INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 5 (2005), #A04

ON THE DISTRIBUTION OF DISTANCES BETWEEN THE POINTS OF AFFINE CURVES OVER FINITE FIELDS

B.V. Petrenko

Department of Mathematics, Texas A&M University, College Station, Texas 77843-3368, USA

petrenko@math.tamu.edu

Received: 9/23/04, Accepted: 2/5/05, Published: 2/15/05

Abstract

Let $\mathbb{F}_q$ be a finite field with q elements, $\bar{\mathbb{F}}_q$ an algebraic closure of $\mathbb{F}_q$, and $\mathbb{A}^n\left(\bar{\mathbb{F}}_q\right)$ an n-dimensional affine space over $\bar{\mathbb{F}}_q$. Let $\mathcal{C}$ be an affine absolutely irreducible curve in $\mathbb{A}^n\left(\bar{\mathbb{F}}_q\right)$. We interpret the points of $\mathcal{C}$ over $\mathbb{F}_q$ as points in the cube $[-1,1]^{n-1}$. The main result of this paper is an asymptotic formula for the distribution of points of $\mathcal{C}$ in $[-1,1]^{n-1}$ provided the characteristic p of $\mathbb{F}_q$ is large, while n, $\log_p q$ are fixed, and the degree of $\mathcal{C}$ is bounded. When $p=q$, this becomes a recent result of Cobeli and Zaharescu.

Keywords: finite field, curves over finite fields, distribution of points, Bombieri's inequality, principle of Lipschitz, Weil's theorem.

AMS Subject Classification: 11G20, 11L05, 11L07, 11T23.

1. Introduction

This paper gives a generalization the main result of Cobeli and Zaharescu [3]. The main result of [3] generalizes that of Zheng [7] and partially generalizes that of Zhang [6]. This will be explained in detail below.

Let p be prime number, and $q=p^m$. Let $\mathcal{C}$ be a curve of degree d in an affine space $\mathbb{A}^r(\bar{\mathbb{F}}_q)$, where $\bar{\mathbb{F}}_q$ is an algebraic closure of a finite field with q elements $\mathbb{F}_q$. The goal of this paper is to study the distribution of the points of $\mathcal{C}$ in the cube $[-1,1]^{mr-1}\subseteq\mathbb{R}^{mr-1}$.

Let us begin by explaining how the points of $\mathcal{C}$ are interpreted as points of $[-1,1]^{mr-1}$. The resulting set will be called $\widetilde{\mathcal{N}_{\mathcal{C}}}$. We assume that $\mathcal{C}$ is not contained in a hyperplane [1] of $\mathbb{A}^{mr}(\bar{\mathbb{F}}_p)$. There is a bijection between $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ and $\{0,\dots,p-1\}$ via $l+p\mathbb{Z}\mapsto l$. Then

[1] In this paper, all hyperplanes are assumed to be affine, i.e. given by an equation $\sum_{k=1}^{mr}\alpha_k x_k = c$ for some $c,\alpha_1,\dots,\alpha_{mr}\in\mathbb{F}_p$.

$\mathbb{F}_q$ can be identified with $\{0,\dots,p-1\}^m$, and it makes sense to consider the set

$$\mathcal{N}_{\mathcal{C}} = \{\mathbf{x} = (x_1,\dots,x_{mr}) \in \{0,\dots,p-1\}^{mr} \mid \mathbf{x} \in \mathcal{C}\}. \tag{1}$$

In general, each such an identification of $\mathcal{C}$ with $\mathcal{N}_{\mathcal{C}}$ corresponds to a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. Nevertheless, the main result of this paper, Theorem 1, is independent of this choice.

Sometimes we will prefer to think of $\mathcal{N}_{\mathcal{C}}$ as a subset of $\mathbb{F}_p^{mr}$. This is legitimate because $\mathcal{N}_{\mathcal{C}}$ will be regarded as the domain of some p-periodic functions related to the exponential function $e^{\frac{2\pi i x}{p}}$.

Definition 1 *We will write $e(t)$ instead of $e^{2\pi i t}$.*

Next we consider the map

$$\widetilde{\ }\colon \mathbb{R}^{mr} \to \mathbb{R}^{mr-1},\ \mathbf{x} = (x_1,\dots,x_{mr}) \mapsto \widetilde{\mathbf{x}} = (\widetilde{x_1},\dots,\widetilde{x_{mr-1}}), \tag{2}$$

where

$$\widetilde{x_j} = \frac{x_{j+1} - x_j}{p}. \tag{3}$$

In this paper we obtain some asymptotic results about the the set

$$\widetilde{\mathcal{N}_{\mathcal{C}}} \tag{4}$$

endowed with the probability measure $\mu_{\mathcal{C}}$ defined by the formula

$$\mu_{\mathcal{C}}(\Omega) = \frac{\#\{\mathbf{x} \in \mathcal{N}_{\mathcal{C}} \mid \widetilde{\mathbf{x}} \in \Omega\}}{\#\mathcal{N}_{\mathcal{C}}}. \tag{5}$$

By placing some restrictions on $\mathcal{C}$, the denominator of (5) may be estimated by a well known theorem of A. Weil. Therefore, the point of this paper is to estimate the numerator of (5). This will involve the theorems of Bombieri ([1], Th. 6, p. 97), Davenport [4], and Weil. Our proof extends that of Cobeli and Zaharescu [3].

Before formulating the main result of this paper, Theorem 1, we would like to describe a certain class $\mathcal{D}_n(h)$ of subsets in $\mathbb{R}^n$. (A more general class has been introduced in an important paper of Davenport [4].) Our Definition 3 below is more restrictive than Davenport's because we additionally impose Conditions 4 and 5.

Remark 1 *It would be desirable not only to relax these restrictions in Definition 3, but also to generalize the main result of [4].*

To make the formulation of Definition 3 less cumbersome, we introduce the following auxiliary

Definition 2 *Let $X \subseteq \mathbb{R}^n$ and $\tau > 0$. We introduce the following tessellation of $\mathbb{R}^n$:*

$$\mathbb{R}^n = \bigcup_{\boldsymbol{t} \in \mathbb{Z}^n} (1/\tau)\boldsymbol{t} + [0, 1/\tau]^n. \tag{6}$$

1. *We define the sets $\mathcal{I}_\tau(X)$ and $\mathcal{E}_\tau(X)$ to be the unions of cubes in (6) contained in X and intersecting X, respectively.*
2. *For any $\varepsilon > 0$, we define the set $\mathcal{E}_{\tau,\varepsilon}(X) = X \cup \Delta_{\tau,\varepsilon}$, where $\Delta_{\tau,\varepsilon}$ consists of the points of $\mathcal{E}_\tau(X)$ whose standard distance to the boundary of $\mathcal{E}_\tau(X)$ is at least ε.*

Now we are ready to give the following

Definition 3 *Let $X \subseteq \mathbb{R}^n$ and h a positive integer. Then $X \in \mathcal{D}_n(h)$ if all of the following conditions are satisfied:*

1. *X is compact.*
2. *Any line parallel to one of the n coordinate axes intersects X in at most h intervals.*
3. *The same is true for any $m \in \{1, \ldots, n-1\}$ and any projection of X on any of the m-dimensional coordinate subspaces.*
4. *Let $V(\cdot)$ denote the (n-dimensional) volume of the set. Then $V(X)$ exists and has the following properties: $V(X) - V(\mathcal{I}_\tau(X)) = O_X(1/\tau)$ and $V(X) - V(\mathcal{E}_\tau(X)) = O_X(1/\tau)$ as $\tau \to +\infty$.*
5. *There exists $\tau_0 \geq 1$, depending on X, such that for any $\tau \geq \tau_0$,*
   (a) *All but $O_X(\tau^{n-1})$ vertices of the grid (6) in $\mathcal{I}_\tau(X)$ possess the following property. For a vertex v there exists a cube C_v of (6) with $v \in C_v \subseteq X$.*
   (b) *Any vertex $w \in \mathcal{E}_\tau(X) \setminus X$ of the grid (6) is a boundary point of $\mathcal{E}_\tau(X)$.*
   (c) *The sets $\mathcal{I}_\tau(X)$, $\mathcal{E}_\tau(X)$, and $\mathcal{E}_{\tau,\varepsilon}(X)$, for any $\varepsilon > 0$, satisfy Conditions 2 and 3 of this definition.*

In some situations, the values of h or n are irrelevant. Therefore, we consecutively define the following two classes of sets:

Definition 4 $\mathcal{D}_n = \bigcup_{h=1}^{\infty} \mathcal{D}_n(h)$.

Definition 5 $\mathcal{D} = \bigcup_{n=1}^{\infty} \mathcal{D}_n$.

At this point, we would like to recall the main result of Davenport [4]. We state it for a possibly smaller class of sets, as explained above.

Remark 2 *Let $X \in \mathcal{D}_n(h)$, $N(X)$ the number of points with integral coordinates in X, $V(X)$ the n-dimensional volume of X, $V_j(X)$ the sum of the j-dimensional volumes of the projections of X on all the j-dimensional coordinate subspaces, and $V_0(X) = 1$ by definition. Then*

$$|N(X) - V(X)| \leq \sum_{j=0}^{n-1} h^{n-j} V_j(X). \tag{7}$$

Next we define the function g_n. Its support is a polytope contained in the cube $[-1,1]^n$. The function g_n will be used to define the probability measure $\mu_{\mathcal{C}}$ in Theorem 1.

Definition 6

$$g_n(t_1, \ldots, t_n) = \max\left\{0, \min_{1\leq k\leq n}\left\{1, 1 - \sum_{s=1}^{k} t_s\right\} + \min_{1\leq k\leq n}\left\{0, \sum_{s=1}^{k} t_s\right\}\right\}. \tag{8}$$

The main result of this paper is the following

Theorem 1 *Let $\{q_j\}$ an increasing sequence of powers of primes $\{p_j\}$ with $\log_{p_j} q_j = m = const.$ Let $\mathcal{C}_j$ be an irreducible affine algebraic curve in $\mathbb{A}^r(\bar{\mathbb{F}}_{q_j})$ of degree $\leq d = const.$ Suppose that $\mathcal{C}_j$ is not contained in a hyperplane of $\mathbb{A}^{mr}(\bar{\mathbb{F}}_{p_j})$. Then for any $\Omega \in \mathcal{D}_{mr-1}$,*

$$\mu_{\mathcal{C}_j}(\Omega) = \int_{\Omega} g_{mr-1}(\boldsymbol{t}) d\boldsymbol{t} + O_{m,r,d,\Omega}\left(q_j^{-\frac{1}{2(mr+1)}} \ln^{\frac{mr}{mr+1}} q_j\right) \tag{9}$$

as $j \to +\infty$. (Here $\ln(\cdot)$ denotes the logarithm to base e.)

In other words, the measures $\mu_{\mathcal{C}_j}$ weakly converge, as $j \to +\infty$, to μ_{mr-1} with density function g_{mr-1}. We believe that Theorem 1 is of interest because g_{mr-1} is independent of d, $\{q_j\}$, $\{\mathcal{C}_j\}$.

Corollary 2 *If $m = 1$, then Theorem 1 becomes the main result of Cobeli and Zaharescu [3]. In turn, let $f \in \mathbb{Z}[x,y]$ be of degree $d \geq 2$, and suppose that f is absolutely irreducible modulo all large primes. If $\mathcal{C}_j$ is a plane curve obtained by reducing f modulo p_j, then we obtain the main result of Zheng [7]. Finally, if the curve is of the form $f(x,y) = xy - 1$, then we partially recover the main result of Zhang [6].*

Remark 3 *Theorem 1 may be strengthened as follows: m and r may be allowed to depend on the curve, provided they are bounded. This formulation of Theorem 1 leaves only finitely many possibilities for the values of m and r, and therefore the same proof is valid in this situation as well.*

Remark 4 *It may be of interest to prove that the formula*

$$\nu_{\mathcal{C}}(\Omega) = \frac{\#\widetilde{\mathcal{N}_{\mathcal{C}}} \cap \Omega}{\#\widetilde{\mathcal{N}_{\mathcal{C}}}}$$

defines an asymptotically well defined conditional probability measure on $\mathbb{R}^{mr-1}$, and to compare its asymptotic behavior to that of $\mu_{\mathcal{C}}$.

Remark 5 *By Weil's theorem, the number of points in the projective closure of the curve $\mathcal{C}_j$ is $q_j + O_{m,r,d}\left(q_j^{1/2}\right)$. By the assumptions in Theorem 1, however, the same estimate holds for the curve $\mathcal{C}_j$ itself. A similar observation about the more general Lang-Weil estimates of [5] has been made in [2], p. 120. This observation also allows us to apply the result of Bombieri ([1], Th. 6, p. 97).*

Acknowledgments. I thank Alexandru Zaharescu for suggesting the problem to me and for his generous sharing of ideas with me. I thank Nigel Boston for many very helpful discussions and for his wonderful hospitality. Anand Pilay has kindly pointed my attention to the paper of Z. Chatzidakis, L. van den Dries, and A. Macintyre [2]. Jeremy Tyson has very helpfully commented on the definition of $\mathcal{D}_n(h)$.

2. Proof of Theorem 1

To simplify the notation, we will denote p_j, q_j, $\mathcal{C}_j$ by p, q, $\mathcal{C}$, respectively.

2.1 The map *.

If $(x_1, \ldots, x_{mr}) \in \mathbb{R}^{mr}$, then define

$$y = \frac{x_1}{p},\ t_1 = \frac{x_2 - x_1}{p},\ \ldots,\ t_{mr-1} = \frac{x_{mr} - x_{mr-1}}{p}. \tag{10}$$

Let $(x_1, \ldots, x_{mr}) \in \mathcal{N}_{\mathcal{C}}$, then $0 \leq x_1, \ldots, x_{mr} \leq p-1$. Therefore

$$0 \leq y,\ y + \sum_{j=1}^{k} t_j = \frac{x_{k+1}}{p} \leq 1, \text{ where } k \in \{1, \ldots, mr-1\}. \tag{11}$$

This can be restated as follows:

$$0 \leq y \leq 1, \ -\sum_{j=1}^{k} t_j \leq y \leq 1 - \sum_{j=1}^{k} t_j, \ k \in \{1, \ldots, mr-1\}. \tag{12}$$

Based on these considerations, for $\Omega \in \mathcal{D}_{mr-1}$, *we define the set* Ω^* by

$$\Omega^* = \{(y, t_1, \ldots, t_{mr-1}) \in \mathbb{R} \times \Omega \mid y, t_1, \ldots, t_{mr-1} \text{ satisfy (12)}\}. \tag{13}$$

We remark that $\Omega^* \in \mathcal{D}_{mr}$.

From (13), we see that the set Ω^* can be described as a cylinder bounded by some two hypersurfaces, $h(t_1, \ldots, t_{mr-1})$ and $H(t_1, \ldots, t_{mr-1})$, as follows:

$$\Omega^* = \{(y, \mathbf{t}) \in \mathbb{R}^{mr} \mid 0 \leq y \leq 1, \, \mathbf{t} \in \Omega, \, h(\mathbf{t}) \leq H(\mathbf{t})\}. \tag{14}$$

We proceed to find equations of these hypersurfaces based on (12).

1. For a given $\mathbf{t} \in \Omega$, the smallest value of y is

$$h(t_1, \ldots, t_{mr-1}) = \max\{0, -t_1, \ldots, -t_1, + \ldots + t_{mr-1}\} = \\ - \min\{0, t_1, \ldots, t_1 + \ldots + t_{mr-1}\}. \tag{15}$$

2. For a given $\mathbf{t} \in \Omega$, the largest value of y is

$$H(t_1, \ldots, t_{mr-1}) = \min\{1, 1 - t_1, \ldots, 1 - t_1 - \ldots - t_{mr-1}\}. \tag{16}$$

We see that

$$g_{mr-1}(\mathbf{t}) = \max\{0, \ H(\mathbf{t}) - h(\mathbf{t})\}. \tag{17}$$

Therefore, the volume of Ω^* may be written as follows:

$$\mathrm{V}(\Omega^*) = \int_{\Omega} g_{mr-1}(t_1, \ldots, t_{mr-1}) dt_1 \ldots dt_{mr-1}. \tag{18}$$

We will use this formula in (54) of 2.4.3.

2.2 Main idea

We will use several rescalings below. One could think of them as changing the unit of length. We firstly pass from Ω^* to $p\Omega^*$, because there is a bijection between $\mathcal{N}_{\mathcal{C}}$ and the set of integral points of $p\Omega^*$, namely,

$$(x_1, \ldots, x_{mr}) = \mathbf{x} \mapsto p\mathbf{x}^* = (x_1, x_2 - x_1, \ldots, x_{mr} - x_{mr-1}). \tag{19}$$

In particular, we may express the numerator of (5) as follows:

$$\#\{\mathbf{x} \in \mathcal{N}_{\mathcal{C}} \mid \widetilde{\mathbf{x}} \in \Omega\} = N\left(\text{preimage of } \Omega \text{ under } \widetilde{\ }\right) = N(p\Omega^*). \tag{20}$$

Therefore, the problem is reduced to estimating $N(p\Omega^*)$.

Let $T \geq 1$. We further restrict the value of T in (39) and (49), and finally specify it in (53). Now we explain how T is used. We represent $\mathbb{R}^{mr}$ as a disjoint union of cubes:

$$\mathbb{R}^{mr} = \bigcup_{k_1,\ldots,k_{mr}\in\mathbb{Z}} \left(k_1\frac{p}{T} + \left[0, \frac{p}{T}\right)\right) \times \ldots \times \left(k_{mr}\frac{p}{T} + \left[0, \frac{p}{T}\right)\right). \tag{21}$$

Let $\mathcal{I}_{p/T}\left(p\Omega^*\right)$ be the union of cubes in (21) contained in $p\Omega^*$, and $\mathcal{E}_{p/T}\left(p\Omega^*\right)$ the union of cubes in (21) intersecting $p\Omega^*$. Then

$$\mathcal{I}_{p/T}\left(p\Omega^*\right) \subseteq p\Omega^* \subseteq \mathcal{E}_{p/T}\left(p\Omega^*\right). \tag{22}$$

In below, we will show that each of the two sets $\mathcal{I}_{p/T}\left(p\Omega^*\right)$ and $\mathcal{E}_{p/T}\left(p\Omega^*\right)$ contain

$$T^{mr}\mathrm{V}(\Omega^*) + O_\Omega(T^{mr-1}) \tag{23}$$

cubes of the tessellation (21). Then in (48) we will estimate the number of integral points each such a cube contains. This in turn will yield (51), an estimate for $N(p\Omega^*)$.

2.3 Proof of (23)

For the purpose of proving (23), we may assume that the cubes in (21) are replaced with the closed cubes. Indeed, since $p\Omega^*$ is closed, the number $\mathcal{A}_T$ of cubes in (21) contained in $p\Omega^*$ equals the number $\mathcal{A}_{c,T}$ of the closures of cubes in (21) contained in $p\Omega^*$. Also, the number $\mathcal{B}_T$ of cubes in (21) intersecting $p\Omega^*$ is at most the number $\mathcal{B}_{c,T}$ of the closures of cubes in (21) intersecting $p\Omega^*$. Then $\mathcal{A}_{c,T} = \mathcal{A}_T \leq \mathcal{B}_T \leq \mathcal{B}_{c,T}$. Hence, if we prove that both $\mathcal{A}_{c,T}$ and $\mathcal{B}_{c,T}$ are $T^{mr}\mathrm{V}(\Omega^*) + O_\Omega(T^{mr-1})$, then the same estimate will hold for $\mathcal{A}_T$ and $\mathcal{B}_T$.

Now we rescale $p\Omega^*$ to $\Omega^* \subseteq [-1,\ 1]^{mr}$, the cube $[-1,\ 1]^{mr}$ being tessellated with the cubes of side length $1/T$. *We will refer to them in this section only as the "tessellation cubes".* From $\Omega \in \mathcal{D}_{mr-1}$ we conclude that $\Omega^* \in \mathcal{D}_{mr}$. Then $\Omega^* \in \mathcal{D}_{mr}(h)$ for some positive integer h. We will prove the estimate (23) in three steps below. We will also assume that T is chosen large enough to satisfy the conditions of Definition 3. This is legitimate, because from (53) it will follow that $T \to +\infty$ as $p \to +\infty$.

1. Let $\mathcal{I}_T\left(\Omega^*\right)$ be the union of the tessellation cubes contained in Ω^*. Then

(a) $\mathcal{I}_T\left(\Omega^*\right) \subseteq \Omega^*$.

(b) $\mathcal{I}_T\left(\Omega^*\right) \in \mathcal{D}_{mr}(h)$ by Condition 5c of Definition 3.

(c) $N_T\left(\mathcal{I}_T\left(\Omega^*\right)\right) = N_T\left(\Omega^*\right) + O_\Omega\left(T^{mr-1}\right)$, where $N_T(\cdot)$ denotes the number of points whose coordinates are multiples of $1/T$. This claim follows from Condition 5a of Definition 3.

(d) *The number of cubes of (21) contained in* $\mathcal{I}_{p/T}\left(p\Omega^*\right)$ is $V_T\left(\mathcal{I}_T\left(\Omega^*\right)\right) = T^{mr}V\left(\mathcal{I}_T\left(\Omega^*\right)\right) = \mathcal{A}_T$, where $V_T(\cdot)$ denotes the (mr-dimensional) volume of the set measured with respect to the unit length $1/T$.

(e) By the inequality (7), rescaled with respect to the unit length $1/T$,

$$\left|V_T\left(\mathcal{I}_T\left(\Omega^*\right)\right) - N_T\left(\Omega^*\right)\right| \leq O_\Omega\left(T^{mr-1}\right) + \sum_{j=0}^{mr-1} V_{T,j}\left(\mathcal{I}_T\left(\Omega^*\right)\right) h^{mr-1} \leq$$

$$O_\Omega\left(T^{mr-1}\right) + \sum_{j=0}^{mr-1} T^j V_j\left(\Omega^*\right) h^{mr-j} = O_\Omega\left(T^{mr-1}\right). \quad (24)$$

In the next step, we obtain a similar estimate for $\left|V_T\left(\mathcal{E}_T\left(\Omega^*\right)\right) - N_T\left(\Omega^*\right)\right|$, where $\mathcal{E}_T\left(\Omega^*\right)$ is the union of the tessellation cubes intersecting Ω^*.

2. We observe the following properties of $\mathcal{E}_T\left(\Omega^*\right)$.

(a) $\Omega^* \subseteq \mathcal{E}_T\left(\Omega^*\right)$.

(b) $\mathcal{E}_T\left(\Omega^*\right) \in \mathcal{D}_{mr}(h)$ by Condition 5c of Definition 3.

(c) $N_T\left(\mathcal{E}_{T,\varepsilon}\left(\Omega^*\right)\right) = N_T\left(\Omega^*\right)$, by Condition 5b of Definition 3.

(d) $V_T\left(\mathcal{E}_{T,\varepsilon}\left(\Omega^*\right)\right) = T^{mr}V\left(\mathcal{E}_{T,\varepsilon}\left(\Omega^*\right)\right) \to T^{mr}V\left(\mathcal{E}_T\left(\Omega^*\right)\right) = \mathcal{B}_T$ as $\varepsilon \to 0$. Also $\mathcal{B}_T$ is equal to *the number of cubes of (21) contained in* $\mathcal{E}_T\left(\Omega^*\right)$

(e) From $\mathcal{E}_T\left(\Omega^*\right) \subseteq [-1,1]^{mr}$, we conclude that there is a positive number κ (independent of T) such that $V_j\left(\mathcal{E}_T\left(\Omega^*\right)\right) \leq \kappa$ for all j.

(f) By the inequality (7),

$$\left|V_T\left(\mathcal{E}_{T,\varepsilon}\left(\Omega^*\right)\right) - N_T\left(\Omega^*\right)\right| \leq \kappa \sum_{j=0}^{mr-1} T^j h^{mr-j}. \quad (25)$$

Therefore, taking the limit as $\varepsilon \to 0$, we obtain

$$\left|V_T\left(\mathcal{E}_T\left(\Omega^*\right)\right) - N_T\left(\Omega^*\right)\right| = O_\Omega\left(T^{mr-1}\right). \quad (26)$$

3. By the triangle inequality, (24), and (26), we conclude that

$$|\mathcal{A}_T - \mathcal{B}_T| = O_\Omega\left(T^{mr-1}\right). \tag{27}$$

At this point, we would like to recall that by Condition 4 of Definition 3, $V\left(\mathcal{I}_T\left(\Omega^*\right)\right) - V\left(\Omega^*\right) = O_\Omega\left(1/T\right)$ and $V\left(\mathcal{E}_T\left(\Omega^*\right)\right) - V\left(\Omega^*\right) = O_\Omega\left(1/T\right)$. This remark together with (27) finally proves (23).

Next section will deal with the number $\mathfrak{N}(\mathbf{J})$ of integral points $\mathbf{x}$ of $\mathcal{N}_\mathcal{C}$ such that $p\mathbf{x}^*$ belongs to a cube of the subdivision (21). The estimation of $\mu_\mathcal{C}(\Omega)$ will be done in 2.4.3.

2.4 Estimating $\mathfrak{N}(\mathbf{J})$

Let $\mathbf{J}$ be a cube in the subdivision (21). Then

$$\mathfrak{N}(\mathbf{J}) = \#\{\mathbf{x} \in \mathcal{N}_\mathcal{C} \mid p\mathbf{x}^* = (x_1, x_2 - x_1, \ldots, x_{mr} - x_{mr-1}) \in \mathbf{J}\}. \tag{28}$$

We write the cube $\mathbf{J}$ as a direct product of intervals:

$$\mathbf{J} = \mathcal{T}_1 \times \ldots \times \mathcal{T}_{mr}. \tag{29}$$

This allows us to express $\mathfrak{N}(\mathbf{J})$ in terms of the characteristic functions $\chi_{\mathcal{T}_j}$ of the intervals $\mathcal{T}_1, \ldots, \mathcal{T}_{mr}$ as follows:

$$\begin{aligned}\mathfrak{N}(\mathbf{J}) = \sum_{\mathbf{y}=(y_1,\ldots,y_{mr})\in\mathbf{J}} \chi_{\mathcal{T}_1}(y_1)\chi_{\mathcal{T}_2}(y_2)\ldots\chi_{\mathcal{T}_{mr}}(y_{mr}) = \\ \{\text{recall that } y_1 = x_1,\ y_2 = x_2 - x_1, \ldots, y_{mr} = x_{mr} - x_{mr-1}\} \\ \sum_{\mathbf{x}=(x_1,\ldots,x_{mr})\in\mathcal{N}_\mathcal{C}} \chi_{\mathcal{T}_1}(x_1)\chi_{\mathcal{T}_2}(x_2 - x_1)\ldots\chi_{\mathcal{T}_{mr}}(x_{mr} - x_{mr-1}).\end{aligned} \tag{30}$$

Now we can write the characteristic function $\chi_\mathcal{T}(x)$ as an exponential sum. In the the next formula, we assume that $x \in \mathcal{J}$, where $\mathcal{J}$ is an interval (closed or not) of length $\leq p$.

$$\chi_\mathcal{T}(x) = p^{-1}\sum_{z\in\mathcal{T}} \sum_{k(\mathrm{mod}p)} e(k(x-z)/p), \tag{31}$$

where the sum $\sum_{z\in\mathcal{T}}$ is taken over the integral points of $\mathcal{T}$. We substitute (31) in (30), and change the order of summation:

$$\mathfrak{N}(\mathbf{J}) = p^{-mr} \sum_{\mathbf{k}=(k_1,\ldots,k_{mr})\in\mathbb{F}_p^{mr}} \prod_{j=1}^{mr} \left(\sum_{y_j\in\mathcal{T}_j} e(-k_j y_j/p)\right) S_\mathbf{k}, \tag{32}$$

where

$$S_\mathbf{k} = \sum_{\mathbf{x}\in\mathcal{N}_\mathcal{C}} e(\mathcal{L}_\mathbf{k}(\mathbf{x})/p) \tag{33}$$

and, in turn,

$$\mathcal{L}_{\mathbf{k}}(\mathbf{x}) = k_{mr}x_{mr} + \sum_{s=1}^{mr-1}(k_s - k_{s+1})x_s. \tag{34}$$

Since we require that $\mathcal{C}$ does not lie in a hyperplane of $\mathbb{A}^{mr}(\bar{\mathbb{F}}_p)$, the linear form $\mathcal{L}_{\mathbf{k}}(\mathbf{x})$ is constant on $\mathcal{C}$ if and only if $k_1 = \ldots = k_{mr} = 0$. (At this point we would like to recall that that our hyperplanes are assumed to be affine). We next show that the sum of the terms in (32) with $k_1 = \ldots = k_{mr} = 0$ is the *main term* in (32). The sum of the remaining terms will be proved to be of the lower order of magnitude, and therefore is the *error term*. We denote the main term and the error term by $M(\mathbf{J})$ and $E(\mathbf{J})$, respectively. Then

$$\mathfrak{N}(\mathbf{J}) = M(\mathbf{J}) + E(\mathbf{J}) \tag{35}$$

We will make this formula more precise below, with the final result stated in (50) of 2.4.3.

2.4.1 The main term in (35)

Each $\mathcal{T}_j$ has length p/T (we denote this by $|\mathcal{T}_j| = p/T$); therefore

$$\mathrm{V}(\mathbf{J}) = (p/T)^{mr}. \tag{36}$$

By (32) and (36),

$$\frac{M(\mathbf{J})}{p^{-mr}\#\mathcal{C}(\mathbb{F}_q)} = \prod_{j=1}^{mr} N(\mathcal{T}_j) = \prod_{j=1}^{mr}\left(p/T + O_{m,r,d}(1)\right) = \mathrm{V}(\mathbf{J})\left(1 + O_{m,r,d}\left(T/p\right)\right). \tag{37}$$

Hence, substituting (36) in (37), we have

$$M(\mathbf{J}) = T^{-mr}\#\mathcal{C}(\mathbb{F}_q)\left(1 + O_{m,r,d}\left(T/p\right)\right). \tag{38}$$

At this point we further assume that

$$1 \le T \le p^{1/2}. \tag{39}$$

We substitute (39) in (38):

$$M(\mathbf{J}) = T^{-mr}\#\mathcal{C}(\mathbb{F}_q)\left(1 + O_{m,r,d}\left(p^{-1/2}\right)\right). \tag{40}$$

2.4.2 The error term in (35)

We need to estimate the error term

$$E(\mathbf{J}) = p^{-mr}\sum_{(0,\ldots,0)\neq(k_1,\ldots,k_{mr})\in\mathbb{F}_p^{mr}}\prod_{j=1}^{mr}\left(\sum_{y_j\in\mathcal{T}_j} e\left(\frac{-k_j y_j}{p}\right)\right) S_{\mathbf{k}}. \tag{41}$$

To estimate the sums of the form $\sum_{y_j\in\mathcal{T}_j}$ in (41), we need the following well known lemma.

Lemma 3 *Let $\|\cdot\|$ denote the distance to the nearest integer on the real line. Then for any real a and integers $l \geq 1$ and n, we have*

$$\left| \sum_{j=n+1}^{n+l} e(ja) \right| \leq \min\left(l, \frac{1}{2\|a\|}\right) \tag{42}$$

Remark 6 *We assume that if $a = 0$, then $min\,(l, 1/(2\|a\|)) = l$.*

Now we return to the question of estimating the sums of the form $\sum_{y_j \in \mathcal{T}_j}$ in (41). By Lemma 3,

$$\left| \sum_{y_j \in \mathcal{T}_j} e\left(-k_j y_j/p\right) \right| \leq \min\left\{ |\mathcal{T}_j| + 1, \frac{1}{2\|k_j/p)\|} \right\}. \tag{43}$$

We use the inequalities $1/x \leq 2/(x+1)$ and $1 + 1/x \leq 2$, for $x \geq 1$, and substitute (43) in (41):

$$E(\mathbf{J}) \leq \sum_{(0,\ldots,0) \neq (k_1,\ldots,k_{mr}) \in \mathbb{F}_p^{mr}} \prod_{j=1}^{mr} \frac{1}{p} \left(\min\left\{ p+1, \frac{p}{|k_j|} \right\} \right) |S_{\mathbf{k}}| \ll_{mr}$$
$$\sum_{(0,\ldots,0) \neq (k_1,\ldots,k_{mr}) \in \mathbb{F}_p^{mr}} \prod_{j=1}^{mr} \left(\frac{1}{1+|k_j|} \right) |S_{\mathbf{k}}|. \tag{44}$$

Next, for each $\mathbf{x} \neq \mathbf{0}$, our hypotheses on the curve $\mathcal{C}$ (see also Remark 5 above) allow us to apply Bombieri's inequality (see [1], Th. 6, p. 97):

$$S_{\mathbf{k}} = O_{m,r,d}\left(q^{1/2}\right). \tag{45}$$

We substitute (45) in (44):

$$|E(\mathbf{J})| = O_{m,r,d}\left(q^{1/2} \ln^{mr} q\right). \tag{46}$$

2.4.3 Conclusion

We recall that Weil's theorem states that (see also Remark 5 above)

$$\#\mathcal{C}(\mathbb{F}_q) = \#\mathcal{N}_{\mathcal{C}} = q + O_{m,r,d}\left(q^{1/2}\right). \tag{47}$$

We substitute (40), (46), and (47) in (35):

$$\mathfrak{N}(\mathbf{J}) = T^{-mr}\left(1 + O_{m,r}\left(p^{-1/2}\right)\right)\left(q + O_{m,r,d}\left(q^{1/2}\right)\right) + O_{m,r,d}\left(q^{1/2}\ln^{mr} q\right) =$$
$$qT^{-mr}\left(1 + O_{m,r,d}\left(q^{\frac{1}{2}}\right) + O_{m,r,d}\left(q^{1-\frac{1}{2m}}\right) + O_{m,r,d}\left(q^{\frac{1}{2}-\frac{1}{2m}}\right)\right) + O_{m,r,d}\left(q^{\frac{1}{2}}\ln^{mr} q\right). \tag{48}$$

At this point, we further restrict T as follows:

$$\frac{q^{1-\frac{1}{2m}}}{T^{mr}} \leq q^{\frac{1}{2}} \ln^{mr} q. \tag{49}$$

This allows us to simplify (48) in the following way:

$$\mathfrak{N}(\mathbf{J}) = q/T^{mr} + O_{m,r,d}\left(q^{1/2} \ln^{mr} q\right). \tag{50}$$

2.5 Estimating $\mu_{\mathcal{C}}(\Omega)$

The formula (20) allows us to estimate the numerator in (5) as the product of the right-hand sides of (23) and (50):

$$\begin{aligned}\#\{\mathbf{x} \in \mathcal{N}_{\mathcal{C}} \mid \widetilde{\mathbf{x}} \in \Omega\} = N(p\Omega^*) = \\ \left(q/T^{mr} + O_{m,r,d}\left(q^{1/2} \ln^{mr} q\right)\right)\left(T^{mr}\mathrm{V}(\Omega^*) + O_{\Omega}\left(T^{mr-1}\right)\right) = \\ q\mathrm{V}(\Omega^*) + O_{m,r,d,\Omega}\left(q/T\right) + O_{m,r,d,\Omega}\left(T^{mr} q^{1/2} \ln^{mr} q\right).\end{aligned} \tag{51}$$

Next, the denominator in (5) can be estimated by (47). This yields

$$\mu_{\mathcal{C}}(\Omega) = \mathrm{V}(\Omega^*) + O_{m,r,d,\Omega}\left(T^{mr} q^{-1/2} \ln^{mr} q\right) + O_{m,r,d,\Omega}(1/T). \tag{52}$$

Now we specify T as the root of the equation $T^{mr} q^{-1/2} \ln^{mr} q = 1/T$:

$$T = q^{\frac{1}{2(mr+1)}} \ln^{\frac{-mr}{mr+1}} q. \tag{53}$$

(We remark that (39), (49), and (53) agree with each other.) The value of T given by (53) allows us to have only one error term in (52):

$$\mu_{\mathcal{C}}(\Omega) = \mathrm{V}(\Omega^*) + O_{m,r,d,\Omega}\left(q^{\frac{-1}{2(mr+1)}} \ln^{\frac{mr}{mr+1}} q\right), \tag{54}$$

and we may apply (18). This finally proves Theorem 1.

References

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

[2] Z. Chatzidakis, L. van den Dries, and A. Macintyre *Definable sets over finite fields.* J. Reine Angew. Math. 427 (1992), 107-135

[3] C. Cobeli and A. Zaharescu, *A question on the distribution of points on a curve over a finite field.* Acta Univ. Apulensis Math. Inform. No. 4 (2002), 65-76.

[4] H. Davenport, *On a principle of Lipschitz.* J. London Math. Soc. 26, (1951). 179-183.

[5] S. Lang and A. Weil, *Number of points of varieties in finite fields.* Amer. J. Math. 76, (1954). 819-827.

[6] W. Zhang, *On the distribution of inverses modulo n.* J. Number Theory 61 (1996), no. 2, 301-310.

[7] Z. Zheng, *The distribution of zeros of an irreducible curve over a finite field.* J. Number Theory 59 (1996), no. 1, 106-118.