Journal of Number Theory 133 (2013) 2863–2873

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

# On the distribution of values and zeros of polynomial systems over arbitrary sets ☆

Bryce Kerr, Igor E. Shparlinski *

*Department of Computing, Macquarie University, Sydney, NSW 2109, Australia*

ARTICLE INFO

*Article history:*
Received 8 January 2013
Accepted 12 February 2013
Available online 23 April 2013
Communicated by Wenzhi Luo

*MSC:*
11D79
11K38
11L07

*Keywords:*
Polynomials over finite fields
Distribution of values
Distribution of zeros
Discrepancy

ABSTRACT

Let $G_1, \ldots, G_n \in \mathbb{F}_p[X_1, \ldots, X_m]$ be $n$ polynomials in $m$ variables over the finite field $\mathbb{F}_p$ of $p$ elements. A result of É. Fouvry and N.M. Katz shows that under some natural condition, for any fixed $\varepsilon$ and sufficiently large prime $p$ the vectors of fractional parts

$$\left(\left\{\frac{G_1(\mathbf{x})}{p}\right\}, \ldots, \left\{\frac{G_n(\mathbf{x})}{p}\right\}\right), \quad \mathbf{x} \in \Gamma,$$

are uniformly distributed in the unit cube $[0,1]^n$ for any cube $\Gamma \in [0, p-1]^m$ with the side length $h \geqslant p^{1/2}(\log p)^{1+\varepsilon}$. Here we use this result to show the above vectors remain uniformly distributed, when $\mathbf{x}$ runs through a rather general set. We also obtain new results about the distribution of solutions to system of polynomial congruences.



## 1. Introduction

Let $p$ be a prime and let $\mathbb{F}_p$ be the finite field of $p$ elements, which we assume to be represented by the set $\{0, 1, \ldots, p-1\}$.

Given $n$ polynomials $G_j(X_1, \ldots, X_m) \in \mathbb{F}_p[X_1, \ldots, X_m]$, $j = 1, \ldots, n$, in $m$ variables with integer coefficients, we consider the following points formed by fractional parts:

$$\left(\left\{\frac{G_1(\mathbf{x})}{p}\right\}, \ldots, \left\{\frac{G_n(\mathbf{x})}{p}\right\}\right), \quad \mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{F}_p^m. \tag{1}$$

☆ This work was supported in part by ARC Grant DP130100237.
* Corresponding author.
*E-mail addresses:* bryce.kerr@mq.edu.au (B. Kerr), igor.shparlinski@mq.edu.au (I.E. Shparlinski).

0022-314X/$ – see front matter 
http://dx.doi.org/10.1016/j.jnt.2013.02.012

We say that the polynomials $G_1, \ldots, G_n$ are *degree* 2 *independent over* $\mathbb{F}_p$ if any nontrivial linear combinations $a_1G_1 + \cdots + a_nG_n$ is a polynomial of degree at least 2 over $\mathbb{F}_p$.

Let $\mathfrak{G}_{m,n,p}$ denote the family of polynomial systems $\{G_1, \ldots, G_n\}$ of $n$ polynomials in $m$ variables that are degree 2 independent over $\mathbb{F}_p$.

Fouvry and Katz [3] have shown that for any $\{G_1, \ldots, G_n\} \in \mathfrak{G}_{m,n,p}$, the points (1) are uniformly distributed in the unit cube $[0,1]^n$, where $\mathbf{x}$ runs through the integral points in any cube $\Gamma \in [0, p-1]^m$ with side length $h \geqslant p^{1/2}(\log p)^{1+\varepsilon}$. Here we use several of the results from [3] combined with some ideas of Schmidt [7] to obtain a similar uniformity of distribution result when $\mathbf{x}$ runs through a set from a very general family. For example, this holds for $\mathbf{x}$ that belong to the dilate $p\Omega$ of a convex set $\Omega \in [0,1]^m$ of Lebesgue measure at least $p^{-1/2+\varepsilon}$ for any fixed $\varepsilon > 0$ and sufficiently large $p$. We note that standard way of moving from boxes to arbitrary convex sets, via the isotropic discrepancy, see [7, Theorem 2], leads to a much weaker result which is nontrivial only for sets $\Omega \in [0,1]^m$ of Lebesgue measure at least $p^{-1/2m+\varepsilon}$.

As in [8], it is crucial for our approach that the error term in the aforementioned asymptotic formula of [3] depends on the size of the cube $\Gamma \in [0, p-1]^m$ and decreases rapidly together with the size of $\Gamma$. We note that a similar idea has also recently been used in [4] in combination with a new upper bound on the number of zeros of multivariate polynomial congruences in small cubes.

Furthermore, given $n$ polynomials $F_j(X_1, \ldots, X_m) \in \mathbb{Z}[X_1, \ldots, X_m]$, $j = 1, \ldots, n$, we consider the distribution of points in the set $\mathcal{X}_p$, of solutions $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{F}_p^m$ to the system of congruences

$$F_j(\mathbf{x}) \equiv 0 \pmod p, \quad j = 1, \ldots, n. \tag{2}$$

Let $\mathfrak{F}_{m,n}$ denote the family of polynomial systems $\{F_1, \ldots, F_n\}$ of $n$ polynomials in $m \geqslant n+1$ variables with integer coefficients, such that the solution set of the system of equations (over $\mathbb{C}$)

$$F_j(\mathbf{x}) = 0, \quad j = 1, \ldots, n,$$

has at least one absolutely irreducible component of dimension $m - n$ and no absolutely irreducible component is contained in a hyperplane. For sufficiently large $p$ all absolutely irreducible components remain of the same dimension and are absolutely irreducible modulo $p$, so by the Lang–Weil theorem [6] we have

$$\#\mathcal{X}_p = \nu p^{m-n} + O\left(p^{m-n-1/2}\right), \tag{3}$$

where $\nu$ is the number of absolutely irreducible components of $\mathcal{X}_p$ of dimension $m - n$. It is shown in [8], that for a rather general class of sets $\Omega$, including all convex sets, we have

$$T_p(\Omega) = \#\mathcal{X}_p\left(\mu(\Omega) + O\left(p^{-1/2(n+1)} \log p\right)\right) \tag{4}$$

with

$$T_p(\Omega) = \#(\mathcal{X}_p \cap \Omega).$$

The asymptotic formula (4) is based on a combination of a result of Fouvry [2] and Schmidt [7].

Here we show that for a more restricted class of sets, which includes such natural sets as $m$-dimensional balls, one can improve (4) and obtain an asymptotic formula which is nontrivial provided that

$$\mu(\Omega) \geqslant p^{-1/2+\varepsilon}$$

for any fixed $\varepsilon > 0$ and a sufficiently large $p$, while (4) is nontrivial only under the condition $\mu(\Omega) \geqslant p^{-1/2(n+1)+\varepsilon}$ (but applies to a wider class of sets).

## 2. Well and very well shaped sets

Let $\mathbb{T}_s = (\mathbb{R}/\mathbb{Z})^s$ be the $s$-dimensional unit torus.

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

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

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

$$\Omega_\varepsilon^+ = \{\mathbf{u} \in \mathbb{T}_m \backslash \Omega\colon \operatorname{dist}(\mathbf{u}, \Omega) < \varepsilon\}$$

and

$$\Omega_\varepsilon^- = \{\mathbf{u} \in \Omega\colon \operatorname{dist}(\mathbf{u}, \mathbb{T}_m \backslash \Omega) < \varepsilon\}.$$

We say that a set $\Omega$ is $C$-*well shaped* if

$$\mu(\Omega_\varepsilon^\pm) \leqslant C\varepsilon, \tag{5}$$

for some constant $C$, where $\mu$ is the Lebesgue measure on $\mathbb{T}_m$.

It is known that any convex set in $\mathbb{T}_m$ is $C$-well shaped for some $C$ depending only on $m$, see [7, Lemma 1].

Finally, a very general result of Weyl [9, Eq. (2)] (taken with $n = m$ and $\nu = n - 1$), that actually expresses $\mu(\Omega_\varepsilon^\pm)$ via a finite sum of powers $\varepsilon^i$, $i = 1, \dots, m$ in the case when the boundary of $\Omega$ is manifold of dimension $n - 1$. Examining the constants in this expansion we see that any such set with a bounded surface size is $C$-well shaped for some $C$.

Furthermore, for $C > 0$, we say that a set $\Omega \subseteq \mathbb{T}_m$ is $C$-*very well shaped* if for every $\varepsilon > 0$ the measures of the sets $\Omega_\varepsilon^\pm$ exist and satisfy

$$\mu(\Omega_\varepsilon^\pm) \leqslant C\left(\mu(\Omega)^{1-1/m}\varepsilon + \varepsilon^m\right). \tag{6}$$

The most natural example of a $C$-very well shaped set (for some $C > 0$ depending only on $m$) is a Euclidean ball.

We recall that the notation $A(t) \ll B(t)$ is equivalent to $A(t) = O(B(t))$, which means that there exists some absolute constant, $\alpha$, such that $|A(t)| \leqslant \alpha B(t)$ for all values of $t$ within a certain range. Throughout the paper, the implied constants in symbols '$O$' and '$\ll$' may depend on the constant $C$ in (5) and (6) and it may also depend on the polynomial system $\{F_1, \dots, F_n\} \in \mathfrak{F}_{m,n}$ (but does not depend on the polynomial system $\{G_1, \dots, G_n\} \in \mathfrak{G}_{m,n,p}$).

## 3. Discrepancy

Given a sequence $\Xi$ of $N$ points

$$\Xi = \{(\xi_{k,1}, \dots, \xi_{k,n})\}_{k=1}^N, \tag{7}$$

in $\mathbb{T}_n$, we define its *discrepancy* as

$$\Delta(\Xi) = \sup_{\Pi \subseteq \mathbb{T}_n} \left| \frac{\#A(\Xi, \Pi)}{N} - \lambda(\Pi) \right|,$$

where $A(\Xi, \Pi)$ is the number of $k \leqslant N$ such that $(\xi_{k,1}, \dots, \xi_{k,n}) \in \Pi$, $\lambda$ is the Lebesgue measure on $\mathbb{T}_n$ and the supremum is taken over all boxes

$$\Pi = [\alpha_1, \beta_1) \times \cdots \times [\alpha_n, \beta_n) \subseteq \mathbb{T}_n, \tag{8}$$

see [1,5].

We also define the discrepancy of an empty sequence as 1.

## 4. Main results

For a set $\Omega \subseteq \mathbb{T}_m$ let $D(\Omega)$ be the discrepancy of the points

$$\left(\left\{\frac{G_1(\mathbf{x})}{p}\right\}, \ldots, \left\{\frac{G_n(\mathbf{x})}{p}\right\}\right), \quad \mathbf{x} \in p\Omega.$$

**Theorem 1.** *For any polynomial system $\{G_1, \ldots, G_n\} \in \mathfrak{G}_{m,n,p}$ and any $C$-well shaped set $\Omega \in \mathbb{T}_m$ for some constant $C$, we have*

$$D(\Omega) \ll \mu(\Omega)^{-1} p^{-1/2} (\log p)^{n+2}.$$

We can get a sharper error term for the case of $C$-very well shaped sets.

**Theorem 2.** *For any polynomial system $\{G_1, \ldots, G_n\} \in \mathfrak{G}_{m,n,p}$ and any $C$-very well shaped set $\Omega \in \mathbb{T}_m$, we have*

$$D(\Omega) \ll \mu(\Omega)^{-1/m} p^{-1/2} (\log p)^{n+2}.$$

We prove the following

**Theorem 3.** *For any polynomial system $\{F_1, \ldots, F_n\} \in \mathfrak{F}_{m,n}$ and any $C$-very well shaped set $\Omega \in \mathbb{T}_m$, we have*

$$T_p(\Omega) = \#\mathcal{X}_p\left(\mu(\Omega) + O\left(\mu(\Omega)^{1-1/m} p^{-1/2(n+1)} \log p + p^{-1/2} (\log p)^{n+2}\right)\right).$$

## 5. Exponential sum and congruences

Typically the bounds on the discrepancy of a sequence are derived from bounds of exponential sums with elements of this sequence. The relation is made explicit in the celebrated *Koksma–Szüsz inequality*, see [1, Theorem 1.21], which we present in the following form.

**Lemma 4.** *Suppose that for the sequence of points (7) for some integer $L \geqslant 1$ and the real number $S$ we have*

$$\left|\sum_{k=1}^{N} \exp\left(2\pi i \sum_{j=1}^{n} a_j \xi_{k,j}\right)\right| \leqslant S,$$

*for all integers $-L \leqslant a_j \leqslant L$, $j = 1, \ldots, n$, not all equal to zero. Then,*

$$D(\Gamma) \ll \frac{1}{L} + \frac{(\log L)^n}{N} S,$$

*where the implied constant depends only on $n$.*

To use Lemma 4 we need the following bound of Fouvry and Katz [3, Eq. (10.6)]

**Lemma 5.** *For any polynomial system $\{G_1, \dots, G_n\} \in \mathfrak{G}_{m,n,p}$ and arbitrary integers $u$ and $w$ with $1 \leqslant w < p$, uniformly over all non-zero modulo $p$ integer vectors $(a_1, \dots, a_n)$ we have*

$$\sum_{x_1,\dots,x_m=u}^{u+w} \exp\left(\frac{2\pi i}{p}\sum_{j=1}^{n} a_j G_j(x_1,\dots,x_m)\right) \ll p^{1/2} w^{m-1} \log p.$$

**Proof.** The bound in [3, Eq. (10.6)], that gives the desired result for $u = 0$ is uniform in polynomials $G_1, \dots, G_m$. It now remains to notice that the property of being degree 2 independent is preserved under the change of variables $X_j \to X_j + u$, $j = 1, \dots, m$. $\square$

The proof of Theorem 3 is based on the following bound for $T_p(\mathcal{C})$ for a cube $\mathcal{C}$ which is essentially a result of Fouvry [2]

**Lemma 6.** *For any polynomial system $\{F_1, \dots, F_n\} \in \mathfrak{F}_{m,n}$ and any cubic box*

$$\mathcal{C} = \left[\gamma_1 + \frac{u_1}{k}, \gamma_1 + \frac{u_1+1}{k}\right] \times \dots \times \left[\gamma_m + \frac{u_m}{k}, \gamma_m + \frac{u_m+1}{k}\right] \subseteq \mathbb{R}^m,$$

*where $u_1, \dots, u_m \in \mathbb{Z}$, of side length $1/k$, we have*

$$T_p(\mathcal{C}) = \#\mathcal{X}_p\left(\frac{1}{k}\right)^m + O\left(p^{(m-n)/2}(\log p)^m + \left(\frac{1}{k}\right)^{m-n-1} p^{m-n-1/2}(\log p)^{n+1}\right).$$

## 6. Proof of Theorem 1

For a set $\Omega \subseteq \mathbb{T}_m$ and a box $\Pi \subseteq \mathbb{T}_n$ of the form (8) let $N(\Omega; \Pi)$ be the number of integer vectors $\mathbf{x} \in p\Omega$ for which the points (1) belong to $\Pi$.

In particular, let $N(\Omega) = N(\Omega; \mathbb{T}_m)$ be the number of integer vectors $\mathbf{x} \in p\Omega$. A simple geometric argument shows that if $\Omega = \Gamma \subseteq \mathbb{T}_m$ is a cube then

$$N(\Gamma) = \mu(\Gamma)p^m + O\left(p^{m-1}\mu(\Gamma)^{(m-1)/m}\right). \tag{9}$$

We start with deriving a lower bound on $N(\Omega; \Pi)$.

We now recall some constructions and arguments from the proof of [7, Theorem 2]. Pick a point $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_m) \in \mathbb{T}_m$ such that all its coordinates are irrational. For positive $k$, let $\mathfrak{C}(k)$ be the set of cubes of the form

$$\left[\gamma_1 + \frac{u_1}{k}, \gamma_1 + \frac{u_1+1}{k}\right] \times \dots \times \left[\gamma_m + \frac{u_m}{k}, \gamma_m + \frac{u_m+1}{k}\right] \subseteq \mathbb{R}^m,$$

where $u_1, \dots, u_m \in \mathbb{Z}$. Note that the above irrationality condition guarantees that the points $p^{-1}\mathbf{x}$ with $\mathbf{x} \in \mathbb{Z}^m$ all belong to the interior of the cubes from $\mathfrak{C}(k)$.

Furthermore, let $\mathcal{C}(k)$ be the set of cubes from $\mathfrak{C}(k)$ that are contained inside of $\Omega$. By [7, Eq. (9)], for any $C$-well shaped set $\Omega \in \mathbb{T}_m$, we have

$$\#\mathcal{C}(k) = k^m\mu(\Omega) + O\left(k^{m-1}\right), \tag{10}$$

where the implied constant depends only on $m$ and $C$. Let $\mathcal{B}_1 = \mathcal{C}(2)$ and for $i = 2, 3, \dots$, let $\mathcal{B}_i$ be the set of cubes $\Gamma \in \mathcal{C}(2^i)$ that are not contained in any cube from $\mathcal{C}(2^{i-1})$. Clearly

$$2^{-im}\#\mathcal{B}_i + 2^{-(i-1)m}\#\mathcal{C}\left(2^{i-1}\right) \leqslant \mu(\Omega), \quad i = 2, 3, \dots.$$

We now see from (10) that

$$\#\mathcal{B}_i \ll 2^{i(m-1)} \tag{11}$$

and also for any integer $M \geqslant 1$,

$$\Omega \setminus \Omega_\varepsilon^- \subseteq \bigcup_{i=1}^{M} \bigcup_{\Gamma \in \mathcal{B}_i} \Gamma \subseteq \Omega$$

with $\varepsilon = m^{1/2}2^{-M}$. Since $\Omega$ is $C$-well shaped, we obtain

$$\mu\left(\bigcup_{i=1}^{M} \bigcup_{\Gamma \in \mathcal{B}_i} \Gamma\right) = \mu(\Omega) + O\left(2^{-M}\right). \tag{12}$$

Using Lemma 4 (taken with $L = (p-1)/2$) and recalling the bound of Lemma 5 we see that the discrepancy $D(\Gamma)$ of the points (1) with $\mathbf{x} \in p\Gamma$, for a cube $\Gamma$ satisfies

$$D(\Gamma) \ll \frac{p^{1/2}(p\mu(\Gamma)^{1/m})^{m-1}}{\mu(\Gamma)p^m}(\log p)^{n+1} = p^{-1/2}\mu(\Gamma)^{-1/m}(\log p)^{n+1}.$$

Therefore, using (9), we derive

$$\begin{aligned} N(\Gamma; \Pi) &= \lambda(\Pi)N(\Gamma) + O\left(N(\Gamma)D(\Gamma)\right) \\ &= \lambda(\Pi)\mu(\Gamma)p^m + O\left(p^{m-1/2}\mu(\Gamma)^{(m-1)/m}(\log p)^{n+1}\right). \end{aligned} \tag{13}$$

Hence

$$N(\Omega; \Pi) \geqslant \sum_{i=1}^{M} \sum_{\Gamma \in \mathcal{B}_i} N(\Gamma; \Pi) = \lambda(\Pi)p^m \sum_{i=1}^{M} \sum_{\Gamma \in \mathcal{B}_i} \mu(\Gamma) + O(R), \tag{14}$$

where

$$R = p^{m-1/2}(\log p)^{n+1} \sum_{i=1}^{M} \#\mathcal{B}_i 2^{-i(m-1)}.$$

We see from (12) that

$$\sum_{i=1}^{M} \sum_{\Gamma \in \mathcal{B}_i} \mu(\Gamma) = \mu\left(\bigcup_{i=1}^{M} \bigcup_{\Gamma \in \mathcal{B}_i} \Gamma\right) = \mu(\Omega) + O\left(2^{-M}\right). \tag{15}$$

Furthermore, using (11), we derive

$$R \ll Mp^{m-1/2}(\log p)^{n+1}. \tag{16}$$

We now choose $M$ to satisfy

$$2^M \leqslant p^{1/2} < 2^{(M+1)}.$$

Now, substituting (15) and (16) in (14) with the above choice of $M$, we obtain

$$N(\Omega;\Pi) \geqslant \lambda(\Pi)\mu(\Omega)p^m + O\left(p^{m-1/2}(\log p)^{n+2}\right). \tag{17}$$

Since the complementary set $\overline{\Omega} = \mathbb{T}_m \setminus \Omega$ is also $C$-well shaped, we also have

$$N(\overline{\Omega};\Pi) \leqslant \lambda(\Pi)\mu(\overline{\Omega})p^m + O\left(p^{m-1/2}(\log p)^{n+2}\right). \tag{18}$$

Note that by (13) we have

$$N(\mathbb{T}_m;\Pi) = \lambda(\Pi)p^m + O\left(p^{m-1/2}(\log p)^{n+1}\right).$$

Now, since

$$N(\overline{\Omega};\Pi) = N(\mathbb{T}_m;\Pi) - N(\Pi) \quad \text{and} \quad \mu(\overline{\Omega}) = 1 - \mu(\Omega),$$

we now see that (18) implies that upper bound

$$N(\Omega;\Pi) \leqslant \lambda(\Pi)\mu(\Omega)p^m + O\left(p^{m-1/2}(\log p)^{n+2}\right)$$

together with (17) leads to the desired asymptotic formula

$$N(\Omega;\Pi) = \lambda(\Pi)\mu(\Omega)p^m + O\left(p^{m-1/2}(\log p)^{n+2}\right).$$

Since $D(\Omega) \leqslant 1$, we can assume that

$$\mu(\Omega) \geqslant c_0 p^{-1/2}(\log p)^{n+2},$$

for a sufficiently large constant $c_0 > 0$ as otherwise the result is trivial. Thus

$$\frac{N(\Omega;\Pi)}{N(\Omega)} = \lambda(\Pi) + O\left(\mu(\Omega)^{-1}p^{-1/2}(\log p)^{n+2}\right)$$

which concludes the proof.

## 7. Proof of Theorem 2

If $\Omega$ is $C$-very well shaped we may use the same method as the proof of Theorem 1 to replace the bounds (11) and (12) with

$$\#\mathcal{B}_i \ll 1 + \mu(\Omega)^{(m-1)/m}2^{i(m-1)} \tag{19}$$

and

$$\mu\left(\bigcup_{i=1}^{M}\bigcup_{\Gamma\in\mathcal{B}_i}\Gamma\right) = \mu(\Omega) + O\left(\mu(\Omega)^{(m-1)/m}2^{-M} + 2^{-Mm}\right). \tag{20}$$

Recalling the lower bound (14)

$$N(\Omega;\Pi) \geqslant \lambda(\Pi)p^m \sum_{i=1}^{M} \sum_{\Gamma\in\mathcal{B}_i} \mu(\Gamma) + O(R),$$

where

$$R = p^{m-1/2}(\log p)^{n+1} \sum_{i=1}^{M} \#\mathcal{B}_i 2^{-i(m-1)}.$$

We use (19) to bound the term $R$. First we note if $\#\mathcal{B}_i > 0$ we must have $2^{-im} \leqslant \mu(\Omega)$. Hence

$$\begin{aligned}
\sum_{i=1}^{M} \#\mathcal{B}_i 2^{-i(m-1)} &= \sum_{i\geqslant -\log\mu(\Omega)/(m\log 2)}^{M} \#\mathcal{B}_i 2^{-i(m-1)} \\
&\ll \sum_{i\geqslant -\log\mu(\Omega)/(m\log 2)}^{M} \bigl(\mu(\Omega)^{(m-1)/m} + 2^{-i(m-1)}\bigr) \\
&\ll M\mu(\Omega)^{(m-1)/m} + \mu(\Omega)^{(m-1)/m} \\
&\ll M\mu(\Omega)^{(m-1)/m}
\end{aligned}$$

so that

$$R \ll M\mu(\Omega)^{(m-1)/m} p^{m-1/2}(\log p)^{n+1}.$$

By (20) we have

$$\sum_{i=1}^{M} \sum_{\Gamma\in\mathcal{B}_i} \mu(\Gamma) = \mu\left(\bigcup_{i=1}^{M} \bigcup_{\Gamma\in\mathcal{B}_i} \Gamma\right) = \mu(\Omega) + O\bigl(\mu(\Omega)^{(m-1)/m} 2^{-M} + 2^{-Mm}\bigr).$$

Hence

$$\begin{aligned}
N(\Omega;\Pi) \geqslant \lambda(\Pi)\mu(\Omega)p^m + O\bigl(&\mu(\Omega)^{(m-1)/m} p^m 2^{-M} + p^m 2^{-Mm} \\
&+ M\mu(\Omega)^{(m-1)/m} p^{m-1/2}(\log p)^{n+1}\bigr).
\end{aligned}$$

Since $D(\Omega) \leqslant 1$, we can assume that

$$\mu(\Omega) \geqslant c_0 p^{-m/2}(\log p)^{m(n+2)}$$

for a sufficiently large constant $c_0 > 0$. Thus, choosing $M$ so that

$$2^M \leqslant p \leqslant 2^{(M+1)},$$

gives

$$N(\Omega;\Pi) \geqslant \lambda(\Pi)\mu(\Omega)p^m + O\bigl(\mu(\Omega)^{(m-1)/m} p^{m-1/2}(\log p)^{n+2}\bigr).$$

The upper bounds for $N(\Omega;\Pi)$ and $D(\Omega)$ follow the same method as in the proof of Theorem 1.

## 8. Proof of Theorem 3

Given a $C$-very well shaped set $\Omega$, we consider the same constructions as in the proof of Theorem 1. As in Theorem 2 we have the bound

$$\#\mathcal{B}_i \ll 1 + \mu(\Omega)^{1-1/m} 2^{i(m-1)}. \tag{21}$$

The set inclusions

$$\Omega \setminus \Omega_\varepsilon^- \subseteq \bigcup_{i=1}^{M} \bigcup_{\Gamma \in \mathcal{B}_i} \Gamma \subseteq \Omega \tag{22}$$

give the approximation

$$\mu\left(\bigcup_{i=1}^{M} \bigcup_{\Gamma \in \mathcal{B}_i} \Gamma\right) = \mu(\Omega) + O\left(\frac{\mu(\Omega)^{1-1/m}}{2^M} + \frac{1}{2^{mM}}\right). \tag{23}$$

Using Lemma 6 and (22),

$$T_p(\Omega) \geqslant \sum_{i=1}^{M} \sum_{\Gamma \in \mathcal{B}_i} T_p(\Gamma) = \#\mathcal{X}_p \sum_{n=1}^{M} \sum_{\Gamma \in \mathcal{B}_i} \mu(\Gamma) + O(R),$$

where

$$R = \sum_{i=1}^{M} \#B_i \big(p^{(m-n)/2} (\log p)^m + 2^{-i(m-n-1)} p^{m-n-1/2} (\log p)^{n+1}\big).$$

By (23)

$$\#\mathcal{X}_p \sum_{n=1}^{M} \sum_{\Gamma \in \mathcal{B}_i} \mu(\Gamma) = \#\mathcal{X}_p \left(\mu(\Omega) + O\left(\frac{\mu(\Omega)^{1-1/m}}{2^M} + \frac{1}{2^{mM}}\right)\right)$$

and using (3) we have

$$\#\mathcal{X}_p \sum_{n=1}^{M} \sum_{\Gamma \in \mathcal{B}_i} \mu(\Gamma) = \#\mathcal{X}_p \mu(\Omega) + O\left(\frac{p^{m-n}\mu(\Omega)^{1-1/m}}{2^M} + \frac{p^{m-n}}{2^{mM}}\right).$$

For the term $R$, by (21)

$$\begin{aligned} R &\ll \sum_{i=1}^{M} \big(p^{(m-n)/2} (\log p)^m + \big(p 2^{-i}\big)^{m-n-1} p^{1/2} (\log p)^{n+1}\big) \\ &\quad + \sum_{i=1}^{M} \big(\mu(\Omega)^{1-1/m} 2^{i(m-1)} p^{(m-n)/2} (\log p)^m + \big(p 2^{-i}\big)^{m-n-1} p^{1/2} (\log p)^{n+1}\big) \end{aligned}$$

$$\begin{aligned}
&\ll Mp^{(m-n)/2}(\log p)^m + p^{m-n-1/2}(\log p)^{n+1}\sum_{i=1}^{M} 2^{-i(m-n-1)} \\
&\quad + \mu(\Omega)^{1-1/m} p^{(m-n)/2}\sum_{i=1}^{M} 2^{i(m-1)}(\log p)^m \\
&\quad + \mu(\Omega)^{1-1/m} p^{m-n-1/2}\sum_{i=1}^{M} 2^{in}(\log p)^{n+1} \\
&\ll M\bigl(p^{(m-n)/2}(\log p)^m + p^{m-n-1/2}(\log p)^{n+1}\bigr) \\
&\quad + \mu(\Omega)^{1-1/m}\bigl(2^{M(m-1)}p^{(m-n)/2}(\log p)^m + 2^{Mn}p^{m-n-1/2}(\log p)^{n+1}\bigr).
\end{aligned}$$

Hence we have

$$T_p(\Omega) \geqslant \#\mathcal{X}_p\mu(\Omega) + O(R_1 + R_2 + R_3) \tag{24}$$

with

$$\begin{aligned}
R_1 &= \frac{p^{m-n}\mu(\Omega)^{1-1/m}}{2^M} + \frac{p^{m-n}}{2^{mM}}, \\
R_2 &= \mu(\Omega)^{1-1/m}\bigl(2^{M(m-1)}p^{(m-n)/2}(\log p)^m + 2^{Mn}p^{m-n-1/2}(\log p)^{n+1}\bigr), \\
R_3 &= Mp^{m-n-1/2}(\log p)^{n+1}.
\end{aligned}$$

It is clear that for the bound to be nontrivial we have to choose $M = O(\log p)$, under which condition we have

$$R_3 = p^{m-n-1/2}(\log p)^{n+2}.$$

Now considering all four ways of balancing the terms of $R_1$ and $R_2$, after straightforward calculations we conclude that the optimal choice of $M$ is defined by the condition

$$2^{-M} \leqslant p^{-1/2(n+1)}\log p < 2^{-M+1},$$

that balances the first term of $R_1$ and the second term of $R_2$. This gives

$$\begin{aligned}
R &\ll p^{m-n-1/2(n+1)}\mu(\Omega)^{1-1/m}\log p + p^{m-n-m/2(n+1)}(\log p)^m \\
&\quad + p^{(m-n)-1/2(n+1)-n(m-1-n)/2(n+1)}\mu(\Omega)^{1-1/m}\log p \\
&\quad + p^{m-n-1/2}(\log p)^{n+2} \\
&\ll p^{m-n-1/2(n+1)}\mu(\Omega)^{1-1/m}\log p + p^{m-n-1/2}(\log p)^{n+2}.
\end{aligned} \tag{25}$$

Hence by (3),

$$T_p(\Omega) \geqslant \#\mathcal{X}_p\bigl(\mu(\Omega) + O\bigl(\mu(\Omega)^{1-1/m}p^{-1/2(n+1)}\log p + p^{-1/2}(\log p)^{n+2}\bigr)\bigr). \tag{26}$$

Although since

$$(\mathbb{T}_m \setminus \Omega)^-_\varepsilon = \Omega^+_\varepsilon \leqslant C\bigl(\mu(\Omega)^{1-1/m}\varepsilon + \varepsilon^m\bigr)$$

we may repeat the above argument to get

$$\begin{aligned} T_p(\mathbb{T}_m \setminus \Omega) \geqslant \#\mathcal{X}_p \mu(\mathbb{T}_m \setminus \Omega) \\ + O\big(\#\mathcal{X}_p\big(\mu(\Omega)^{1-1/m} p^{-1/2(n+1)} \log p + p^{-1/2}(\log p)^{n+2}\big)\big). \end{aligned} \tag{27}$$

Finally, combining (3), (26) and (27), gives the desired result.

## References

[1] M. Drmota, R. Tichy, Sequences, Discrepancies and Applications, Springer-Verlag, Berlin, 1997.
[2] É. Fouvry, Consequences of a result of N. Katz and G. Laumon concerning trigonometric sums, Israel J. Math. 120 (2000) 81–96.
[3] É. Fouvry, N. Katz, A general stratification theorem for exponential sums, and applications, J. Reine Angew. Math. 540 (2001) 115–166.
[4] B. Kerr, Solutions to polynomial congruences in well shaped sets, Bull. Aust. Math. Soc., in press.
[5] L. Kuipers, H. Niederreiter, Uniform Distribution of Sequences, Wiley–Interscience, New York, 1974.
[6] S. Lang, A. Weil, Number of points of varieties in finite fields, Amer. J. Math. 76 (1954) 819–827.
[7] W. Schmidt, Irregularities of distribution. IX, Acta Arith. 27 (1975) 385–396.
[8] I.E. Shparlinski, On the distribution of solutions to polynomial congruences, Arch. Math. 99 (2012) 345–351.
[9] H. Weyl, On the volume of tubes, Amer. J. Math. 61 (1939) 461–472.