On the Distribution of Values and Zeros of Polynomial Systems over Arbitrary Sets

BRYCE KERR
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
bryce.kerr@mq.edu.au

IGOR E. SHPARLINSKI*
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor.shparlinski@mq.edu.au

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

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

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

*This work was supported in part by ARC Grant DP1092835
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:

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

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

Let $\mathcal{G}_{m,n,p}$ 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 $\{G_1, \ldots, G_n\} \in \mathcal{G}_{m,n,p}$, the points (1) are uniformly distributed in the unit cube $[0, 1]^n$, where $x$ runs through the integral points in any cube $\Gamma \in [0, p - 1]^m$ with side length $h \geq p^{1/2}(\log p)^{1+\varepsilon}$. 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 $x$ runs through a set from a very general family. For example, this holds for $x$ 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 \( m \geq n+1 \) 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

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

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

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

with

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

The asymptotic formula \([4]\) is based on a combination of a result of Fouvy \([2]\) 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

\[
\mu(\Omega) \geq p^{-1/2+\varepsilon}
\]

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

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

We define the distance between a vector \( u \in T_m \) and a set \( \Omega \subseteq T_m \) by
\[
\text{dist}(u, \Omega) = \inf_{w \in \Omega} \|u - w\|,
\]
where \( \|v\| \) denotes the Euclidean norm of \( v \). Given \( \varepsilon > 0 \) and a set \( \Omega \subseteq T_m \), we define the sets
\[
\Omega^+_\varepsilon = \{ u \in T_m \setminus \Omega : \text{dist}(u, \Omega) < \varepsilon \}
\]
and
\[
\Omega^-_\varepsilon = \{ u \in \Omega : \text{dist}(u, T_m \setminus \Omega) < \varepsilon \}.
\]

We say that a set \( \Omega \) is well shaped if
\[
\mu(\Omega^+_\varepsilon) \leq C\varepsilon,
\]
for some constant \( C \), where \( \mu \) is the Lebesgue measure on \( T_m \).

It is known that any convex set is well shaped, see [7, Lemma 1].

Finally, a very general result of Weyl [9, Equation (2)] (taken with \( n = m \) and \( \nu = n - 1 \)), that actually expresses \( \mu(\Omega^+_\varepsilon) \) via a finite sum of powers \( \varepsilon^i \), \( i = 1, \ldots, m \) 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 well shaped.

Furthermore, we say that a set \( \Omega \subseteq T_m \) is very well shaped if for every \( \varepsilon > 0 \) the measures of the sets \( \Omega^+_\varepsilon \) exist and satisfy
\[
\mu(\Omega^+_\varepsilon) \leq C (\mu(\Omega)^{1 - 1/m}\varepsilon + \varepsilon^m)
\]
for some \( C > 0 \), the most natural example of a very well shaped set being a Euclidian 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 \( |A(t)| \leq \alpha B(t) \) 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 \( \{F_1, \ldots, F_n\} \in \mathcal{F}_{m,n} \) (but does not depend on the polynomial system \( \{G_1, \ldots, G_n\} \in \mathcal{G}_{m,n,p} \)).
3 Discrepancy

Given a sequence $\Xi$ of $N$ points
\[ \Xi = \{(\xi_{k,1}, \ldots, \xi_{k,n})\}_{k=1}^N, \tag{7} \]
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 $k \leq N$ such that $(\xi_{k,1}, \ldots, \xi_{k,n}) \in \Pi$, $\lambda$ is the Lebesgue measure on $\mathbb{T}_n$ and the supremum is taken over all boxes \[ \Pi = [\alpha_1, \beta_1) \times \ldots \times [\alpha_n, \beta_n) \subseteq \mathbb{T}_n, \tag{8} \]
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
\[ \left( \left\{ \frac{G_1(x)}{p} \right\}, \ldots, \left\{ \frac{G_n(x)}{p} \right\} \right), \quad x \in p\Omega. \]

**Theorem 1.** For any polynomial system $\{G_1, \ldots, G_n\} \in \mathfrak{G}_{m,n,p}$ and any well shaped set $\Omega \in \mathbb{T}_m$, we have
\[ D(\Omega) \ll \mu(\Omega)^{-1/p}p^{-1/2}(\log p)^{n+2}. \]

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

**Theorem 2.** For any polynomial system $\{G_1, \ldots, G_n\} \in \mathfrak{G}_{m,n,p}$ and any 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 very well shaped set $\Omega \in \mathbb{T}_m$, we have
\[ T_p(\Omega) = \#X_p \left( \mu(\Omega) + O(\mu(\Omega)^{1-1/m}p^{-1/(n+1)} \log p + p^{-1/2}(\log p)^{n+2}) \right). \]
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–Sz"usz 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 \( L \geq 1 \) and the real number \( S \) we have

\[
\left| \sum_{k=1}^{N} \exp \left( 2\pi i \sum_{j=1}^{n} a_{j} \xi_{k,j} \right) \right| \leq S,
\]

for all integers \(-L \leq a_{j} \leq L, j = 1, \ldots, n, \) 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, Equation (10.6)]

**Lemma 5.** For any polynomial system \( \{G_{1}, \ldots, G_{n}\} \in \mathcal{G}_{m,n,p} \) and arbitrary integers \( u \) and \( w \) with \( 1 \leq w < p \), uniformly over all non-zero modulo \( p \) integer vectors \( (a_{1}, \ldots, a_{n}) \) we have

\[
\sum_{x_{1}, \ldots, x_{m} = u}^{u+w} \exp \left( \frac{2\pi i}{p} \sum_{j=1}^{n} a_{j} G_{j}(x_{1}, \ldots, x_{m}) \right) \ll p^{1/2} w^{m-1} \log p.
\]

**Proof.** The bound in [3, Equation (10.6)], that gives the desired result for \( u = 0 \) is uniform in polynomials \( G_{1}, \ldots, G_{m} \). It now remains to notice that the property of being degree 2 independent is preserved under the change of variables \( X_{j} \rightarrow X_{j} + u, j = 1, \ldots, m. \)

\[\square\]

The proof of Theorem 3 is based on the following bound for \( T_{p}(C) \) for a cube \( C \) which is essentially a result of Fouvry [2]
Lemma 6. For any polynomial system \( \{ F_1, \ldots, F_n \} \in \mathbb{R}_{m,n} \) and any cubic box
\[
\mathcal{C} = \left[ \gamma_1 + \frac{u_1}{k}, \gamma_1 + \frac{u_1 + 1}{k} \right] \times \cdots \times \left[ \gamma_m + \frac{u_m}{k}, \gamma_m + \frac{u_m + 1}{k} \right] \subseteq \mathbb{R}^m,
\]
where \( u_1, \ldots, u_m \in \mathbb{Z} \), of side length \( 1/k \), we have
\[
T_p(\mathcal{C}) = \#\mathcal{X}_p \left( \frac{1}{k} \right)^m + O \left( p^{(m-n)/2} (\log p)^m + \left( \frac{1}{k} \right)^{m-1} p^{m-n-1/2} (\log p)^{n+1} \right).
\]

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 \( x \in p\Omega \) for which the points (1) belong to \( \Pi \).

In particular, let \( N(\Omega) = N(\Omega; \mathbb{T}_m) \) be the number of integer vectors \( x \in p\Omega \). 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 \( \gamma = (\gamma_1, \ldots, \gamma_m) \in \mathbb{T}_m \) such that all its coordinates are irrational. For positive \( k \), let \( \mathcal{C}(k) \) be the set of cubes of the form
\[
\left[ \gamma_1 + \frac{u_1}{k}, \gamma_1 + \frac{u_1 + 1}{k} \right] \times \cdots \times \left[ \gamma_m + \frac{u_m}{k}, \gamma_m + \frac{u_m + 1}{k} \right] \subseteq \mathbb{R}^m,
\]
where \( u_1, \ldots, u_m \in \mathbb{Z} \). Note that the above irrationality condition guarantees that the points \( p^{-1}x \) with \( x \in \mathbb{Z}^m \) all belong to the interior of the cubes from \( \mathcal{C}(k) \).

Furthermore, let \( \mathcal{C}(k) \) be the set of cubes from \( \mathcal{C}(k) \) that are contained inside of \( \Omega \). By [7, Equation (9)], for any well shaped set \( \Omega \in \mathbb{T}_m \), we have
\[
\#\mathcal{C}(k) = k^m \mu(\Omega) + O(k^{m-1}). \tag{10}
\]
Let $B_1 = C(2)$ and for $i = 2, 3, \ldots$, let $B_i$ be the set of cubes $\Gamma \in C(2^i)$ that are not contained in any cube from $C(2^{i-1})$. Clearly

$$2^{-im} \#B_i + 2^{-(i-1)m} \#C(2^{i-1}) \leq \mu(\Omega), \quad i = 2, 3, \ldots.$$ 

We now see from (10) that

$$\#B_i \ll 2^{i(m-1)} \quad (11)$$

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

$$\Omega \setminus \Omega_\varepsilon \subseteq \bigcup_{i=1}^M \bigcup_{\Gamma \in B_i} \Gamma \subseteq \Omega$$

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

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

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 (11) with $x \in p\Gamma$, 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

$$N(\Omega; II) = \lambda(II)N(\Gamma) + O(N(\Gamma)D(\Gamma))$$

$$= \lambda(II)\mu(\Gamma)p^m + O\left(p^{m-1/2} \mu(\Gamma)^{m-1/m}(\log p)^{n+1}\right). \quad (13)$$

Hence

$$N(\Omega; II) \geq \sum_{i=1}^M \sum_{\Gamma \in B_i} N(\Gamma; II) = \lambda(II)p^m \sum_{i=1}^M \sum_{\Gamma \in B_i} \mu(\Gamma) + O(R), \quad (14)$$

where

$$R = p^{m-1/2}(\log p)^{n+1} \sum_{i=1}^M \#B_i 2^{-i(m-1)}.$$
We see from (12) that
\[
\sum_{i=1}^{M} \sum_{\Gamma \in B_i} \mu(\Gamma) = \mu\left( \bigcup_{i=1}^{M} \bigcup_{\Gamma \in B_i} \Gamma \right) = \mu(\Omega) + O(2^{-M}). \tag{15}
\]

Furthermore, using (14), we derive
\[
R \ll Mp^{m-1/2}(\log p)^{n+1}. \tag{16}
\]

We now choose \(M\) to satisfy
\[
2^M \leq p^{1/2} < 2^{(M+1)}.
\]

Now, substituting (15) and (16) in (14) with the above choice of \(M\), we obtain
\[
N(\Omega; \Pi) \geq \lambda(\Pi) \mu(\Omega) p^m + O\left(p^{m-1/2}(\log p)^{n+2}\right). \tag{17}
\]

Since the complementary set \(\overline{\Omega} = \mathbb{T}_m \setminus \Omega\) is also well shaped, we also have
\[
N(\overline{\Omega}; \Pi) \leq \lambda(\Pi) \mu(\overline{\Omega}) p^m + O\left(p^{m-1/2}(\log p)^{n+2}\right). \tag{18}
\]

Note that by (13) we have
\[
N(\Omega; \Pi) = \lambda(\Pi) p^m + O \left(p^{m-1/2}(\log p)^{n+1}\right).
\]

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
\[
N(\Omega; \Pi) \leq \lambda(\Pi) \mu(\Omega) p^m + O\left(p^{m-1/2}(\log p)^{n+2}\right)
\]
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 \(D(\Omega) \leq 1\), we can assume that
\[
\mu(\Omega) \geq c_0 p^{-1/2}(\log p)^{n+2}.
\]

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 very well shaped we may use the same method as the proof of Theorem 1 to replace the bounds (11) and (12) with

$$\#B_i \ll 1 + \mu(\Omega)^{(m-1)/m}2^{i(m-1)}$$  \hspace{1cm} (19)

and

$$\mu \left( \bigcup_{i=1}^{M} \bigcup_{\Gamma \in B_i} \Gamma \right) = \mu(\Omega) + O(\mu(\Omega)^{(m-1)/m}2^{-M} + 2^{-Mm}).$$  \hspace{1cm} (20)

Recalling the lower bound (14)

$$N(\Omega; \Pi) \geq \lambda(\Pi)p^\alpha \sum_{i=1}^{M} \sum_{\Gamma \in B_i} \mu(\Gamma) + O(R),$$

where

$$R = p^{m-1/2}p^{n+1} \sum_{i=1}^{M} \#B_i 2^{-i(m-1)}.$$  \hspace{1cm} (14)

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

$$\sum_{i=1}^{M} \#B_i 2^{-i(m-1)} = \sum_{i \geq -\log \mu(\Omega)/(m \log 2)}^{M} \#B_i 2^{-i(m-1)}$$

$$\ll \sum_{i \geq -\log \mu(\Omega)/(m \log 2)}^{M} (\mu(\Omega)^{(m-1)/m} + 2^{-i(m-1)})$$

$$\ll M \mu(\Omega)^{(m-1)/m} + \mu(\Omega)^{(m-1)/m}$$

$$\ll M \mu(\Omega)^{(m-1)/m}$$

so that

$$R \ll M \mu(\Omega)^{(m-1)/m} p^{m-1/2}p^{n+1}.$$  \hspace{1cm} (20)

By (20) we have,

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

10
Hence

\[ N(\Omega; \Pi) \geq \lambda(\Pi) \mu(\Omega) p^m + O(\mu(\Omega)^{(m-1)/m} p^m 2^{-M} + p^m 2^{-M m} + M \mu(\Omega)^{(m-1)/m} p^{m-1/2} (\log p)^{n+1}). \]

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

\[ \mu(\Omega) \geq c_0 p^{-m/2} (\log p)^{m(n+2)} \]

for a sufficiently large constant \( c_0 > 0 \). Thus, choosing \( M \) so that

\[ 2^M \leq p \leq 2^{(M+1)}, \]

gives

\[ N(\Omega; \Pi) \geq \lambda(\Pi) \mu(\Omega) p^m + O(\mu(\Omega)^{(m-1)/m} p^{m-1/2} (\log p)^{n+2}). \]

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 \( \Omega \) very well shaped, we consider the same constructions in the proof of Theorem 1. As in Theorem 2 we have the bound

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

The set inclusions

\[ \Omega \setminus \Omega^{-} \subseteq \bigcup_{i=1}^{M} \bigcup_{\Gamma \in \mathcal{B}_i} \Gamma \subseteq \Omega \] (22)

give the approximation

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

Using Lemma 6 and (22),

\[ T_p(\Omega) \geq \sum_{i=1}^{M} \sum_{\Gamma \in \mathcal{B}_i} T_p(\Gamma) = \#\mathcal{X}_p \sum_{n=1}^{M} \sum_{\Gamma \in \mathcal{B}_i} \mu(\Gamma) + O(R), \]
where
\[
R = \sum_{i=1}^{M} \#B_i \left( p^{(m-n)/2}(\log p)^m + 2^{-i(m-n-1)} p^{m-n-1/2}(\log p)^{n+1} \right).
\]

By (23)
\[
\#X_p \sum_{n=1}^{M} \sum_{\Gamma \in B_i} \mu(\Gamma) = \#X_p \left( \mu(\Omega) + O \left( \frac{\mu(\Omega)^{1-1/m}}{2M} + \frac{1}{2mM} \right) \right)
\]
and using (3) we have
\[
\#X_p \sum_{n=1}^{M} \sum_{\Gamma \in B_i} \mu(\Gamma) = \#X_p \mu(\Omega) + O \left( \frac{p^{m-n} \mu(\Omega)^{1-1/m}}{2M} + \frac{p^{m-n}}{2mM} \right).
\]

For the term \( R \), by (21)
\[
R \ll \sum_{i=1}^{M} \left( p^{(m-n)/2}(\log p)^m + (p2^{-i})^{m-n-1} p^{1/2}(\log p)^{n+1} \right)
\]
\[
+ \sum_{i=1}^{M} \left( \mu(\Omega)^{1-1/m} 2^{i(m-1)} p^{(m-n)/2}(\log p)^m + (p2^{-i})^{m-n-1} p^{1/2}(\log p)^{n+1} \right)
\]
\[
\ll M p^{(m-n)/2}(\log p)^m + p^{m-n-1/2}(\log p)^{n+1} \sum_{i=1}^{M} 2^{-i(m-n-1)}
\]
\[
+ \mu(\Omega)^{1-1/m} p^{(m-n)/2} \sum_{i=1}^{M} 2^{i(m-1)}(\log p)^m
\]
\[
+ \mu(\Omega)^{1-1/m} p^{m-n-1/2} \sum_{i=1}^{M} 2^m(\log p)^{n+1}
\]
\[
\ll M \left( p^{(m-n)/2}(\log p)^m + p^{m-n-1/2}(\log p)^{n+1} \right)
\]
\[
+ \mu(\Omega)^{1-1/m} \left( 2^{M(m-1)} p^{(m-n)/2}(\log p)^m + 2^{Mn} p^{m-n-1/2}(\log p)^{n+1} \right).
\]

Hence we have
\[
T_p(\Omega) \geq \#X_p \mu(\Omega) + O(R_1 + R_2 + R_3) \quad (24)
\]
with
\[ R_1 = \frac{p^{m-n} \mu(\Omega)^{1-1/m}}{2M} + \frac{p^{m-n}}{2mM}, \]
\[ R_2 = \mu(\Omega)^{1-1/m} \left( 2^{M(m-1)} p^{(m-n)/2} (\log p)^m + 2^M p^{m-n-1/2} (\log p)^{n+1} \right), \]
\[ R_3 = Mp^{m-n-1/2} (\log p)^{n+1}. \]

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
\[ 2^{-M} \leq p^{-1/2(n+1)} \log p < 2^{-M+1}. \]

that balances the first term of \( R_1 \) and the second term of \( R_2 \). This gives
\[ R \ll p^{m-n-1/2(n+1)} \mu(\Omega)^{1-1/m} \log p + p^{m-n-m/2(n+1)} (\log p)^m \]
\[ + p^{(m-n)-1/2(n+1)-n(m-1-n)/2(n+1)} \mu(\Omega)^{1-1/m} \log p \]
\[ + p^{m-n-1/2} (\log p)^{n+2} \]
\[ \ll p^{m-n-1/2(n+1)} \mu(\Omega)^{1-1/m} \log p + p^{m-n-1/2} (\log p)^{n+2}. \]

Hence by (3),
\[ T_P(\Omega) \]
\[ \geq \# X_p (\mu(\Omega) + O (\mu(\Omega)^{1-1/m} p^{-1/2(n+1)} \log p + p^{-1/2} (\log p)^{n+2})). \]

Although since
\[ (\mathbb{T}_m \setminus \Omega)_{\bar{\varepsilon}} = \Omega_\varepsilon^+ = C (\mu(\Omega)^{1-1/m} \varepsilon + \varepsilon^m) \]
we may repeat the above argument to get,
\[ T_P(\mathbb{T}_m \setminus \Omega) \geq \# X_p \mu(\mathbb{T}_m \setminus \Omega) \]
\[ + O \left( \# X_p (\mu(\Omega)^{1-1/m} p^{-1/2(n+1)} \log p + p^{-1/2} (\log p)^{n+2}) \right). \]

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

[1] M. Drmota and 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 and 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’, *Preprint*, (available from [http://arxiv.org/abs/1210.1623](http://arxiv.org/abs/1210.1623)).

[5] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Intersci., New York, 1974.

[6] S. Lang and 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’, *Archiv Math.*, (to appear).

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