Bull. Aust. Math. Soc. **88** (2013), 435–447
doi:10.1017/S0004972713000324

SOLUTIONS TO POLYNOMIAL CONGRUENCES IN WELL-SHAPED SETS

BRYCE KERR

(Received 1 October 2012; accepted 19 February 2013; first published online 12 June 2013)

Abstract

We use a generalisation of Vinogradov's mean value theorem of Parsell *et al*. ['Near-optimal mean value estimates for multidimensional Weyl sums', arXiv:1205.6331] and ideas of Schmidt ['Irregularities of distribution. IX', *Acta Arith.* **27** (1975), 385–396] to give nontrivial bounds for the number of solutions to polynomial congruences, when the solutions lie in a very general class of sets, including all convex sets.

2010 *Mathematics subject classification*: primary 11D79; secondary 11K38.
Keywords and phrases: polynomial congruences, distribution of points.

1. Introduction

Given an integer m and a polynomial $F(X_1, \dots, X_d) \in \mathbb{Z}_m[X_1, \dots, X_d]$ and some $\Omega \subseteq [0, 1]^d$, we let $N_F(\Omega)$ denote the number of solutions $\mathbf{x} = (x_1, \dots, x_d) \in \mathbb{Z}^d$ to the congruence

$$F(\mathbf{x}) \equiv 0 \pmod m \quad \text{with} \left(\frac{x_1}{m}, \dots, \frac{x_d}{m}\right) \in \Omega. \tag{1.1}$$

Questions concerning the distribution of solutions to polynomial congruences have been considered in a number of works (for example, [3, 7, 12, 17]). In [5], Fouvry gives an asymptotic formula for the number of solutions to systems of polynomial congruences in small cubic boxes for a wide class of systems (see also [6, 8, 14, 15]). Shparlinski [13] uses the results of [5] and ideas of [10] to obtain an asymptotic formula for the number of solutions to the same systems when the solutions lie in a very general class of sets. For the case of a single polynomial F in d variables, Shparlinski [13] shows that for suitable Ω, when the modulus $m = p$ is prime,

$$N_F(\Omega) = p^{d-1}(\mu(\Omega) + O(p^{-1/4} \log p)),$$

provided F is irreducible over $\mathbb{C}$ and μ denotes the Lebesgue measure on $[0, 1]^d$. This gives an asymptotic formula for $N_F(\Omega)$ provided $\mu(\Omega) \geq p^{-1/4+\epsilon}$ and a nontrivial upper bound for $N_F(\Omega)$ when $\mu(\Omega) \geq p^{-5/4+\varepsilon}$. We follow the method of [13] to give an upper

bound for $N_F(\Omega)$ without any restrictions on our polynomial F when the modulus m is composite. We first establish an upper bound for $N_F(\Omega)$ when Ω is a cube. This gives a generalisation of [4, Theorem 1]. Although we follow the same argument, the difference is our use of a multidimensional version of Vinogradov's mean value theorem [9, Theorem 1.1]. To extend the bound from cubes to more general sets Ω, we approximate Ω by cubes using ideas based on [10, Theorem 2].

2. Definitions

We let μ denote the Lebesgue measure on $[0,1]^d$, $\|\cdot\|$ the Euclidian norm and define the distance between $\mathbf{x} \in [0,1]^d$ and $\Omega \subseteq [0,1]^d$ to be

$$\operatorname{dist}(\mathbf{x}, \Omega) = \inf_{\mathbf{y}\in\Omega} \|\mathbf{x} - \mathbf{y}\|.$$

As in [13], we say that $\Omega \subseteq [0,1]^d$ is *well shaped* if there exists $C = C(\Omega)$ such that for every $\varepsilon > 0$ the measures of the sets

$$\Omega_\varepsilon^+ = \{\mathbf{u} \in [0,1]^d \backslash \Omega : \operatorname{dist}(\mathbf{u}, \Omega) < \varepsilon\},$$
$$\Omega_\varepsilon^- = \{\mathbf{u} \in \Omega : \operatorname{dist}(\mathbf{u}, [0,1]^d \backslash \Omega) < \varepsilon\}$$

exist and satisfy

$$\mu(\Omega_\varepsilon^\pm) \le C\varepsilon. \tag{2.1}$$

From [10, Lemma 1] all convex subsets of $[0,1]^d$ are well shaped and from [16, Equation (2)], if the boundary of Ω is a manifold of dimension $n-1$ with bounded surface area then Ω is well shaped, for suitably chosen C.

For $\mathbf{x} = (x_1, \dots, x_d)$ we write $a \le \mathbf{x} \le b$ if $a \le x_1, \dots, x_d \le b$. Given a d-tuple of nonnegative integers $\mathbf{i} = (i_1, i_2, \dots, i_d)$, set $\mathbf{x}^\mathbf{i} = x_1^{i_1} x_2^{i_2} \dots x_d^{i_d}$ and $|\mathbf{i}| = i_1 + i_2 + \cdots + i_d$. We let r denote the number of distinct d-tuples $\mathbf{i}$ with $1 \le |\mathbf{i}| \le k$, so that

$$r = \binom{k+d}{d} - 1. \tag{2.2}$$

We will always suppose m is an integer greater than two. Given $F \in \mathbb{Z}_m[X_1, \dots, X_d]$, we let k denote the degree of F and d the number of variables. Writing

$$F(\mathbf{x}) = \sum_{0\le|\mathbf{i}|\le k} \beta_\mathbf{i} \mathbf{x}^\mathbf{i}, \quad \beta_\mathbf{i} \in \mathbb{Z}_m,$$

we define

$$g_F = \min_{|\mathbf{i}|=k} \gcd(m, \beta_i).$$

We use $g(t) \ll f(t)$ and $g(t) = O(f(t))$ to mean that there exists some absolute constant α such that $|g(t)| \le \alpha f(t)$ for all values of t within some specified range. Whenever we use $\ll$ and O, unless stated otherwise the implied constant will depend only on d, k and the particular C in (2.1). Similarly, $o(1)$ denotes a term which is sufficiently small when our parameter is large enough in terms of d, k and C.

https://doi.org/10.1017/S0004972713000324 Published online by Cambridge University Press

3. Main results

We can now present our main results.

THEOREM 3.1. *For positive $K_1, \dots, K_d, L, H, R \geq 1$, integer m and*

$$F(\mathbf{x}) = \sum_{0 \leq |\mathbf{i}| \leq k} \beta_{\mathbf{i}} \mathbf{x}^{\mathbf{i}} \in \mathbb{Z}_m[X_1, \dots, X_d]$$

of degree $k \geq 2$ with $g_F = 1$, let $M_F(H, R)$ denote the number of solutions to the congruence

$$F(\mathbf{x}) \equiv y \pmod{m} \tag{3.1}$$

with

$$(\mathbf{x}, y) \in [K_1 + 1, K_1 + H] \times \cdots \times [K_d + 1, K_d + H] \times [L + 1, L + R].$$

Then uniformly over all $K_1, \dots, K_d, L \geq 1$

$$M_F(H, R) \leq H^d \left(\left(\frac{R}{H^k} \right)^{1/2r(k+1)} + \left(\frac{R}{m} \right)^{1/2r(k+1)} \right) m^{o(1)}$$

as $H \to \infty$.

Arguing from heuristics, we expect the bound for $M_F(H, R)$ to be around

$$M_F(H, R) \leq H^d \left(\frac{R}{m} \right) m^{o(1)}$$

which can be directly compared with Theorem 3.1. Similarly, by considering the first term in Theorem 3.1 we immediately see when this bound for $M_F(H, R)$ is worse than the trivial bound $M_F(H, R) \leq H^d$.

Also, if $m = p$ is prime and $F[X_1, \dots, X_d]$ is not multilinear, that is, F is not linear in each of its variables, then Theorem 3.1 is trivial. This may be seen by the following argument. First we may show by slightly adjusting the proof of [4, Theorem 1] that, for $G \in \mathbb{Z}_p[X]$ of degree $k \geq 2$,

$$M_G(H, R) \leq H \left(\left(\frac{R}{H^k} \right)^{1/2k(k+1)} + \left(\frac{R}{p} \right)^{1/2k(k+1)} \right) p^{o(1)}. \tag{3.2}$$

Supposing $F \in \mathbb{Z}_p[X_1, \dots, X_d]$ is not multilinear, then after reordering the variables we may suppose for some $k_0 \geq 2$ that

$$F[X_1, \dots, X_d] = \sum_{i=0}^{k_0} X_d^i F_i[X_1, \dots, X_{d-1}] \tag{3.3}$$

with $F_{k_0} \neq 0$ and consider separately the values of $X_1, \dots, X_{d-1}$ such that

$$F_{k_0}[X_1, \dots, X_{d-1}] \equiv 0 \pmod{p}$$

https://doi.org/10.1017/S0004972713000324 Published online by Cambridge University Press

and

$$F_{k_0}[X_1, \dots, X_{d-1}] \not\equiv 0 \pmod{p}.$$

For the first case we use the assumption that p is prime and induction on d to bound the number of values $X_1, \dots, X_{d-1}$ such that $F_{k_0}[X_1, \dots, X_{d-1}] \equiv 0 \pmod{p}$ by $O(H^{d-2})$ and bound the number of solutions to

$$F[X_1, \dots, X_d] \equiv y \pmod{p}$$

in the remaining variables X_d, Y trivially by RH.

For the second case, we bound the number of $X_1, \dots, X_{d-1}$ such that $F_{k_0}[X_1, \dots, X_{d-1}] \not\equiv 0 \pmod{p}$ trivially by H^{d-1} and bound the number of solutions in the remaining variables X_d, Y by applying (3.2) to (3.3). Combining the above two cases gives

$$M_F(H, R) \le H^d\Big(\frac{R}{H} + \Big(\frac{R}{H^k}\Big)^{1/2k(k+1)} + \Big(\frac{R}{m}\Big)^{1/2k(k+1)}\Big)p^{o(1)},$$

which can be compared with Theorem 3.1.

Taking $R = 1$ in Theorem 3.1 we get the following corollary.

COROLLARY 3.2. *For any cube $B \subseteq [0,1]^d$ of side length $1/h$, $F \in \mathbb{Z}_m[X_1, \dots, X_d]$ of degree $k \ge 2$ with $g_F = 1$,*

$$N_F(B) \le \Big(\frac{m}{h}\Big)^{d-k/2r(k+1)+o(1)} + m^{d-1/2r(k+1)+o(1)}\Big(\frac{1}{h}\Big)^{d+o(1)}$$

as the $m/h \to \infty$.

Taking $R = H$ in Theorem 3.1 we get the following corollary.

COROLLARY 3.3. *Suppose $F \in \mathbb{Z}_m[X_1, \dots, X_d]$ of degree $k \ge 2$ with $g_F = 1$ is of the form*

$$F(X_1, \dots, X_d) = G(X_1, \dots, X_{d-1}) - X_d$$

for some $G \in \mathbb{Z}_m[X_1, \dots, X_{d-1}]$. Then for any cube $B \subseteq [0,1]^d$ of side length $1/h$,

$$N_F(B) \le \Big(\frac{m}{h}\Big)^{d-1-(k-1)/2r(k+1)+o(1)} + m^{d-1+o(1)}\Big(\frac{1}{h}\Big)^{d-1+1/2r(k+1)+o(1)}$$

as $m/h \to \infty$, where r corresponds to $d-1$ in the definition (2.2).

We use the above corollaries to estimate $N_F(\Omega)$ for well-shaped Ω.

THEOREM 3.4. *Suppose $F \in \mathbb{Z}_m[X_1, \dots, X_d]$ satisfies the conditions of Corollary 3.2 and $\Omega \subset [0,1]^d$ is well shaped with $\mu(\Omega) \ge m^{-1}$. Then*

$$N_F(\Omega) \le m^{d-k/2r(k+1)+o(1)}\mu(\Omega)^{1-k/2r(k+1)} + m^{d-1/2r(k+1)+o(1)}\mu(\Omega)$$

as $m \to \infty$.

https://doi.org/10.1017/S0004972713000324 Published online by Cambridge University Press

THEOREM 3.5. *Suppose* $F \in \mathbb{Z}_m[X_1, X_2, \ldots, X_d]$ *satisfies the conditions of Corollary 3.3 and* $\Omega \subset [0,1]^d$ *is well shaped. Then*

$$N_F(\Omega) \le \begin{cases} m^{d-1+o(1)}\mu(\Omega)^{1/2r(k+1)} & \text{if } \mu(\Omega) \ge m^{-1+1/k}, \\ m^{d-1-(k-1)/2r(k+1)+o(1)}\mu(\Omega)^{-(k-1)/2r(k+1)} & \text{if } m^{-1} \le \mu(\Omega) < m^{-1+1/k}, \end{cases}$$

as $m \to \infty$.

4. Proof of Theorem 3.1

Making a change of variables we may assume $(\mathbf{K}, L) = (0, \ldots, 0)$. Suppose for integer s we have $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{2s}$ satisfying (3.1) with $\mathbf{x}_j = (x_{j,1}, x_{j,2}, \ldots, x_{j,d})$. Then

$$F(\mathbf{x}_1) + F(\mathbf{x}_2) + \cdots + F(\mathbf{x}_s) - F(\mathbf{x}_{s+1}) - \cdots - F(\mathbf{x}_{2s}) \equiv z \pmod m$$

for some $-sR \le z \le sR$. Hence there exists $-sR \le u \le sR$ such that

$$M_F(H,R)^{2s} \le (1+2sR)T(u,H) \tag{4.1}$$

with $T(u,H)$ equal to the number of solutions to the congruence

$$F(\mathbf{x}_1) + F(\mathbf{x}_2) + \cdots + F(\mathbf{x}_s) - F(\mathbf{x}_{s+1}) - \cdots - F(\mathbf{x}_{2s}) \equiv u \pmod m \tag{4.2}$$

with each coordinate of $\mathbf{x_j}$ between 1 and H.

Since

$$F(\mathbf{x}) = \sum_{0 \le |\mathbf{i}| \le k} \beta_{\mathbf{i}} \mathbf{x}^{\mathbf{i}} \quad \text{for some } \beta_{\mathbf{i}} \in \mathbb{Z}_m,$$

we may write (4.2) in the form

$$\sum_{1 \le |\mathbf{i}| \le k} \beta_{\mathbf{i}} \lambda_{\mathbf{i}} \equiv u \pmod m \tag{4.3}$$

with

$$\lambda_{\mathbf{i}} = \mathbf{x}_1^{\mathbf{i}} + \cdots + \mathbf{x}_s^{\mathbf{i}} - \mathbf{x}_{s+1}^{\mathbf{i}} - \cdots - \mathbf{x}_{2s}^{\mathbf{i}}. \tag{4.4}$$

Since $g_F = 1$, we choose $\mathbf{i}_0$ with $|\mathbf{i}_0| = k$ and $\gcd(\beta_{\mathbf{i}_0}, m) = 1$. Considering (4.3) as a linear equation in $\lambda_{\mathbf{i}}$, if we let $\lambda_{\mathbf{i}}$, $\mathbf{i} \ne \mathbf{i}_0$, take arbitrary values, then $\lambda_{\mathbf{i}_0}$ is determined uniquely (mod m). Since

$$-sH^{|\mathbf{i}|} \le \lambda_{\mathbf{i}} \le sH^{|\mathbf{i}|}$$

there are at most

$$\left(1 + (2s+1)\frac{H^k}{m}\right) \prod_{\substack{\mathbf{i} \ne \mathbf{i}_0 \\ 1 \le |\mathbf{i}| \le k}} (2s+1)H^{|\mathbf{i}|} = (2s+1)^{r-1}H^{K-k}\left(1 + (2s+1)\frac{gH^k}{m}\right) \tag{4.5}$$

https://doi.org/10.1017/S0004972713000324 Published online by Cambridge University Press

solutions to (4.3) in integer variables $\lambda_{\mathbf{i}}$, with

$$K = \sum_{1\le|\mathbf{i}|\le k} |\mathbf{i}| = \frac{d}{d+1}(r+1)k.$$

For $U = (u_{\mathbf{i}})_{1\le|\mathbf{i}|\le k}$ with each $u_{\mathbf{i}} \in \mathbb{Z}$, let $J_{s,k,d}(U, H)$ denote the number of solutions in integers, $\lambda_{\mathbf{i}}$, to

$$\lambda_{\mathbf{i}} = u_{\mathbf{i}}, \quad 1 \le |\mathbf{i}| \le k,$$

with each $\mathbf{x}_j$ having components between 1 and H and write $J_{s,k,d}(U, H) = J_{s,k,d}(H)$ when $U = (0)_{1\le|\mathbf{i}|\le k}$. Let $\mathcal{U}$ be the collection of sets $U = (u_{\mathbf{i}})_{1\le|\mathbf{i}|\le k}$ such that $|u_{\mathbf{i}}| \le sH^{|\mathbf{i}|}$ and

$$\sum_{1\le|\mathbf{i}|\le k} \beta_{\mathbf{i}} u_{\mathbf{i}} \equiv u \pmod m$$

so that the cardinality of $\mathcal{U}$ is bounded by (4.5). We see that

$$T(u, H) \le \sum_{U\in\mathcal{U}} J_{s,k,d}(U, H), \tag{4.6}$$

since if $\mathbf{x}_{0,1} \dots \mathbf{x}_{0,2s}$ is a solution to (4.2), then the integers $\lambda_{0,\mathbf{i}}$, defined by

$$\lambda_{0,\mathbf{i}} = \mathbf{x}_{0,1}^{\mathbf{i}} + \cdots + \mathbf{x}_{0,s}^{\mathbf{i}} - \mathbf{x}_{0,s+1}^{\mathbf{i}} - \cdots - \mathbf{x}_{0,2s}^{\mathbf{i}}, \quad 1 \le |\mathbf{i}| \le k,$$

are a solution to (4.3) and the $\mathbf{x}_{0,1} \dots \mathbf{x}_{0,2s}$ are a solution to

$$\lambda_{\mathbf{i}} = \lambda_{0,\mathbf{i}}, \quad 1 \le |\mathbf{i}| \le k.$$

So if we let $U_0 = (\lambda_{0,\mathbf{i}})_{1\le|\mathbf{i}|\le k}$, then we see that the solution to (4.2), $\mathbf{x}_{0,1} \dots \mathbf{x}_{0,2s}$, is counted by the term $J_{s,k,d}(U_0, H)$ in (4.6). By (4.5) and (4.6),

$$T(u, H) \le (2s+1)^{r-1} H^{K-k}\Big(1 + (2s+1)\frac{H^k}{m}\Big) J_{s,k,d}(V, H) \tag{4.7}$$

for some $V \in \mathcal{U}$. For any $U \in \mathcal{U}$ we have the inequality

$$J_{s,k,d}(U, H) \le J_{s,k,d}(H).$$

To see this, let $\boldsymbol{\alpha} = (\alpha_{\mathbf{i}})_{1\le|\mathbf{i}|\le k}$ and

$$S(\boldsymbol{\alpha}) = \sum_{1\le\mathbf{x}\le H} \exp\Big(2\pi i \sum_{1\le|\mathbf{i}|\le k} \alpha_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}\Big).$$

Then, for $\lambda_{\mathbf{i}}$ defined as in (4.4),

$$\begin{aligned} J_{s,k,d}(U, H) &= \sum_{1\le\mathbf{x}_1,\dots,\mathbf{x}_{2s}\le H} \int_{[0,1]^r} \exp\Big(2\pi i \sum_{1\le|\mathbf{i}|\le k} \alpha_{\mathbf{i}}(\lambda_{\mathbf{i}} - u_{\mathbf{i}})\Big)\, d\boldsymbol{\alpha} \\ &= \int_{[0,1]^r} |S(\boldsymbol{\alpha})|^{2s} \exp\Big(-2\pi i \sum_{1\le|\mathbf{i}|\le k} \alpha_{\mathbf{i}} u_{\mathbf{i}}\Big)\, d\boldsymbol{\alpha} \\ &\le \int_{[0,1]^r} |S(\boldsymbol{\alpha})|^{2s}\, d\boldsymbol{\alpha} = J_{s,k,d}(H), \end{aligned}$$

https://doi.org/10.1017/S0004972713000324 Published online by Cambridge University Press

where the integral is over the variables $\alpha_{\mathbf{i}}$, $1 \le |\mathbf{i}| \le k$. Hence, by (4.1) and (4.7),

$$M_F(H,R)^{2s} \le (1+2sR)(2s+1)^{r-1}H^{K-k}\Big(1+(2s+1)\frac{H^k}{m}\Big)J_{s,k,d}(H). \tag{4.8}$$

By [9, Theorem 1.1], we have for $s \ge r(k+1)$ that

$$J_{s,k,d}(H) \ll H^{2sd-K+\epsilon}$$

for any $\epsilon > 0$ provided H is sufficiently large in terms of k, d and s. Inserting this bound into (4.8) gives

$$M_F(H,R)^{2s} \ll RH^{K-k}\Big(1+\frac{H^k}{m}\Big)H^{2sd-K+\epsilon}$$

and the result follows taking $s = r(k+1)$. □

5. Proof of Theorem 3.4

As in [10] we begin by choosing $\mathbf{a} = (a_1, \dots, a_d)$ with each coordinate irrational. For integer j let $\mathfrak{C}(j)$ be the set of cubes of the form

$$\Big[a_1+\frac{u_1}{j}, a_1+\frac{u_1+1}{j}\Big]\times\cdots\times\Big[a_d+\frac{u_d}{j}, a_d+\frac{u_d+1}{j}\Big], \quad u_i \in \mathbb{Z}. \tag{5.1}$$

Since each a_i is irrational, no point (1.1) lies in two distinct cubes (5.1). Given integer $M > 0$, let $\varepsilon = 2d^{\frac{1}{2}}/2^M$ and consider the set

$$\Omega_\varepsilon = \Omega \cup \Omega_\varepsilon^+.$$

Since Ω is well shaped,

$$\mu(\Omega_\epsilon) = \mu(\Omega) + O\Big(\frac{1}{2^M}\Big). \tag{5.2}$$

Let $C(j)$ be the cubes of $\mathfrak{C}(j)$ lying inside Ω_ε and suppose $j \le 2^M$. Then, by (5.2),

$$\#C(j) \le j^d\mu(\Omega_\varepsilon) \le j^d\mu(\Omega) + O\Big(\frac{j^d}{2^M}\Big) = j^d\mu(\Omega) + O(j^{d-1}). \tag{5.3}$$

Also, since a cube of side length $1/j$ has diameter $\varepsilon_j = d^{\frac{1}{2}}/j$, we see that the cubes of $C(j)$ cover $\Omega_\epsilon \setminus (\Omega_\varepsilon)_{\varepsilon_j}^-$ and hence

$$\#C(j) \ge j^d(\mu(\Omega_\varepsilon) - \mu((\Omega_\varepsilon)_{\varepsilon_j}^-)).$$

But, for $j \le 2^M$,

$$(\Omega_\varepsilon)_{\varepsilon_j}^- \subseteq \Omega_{\varepsilon_j}^- \cup \Omega_\varepsilon^+$$

https://doi.org/10.1017/S0004972713000324 Published online by Cambridge University Press

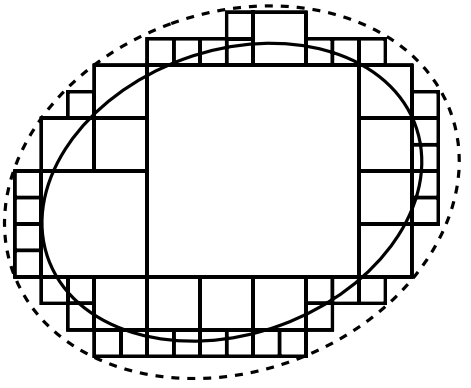

FIGURE 1. The sets Ω_ε and Ω with the corresponding $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3, \mathcal{B}_4$.

and since Ω is well shaped,

$$\mu((\Omega_\varepsilon)^-_{\varepsilon_j}) \le \mu(\Omega^-_{\varepsilon_j}) + \mu(\Omega^+_\varepsilon) \ll \frac{1}{j},$$

so we get

$$\#C(j) \ge j^d \mu(\Omega_\varepsilon) + O(j^{d-1}).$$

Combining this with (5.3) gives

$$\#C(j) = j^d \mu(\Omega) + O(j^{d-1}) \quad \text{for } j \le 2^M. \tag{5.4}$$

Let $\mathcal{B}_1 = C(2)$ and for $2 \le i \le M$ let $\mathcal{B}_i$ be the set of cubes from $C(2^i)$ that are not contained in any cubes from $C(2^{i-1})$. Then we have $\#\mathcal{B}_1 = \#C(2)$ and for $2 \le i \le M$, the cubes from both $\mathcal{B}_i$ and $C(2^{i-1})$ are contained in Ω_ε. (See Figure 1 for a representation with $M = 4$.) This gives

$$\#\mathcal{B}_i + 2^d \#C(2^{i-1}) \le 2^{id}\mu(\Omega) + O\left(\frac{2^{id}}{2^M}\right) \le 2^{id}\mu(\Omega) + O(2^{i(d-1)})$$

and hence by (5.4)

$$\#\mathcal{B}_i \ll 2^{i(d-1)}. \tag{5.5}$$

We have

$$\Omega \subseteq \bigcup_{i=1}^{M} \bigcup_{\Gamma \in \mathcal{B}_i} \Gamma, \tag{5.6}$$

which we see as follows. If $\mathbf{x} \in \Omega$ then

$$\operatorname{dist}(\mathbf{x}, [0,1]^d \setminus \Omega_\varepsilon) \ge \varepsilon;$$

but $\mathbf{x} \in \Gamma$ for some $\Gamma \in \mathfrak{C}(2^M)$ and since Γ has diameter $\varepsilon/2$ we have $\Gamma \in C(2^M)$, which shows (5.6). Since the union of the cubes from $C(2^{i-1})$ is contained in the union

https://doi.org/10.1017/S0004972713000324 Published online by Cambridge University Press

from $C(2^i)$ we get (5.6). Hence

$$N_F(\Omega) \le \sum_{i=1}^{M} \sum_{\Gamma \in \mathcal{B}_i} N_F(\Gamma)$$

and using Corollary 3.2, as $m2^{-M} \to \infty$,

$$\begin{aligned}\sum_{i=1}^{M} \sum_{\Gamma \in \mathcal{B}_i} N_F(\Gamma) &\ll \sum_{i=1}^{M} \sum_{\Gamma \in \mathcal{B}_i} \left(\frac{m}{2^i}\right)^{d-k/2r(k+1)+o(1)} \\ &\quad + \sum_{i=1}^{M} \sum_{\Gamma \in \mathcal{B}_i} m^{d-1/2r(k+1)+o(1)} 2^{-i(d+o(1))} \\ &\ll m^{d-k/2r(k+1)+o(1)} 2^{o(M)} \sum_{i=1}^{M} 2^{ik/2r(k+1)} \frac{\#\mathcal{B}_i}{2^{id}} \\ &\quad + m^{d-1/2r(k+1)+o(1)} 2^{o(M)} \sum_{i=1}^{M} \frac{\#\mathcal{B}_i}{2^{id}}.\end{aligned}$$

We use (5.2) to bound

$$\sum_{i=1}^{M} \frac{\#\mathcal{B}_i}{2^{id}} \le \mu(\Omega_\varepsilon) = \mu(\Omega) + O\left(\frac{1}{2^M}\right)$$

and from (5.5), for $N \le M$,

$$\begin{aligned}\sum_{i=1}^{M} 2^{ik/2r(k+1)} \frac{\#\mathcal{B}_i}{2^{id}} &= \sum_{i=1}^{N} 2^{ik/2r(k+1)} \frac{\#\mathcal{B}_i}{2^{id}} + \sum_{i=N+1}^{M} 2^{ik/2r(k+1)} \frac{\#B_i}{2^{id}} \\ &\ll 2^{Nk/2r(k+1)} \sum_{i=1}^{N} \frac{\#\mathcal{B}_i}{2^{id}} + \sum_{i=N+1}^{M} 2^{ik/2r(k+1)} \frac{2^{i(d-1)}}{2^{id}} \\ &\ll 2^{Nk/2r(k+1)} (\mu(\Omega) + 2^{-M}) + 2^{-N(1-k/2r(k+1))} \\ &\ll 2^{Nk/2r(k+1)} (\mu(\Omega) + 2^{-N}).\end{aligned}$$

Hence

$$\begin{aligned}N_F(\Omega) &\le m^{d-k/2r(k+1)+o(1)} 2^{Nk/2r(k+1)+o(M)} (\mu(\Omega) + 2^{-N}) \\ &\quad + 2^{o(M)} m^{d-1/2r(k+1)+o(1)} (\mu(\Omega) + 2^{-M}).\end{aligned} \tag{5.7}$$

Recalling that $\mu(\Omega) \ge m^{-1}$, to balance the two terms involving N, we choose

$$2^{-N} \le \mu(\Omega) \log m < 2^{-N+1}.$$

Substituting this choice into (5.7) gives

$$\begin{aligned}N_F(\Omega) &\le m^{d-k/2r(k+1)} 2^{o(M)} \mu(\Omega)^{1-k/2r(k+1)} \\ &\quad + m^{d-1/2r(k+1)+o(1)} 2^{o(M)} (\mu(\Omega) + 2^{-M}).\end{aligned}$$

https://doi.org/10.1017/S0004972713000324 Published online by Cambridge University Press

The same choice for M is essentially optimal,

$$2^{-M} \le m^{-1} \log m \le 2^{-M+1}. \tag{5.8}$$

This gives

$$N_F(\Omega) \le m^{d-k/2r(k+1)+o(1)}\mu(\Omega)^{1-k/2r(k+1)} + m^{d-1/2r(k+1)+o(1)}\mu(\Omega),$$

where we have replaced $2^{o(M)}$ with $m^{o(1)}$ since $\mu(\Omega) \ge m^{-1}$. Theorem 3.4 follows since for the choice of M in (5.8), for $\mu(\Omega) \ge m^{-1}$,

$$m2^{-M} \gg m^{-1}\mu(\Omega) \log m \ge \log m,$$

which tends to infinity as $m \to \infty$. □

6. Proof of Theorem 3.5

Using the same constructions from Theorem 3.5,

$$N_F(\Omega) \le \sum_{i=1}^{M} \sum_{\Gamma \in \mathcal{B}_i} N_F(\Gamma).$$

Hence by Corollary 3.3,

$$\begin{aligned} N_F(\Omega) \le{}& 2^{o(M)} m^{d-1-(k-1)/2r(k+1)+o(1)} \sum_{i=1}^{M} 2^{i(1+(k-1)/2r(k+1))} \frac{\#\mathcal{B}_i}{2^{id}} \\ &+ 2^{o(M)} m^{d-1+o(1)} \sum_{i=1}^{M} 2^{i(1-1/2r(k+1))} \frac{\#\mathcal{B}_i}{2^{id}}. \end{aligned} \tag{6.1}$$

For the first sum, by (5.5),

$$\sum_{i=1}^{M} 2^{i(1+(k-1)/2r(k+1))} \frac{\#\mathcal{B}_i}{2^{id}} \le \sum_{i=1}^{M} 2^{i(k-1)/2r(k+1)} \ll 2^{M(k-1)/2r(k+1)}.$$

For the second sum,

$$\begin{aligned} \sum_{i=1}^{M} 2^{i(1-1/2r(k+1))} \frac{\#\mathcal{B}_i}{2^{id}} &= \sum_{i=1}^{N} 2^{i(1-1/2r(k+1))} \frac{\#\mathcal{B}_i}{2^{id}} + \sum_{i=N+1}^{M} 2^{i(1-1/2r(k+1))} \frac{\#\mathcal{B}_i}{2^{id}} \\ &\ll 2^{N(1-1/2r(k+1))}\left(\mu(\Omega) + \frac{1}{2^M}\right) + 2^{-N/2r(k+1)} \\ &\ll 2^{N(1-1/2r(k+1))}\mu(\Omega) + 2^{-N/2r(k+1)}. \end{aligned}$$

Substituting the above bounds into (6.1) gives

$$\begin{aligned} N_F(\Omega) \le{}& 2^{o(M)} m^{d-1-(k-1)/2r(k+1)+o(1)} 2^{M(k-1)/2r(k+1)} \\ &+ 2^{o(M)} m^{d-1+o(1)} (2^{N(1-1/2r(k+1))}\mu(\Omega) + 2^{-N/2r(k+1)}). \end{aligned}$$

https://doi.org/10.1017/S0004972713000324 Published online by Cambridge University Press

For $\mu(\Omega) \geq m^{-1+1/k}$ we choose N to balance the first and last terms, then choose M to balance the remaining terms, so that

$$2^{M-1} < \mu(\Omega)^{1/(k-1)} m \leq 2^M,$$
$$2^{-N} \leq 2^{M(k-1)} m^{-(k-1)} < 2^{-N+1},$$

which gives $N \leq M$ and

$$N_F(\Omega) \leq m^{d-1+o(1)} \mu(\Omega)^{1/2r(k+1)}.$$

If $m^{-1} \leq \mu(\Omega) < m^{-1+1/k}$ then we choose N to balance the last two terms and take M as small as possible subject to the condition $N \leq M$. This gives

$$2^{-M} \leq \mu(\Omega) < 2^{-M+1},$$
$$N = M$$

and

$$N_F(\Omega) \leq m^{d-1-(k-1)/2r(k-1)} \mu(\Omega)^{-(k-1)/2r(k+1)} + m^{d-1+o(1)} \mu(\Omega)^{1/2r(k+1)}.$$

Combining the above two bounds completes the proof. □

7. Comments

Using the methods of Theorems 3.4 and 3.5, we have not been able to give bounds for $N_F(\Omega)$ which are nontrivial when $\mu(\Omega) \leq m^{-1}$. This seems to be caused by two factors, the bound from Corollary 3.2 and the bounds for $\mu(\Omega_\varepsilon)^{\pm}$, which affect the estimates (5.2) and (5.5). For certain cases with prime modulus we may be able to do better than Theorem 3.5. For example, the same method may be combined with other bounds replacing Corollary 3.3 for more specific families of polynomials. This has the potential to obtain sharper estimates for such polynomials and also to increase the range of values of $\mu(\Omega)$ for which an analogue of Theorem 3.5 would apply. For example, Bourgain *et al.* [1] consider the number $J_\nu(p, h, s; \lambda)$ of solutions to the congruence

$$(x_1 + s) \cdots (x_\nu + s) \equiv \lambda \pmod{p}, \quad 1 \leq x_1, \ldots, x_\nu \leq h.$$

They show that if $h < p^{1/(\nu^2-1)}$ then we have the bound

$$J_\nu(p, h, s; \lambda) \leq \exp\left(c(\nu) \frac{\log h}{\log \log h}\right)$$

for some constant $c(\nu)$ depending only on ν [1, Lemma 2.33].

https://doi.org/10.1017/S0004972713000324 Published online by Cambridge University Press

In [2], the same authors consider the number $K_\nu(p, h, s)$ of solutions to the congruence

$$(x_1 + s) \cdots (x_\nu + s) \equiv (y_1 + s) \cdots (y_\nu + s) \not\equiv 0 \pmod{p},$$
$$1 \le x_1, \ldots, x_\nu, y_1, \ldots, y_\nu \le h,$$

and show that

$$K_\nu(p, h, s) \le \left(\frac{h^\nu}{p^{\nu/e_\nu}} + 1\right) h^\nu \exp\left(c(\nu)\frac{\log h}{\log\log h}\right)$$

for some constants e_ν and $c(\nu)$ depending only on ν [2, Theorem 17].

Another possible way to improve on our results for certain classes of well-shaped sets is to use Weyl's formula for tubes [16, Equation (2)] and Steiner's formula for convex bodies [11, Equation (4.2.27)] to give an explicit constant in (2.1) for certain subsets of $[0, 1]^d$ for which these formulas are valid. This would have the effect of improving on the bounds (5.2) and (5.5) and hence the bound for $N_F(\Omega)$ and possibly the range of values of $\mu(\Omega)$ for which this bound would be valid.

Acknowledgements

The author would like to thank Igor Shparlinski for suggesting this problem and for his guidance while working on it and writing the current paper. The author would also like to thank the referees for their numerous suggestions and advice in improving the paper.

References

[1] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, 'On the hidden shifted power problem', *SIAM J. Comput.* **41** (2012), 1524–1557.
[2] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, 'On congruences with products of variables from short intervals and applications', *Proc. Steklov Inst. Math.* **280** (2013), 67–96.
[3] M.-C. Chang, J. Cilleruelo, M. Z. Garaev, J. Hernández, I. E. Shparlinski and A. Zumalacárregui, 'Concentration of points and isomorphism classes of hyperelliptic curves over a finite field in some thin families', arXiv:1111.1543.
[4] J. Cilleruelo, M. Garaev, A. Ostafe and I. E. Shparlinski, 'On the concentration of points of polynomial maps and applications', *Math. Z.* **272** (2012), 825–837.
[5] É. Fouvry, 'Consequences of a result of N. Katz and G. Laumon concerning trigonometric sums', *Israel J. Math.* **120** (2000), 81–96.
[6] É. Fouvry and N. Katz, 'A general stratification theorem for exponential sums, and applications', *J. reine angew. Math.* **540** (2001), 115–166.
[7] A. Granville, I. E. Shparlinski and A. Zaharescu, 'On the distribution of rational functions along a curve over $\mathbb{F}_p$ and residue races', *J. Number Theory* **112** (2005), 216–237.
[8] W. Luo, 'Rational points on complete intersections over $\mathbb{F}_p$', *Int. Math. Res. Not. IMRN* **1999** (1999), 901–907.
[9] S. Parsell, S. Prendiville and T. Wooley, 'Near-optimal mean value estimates for multidimensional Weyl sums', arXiv:1205.6331.
[10] W. Schmidt, 'Irregularities of distribution. IX', *Acta Arith.* **27** (1975), 385–396.
[11] R. Schneider, *Convex Bodies: The Brunn-Minkowski Theory*, Encyclopedia of Mathematics and its Applications 44 (Cambridge University Press, 1993).

https://doi.org/10.1017/S0004972713000324 Published online by Cambridge University Press

[12] I. E. Shparlinski, 'On the distribution of points on multidimensional modular hyperbolas', *Proc. Japan Acad. Sci. Ser. A* **83** (2007), 5–9.
[13] I. E. Shparlinski, 'On the distribution of solutions to polynomial congruences', *Archiv. Math.* **99** (2012), 345–351.
[14] I. E. Shparlinski and A. N. Skorobogatov, 'Exponential sums and rational points on complete intersections', *Mathematika* **37** (1990), 201–208.
[15] A. N. Skorobogatov, 'Exponential sums, the geometry of hyperplane sections, and some Diophantine problems', *Israel J. Math.* **80** (1992), 359–379.
[16] H. Weyl, 'On the volume of tubes', *Amer. J. Math.* **61** (1939), 461–472.
[17] A. Zumalacárregui, 'Concentration of points on modular quadratic forms', *Int. J. Number Theory* **7** (2011), 1835–1839.

BRYCE KERR, Department of Computing, Macquarie University,
Sydney, NSW 2109, Australia
e-mail: bryce.kerr@students.mq.edu.au

https://doi.org/10.1017/S0004972713000324 Published online by Cambridge University Press