots, h_{s_0}\}$ is such a subset. Thus in what follows we assume that $1, h_1, \ldots, h_{s_0}$ are linearly independent along $\mathcal{C}$, and for any $s_0 < i \leq s$, h_i can be written as a linear combination of $1, h_1, \ldots, h_{s_0}$ along the curve $\mathcal{C}$. In other words, there are (uniquely defined) integers $c_{ij} \in \{\frac{1-p}{2}, \ldots, \frac{p-1}{2}\}$, $s_0 + 1 \leq i \leq s$, $0 \leq j \leq s_0$, such that $\mathcal{C}$ lies inside each of the hyper-surfaces defined modulo p by

$$h_i(\mathbf{x}) = \sum_{0 \leq j \leq s_0} c_{ij} h_j(\mathbf{x}).$$

Then for $x \in \mathcal{C}(\mathbb{F}_p)$ the vector $\mathbf{h}(x) = (h_1(x), \ldots, h_s(x)) \in \mathbb{F}_p^s$ lies inside the subset W of $\mathbb{F}_p^s$ given by

$$W = \{(y_1, \ldots, y_s) \in \mathbb{F}_p^s : y_i = c_{i0} + \sum_{1 \leq j \leq s_0} c_{ij} y_j, s_0 + 1 \leq i \leq s\}.$$

Thus W is a translate of a proper vector subspace of $\mathbb{F}_p^s$, and it is the smallest translate of a proper vector subspace of $\mathbb{F}_p^s$ which contains $\mathbf{h}(\mathcal{C}(\mathbb{F}_p))$.

One would naturally like to have a geometric image of this situation, so we are interested to see how $t(W)$, which contains the set $t(\mathbf{h}(\mathcal{C}(\mathbb{F}_p)))$ whose distribution we are investigating, sits inside the torus $(\mathbb{R}/\mathbb{Z})^s$. Now $(\mathbb{R}/\mathbb{Z})^s$ is not a vector space, but it is a $\mathbb{Z}-$module. So it makes sense to consider

the subset, call it $E_{\mathcal{C},\mathbf{h}}$, of $(\mathbb{R}/\mathbb{Z})^s$, defined by

$$E_{\mathcal{C},\mathbf{h}} = \{(z_1, \ldots, z_s) \in (\mathbb{R}/\mathbb{Z})^s : z_i = \frac{c_{i0}}{p} + \sum_{1 \le j \le s_0} c_{ij} z_j, s_0 + 1 \le i \le s\}.$$

Note that $E_{\mathcal{C},\mathbf{h}}$ is nonempty, since from the definition of the map t it follows that for any $(y_1, \ldots, y_s) \in W$ one has $(t(y_1), \ldots, t(y_s)) \in E_{\mathcal{C},\mathbf{h}}$. Therefore

$$t(\mathbf{h}(\mathcal{C}(\mathbb{F}_p))) \subseteq t(W) \subseteq E_{\mathcal{C},\mathbf{h}}. \tag{3}$$

Sometimes, referring to (3), we say that $t(\mathbf{h}(\mathcal{C}))$ is embedded inside a translate of a proper subspace of $(\mathbb{R}/\mathbb{Z})^s$, although, strictly speaking, $E_{\mathcal{C},\mathbf{h}}$ is a translate of a $\mathbb{Z}-$submodule of $(\mathbb{R}/\mathbb{Z})^s$. More generally, by a translate of a proper subspace of $(\mathbb{R}/\mathbb{Z})^s$ we mean a set of the form

$$\{(z_1, \ldots, z_s) \in (\mathbb{R}/\mathbb{Z})^s : \sum_{1 \le j \le s} c_{ij} z_j = \beta_i, 1 \le i \le l\},$$

where $c_{ij} \in \mathbb{Z}$ and $\beta_i \in (\mathbb{R}/\mathbb{Z})$ for $1 \le i \le l$, $1 \le j \le s$. We now fix some notation and proceed to describe our results. The set of hyper-surfaces of the form (2) which contain $\mathcal{C}$ form a vector space over $\mathbb{F}_p$, which we will denote $V^\perp$; that is

$$V^\perp := \{\mathbf{u} \in \mathbb{F}_p^s : \mathbf{u} \cdot \mathbf{h}(\mathbf{x}) \text{ is constant for } \mathbf{x} \in \mathcal{C}\}.$$

For each $\mathbf{u} \in V^\perp$ we define $\lambda(\mathbf{u}) := \mathbf{u} \cdot \mathbf{h}(\mathbf{x})$, so that $\mathcal{C}$ lies inside the hypersurface given by the equation

$$u_1 h_1(\mathbf{x}) + \cdots + u_s h_s(\mathbf{x}) = \lambda(\mathbf{u}), \tag{4}$$

for every $\mathbf{u} = (u_1, \ldots, u_k) \in V^\perp$.

Let V be the vector space perpendicular to $V^\perp$ in $\mathbb{F}_p^s$, so that $\mathbf{u} \cdot \mathbf{v} = 0$ for all $\mathbf{v} \in V, \mathbf{u} \in V^\perp$. Let Δ_λ be a vector for which $\mathbf{u} \cdot \Delta_\lambda = \lambda(\mathbf{u})/p$ for all $\mathbf{u} \in V^\perp$, so that

$$\{y \in \mathbb{F}_p^s : \ \mathbf{u} \cdot y = \lambda(\mathbf{u}) \text{ for all } \mathbf{u} \in V^\perp\} = p\Delta_\lambda + V. \tag{5}$$

Therefore $\mathbf{h}(\mathcal{C}(\mathbb{F}_p))$ is embedded inside the translation $p\Delta_\lambda + V$ of the proper subspace V of $\mathbb{F}_p^s$; and so $t(\mathbf{h}(\mathcal{C}(\mathbb{F}_p)))$ is embedded inside $\Delta_\lambda + t(V)$.

Note that no proper subspace of $\Delta_\lambda + t(V)$ can contain $t(\mathbf{h}(\mathcal{C}))$, because such a subspace will then have an orthogonal space which is larger than $V^\perp$, and this contradicts the definition of $V^\perp$. In other words, in the notation from the beginning of this section we have

$$\Delta_\lambda + t(V) = t(W) \subseteq E_{\mathcal{C},\mathbf{h}}.$$

Theorem 2. *Let $r \geq 2$ and $s, d, D \geq 1$ be integers. Let $E \subseteq \mathbb{T}^s$ be a translate of a subspace of dimension s_0 of $\mathbb{T}^s$, and let Ω be a domain in $\mathbb{T}^s$ whose intersection with E has piecewise smooth boundary. For any absolutely irreducible curve $\mathcal{C}$ of degree d in $\mathbb{A}^r(\overline{\mathbb{F}}_p)$ defined over $\mathbb{F}_p$ and any suitable rational map $\mathbf{h} : \mathcal{C} \to \mathbb{A}^s(\overline{\mathbb{F}}_p)$ of degree D, for which $E_{\mathcal{C},\mathbf{h}} = E$,*

$$\mu_{\mathcal{C},\mathbf{h}}(\Omega) = \mu_E(\Omega) + O_{r,s,d,D,E,\Omega}\left(p^{-1/2s_0} \log p\right),$$

where $\mu_E(\Omega) := \mu_E(\Omega \cap E)$, and μ_E denotes the normalized Haar measure on E.

Thus we now have results which apply in all cases, and with better error terms than in previous literature. Note that the error term here depends on E. In section 11 we obtain such a result in which the error term is independent of E, but which only holds for boxes (with edges parallel to the co-ordinate axes).

4 Global Geometry and Distribution Questions

In the previous section we assumed that prime p was fixed. In this section we shall assume that $\mathcal{C}$ is an absolutely irreducible curve of degree d, defined over $\mathbb{Z}$, embedded in affine space $\mathbb{A}^r(\mathbb{C})$ and that $\mathbf{h} = (h_1, \ldots, h_s)$ is a suitable rational map $\mathcal{C} \to \mathbb{A}^s(\mathbb{C})$, with $h_j = f_j/g_j$, where $f_j, g_j \in \mathbb{Z}[X_1, \ldots, X_r]$. We now define

$$V^\perp := \{\mathbf{u} \in \mathbb{Z}^s : \mathbf{u} \cdot \mathbf{h}(\mathbf{x}) \text{ is constant for } \mathbf{x} \in \mathcal{C}\}.$$

For each $\mathbf{u} \in V^\perp$ we define $\lambda(\mathbf{u}) := \mathbf{u} \cdot \mathbf{h}(\mathbf{x})$, so that $\mathcal{C}$ lies inside the hypersurface given by the equation

$$u_1 h_1(\mathbf{x}) + \cdots + u_s h_s(\mathbf{x}) = \lambda(\mathbf{u}), \tag{6}$$

for every $\mathbf{u} = (u_1, \ldots, u_k) \in V^\perp$.

Let V be the vector space perpendicular to $V^\perp$ in $\mathbb{Q}^s$, so that $\mathbf{u} \cdot \mathbf{v} = 0$ for all $\mathbf{v} \in V, \mathbf{u} \in V^\perp$. Let Δ_λ be a vector for which $\mathbf{u} \cdot \Delta_\lambda = \lambda(\mathbf{u})$ for all $\mathbf{u} \in V^\perp$. Therefore $\mathbf{h}(\mathcal{C}(\mathbb{Q}))$ is embedded inside $\Delta_\lambda + V$.

In order to simplify the presentation, let us assume in what follows that $h_0 := 1, h_1, \ldots, h_{s_0}$ are linearly independent along C and that there are $c_{ij} \in$

$\mathbb{Z}$, $s_0+1 \le i \le s$, $0 \le j \le s_0$ such that $\mathcal{C}$ lies inside each of the hyper-surfaces given by

$$h_i(X) = \sum_{0 \le j \le s_0} c_{ij} h_j(X).$$

Then $V^\perp$ will be generated by the vectors $(c_{i0}, \ldots, c_{is_0}, 0, \ldots, 0, -1, 0, \ldots, 0)$ $s_0 + 1 \le i \le s$. We also consider the subspace $E_{\mathcal{C},\mathbf{h}}$ of $(\mathbb{R}/\mathbb{Z})^s$ given by

$$E_{\mathcal{C},\mathbf{h}} = \{(z_1, \ldots, z_s) \in (\mathbb{R}/\mathbb{Z})^s : z_i = \sum_{1 \le j \le s_0} c_{ij} z_j, s_0 + 1 \le i \le s\}.$$

Let us denote the reductions of $\mathcal{C}$ and $\mathbf{h}$ into $\mathbb{F}_p$ by $\mathcal{C}_p$ and $\mathbf{h}_p$, respectively. Let

$$V_p^\perp := \{\mathbf{u} \in \mathbb{F}_p^s : \mathbf{u} \cdot \mathbf{h}_p(\mathbf{x}) \text{ is constant for } \mathbf{x} \in \mathcal{C}_p\}.$$

and let $E_{\mathcal{C}_p,\mathbf{h}_p}$ have the same meaning as in the previous section. Note that the reduction mod p of any vector from $V^\perp$ lies in $V_p^\perp$. Note also that there may be integer vectors $\mathbf{u}$ for which $\mathbf{u} \cdot \mathbf{h}(\mathbf{x})$ is not constant along the curve $\mathcal{C}$, while its reduction is constant modulo p. We will show hovewer that such vectors $\mathbf{u}$ and such primes p are rare enough so that on average over p, the measure $\mu_{\mathcal{C}_p,\mathbf{h}_p}$ looks like the normalized Haar measure on $E_{\mathcal{C},\mathbf{h}}$. More precisely, we will prove the following result.

Theorem 3. *Let $r \ge 2$ and $s, d, D \ge 1$ be integers. Let $\mathcal{C}$ be an absolutely irreducible curve of degree d, defined over $\mathbb{Z}$, embedded in affine space $\mathbb{A}^r(\mathbb{C})$ and let $\mathbf{h} = (h_1, \ldots, h_s)$ be a suitable rational map $\mathcal{C} \to \mathbb{A}^s(\mathbb{C})$, with $h_j = f_j/g_j$, where $f_j, g_j \in \mathbb{Z}[X_1, \ldots, X_r]$, of degree at most D. Let s_0 denote the dimension of $E_{\mathcal{C},\mathbf{h}}$, and let Ω be a domain in $\mathbb{T}^s$ whose intersection with $E_{\mathcal{C},\mathbf{h}}$ has piecewise smooth boundary. Then*

$$\mu_{\mathcal{C}_p,\mathbf{h}_p}(\Omega) = \mu_{E_{\mathcal{C},\mathbf{h}}}(\Omega) + O_{r,s,s_0,d,D,E,\mathcal{C},\mathbf{h},\Omega}\left(p^{-1/2s_0 s}\right),$$

for all but $O(\sqrt{P})$ primes $p \in [P, 2P]$, where $\mu_{E_{\mathcal{C},\mathbf{h}}}(\Omega) := \mu_{E_{\mathcal{C},\mathbf{h}}}(\Omega \cap E)$, and $\mu_{E_{\mathcal{C},\mathbf{h}}}$ denotes the normalized Haar measure on E.

5 Residue Races

In a "residue race" we seek to determine the number $R_{\mathcal{C},\mathbf{h}}$ of $\mathbf{x} \in \mathcal{C}(\mathbb{F}_p)$ for which

$$t(h_1(\mathbf{x})) < \ldots < t(h_s(\mathbf{x})) \tag{7}$$

(we let $t(h_i(\mathbf{x})) = 1$ if h_i has a pole at $\mathbf{x}$). Theorem 2 implies an estimate for any suitable h in terms of the measure of a certain domain. (This problem has previously been studied for $h_i(x) = a_i x \in \mathbb{F}_p[x]$ in [8], for $h_i(x) = 1/(x + a_i)$ over arbitrary residue rings in [4], and for $h_i(x, y) \in \mathbb{F}_p(x, y)$ with $s = 2$ in [15].) If $1, h_1, \ldots, h_s$ are linearly independent along $\mathcal{C}$, we can use Theorem 1 directly to show that all the $s!$ possible orders among the numbers $t(h_1(\mathbf{x})), \ldots, t(h_s(\mathbf{x}))$ in (7) are asymptotically equally likely. Indeed, since the simplex $\Sigma_s = \{(\alpha_1, \ldots, \alpha_s) \in \mathbb{T}^s : 0 \leq \alpha_1 < \ldots < \alpha_s < 1\}$ satisfies the conditions of Theorem 1 and $\mu(\Sigma_s) = 1/s!$, we derive the following result:

Corollary 1. *Let $r \geq 2$ and $s, d, D \geq 1$ be integers. For any absolutely irreducible curve $\mathcal{C}$ of degree d in $\mathbb{A}^r(\overline{\mathbb{F}}_p)$ defined over $\mathbb{F}_p$ and any suitable rational map $\mathbf{h} : \mathcal{C} \to \mathbb{A}^s(\overline{\mathbb{F}}_p)$ of degree D which is L-free along $\mathcal{C}$, one has*

$$R_{\mathcal{C},\mathbf{h}} = \frac{p}{s!} + O_{r,s,d,D}\left(pL^{-1/s} + p^{1-1/2s} \log L\right).$$

In particular if $1, h_1, \ldots, h_s$ are linearly independent along $\mathcal{C}$ we may take $L = \sqrt{p}$ and obtain an error term $O_{r,s,d,D}(p^{1-1/2s} \log p)$.

When $\mathcal{C} = \mathbb{F}_p$ one can imagine such a "residue race" taking place on a stadium of unit length where the "competitors" $h_1, \ldots, h_s$ are at the points $t(h_1(x)), \ldots, t(h_s(x))$ after x seconds, for $x = 0, 1, \ldots, p - 1$. Corollary 1 may be interpreted as saying that each of the $s!$ possible orderings of the competitors occurs about $1/s!$ of the time. Moreover the condition that $1, h_1(x), \ldots, h_s(x)$ are linearly independent modulo p is equivalent to the condition that the speeds $h_1'(x), \ldots, h_s'(x)$ of the competitors are linearly independent modulo p.

The residue races discussed just above are "long races"; for example when $\mathcal{C} = \mathbb{F}_p$, they are races over a complete set of representatives modulo p. However we might also wish to consider shorter races where, instead in our example, the race is only over a subinterval J of $[0, 1]$; that is, for what proportion of $x \in t^{-1}(J)$ does (7) hold? More generally we might restrict our attention to when $x \in t^{-1}(\Omega_1)$ for some given region $\Omega_1 \subseteq [0, 1]^r$. Thus we denote by $\rho_{\mathcal{C},\mathbf{h}}(\Omega_1, \Omega_2)$ the proportion of elements $\mathbf{x} \in \mathcal{C}(\mathbb{F}_p) \cap t^{-1}(\Omega_1)$ for

which $t(\mathbf{h}(\mathbf{x})) \in \Omega_2$, so that

$$\begin{aligned}\rho_{\mathcal{C},\mathbf{h}}(\Omega_1,\Omega_2) &= \frac{\#\{\mathbf{x}\in\mathcal{C}(\mathbb{F}_p)\cap t^{-1}(\Omega_1) \mid t(\mathbf{h}(\mathbf{x}))\in\Omega_2\}}{\#\{\mathbf{x}\in\mathcal{C}(\mathbb{F}_p)\cap t^{-1}(\Omega_1)\}}\\ &= \frac{\#\{\mathbf{x}\in\mathcal{C}(\mathbb{F}_p) \mid t(\mathbf{x})\in\Omega_1 \text{ and } t(\mathbf{h}(\mathbf{x}))\in\Omega_2\}}{\#\{\mathbf{x}\in\mathcal{C}(\mathbb{F}_p) \mid t(\mathbf{x})\in\Omega_1\}}\\ &= \frac{\rho_{\mathcal{C},\mathbf{H}}(\Omega)}{\rho_{\mathcal{C},\mathbf{Id}}(\Omega_1)},\end{aligned}$$

where $\Omega = \Omega_1\times\Omega_2 \in \mathbb{T}^{r+s}$, and $\mathbf{H}$ is the rational map $\mathbf{Id}\times\mathbf{h}:\ \mathcal{C}\to\mathbb{A}^{r+s}(\overline{\mathbb{F}}_p)$, given by $\mathbf{H}_j = \mathbf{x}_j$ for $1\le j\le r$, and $\mathbf{H}_j = \mathbf{h}_{j-r}$ for $r+1\le j\le r+s$. If Theorem 1 is applicable then

$$\rho_{\mathcal{C},\mathbf{H}}(\Omega) = \mu(\Omega) + O_{r,s,d,D,\Omega_1,\Omega_2}\left(L^{-1/(r+s)} + p^{-1/2(r+s)}\log p\right)$$

and

$$\rho_{\mathcal{C},\mathbf{Id}}(\Omega_1) = \mu(\Omega_1) + O_{r,d,\Omega_1}\left(p^{-1/2r}\log p\right);$$

and we have $\mu(\Omega) = \mu(\Omega_1)\mu(\Omega_2)$ by definition, so that we obtain the following result.

Corollary 2. *Let $r\ge 2$ and $s,d,D\ge 1$ be integers. For any domains $\Omega_1\subseteq\mathbb{T}^r$, $\Omega_2\subseteq\mathbb{T}^s$ with piecewise smooth boundaries, any absolutely irreducible curve $\mathcal{C}$ of degree d in $\mathbb{A}^r(\overline{\mathbb{F}}_p)$ defined over $\mathbb{F}_p$ and any suitable rational map $\mathbf{h}:\mathcal{C}\to\mathbb{A}^s(\overline{\mathbb{F}}_p)$ of degree D, for which the map $\mathbf{H} := (x_1,\dots,x_r,h_1,\dots,h_s)$ is L-free along $\mathcal{C}$, one has*

$$\rho_{\mathcal{C},\mathbf{h}}(\Omega_1,\Omega_2) = \mu(\Omega_2) + O_{r,s,d,D,\Omega_1,\Omega_2}\left(L^{-1/(r+s)} + p^{-1/2(r+s)}\log L\right).$$

Given a domain Ω in $\mathbb{T}^r$ with a piecewise smooth boundary, define $R_{\mathcal{C},\mathbf{h}}(\Omega)$ to be the number of points $\mathbf{x}$ from $\mathcal{C}(\mathbb{F}_p)$ which lie inside the region Ω and for which (7) holds. Then from Corollary 2 we derive:

Corollary 3. *Let $r\ge 2$ and $s,d,D\ge 1$ be integers. For any domain $\Omega\subseteq\mathbb{T}^r$ with piecewise smooth boundary, any absolutely irreducible curve $\mathcal{C}$ of degree d in $\mathbb{A}^r(\overline{\mathbb{F}}_p)$ defined over $\mathbb{F}_p$ and any suitable rational map $\mathbf{h}:\mathcal{C}\to\mathbb{A}^s(\overline{\mathbb{F}}_p)$ of degree D, for which the map $\mathbf{H} := (x_1,\dots,x_r,h_1,\dots,h_s)$ is L-free along $\mathcal{C}$, one has*

$$R_{\mathcal{C},\mathbf{h}}(\Omega) = \frac{p}{s!}\left(1 + O_{r,s,d,D,\Omega}\left(L^{-1/(r+s)} + p^{-1/2(r+s)}\log L\right)\right).$$

6 The Spectrum of Ω, and Lines

Let $r \geq 2$ and $s, d, D \geq 1$ be integers. For any given domain $\Omega \subseteq \mathbb{T}^s$ with piecewise smooth boundary let $\Gamma_p(\Omega)$ be the set of values $\mu_{\mathcal{C},\mathbf{h}}(\Omega)$, where $\mathcal{C}$ and $\mathbf{h}$ are as in Theorem 2. Let the *spectrum* $\Gamma(\Omega) := \lim_{p\to\infty} \Gamma_p(\Omega)$ (where we define $A_\infty = \lim_{n\to\infty} A_n$ for sets of points A_n, by $z \in A_\infty$ if and only if there exists $z_n \in A_n$ such that $\lim_{n\to\infty} z_n = z$). Let $\Lambda_p(\Omega)$ be the set of values $\mu_{\mathcal{L},\mathbf{Id}}(\Omega)$ where $\mathcal{L}$ runs over the set of lines, and $\mathbf{Id}$ is the identity; and $\Lambda(\Omega) := \lim_{p\to\infty} \Lambda_p(\Omega)$. We prove the following result which implies, in essence, that all values of our measure on Ω are obtained when we simply consider the set of lines:

Theorem 4. *With the definitions as above, for any given domain $\Omega \subseteq \mathbb{T}^s$ with piecewise smooth boundary, we have $\Gamma(\Omega) = \Lambda(\Omega)$.*

Given nonzero $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^s$ and prime p, define the line $\mathcal{L}_p := \{\mathbf{a} + t\mathbf{b} : \ t \in \mathbb{F}_p\}$. As in [8], one can easily show that

$$\mu_{\mathcal{L}_p,\mathbf{id}}(\Omega) = \int_{\substack{0\leq t<1 \\ \mathbf{a}/p+t\mathbf{b}\in\Omega}} 1dt + O\left(\frac{1}{p^{1/s}}\right).$$

Therefore

$$\Gamma(\Omega) = \Lambda(\Omega) = \left\{ \int_{\substack{0\leq t<1 \\ \mathbf{a}+t\mathbf{b}\in\Omega}} 1dt : \ \mathbf{a} \in \mathbb{T}^s, \mathbf{b} \in \mathbb{Z}^s \right\}.$$

It is an interesting, and perhaps tractable, problem to determine $\Lambda(\Omega)$. By varying $\mathbf{a}$ continuously , one can easily show that $\Lambda(\Omega)$ is a union of intervals. For example, in the "Residue Race" problem of the previous section we have $\Omega = \Sigma_s$, and it is easy to see that $\Lambda(\Sigma_s) = [0, 1)$ simply by taking the lines $\{\epsilon(0, 1, 2, \ldots, s-1) + t(1, 1, \ldots, 1) : \ t \in [0, 1)\}$ to get measure 0 if $\epsilon = 0$, and $1 - (s-1)\epsilon$ for $0 < \epsilon < 1/(s-1)$.

The paper [8] considers the residue race problem for lines going through the origin with $\Omega = \Sigma_s$: Define $\Gamma_p^{(0)}(\Omega)$ be the set of values $\mu_{\mathcal{C},\mathbf{h}}(\Omega)$, where $\mathcal{C}$ and $\mathbf{h}$ are as in Theorem 2 and $\mathbf{0} \in \mathbf{h}(\mathcal{C})$, and let $\Gamma^{(0)}(\Omega) := \lim_{p\to\infty} \Gamma_p^{(0)}(\Omega)$. Similarly define $\Lambda^{(0)}(\Omega)$. We note in the proof of Theorem 4 that $\Gamma^{(0)}(\Omega) = \Lambda^{(0)}(\Omega)$. Thus, [8] studied $\Lambda^{(0)}(\Sigma_s)$ $(= \Gamma^{(0)}(\Sigma_s))$ and found that it is rather complicated (in contrast to $\Lambda(\Sigma_s)$, determined above). We quote some of the results from there:

It is trivial to show that $\Lambda^{(0)}(\Sigma_2) = \{0, 1/2\}$ since we get 0 taking the line $t(1,1)$, and if $\mathbf{b}$ is not a scalar multiple of $(1,1)$, then $t\mathbf{b} \in \Sigma_2$ if and only if $(1-t)\mathbf{b} \notin \Sigma_2$.

The spectrum $\Lambda^{(0)}(\Sigma_3)$ is also discrete. It has smallest elements 0 and then 1/12, and largest element 1/3. The set of accumulation points,

$\mathrm{Acc}(\Lambda^{(0)}(\Sigma_3)) = \{0, 1/6\} \cup \{1/6 + 1/12d : \ d \neq 0, -1\} \subset \{0\} \cup [1/8, 1/4]$. In fact $\{u \in \Lambda^{(0)}(\Sigma_3) : \ u \geq 1/4\} = \{1/4\} \cup \{(1/4)(1+1/d) : \ \text{odd } d \geq 3\}$, and $\{u \in \Lambda^{(0)}(\Sigma_3) : \ u \leq 1/8\} = \{1/8\} \cup \{(1/8)(1-1/d) : \ \text{odd } d \geq 1\}$

The spectrum $\Lambda^{(0)}(\Sigma_4)$ is also discrete. It has largest element 1/4 and smallest elements

$$0, \frac{1}{462}, \frac{1}{420}, \frac{1}{390}, \frac{1}{336}, \frac{1}{330}, \frac{1}{312}, \frac{1}{308}, \frac{1}{288}, \frac{1}{286}, \frac{1}{273}, \frac{1}{270}, \frac{1}{266}, \frac{1}{264}, \frac{1}{260}, \frac{1}{255} \ldots$$

One can completely determine $\mathrm{Acc}(\Lambda^{(0)}(\Sigma_4))$, and show $\{u \in \Lambda^{(0)}(\Sigma_3) : \ u \geq 1/6\} = \{1/6\} \cup \{(1/6)(1+2/d) : \ d \geq 4 \text{ and } d \equiv 1 \pmod 3\}$.

It is also shown that $1/s$ is the largest element of $\mathrm{Acc}(\Lambda^{(0)}(\Sigma_s))$ for $s \geq 42$ (and this is probably true for all s), though little else is known about these spectra. One interesting question is to determine the smallest element of the spectrum other than 0: these are $1/2, 1/12, 1/462$ for $s = 2, 3, 4$ and at most $1/47475$ for $s = 5$.

7 A Discussion of Discrepancies

For a finite set $\mathcal{A} \subseteq \mathbb{T}^k$ and domain $\Omega \subseteq \mathbb{T}^k$, we define the *discrepancy*

$$\Delta(\mathcal{A}, \Omega) := \left| \frac{\#\{a \in \mathcal{A} : \ a \in \Omega\}}{\#\{a \in \mathcal{A}\}} - \mu(\Omega) \right|,$$

and the *box discrepancy* of $\mathcal{A}$,

$$D(\mathcal{A}) := \sup_{\mathbb{B} \subseteq \mathbb{T}^k} \Delta(\mathcal{A}, \mathbb{B}),$$

where the supremum is taken over all boxes $\mathbb{B} = [\alpha_1, \beta_1] \times \ldots \times [\alpha_k, \beta_k]$.

We define the distance between a vector $\mathbf{u} \in \mathbb{T}^k$ and a set $\Gamma \subseteq \mathbb{T}^k$ by

$$\mathrm{dist}(\mathbf{u}, \Gamma) = \inf_{\mathbf{w} \in \Gamma} \|\mathbf{u} - \mathbf{w}\|$$

where $\|\mathbf{v}\|$ denotes the Euclidean norm of $\mathbf{v}$. Given $\varepsilon > 0$ and a domain $\Omega \subseteq \mathbb{T}^k$ we define the sets

$$\Omega_\varepsilon^+ = \left\{\mathbf{u} \in \mathbb{T}^k \backslash \Omega \mid \operatorname{dist}(\mathbf{u}, \Omega) < \varepsilon\right\}$$

and

$$\Omega_\varepsilon^- = \left\{\mathbf{u} \in \Omega \mid \operatorname{dist}(\mathbf{u}, \mathbb{T}^k \backslash \Omega) < \varepsilon\right\}.$$

Let $b(\varepsilon)$ be any increasing function defined for $\varepsilon > 0$ and such that $\lim_{\varepsilon \to 0} b(\varepsilon) = 0$. Following [10, 11], we define the class $\mathcal{M}_b$ of domains $\Omega \subseteq \mathbb{T}^k$ for which

$$\mu\left(\Omega_\varepsilon^+\right) \leq b(\varepsilon) \qquad \text{and} \qquad \mu\left(\Omega_\varepsilon^-\right) \leq b(\varepsilon).$$

A relation between $D(\mathcal{A})$ and $\Delta(\mathcal{A}, \Omega)$ for $\Omega \in \mathcal{M}_b$ is given by the following inequality from [10] (see also [11]).

Lemma 1. *For any domain $\Omega \in \mathcal{M}_b$, we have*

$$\Delta(\mathcal{A}, \Omega) = O_k\left(b\left(k^{1/2} D(\mathcal{A})^{1/k}\right)\right).$$

The *Koksma–Szüsz inequality* [9, 12] (see also Theorem 1.21 of [6]), which generalizes the Erdős-Turan inequality, provides an important link between box discrepancy and exponential sums:

Lemma 2. *For integer $L > 1$, and a set $\mathcal{A} \subseteq \mathbb{T}^k$ of N points, one has*

$$D(\mathcal{A}) = O\left(\frac{1}{L} + \frac{1}{N} \sum_{\substack{\mathbf{c}=(c_1,\ldots,c_k) \in \mathbb{Z}^k \backslash \{\mathbf{0}\} \\ |c_j| \leq L \text{ for each } j}} \frac{1}{\prod_{i=1}^k (1 + |c_i|)} \left|\sum_{\mathbf{a} \in \mathcal{A}} \mathbf{e}\left(\mathbf{c} \cdot \mathbf{a}\right)\right|\right).$$

For brevity, we define $\mathbf{e}_p(z) = \mathbf{e}(z/p)$ in this section.

The following statement is a generalization of the bound (17) of [13]:

Lemma 3. *Let $r \geq 2$ and $s, d, D \geq 1$ be integers. For any absolutely irreducible curve $\mathcal{C}$ of degree d in $\mathbb{A}^r(\overline{\mathbb{F}}_p)$ defined over $\mathbb{F}_p$ and any suitable rational map $\mathbf{h} : \mathcal{C} \to \mathbb{A}^s(\overline{\mathbb{F}}_p)$ of degree D, define $\mathcal{H} = \{t(\mathbf{h}(\mathbf{x})) \mid \mathbf{x} \in \mathcal{C}(\mathbb{F}_p)\}$. If $\mathbf{h}$ is L-free then the box discrepancy*

$$D(\mathcal{H}) = O_{s,r,d,D}\left(L^{-1} + p^{-1/2} \log^s L\right).$$

Proof. As in [13] we remark that Theorem 6 of Bombieri [2] implies the bound

$$\sum_{\mathbf{x}\in\mathcal{C}(\mathbb{F}_p)} \mathbf{e}_p\left(\sum_{j=1}^{s} c_j h_j(\mathbf{x})\right) = O_{k,r,d,D}\left(p^{1/2}\right). \tag{8}$$

whenever the function $c_1h_1+\ldots+c_sh_s$ is nonconstant along the curve $\mathcal{C}$. Since $\mathbf{h}$ is L-free along $\mathcal{C}$, the sum in Lemma 2 only contains terms for which (8) applies, and so we obtain the desired result. □

Proof of Theorem 1. We have $\mu_{\mathcal{C},\mathbf{h}}(\mathbb{B}) = \mu(\mathbb{B}) + O_{r,s,d,D,\mathbb{B}}\left(L^{-1} + p^{-1/2}\log^s L\right)$ whenever $\mathbb{B}$ is a box, by Lemma 3. Now, since Ω has a piecewise smooth boundary, one has, for any small $\varepsilon > 0$, that $\mu\left(\Omega_\varepsilon^{\pm}\right) \ll_\Omega \varepsilon$, see [14] for a more precise statement. Therefore $|\mu_{\mathcal{C},\mathbf{h}}(\Omega) - \mu(\Omega)| \le \Delta(\mathcal{H},\Omega) \ll_{s,\Omega} D(\mathcal{H})^{1/s} \ll L^{-1/s} + p^{-1/2s}\log L$ by Lemma 1, which is Theorem 1. □

8 The Non-free Case: Proof of Theorem 2

Let $r, s, s_0, d, D, E, \Omega, \mathcal{C}$ and $\mathbf{h}$ be as in the statement of Theorem 2.

We select a maximal subset of $\{h_1, \ldots, h_s\}$ which, together with the constant function $h_0(\mathbf{x}) = 1$, form a set which is linearly independent along $\mathcal{C}$. We assume in what follows that $\{h_1, \ldots, h_{s_0}\}$ is such a set. Thus $1, h_1, \ldots, h_{s_0}$ are linearly independent along $\mathcal{C}$, and there are integers $c_{ij} \in \{\frac{1-p}{2}, \ldots, \frac{p-1}{2}\}$, $s_0 + 1 \le i \le s$, $0 \le j \le s_0$, such that $\mathcal{C}$ lies inside each of the hyper-surfaces given by

$$h_i(\mathbf{x}) = \sum_{0\le j\le s_0} c_{ij} h_j(\mathbf{x}).$$

Let $\mathrm{Proj} : \mathbb{T}^s \to \mathbb{T}^{s_0}$ denote the projection on the first s_0 coordinates, that is, $\mathrm{Proj}((y_1, \ldots, y_s)) = (y_1, \ldots, y_{s_0}) \in \mathbb{T}^{s_0}$, for any $(y_1, \ldots y_s) \in \mathbb{T}^s$.

Consider also the linear map $A : \mathbb{T}^{s_0} \to \mathbb{T}^s$ given for any $(z_1, \ldots, z_{s_0}) \in \mathbb{T}^{s_0}$ by $A((z_1, \ldots, z_{s_0})) = (z_1, \ldots, z_s) \in \mathbb{T}^s$, where for any $s_0 + 1 \le i \le s$, z_i is defined by

$$z_i = \sum_{0\le j\le s_0} c_{ij} z_j.$$

Note that for points $\mathbf{y} = (y_1, \ldots, y_s) \in \mathbb{T}^s$ of the form $\mathbf{y} = t(\mathbf{h}(\mathbf{x}))$ with $\mathbf{x}$ on the curve $\mathcal{C}$, one has

$$A(\mathrm{Proj}(\mathbf{y})) = \mathbf{y}.$$

Also, if we denote

$$\tilde{\mathbf{h}} = (h_1, \ldots, h_{s_0}) = \mathrm{Proj} \circ \mathbf{h},$$

then for any point $\mathbf{z} = (z_1, \ldots, z_{s_0}) \in \mathbb{T}^{s_0}$ of the form $\mathbf{z} = t(\tilde{\mathbf{h}}(\mathbf{x}))$ with $\mathbf{x}$ on the curve $\mathcal{C}$, we have

$$\mathrm{Proj}(A(\mathbf{z})) = \mathbf{z}.$$

Since $1, h_1, \ldots, h_{s_0}$ are linearly independent along $\mathcal{C}$, the image $t(\tilde{\mathbf{h}}(\mathcal{C}))$ of $\tilde{\mathbf{h}}(\mathcal{C})$ in $\mathbb{T}^{s_0}$ will not be contained in any translate of a proper subspace of $\mathbb{T}^{s_0}$. Therefore $A(t(\tilde{\mathbf{h}}(\mathcal{C})))$, which coincides with $t(\mathbf{h}(\mathcal{C}))$, will be contained in $A(\mathbb{T}^{s_0})$ but will not be contained in any proper subspace of $A(\mathbb{T}^{s_0})$. This says that $A(\mathbb{T}^{s_0}) = E_{\mathcal{C},\mathbf{h}} = E$.

Next, by the definition of $\mu_{\mathcal{C},\mathbf{h}}$ and the fact that the $\mathbb{F}_p-$points on $\mathcal{C}$ are sent through the map $\mathbf{h}$ inside E, we see that for any domain $\Omega \in \mathbb{T}^s$,

$$\mu_{\mathcal{C},\mathbf{h}}(\Omega) = \mu_{\mathcal{C},\mathbf{h}}(\Omega \cap E).$$

Also, if we denote

$$\tilde{\Omega} := \mathrm{Proj}(\Omega \cap E) = A^{-1}(\Omega \cap E),$$

then by the definition of $\mu_{\mathcal{C},\tilde{\mathbf{h}}}$ we find that

$$\mu_{\mathcal{C},\tilde{\mathbf{h}}}(\tilde{\Omega}) = \mu_{\mathcal{C},\mathbf{h}}(\Omega \cap E).$$

Therefore

$$\mu_{\mathcal{C},\mathbf{h}}(\Omega) = \mu_{\mathcal{C},\tilde{\mathbf{h}}}(\tilde{\Omega}). \tag{9}$$

Now, when we send objects via the map $A : \mathbb{T}^{s_0} \to E \subseteq \mathbb{T}^s$, the measure gets multiplied by a constant factor (given by the Jacobian of the linear map A). However, the normalized Haar measure on $\mathbb{T}^{s_0}$ corresponds via A to the normalized Haar measure on E. Hence

$$\mu_{\mathbb{T}^{s_0}}(\tilde{\Omega}) = \mu_E(\Omega \cap E). \tag{10}$$

At this point we apply Theorem 1 to $\mathcal{C}$, $\tilde{\mathbf{h}}$, $\tilde{\Omega}$ and $L = (p-1)/2$. It follows that

$$|\mu_{\mathcal{C},\tilde{\mathbf{h}}}(\tilde{\Omega}) - \mu_{\mathbb{T}^{s_0}}(\tilde{\Omega})| \leq C p^{-1/2s_0} \log p, \tag{11}$$

where the constant C depends on r, s, s_0, d, D and the region $\tilde{\Omega}$. The region $\tilde{\Omega}$ depends in turn on A, Ω and E. Here A is a linear map from $\mathbb{T}^{s_0}$ into $\mathbb{T}^s$ which sends $\mathbb{T}^{s_0}$ to E, and so A depends on the given subspace E of $\mathbb{T}^s$. Theorem 2 now follows from (9), (10) and (11). $\square$

9 Averaging Over p: Proof of Theorem 3

Let $r, s, s_0, d, D, E, \Omega, \mathcal{C}$ and $\mathbf{h}$ be as in the statement of the theorem. Take a large P, and for any prime $p \in [P, 2P]$, consider the reductions $\mathcal{C}_p$ and $\mathbf{h}_p$ of $\mathcal{C}$ and $\mathbf{h}$ into $\mathbb{F}_p$. By Theorem 9.7.7 of SGA IV [5] it follows that $\mathcal{C}_p$ is absolutely irreducible for p large enough.

We now claim that for any $\mathbf{a} \in \mathbb{Z}^s \setminus V^\perp$ with each $|a_j| \leq \sqrt{P}$, there are at most $\log N / \log P \ll_{\mathcal{C},\mathbf{h}} 1$ primes $p \in (P, 2P]$ for which $\mathbf{a} \in V_p^\perp$.

Indeed, a curve $\mathcal{C}$ in $\mathbb{A}^r(\overline{\mathbb{Q}})$ that is defined over $\mathbb{Z}$, can be assumed to be written as (the intersection of) $r-1$ polynomials in $x_1, \ldots, x_r$. By taking resultants to eliminate variables, this can be rewritten as (the intersection of) $r-1$ polynomials $w_j(x_j, x_1) \in \mathbb{Z}[x_j, x_1]$ for $2 \leq j \leq r$.

For given $\mathbf{a} \in \mathbb{Z}^s \setminus V^\perp$ let $f_\mathbf{a}/g_\mathbf{a} = \mathbf{h} \cdot \mathbf{a}$ with $f_\mathbf{a}, g_\mathbf{a} \in \mathbb{Z}[x_1, \cdots, x_r]$. Taking the resultant of $f_\mathbf{a} - \lambda g_\mathbf{a}$ with each w_j in turn, to eliminate $x_2, \ldots, x_r$, we obtain a polynomial $F(\lambda, x_1) \in \mathbb{Z}[x_1, \lambda]$. Note that $\deg f_\mathbf{a}$ and $\deg g_\mathbf{a}$ can be bounded independently of $\mathbf{a}$, and thus so can $\deg F$. Write $F(\lambda, x_1) = \sum c_i(\lambda) x^i$, and then let I_λ be the ideal generated by the $c_i(\lambda)$ over $\mathbb{Z}[\lambda]$. We claim that I_λ contains a non-zero integer, for if not then all the $c_i(\lambda)$ are divisible by a common factor over $\mathbb{Q}[\lambda]$ and thus have a common root, say λ_0, so that $\mathbf{h} \cdot \mathbf{a} = \lambda_0$ on $\mathcal{C}$ and therefore $\mathbf{a} \in V^\perp$. Let N be the smallest positive integer in I_λ, which evidently can be bounded in terms of the degree and coefficients of $F(\lambda, x_1)$, and thus by a power of $\max_j |a_j|$ times a constant depending only on $\mathcal{C}$ and $\mathbf{h}$.

Suppose P is sufficiently large (depending only on $\mathcal{C}$ and $\mathbf{h}$), so that $\mathcal{C}_p$ is absolutely irreducible for all primes $p \in (P, 2P]$. If, for a given integer λ, the polynomial $F(\lambda, x_1)$ is not identically zero mod p, then there are at most $\deg F$ values of x_1 satisfying $F(\lambda, x_1) \equiv 0 \pmod{p}$. For each such x_1 there are at most $\deg w_j$ values of x_j with $w_j(x_j, x_1) \equiv 0 \pmod{p}$ (since p is larger than the coefficients of any of the w_j), and thus there are $O_{\mathcal{C},\mathbf{h}}(1)$ points on the intersection of $\mathcal{C}$ and $\mathbf{h} \cdot \mathbf{a} - \lambda$. Therefore $\mathbf{a} \notin V_p^\perp$ else this intersection contains $\mathcal{C}(\mathbb{F}_p)$, which has $p + O_{\mathcal{C},\mathbf{h}}((p^{1/2})) \gg p$ points (by Weil's Theorem), giving a contradiction as $p > P$ is sufficiently large.

Therefore if $\mathbf{a} \in V_p^\perp$ then the polynomial $F(\lambda, x_1)$ is identically zero mod p for some integer λ. But then each $c_i(\lambda) = 0$ and so p divides N. Thus for a given $\mathbf{a} \in \mathbb{Z}^s \setminus V^\perp$ with each $|a_j| \leq \sqrt{P}$, there are at most $\log N / \log P \ll_{\mathcal{C},\mathbf{h}} 1$ primes $p \in (P, 2P]$ for which $\mathbf{a} \in V_p^\perp$. This proves the claim.

Let now $L = P^{1/2s}$. Then the number of vectors $\mathbf{a} \in \mathbb{Z}^s \setminus V^\perp$ with each

$|a_j| \leq L$ is $O_s(\sqrt{P})$. For each of these vectors $\mathbf{a}$ we know that there are $O_{\mathcal{C},\mathbf{h}}(1)$ primes $p \in (P, 2P]$ for which $\mathbf{a} \in V_p^{\perp}$. Therefore, for any prime number $p \in [P, 2P]$ outside an exceptional set having $O_{\mathcal{C},\mathbf{h}}(\sqrt{P})$ elements, we may assume in what follows that for any $\mathbf{a} \in V_p^{\perp}$ with each $|a_j| \leq L$ we have $\mathbf{a} \in V^{\perp}$.

In order to finish the roof of the theorem, we proceed as in the proof of Theorem 2. Thus we consider the projection $\mathrm{Proj} : \mathbb{T}^s \to \mathbb{T}^{s_0}$ and the linear map $A : \mathbb{T}^{s_0} \to E \subseteq \mathbb{T}^s$. Note that A is independent of p. At the same time we should remark that the maps Proj and A do not have exactly the same meaning as in the proof of Theorem 2 for any given p, since E and $E_{\mathcal{C}_p,\mathbf{h}_p}$ may be distinct. What we know however is that for any p outside the above exceptional set of primes, if we denote $\tilde{\mathbf{h}}_p := \mathrm{Proj} \circ \mathbf{h}$, then the map $\tilde{\mathbf{h}}_p$ is almost $L-$free. Actually, the linear map A may increase or decrease the lengths of our vectors $\mathbf{a} \in V_p^{\perp}$. But, since A is kept fixed, these lengths increase or decrease by at most a factor which is independent of p. Therefore $\tilde{\mathbf{h}}_p$ is $c_A L-$free, for some constant $c_A > 0$ depending on A. We may then apply Theorem 1 for $\mathcal{C}_p$, $\tilde{\mathbf{h}}_p$, $\tilde{\Omega} := A^{-1}(\Omega \cap E)$ and $c_A L$, for each p not in the exceptional set, in order to finish the proof as in the proof of Theorem 2. $\square$

10 Boxes and parallelepipeds

Here by a box we mean a rectangular parallelepiped. Thus a box in $\mathbb{R}^s$ or in $\mathbb{T}^s$ will be a subset of the form $\mathbb{B} = [\gamma_1, \delta_1] \times \cdots \times [\gamma_s, \delta_s]$, while a parallelepiped is any set that can be sent to a box by a linear map.

Note that the error term in Theorem 1 for a general region Ω with piecewise smooth boundary is significantly worse than the error term from Lemma 3, which corresponds to the case when Ω is a box.

One may then naturally expect that the error terms in Theorems 2 and 3 could also be substantially improved in the particular case when the region Ω is a box.

One easy way to obtain such an improvement in Theorem 2 is to let Ω be any parallelepiped in $\mathbb{T}^s$ whose image in $\mathbb{T}^{s_0}$ via our projection Proj, is a box. In this way one obtains a result as accurate as the one from Lemma 3. This result, however, will only concern a particular class of parallelepipeds in $\mathbb{T}^s$, and, depending on the position of the given subspace E inside $\mathbb{T}^s$, this class of parallelepipeds may or may not contain any boxes.

Below we describe a general method, which does apply to general boxes.

The method works in the context of Theorem 2, and then can also be used in combination with averaging over p, in the context of Theorem 3. In the process we also investigate the Fourier expansion of our measures, which can also be used as a tool to understand the given measures.

For any integer vector $\mathbf{a} = (a_1, \ldots, a_s)$ let $\mu_{\mathbf{a}}$ denote the Borel complex measure on the torus $\mathbb{T}^s$ with density function given by $\mathbf{x} \mapsto \mathbf{e}(\mathbf{a} \cdot \mathbf{x})$ (where, here and henceforth, $\mathbf{e}(z) = \exp(2i\pi z)$), that is, for any domain $\Omega \subseteq \mathbb{T}^s$

$$\mu_{\mathbf{a}}(\Omega) = \int_{\mathbf{x} \in \Omega} \mathbf{e}(\mathbf{a} \cdot \mathbf{x}) d\mathbf{x}. \tag{12}$$

In particular $\mu_{\mathbf{0}} = \mu$, our normalized Haar measure. Then

$$\mu_{t(V)}(\Omega - \Delta_\lambda) \approx \sum_{\mathbf{a} \in V^\perp} \mathbf{e}\left(\lambda(\mathbf{a})/p\right) \mu_{\mathbf{a}}(\Omega) \tag{13}$$

(see (10) and (12) below). We remark that if $1, h_1, \ldots, h_s$ are linearly independent along $\mathcal{C}$ then the sum on the right side of (13) consists of only the $\mathbf{a} = 0$ term, so we obtain our normalized Haar measure μ.

We now proceed to investigate the measure from Theorem 2 in the case when Ω is a box.

As above we associate $\mathbb{F}_p$ with $p\mathbb{T} \cap \mathbb{Z}$ and we also use $\mathbf{e}_p(z) = \mathbf{e}(z/p)$. We may suppose $V^\perp$ has basis $\mathbf{u}_1, \ldots, \mathbf{u}_{s-\ell}$ where all coordinates of these vectors are integers, and we will think of V as a subspace of $\mathbb{T}^s$. For any box $\mathbb{B} = [\gamma_1, \delta_1] \times \cdots \times [\gamma_s, \delta_s]$ define $\mu_V(\mathbb{B}) = \mu(\mathbb{B} \cap V)$, an $\ell-$dimensional volume (which is $\mu_{t(V)}$, or μ_E after a translation, in the statement of Theorem 2). Then

$$\begin{aligned} \#\big(p\mathbb{B} \cap pV \cap \mathbb{Z}^s\big) &= \#\{(a_1, \ldots, a_s) \in \mathbb{Z}^s : (a_1/p, \ldots, a_s/p) \in \mathbb{B} \cap V\} \\ &= p^\ell \mu(\mathbb{B} \cap V) + O_V(p^{\ell-1}) = p^\ell \mu_V(\mathbb{B}) + O_V(p^{\ell-1}), \end{aligned} \tag{14}$$

by a simple lattice point counting argument. Therefore, by (5),

$$\#\{\mathbf{x} \in p\mathbb{B} \cap \mathbb{Z}^s : \mathbf{x} \cdot \mathbf{u} = \lambda(\mathbf{u}) \text{ for all } \mathbf{u} \in V^\perp\} = p^\ell \mu_V\left(\mathbb{B} - \Delta_\lambda\right) + O_V(p^{\ell-1}). \tag{15}$$

The characteristic function to determine whether $\mathbf{x} \in \mathbb{F}_p^s$ belongs to $p\mathbb{B}$ is

$$\begin{aligned}\chi_{p\mathbb{B}}(\mathbf{x}) &= \sum_{\substack{p\gamma_1 \le u_1 \le p\delta_1 \\ \cdots \\ p\gamma_s \le u_s \le p\delta_s}} \prod_{j=1}^{s} \left(\frac{1}{p} \sum_{a_j=0}^{p-1} \mathbf{e}_p\left(a_j(x_j - u_j)\right) \right) \\ &= \frac{1}{p^s} \sum_{|a_1|,\ldots,|a_s| \le p/2} \mathbf{e}_p\left(\mathbf{a}\cdot\mathbf{x}\right) \prod_{j=1}^{s} \sum_{p\gamma_j \le u_j \le p\delta_j} \mathbf{e}_p\left(-a_j u_j\right).\end{aligned} \tag{16}$$

Therefore

$$\begin{aligned}\#\{\mathbf{x} \in p\mathbb{B} \cap \mathbb{Z}^s : \mathbf{x}\cdot\mathbf{u} = \lambda(\mathbf{u}) \text{ for all } \mathbf{u} \in V^\perp\} &= \sum_{\substack{\mathbf{x} \in (p\mathbb{T})^s \cap \mathbb{Z}^s \\ \mathbf{x}\cdot\mathbf{u} = \lambda(\mathbf{u}), \mathbf{u} \in V^\perp}} \chi_{p\mathbb{B}}(\mathbf{x}) \\ = \frac{1}{p^s} \sum_{|a_1|,\ldots,|a_s| \le p/2} \sum_{\substack{\mathbf{x} \in \mathbb{F}_p^s \\ \mathbf{x}\cdot\mathbf{u} = \lambda(\mathbf{u}), \mathbf{u} \in V^\perp}} \mathbf{e}_p(\mathbf{a}\cdot\mathbf{x}) \prod_{j=1}^{s} \sum_{p\gamma_j \le u_j \le p\delta_j} \mathbf{e}_p(-a_j u_j).\end{aligned}$$

We now study the internal sum:

If $\mathbf{a} \in V^\perp$ then $\mathbf{a}\cdot\mathbf{x} = \lambda(\mathbf{a})$ so the summand is always $\mathbf{e}_p(\lambda(\mathbf{a}))$. The number of terms in this sum is $\#\{\mathbf{x} \in \mathbb{F}_p^s : \mathbf{x}\cdot\mathbf{u} = \lambda(\mathbf{u}) \text{ for all } \mathbf{u} \in V^\perp\} = p^\ell$. If $\mathbf{a} \notin V^\perp$ then the internal sum runs freely through at least one variable (perhaps after a suitable change of basis) so that the sum is 0. Therefore

$$\begin{aligned}&\frac{1}{p^\ell} \#\{\mathbf{x} \in p\mathbb{B} \cap \mathbb{Z}^s : \mathbf{x}\cdot\mathbf{u} = \lambda(\mathbf{u}) \text{ for all } \mathbf{u} \in V^\perp\} \\ &\qquad = \frac{1}{p^s} \sum_{\mathbf{a} \in V^\perp \cap \mathbb{F}_p^s} \mathbf{e}_p\left(\lambda(\mathbf{a})\right) \prod_{j=1}^{s} \sum_{p\gamma_j \le u_j \le p\delta_j} \mathbf{e}_p\left(-a_j u_j\right),\end{aligned} \tag{17}$$

which should be compared to (15).

Now, under the hypothesis we have, by (16),

$$\begin{aligned}\#\{\mathbf{y} \in \mathcal{C}(\mathbb{F}_p) : \mathbf{h}(\mathbf{y}) \in p\mathbb{B} \cap \mathbb{Z}^s\} &= \sum_{\mathbf{y} \in \mathcal{C}(\mathbb{F}_p)} \chi_{p\mathbb{B}}(\mathbf{h}(\mathbf{y})) \\ = \frac{1}{p^s} \sum_{|a_1|,\ldots,|a_s| \le p/2} \left(\sum_{\mathbf{y} \in \mathcal{C}(\mathbb{F}_p)} \mathbf{e}_p\left(\mathbf{a}\cdot\mathbf{h}(\mathbf{y})\right) \right) \prod_{j=1}^{s} \sum_{p\gamma_j \le u_j \le p\delta_j} \mathbf{e}_p\left(-a_j u_j\right).\end{aligned}$$

If $\mathbf{a} \in V^\perp$ then the internal summand is always $\lambda(\mathbf{a})$ and so these terms contribute

$$\frac{\#\mathcal{C}(\mathbb{F}_p)}{p^s} \sum_{\mathbf{a} \in V^\perp \cap \mathbb{F}_p^s} \mathbf{e}_p\left(\lambda(\mathbf{a})\right) \prod_{j=1}^{s} \sum_{p\gamma_j \le u_j \le p\delta_j} \mathbf{e}_p\left(-a_j u_j\right).$$

The contributions of those terms with $\mathbf{a} \notin V^\perp$ is, by Bombieri's bound (8),

$$O\left(\frac{1}{p^s} \sum_{|a_1|,\ldots,|a_s|<p/2} \sqrt{p}\, \frac{p^s}{(|a_1|+1)\cdots(|a_s|+1)}\right) = O_s\left(\sqrt{p}\,\log^s p\right),$$

since

$$\begin{aligned} \frac{1}{p} \sum_{p\gamma \le u \le p\delta} \mathbf{e}_p\left(-au\right) &= O\left(\frac{1}{p}\right) + \begin{cases} \dfrac{\mathbf{e}(-a\delta) - \mathbf{e}(-a\gamma)}{-2\pi i a} & \text{if } a \neq 0 \\ \delta - \gamma & \text{if } a = 0 \end{cases} \\ &\ll \frac{1}{|a|+1} \qquad\qquad \text{if } |a| \le p/2. \end{aligned} \tag{18}$$

Therefore

$$\begin{aligned} \mu_{\mathcal{C},\mathbf{h}}(\mathbb{B}) &= \frac{\#\{\mathbf{y} \in \mathcal{C}(\mathbb{F}_p) : \mathbf{h}(\mathbf{y}) \in p\mathbb{B} \cap \mathbb{Z}^s\}}{\#\mathcal{C}(\mathbb{F}_p)} \\ &= \frac{1}{p^s} \sum_{\mathbf{a} \in V^\perp \cap \mathbb{F}_p^s} \mathbf{e}_p\left(\lambda(\mathbf{a})\right) \prod_{j=1}^{s} \sum_{p\gamma_j \le u_j \le p\delta_j} \mathbf{e}_p(-a_j u_j) + O\left(\frac{\log^s p}{p^{1/2}}\right) \qquad (19) \\ &= \mu_V\left(\mathbb{B} - \Delta_\lambda\right) + O\left(\frac{\log^s p}{p^{1/2}}\right), \end{aligned}$$

by (15) and (17). This gives the desired improvement of Theorem 2 in the case when Ω is a box.

11 Truncating the "Fourier Expansion"

By (12) and (18) we see that

$$\frac{1}{p^s} \prod_{j=1}^{s} \sum_{p\gamma_j \le u_j \le p\delta_j} \mathbf{e}_p(-a_j u_j) = \mu_{\mathbf{a}}(\mathbb{B}) + O(1/p)$$

where $\mu_{\mathbf{a}}(\mathbb{B})$ satisfies

$$\mu_{\mathbf{a}}(\mathbb{B}) \ll \prod_{j=1}^{s} \frac{1}{1+|a_j|} \tag{20}$$

Therefore

$$\mu_{\mathcal{C},\mathbf{h}}(\mathbb{B}) = \sum_{\mathbf{a}\in V^{\perp}\cap\mathbb{F}_p^s} \mathbf{e}_p\left(\lambda(\mathbf{a})\right)\mu_{\mathbf{a}}(\mathbb{B}) + O\left(\frac{\log^s p}{p^{1/2}}\right) \tag{21}$$

by (19). In Theorem 1 we saw that it was advantageous to assume that a curve is L-free, which means that there is no non-zero $\mathbf{a} \in V^{\perp}$ with each $|a_j| \leq L$. Inspired by this we now seek to estimate $\mu_{\mathcal{C},\mathbf{h}}(\mathbb{B})$ by truncating the sum in (21):

We may assume that the ith unit vector $\mathbf{e}_i \notin V^{\perp}$ for all i, else $v_i = 0$ for all $\mathbf{v} \in V$ so we can pass to $\mathbb{T}^{s-1}$ (moreover if $\mathbf{e}_i \in V^{\perp}$ then $h_i(\mathbf{x})$ is constant for $\mathbf{x} \in \mathcal{C}$). We write $\mathbf{a} = (a_1, \ldots, a_s)$ with each $|a_j| < p/2$. We shall consider the contribution to the sum in (21) of those $\mathbf{a} \in V^{\perp}$ with $\max_j |a_j| \in (L, 2L]$, for which $|a_i| = \max_j |a_j|$. Note that any given values of $\{a_j : j \neq i\}$ give rise to at most one a_i. Therefore, by (20) these terms contribute at most

$$\sum_{|a_j|\leq 2L \text{ for } j\neq i} \frac{1}{\prod_{j\neq i}(|a_j|+1)} \cdot \frac{1}{L} \ll \frac{(\log 2L)^{s-1}}{L}.$$

Summing up over $i = 1, 2, \ldots, s$ and $L, 2L, 4L, \ldots$, we deduce that

$$\left| \sum_{\substack{\mathbf{a}\in V^{\perp}\cap\mathbb{F}_p^s \\ |a_i|>L \text{ for some } i}} \mathbf{e}_p\left(\lambda(\mathbf{a})\right)\mu_{\mathbf{a}}(\mathbb{B}) \right| \ll \frac{(\log 2L)^{s-1}}{L};$$

which with (21) gives

$$\mu_{\mathcal{C},\mathbf{h}}(\mathbb{B}) = \sum_{\substack{\mathbf{a}\in V^{\perp}\cap\mathbb{F}_p^s \\ |a_j|\leq L \text{ for all } j}} \mathbf{e}_p\left(\lambda(\mathbf{a})\right)\mu_{\mathbf{a}}(\mathbb{B}) + O\left(\frac{(\log 2L)^{s-1}}{L}\right) \tag{22}$$

for $1 \leq L \leq \sqrt{p}/\log p$.

12 Averaging Over p in the case of boxes

We work in the context of Theorem 3, in the case when the domain Ω is a box. With notations as in Theorem 3, let us fix a box $\mathbb{B}$ in $\mathbb{T}^s$. By (19) we know that

$$\mu_{\mathcal{C}_p,\mathbf{h}_p}(\mathbb{B}) = \sum_{\mathbf{a}\in V_p^{\perp}} \mathbf{e}_p\left(\lambda(\mathbf{a})\right)\mu_{\mathbf{a}}(\mathbb{B}) + O_{r,s,d,D}\left(p^{-1/2}\log p\right),$$

and we ask whether this is close to

$$\mu_{\mathcal{C},\mathbf{h},p}(\mathbb{B}) := \sum_{\mathbf{a}\in V^{\perp}} \mathbf{e}\left(\lambda(\mathbf{a})_p\right)\mu_{\mathbf{a}}(\mathbb{B}), \tag{23}$$

for most primes p (where integer $\lambda(\mathbf{a})_p \equiv \lambda(\mathbf{a}) \pmod p$)? We proceed to prove that

$$\mu_{\mathcal{C}_p,\mathbf{h}_p}(\mathbb{B}) = \mu_{\mathcal{C},\mathbf{h},p}(\mathbb{B}) + O(p^{-1/2}(\log p)^s), \tag{24}$$

for all but $O(\sqrt{P})$ primes $p \le P$.

We assume that P is large enough so that for any $p > P$, the reduction of $\mathcal{C}$ is absolutely irreducible in $\mathbb{F}_p$ By the argument used at the end of the last section to obtain (22) we get

$$\mu_{\mathcal{C},\mathbf{h},p}(\mathbb{B}) = \sum_{\substack{\mathbf{a}\in V^{\perp}\\ |a_j|\le L \text{ for all } j}} \mathbf{e}_p\left(\lambda(\mathbf{a})\right)\mu_{\mathbf{a}}(\mathbb{B}) + O\left(\frac{(\log 2L)^{s-1}}{L}\right);$$

and combining this with (22) for $L = \sqrt{p}/\log p$ implies that

$$\mu_{\mathcal{C}_p,\mathbf{h}_p}(\mathbb{B}) - \mu_{\mathcal{C},\mathbf{h},p}(\mathbb{B}) = \sum_{\substack{\mathbf{a}\in (V_p^{\perp}\setminus V^{\perp})\cap\mathbb{F}_p^s\\ |a_j|\le\sqrt{p/2} \text{ for all } j}} \mathbf{e}_p\left(\lambda(\mathbf{a})\right)\mu_{\mathbf{a}}(\mathbb{B}) + O\left(\frac{(\log p)^s}{\sqrt{p}}\right). \tag{25}$$

Therefore, if $\mathcal{P}$ is the set of primes $p \in [P, 2P]$ for which $\mathcal{C}_p$ is absolutely

irreducible then

$$\sum_{p\in\mathcal{P}}\left|\sum_{\substack{\mathbf{a}\in(V_p^\perp\setminus V^\perp)\cap\mathbb{F}_p^s\\ |a_j|\le\sqrt{p/2}\text{ for all }j}}\mathbf{e}_p\left(\lambda(\mathbf{a})\right)\mu_{\mathbf{a}}(\mathbb{B})\right|\le$$
$$\le\sum_{\substack{\mathbf{a}\in\mathbb{Z}^s\setminus V^\perp\\ |a_j|\le\sqrt{P}\text{ for all }j}}\mu_{\mathbf{a}}(\mathbb{B})\#\{p\in\mathcal{P}:\ \mathbf{a}\in V_p^\perp\}\tag{26}$$
$$\ll(\log P)^s\max_{\substack{\mathbf{a}\in\mathbb{Z}^s\setminus V^\perp\\ |a_j|\le\sqrt{P}\text{ for all }j}}\#\{p\in\mathcal{P}:\ \mathbf{a}\in V_p^\perp\},$$

by the bound (20).

Now recall from the proof of Theorem 3 that for a given $\mathbf{a}\in\mathbb{Z}^s\setminus V^\perp$ with each $|a_j|\le\sqrt{P}$, there are at most $\log N/\log P\ll_{\mathcal{C},\mathbf{h}}1$ primes $p\in(P,2P]$ for which $\mathbf{a}\in V_p^\perp$. So (25) and (26) imply that (24) holds for all but $O(\sqrt{P})$ primes $p\in(P,2P]$.

13 Lines Instead of Curves

In this section we prove Theorem 4. We start with a simple lemma:

Lemma 4. *Let U be a subspace of $\mathbb{F}_p^s$ of dimension $\ell\le s-2$. There exists a subspace W of $\mathbb{F}_p^s$ of dimension $\ell+1$, containing U, such that if $w\in W\setminus U$ then $\max_j|w_j|>L:=p^{1/s}/3$.*

Proof. There are $(2L+1)^s$ vectors $r\in\mathbb{F}_p^s$ such that $\max_j|r_j|\le L$. For each such r there are $p^{\ell+1}-p^\ell$ vectors u in $\langle U,r\rangle\setminus U$, and thus there are $<(2L+1)^sp^{\ell+1}(1-1/p)$ vectors u such that $\langle U,u\rangle\setminus U$ contains a vector r with $\max_j|r_j|\le L$. For any vector w that is not included in any of these $\langle U,u\rangle$ we may take $W=\langle U,w\rangle$, and such a w exists since $(2L+1)^sp^{\ell+1}(1-1/p)<p^s-p^\ell$. □

Proof of Theorem 4. Given $p,\mathcal{C}$ and $\mathbf{h}$ we obtain a vector space $V^\perp\subset\mathbb{F}_p^s$, as at the start of section 3. By lemma 4 there exists an $(s-1)$-dimensional subspace W of $\mathbb{F}_p^s$, containing $V^\perp$, such that if $w\in W\setminus V^\perp$ then $\max_j|w_j|>L:=p^{1/s}/3$. Let $u_1,\dots,u_{s-1}$ be a basis for W (extending the basis for $V^\perp$

given at the start of section 8), and define $\lambda(u_j) = 0$ for $s-\ell+1 \le j \le s-1$. Let $\mathcal{L}$ be the line $\{\mathbf{b} \in \mathbb{F}_p^s : \mathbf{b}\cdot\mathbf{w} = \lambda(w) \text{ for all } w \in W\}$. Note that $V_{\mathcal{L}}^{\perp} = W$, and that the set of $\mathbf{a} \in V^{\perp}$ for which $\max_j |a_j| \le L$ for all j, is the same as the set of $\mathbf{a} \in V_{\mathcal{L}}^{\perp}$ for which $\max_j |a_j| \le L$ for all j. Thus by (22) we have that $\mu_{\mathcal{C},\mathbf{h}}(\mathbb{B}) = \mu_{\mathcal{L},\mathbf{id}}(\mathbb{B}) + O((\log p)^{s-1}/p^{1/s})$, and the first part of the result follows.

If there exists $\mathbf{x} \in \mathcal{C}$ such that $\mathbf{h}(\mathbf{x}) = \mathbf{0}$, then $\lambda(\mathbf{v}) = 0$ for all $\mathbf{v} \in V^{\perp}$, so $\mathbf{0} \in \mathcal{L}$. That is, our line goes through the origin. $\square$

Acknowledgement: Our thanks to Henri Darmon for a useful discussion concerning the geometry in Section 9.

References

[1] J. Beck and M. R. Khan, *On the distribution of of inverses modulo n,* Period. Math. Hungarica, **44** (2002), 147–155.

[2] E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math., **88** (1966) , 71–105.

[3] C. Cobeli and A. Zaharescu, *On the distribution of the $\mathbb{F}_p$-points on an affine curve in r dimensions,* Acta Arithmetica, **99** (2001), no 4, 321–329.

[4] C. Cobeli and A. Zaharescu, *The order of inverses* mod q, Mathematika, **47** (2000), 87–108.

[5] J. Dieudonné and A. Grothendieck, *Elements de geometrie algebrique. IV. Etude locale des schemas et des morphismes de schemas*, Inst. Hautes Etudes Sci. Publ. Math. **32** (1967)

[6] M. Drmota and R. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997.

[7] P. Erdös and P. Turán, *On a problem in the theory of uniform distribution I*, Indag. Math., **10** (1948), 370–378.

[8] A. Granville, D. Shiu and P. Shiu, *Residue races,* Preprint, 2002.

[9] J. F. Koksma, *Some theorems on diophantine inequalities,* Math. Centrum Scriptum no. 5, Amsterdam, 1950.

[10] M. Laczkovich, *Discrepancy estimates for sets with small boundary,* Studia Sci. Math. Hungar., **30** (1995), 105–109.

[11] H. Niederreiter and J. M. Wills, *Diskrepanz und Distanz von Massen bezuglich konvexer und Jordanscher Mengen,* Math. Z., **144** (1975), 125–134.

[12] P. Szüsz, *On a problem in the theory of uniform distribution*, Comptes Rendus Premier Congrès Hongrois, Budapest, 1952, 461–472 (in Hungarian).

[13] M. Vajaitu and A. Zaharescu, *Distribution of values of rational maps on the $\mathbb{F}_p$-points on an affine curve,* Monatsh. Math., **136** (2002), 81–86.

[14] H. Weyl, *On the volume of tubes,* Amer. J. Math. **61** (1939), 461–472.

[15] A. Zaharescu, *The distribution of the values of a rational function modulo a big prime,* J. Theor. Nombres Bordeaux (to appear).

[16] W. Zhang, *On the distribution of inverses modulo n*, J. Number Theory, **61** (1996), 301–310.

[17] Z. Zheng, *The distribution of zeros of an irreducible curve over a finite field,* J. Number Theory, **59** (1996), 106–118.