ON THE SPACES GENERATED BY VECTORS WITH COORDINATES IN INCOMPLETE RESIDUE SYSTEMS

ANDREW KRESCH

Abstract. We characterize one-dimensional subspaces of three-dimensional space over a finite field of odd prime order, containing a vector whose coordinates are constrained to half of the nonzero residue classes.

1. Introduction

Let p be a prime number, n a positive integer, and $S \subset (\mathbf{Z}/p\mathbf{Z})^n$ the solution set to a system of polynomial equations. It is of interest to understand the number and distribution of points in S; see, e.g., [6], [3], [8], [7], [4], [5]. To understand the number of points in a subset $B \subset (\mathbf{Z}/p\mathbf{Z})^n$ — often the reduction mod p of a product of integer intervals — the formula (with notation $\cdot$ for standard dot product of vectors)

$$\sum_{\mathbf{c}\in(\mathbf{Z}/p\mathbf{Z})^n} \sum_{\mathbf{j}\in B} e^{2\pi i \frac{\mathbf{c}\cdot\mathbf{j}}{p}} \sum_{\mathbf{k}\in S} e^{-2\pi i \frac{\mathbf{c}\cdot\mathbf{k}}{p}} = p^n |B \cap S|$$

leads to useful asymptotic estimates as $p \to \infty$ when S is, in some sense, sufficiently nonlinear. Useful asymptotic estimates are obtained, for instance, in [8] for S defined by a single equation without linear factor, by exhibiting a bound on the absolute value of the innermost sum for $\mathbf{c} \neq 0$ of the form $Cp^{n-\frac{3}{2}}$, with constant C depending only on n and the degree of the defining equation of S.

When S is a linear subspace, the innermost sum is $p^{\dim(S)}$ when $\mathbf{c} \in S^\perp$, and zero otherwise. Having no improvement to the exponent of p, the usefulness of the asymptotic estimates is sensitive to the defining equations. This article treats the case that S has dimension 1 and is not contained in any coordinate hyperplane, p is odd, and

$$B = \{1, \dots, \frac{p-1}{2}\} \times \cdots \times \{1, \dots, \frac{p-1}{2}\}.$$

The particular choice of B is motivated by a problem in algebraic geometry concerning algebraic stacks which is described in Section 5 and leads us to ask when $B \cap S$ can be empty. We focus our attention on the case $n = 3$, which is the first interesting case, since the case $n = 1$ is trivial and when $n = 2$ it is more or less immediate that $B \cap S = \emptyset$ if and only if $S = \operatorname{span}(1, -1)$. For any n it is clear that having a pair of coordinates of points of S that sums to zero is a sufficient condition for $B \cap S$ to be empty. When $n = 3$, our main theorem (Theorem 2) asserts that the condition is necessary as well, with one exception: $p = 7$ with $S = \operatorname{span}(1, 2, 4)$, up to permutation of coordinates.

Well known bounds on exponential sums (Section 2) lead to results that, while theoretically optimal, are far from practical for obtaining a statement such as the

Date: August 6, 2018.

2010 *Mathematics Subject Classification.* 11K36 (primary); 11T23, 14M25 (secondary).

main theorem. Elementary methods suffice to bridge the gap between impractical and practical bounds (Section 3), leading to a proof of the main theorem (Section 4).

The proof of the main theorem is supported by computations, performed over the course of several weeks. Scripts for the computer algebra system `magma` to carry out the most computationally demanding tasks have been made available on the author's webpage `http://www.math.uzh.ch/kresch`. The first of these carries out the case-by-case verification of the main theorem for specific values of p and is used for the verification for all $p < 12000$, mentioned at the beginning of the proof of Theorem 2. Toward the end of the proof a computational treatment of finitely many pairs (a, b) of integers is mentioned, and the second `magma` script is used for this task. On an 80-core computational server, the exhaustive verification for all $p < 12000$ required about one week of computation, and the treatment of (a, b) pairs, about two weeks. Attention was not given to optimization; rather, the tasks were coded quickly in `magma` and computations undertaken, once it was recognized that a practical running time could be achieved.

2. Basic estimates

We start by recalling some estimates due to Vinogradov [9, Chap. III, Prob. 11]. Here m is a positive integer, I is an interval in $\mathbf{Z}/m\mathbf{Z}$ (i.e., a subset obtained by reduction mod m of an integer interval), and a is a nonzero integer with $|a| \le m/2$. Then:

$$\Big|\sum_{j\in I} e^{2\pi i \frac{aj}{m}}\Big| \le \begin{cases} \frac{m}{3|a|} & \text{if } |a| \le \frac{m}{6}, \\ \frac{m}{2|a|} & \text{if } \frac{m}{6} < |a| \le \frac{m}{2}, \end{cases}$$

$$\sum_{b=0}^{m-1} \Big|\sum_{j\in I} e^{2\pi i \frac{bj}{m}}\Big| \le \begin{cases} m\log m + m & \text{if } m < 60, \\ m\log m & \text{if } m \ge 60. \end{cases}$$

As well, for $3 \le a \le m/6$ we have

$$\sum_{b=-a}^{a} \Big|\sum_{j\in I} e^{2\pi i \frac{bj}{m}}\Big| \le m\Big(\frac{2}{3}\log a + \frac{1}{2} + \frac{|I|}{m}\Big).$$

Theorem 1. *Let n be a positive integer and $0 \le \alpha_i < \beta_i \le 1$ for $i = 1, \ldots, n$. For $\varepsilon > 0$ there exists a finite collection of nonzero integer vectors $\mathbf{b}^{(1)}, \ldots, \mathbf{b}^{(r)} \in \mathbf{Z}^n$, such that for all primes p and vectors $\mathbf{v} \in (\mathbf{Z}/p\mathbf{Z})^n$ satisfying $\sum_{i=1}^n \mathbf{b}_i^{(j)}\mathbf{v}_i \ne 0$ for $j = 1, \ldots, r$, if we identify elements of $\mathbf{Z}/p\mathbf{Z}$ with integers in $\{0, 1, \ldots, p-1\}$ and define*

$$B_p = I_{p,1} \times \cdots \times I_{p,n}, \qquad I_{p,i} = \{k \in \mathbf{Z}/p\mathbf{Z} \,|\, \alpha_i p < k < \beta_i p\},$$

then we have

$$\left|\frac{B_p \cap (\mathbf{Z}/p\mathbf{Z})\mathbf{v}}{p} - \prod_{i=1}^n (\beta_i - \alpha_i)\right| < \varepsilon.$$

The proof is based on the formula

$$\sum_{\mathbf{c}\in\mathbf{v}^\perp} \sum_{\mathbf{j}\in B_p} e^{2\pi i \frac{\mathbf{c}\cdot\mathbf{j}}{p}} = p^{n-1}|B_p \cap (\mathbf{Z}/p\mathbf{Z})\mathbf{v}|.$$

The inner sum on the left corresponding to $\mathbf{c} = 0$ has value asymptotically approaching $p^n \prod_{i=1}^n (\beta_i - \alpha_i)$. Therefore it suffices to bound

$$p^{-n} \Big| \sum_{\mathbf{c} \in \mathbf{v}^\perp \setminus \{0\}} \sum_{\mathbf{j} \in B_p} e^{2\pi i \frac{\mathbf{c} \cdot \mathbf{j}}{p}} \Big| = \sum_{\mathbf{c} \in \mathbf{v}^\perp \setminus \{0\}} \Big(p^{-1} \sum_{j \in I_{p,1}} e^{2\pi i \frac{\mathbf{c}_1 j}{p}} \Big) \cdots \Big(p^{-1} \sum_{j \in I_{p,n}} e^{2\pi i \frac{\mathbf{c}_n j}{p}} \Big).$$

The collection of integer vectors in the statement can be taken to consist of all nonzero integer vectors with coordinates bounded in absolute value by a suitable positive integer M, together with $(N, 0, \ldots, 0)$, $(0, N, \ldots, 0)$, $\ldots$, $(0, \ldots, 0, N)$ for suitable positive N, the latter serving to ensure $p \gg 1$ and $\mathbf{v}_i \neq 0$ for all i. Suitable M and N arise from the following estimate.

In Lemma 1 we write $|k|$, for $k \in \mathbf{Z}/p\mathbf{Z}$, to mean $|k_0|$ for a representative $k_0 \in \mathbf{Z}$ of k of absolute value at most $p/2$.

Lemma 1. *Let p be a prime number, n a positive integer, $\mathbf{v} \in (\mathbf{Z}/p\mathbf{Z})^n$ a vector with nonzero coordinates, $u_k \in \mathbf{R}_{\geq 0}$ for all $k \in \mathbf{Z}/p\mathbf{Z}$, and A, B, C, $D \in \mathbf{R}_{>0}$ such that $u_k \leq C$ for all $k \in \mathbf{Z}/p\mathbf{Z}$ with $A < |k| \leq B$ and $\sum_{|k| \leq B} u_k \leq D$. Then*

$$\sum_{\substack{\mathbf{c} \in \mathbf{v}^\perp \\ |\mathbf{c}_1|, \ldots, |\mathbf{c}_n| \leq B \\ \max(|\mathbf{c}_1|, \ldots, |\mathbf{c}_n|) > A}} u_{\mathbf{c}_1} \cdots u_{\mathbf{c}_n} \leq nCD^{n-1}.$$

Proof. We may bound the sum from above by

$$\sum_{i=1}^n \sum_{\substack{\mathbf{c} \in \mathbf{v}^\perp \\ |\mathbf{c}_1|, \ldots, |\mathbf{c}_n| \leq B \\ |\mathbf{c}_i| > A}} u_{\mathbf{c}_1} \cdots u_{\mathbf{c}_n}. \tag{1}$$

The orthogonality requirement expresses $\mathbf{c}_i$ as a linear function in the other coordinates of $\mathbf{c}$. For each term, we have $u_{\mathbf{c}_i} \leq C$. We apply the inequality involving D to each of the other coordinates to obtain the desired inequality. □

For given M, we observe that $\mathbf{c} \in \mathbf{v}^\perp \setminus \{0\}$ implies $\max(|\mathbf{c}_1|, \ldots, |\mathbf{c}_n|) > M$. We suppose $M \geq 5$ and define $b = [\log(p/12M)/\log 2]$, which for $p > 12M$ is a nonnegative integer, the largest with $2^{b+1} M \leq p/6$. Now

$$\begin{aligned} p^{-n} \Big| \sum_{\mathbf{c} \in \mathbf{v}^\perp \setminus \{0\}} \sum_{\mathbf{j} \in B_p} e^{2\pi i \frac{\mathbf{c} \cdot \mathbf{j}}{p}} \Big| = \\ \sum_{a=0}^{b} \sum_{\substack{\mathbf{c} \in \mathbf{v}^\perp \\ |\mathbf{c}_1|, \ldots, |\mathbf{c}_n| \leq 2^{a+1} M \\ \max(|\mathbf{c}_1|, \ldots, |\mathbf{c}_n|) > 2^a M}} \Big(p^{-1} \sum_{j \in I_{p,1}} e^{2\pi i \frac{\mathbf{c}_1 j}{p}} \Big) \cdots \Big(p^{-1} \sum_{j \in I_{p,n}} e^{2\pi i \frac{\mathbf{c}_n j}{p}} \Big) \\ + \sum_{\substack{\mathbf{c} \in \mathbf{v}^\perp \\ \max(|\mathbf{c}_1|, \ldots, |\mathbf{c}_n|) > 2^{b+1} M}} \Big(p^{-1} \sum_{j \in I_{p,1}} e^{2\pi i \frac{\mathbf{c}_1 j}{p}} \Big) \cdots \Big(p^{-1} \sum_{j \in I_{p,n}} e^{2\pi i \frac{\mathbf{c}_n j}{p}} \Big). \end{aligned}$$

For each value of a, we obtain a bound for the corresponding summand of the first term on the right from the lemma with $A = 2^a M$, $B = 2A$, $C = 1/3A$, and $D = (2/3) \log B + 3/2$. To bound the second term on the right, we apply the lemma with

$A = 2^{b+1}M$, $B = (p-1)/2$, $C = 4/p$ (valid since $p/12 < A \le p/6$), and $D = \log p$. Combining these yields a bound of

$$\sum_{a=0}^{b} \frac{n}{3 \cdot 2^a M} \Big(\frac{2}{3} \log(2^{a+1}M) + \frac{3}{2} \Big)^{n-1} + \frac{4n}{p} (\log p)^{n-1}.$$

The first term is a partial sum of a convergent series, whose sum can be made arbitrarily small by increasing M. The second term tends to zero as p increases. So suitable M and N exist.

3. Bounds and improvement

Theorem 1 is optimal from a theoretical perspective. For the sake of discussion we fix $\alpha_i = 0$ and $\beta_i = 1/2$ for all i, although similar phenomena will be observed with arbitrary values (other than the trivial case $\alpha_i = 0$ and $\beta_i = 1$). A condition such as $\mathbf{v}_i + \mathbf{v}_j = 0$ for some i and j presents a clear obstruction to a result as in Theorem 1. There are other instances of failure, such as $n = 4$, $\mathbf{v} = (1, 2, -3, 4)$. So it is necessary to include a genericity hypothesis, as we did.

Practically, what we have is not very encouraging. Let us focus on $n = 3$, as in the main theorem. Then we need to take M well over 500 for the argument to lead to $B_p \cap (\mathbf{Z}/p\mathbf{Z})\mathbf{v} \neq \emptyset$ for $p \gg 1$. (This is so, even with the improvement to $D = (2/3)\log B + 1$, coming from intervals $I = \{1, \dots, (p-1)/2\}$ with $|I|/p < 1/2$.)

The proof of Lemma 1, where we count for every choice of $n-1$ coordinates of absolute value $\le |B|$ a contribution with $A < |\mathbf{c}_i| \le B$, leads to a gross overestimation which we can easily refine.

Proposition 1. *We adopt the notation of Lemma 1 and suppose, furthermore, that we have $E \ge 2B$ satisfying*

$$a\mathbf{v}_i + b\mathbf{v}_j \neq 0$$

for all $i \neq j$ and a, $b \in \mathbf{Z}$, not both zero, with $|a|, |b| \le E$. Then

$$\sum_{\substack{\mathbf{c} \in \mathbf{v}^\perp \\ |\mathbf{c}_1|, \dots, |\mathbf{c}_n| \le B \\ \max(|\mathbf{c}_1|, \dots, |\mathbf{c}_n|) > A}} u_{\mathbf{c}_1} \cdots u_{\mathbf{c}_n} \le nCD^{n-2} \max_{|k| \le B} u_k.$$

Proof. Suppose $\mathbf{c}$, $\mathbf{c}' \in \mathbf{v}^\perp$ differ only in the ith and jth coordinates. Suppose, furthermore, $|\mathbf{c}_i|$ and $|\mathbf{c}'_i|$ are both $\le B$, so $|\mathbf{c}'_i - \mathbf{c}_i| \le 2B \le E$. By the hypothesis, $|\mathbf{c}'_j - \mathbf{c}_j| > E$. Then $|\mathbf{c}_j|$ and $|\mathbf{c}'_j|$ cannot both be $\le B$. □

Proposition 2. *Suppose that we are in the situation of Proposition 1 with $n = 3$. Then*

$$\sum_{\substack{\mathbf{c} \in \mathbf{v}^\perp \\ |\mathbf{c}_1|, |\mathbf{c}_2|, |\mathbf{c}_3| \le B \\ \max(|\mathbf{c}_1|, |\mathbf{c}_2|, |\mathbf{c}_3|) > A}} u_{\mathbf{c}_1} u_{\mathbf{c}_2} u_{\mathbf{c}_3} \le 3C \sum_{1 \le |k| \le B} u_k^2.$$

Proof. Continuing with the notation of the proof of Proposition 1, if k is such that $\{i, j, k\} = \{1, 2, 3\}$, the ith summand in (1) never has contribution from distinct $\mathbf{c}$ and $\mathbf{c}'$ with $\mathbf{c}_j = \mathbf{c}'_j$ or $\mathbf{c}_k = \mathbf{c}'_k$, nor has contribution from any $\mathbf{c}$ with $\mathbf{c}_j = 0$ or $\mathbf{c}_k = 0$. So each summand in (1) has an upper bound of the form $C \sum_{1 \le |\ell| \le B} u_\ell u_{\sigma(\ell)}$ for some permutation σ of $\{\pm 1, \dots, \pm B\}$. We conclude by application of the Cauchy-Schwarz inequality. □

Returning to our case of interest ($n = 3$ with $\alpha_i = 0$ and $\beta_i = 1/2$ for all i), Proposition 2 yields an upper bound, under the assumption $B < p/6$, of

$$\frac{1}{A}\Big(2\sum_{n=1}^{\infty}\frac{1}{(3n)^2}\Big) = \frac{1}{A}\Big(\frac{\pi^2}{27}\Big).$$

We initially assume $p > 96000$. We fix $E = 2000$, i.e., we assume that $(\mathbf{Z}/p\mathbf{Z})\mathbf{v}$ has no element with two coordinates in $\{\pm 1, \dots, \pm 2000\}$. We also assume:

$$\begin{aligned}\mathbf{v} \not\perp \mathbf{c} \quad \text{for} \quad \mathbf{c} \in \{&(\pm 1, \pm 1, \pm 1), (\pm 1, \pm 1, \pm 2), (\pm 1, \pm 2, \pm 1), (\pm 2, \pm 1, \pm 1),\\ &(\pm 1, \pm 1, \pm 3) \text{ and cyclic permutations}, (\pm 1, \pm 1, \pm 4) \text{ and cyclic permutations},\\ &(\pm 1, \pm 2, \pm 2) \text{ and cyclic permutations}\}.\end{aligned} \tag{2}$$

These assumptions imply $\mathbf{v} \perp \mathbf{c}$ for at most one $\mathbf{c}$ with coordinates in $\{\pm 1, \dots, \pm 30\}$ and its scalar multiples. For instance, $\mathbf{v} \perp \mathbf{c}$ for $\mathbf{c} = (\pm 1, \pm 1, \pm 5)$ leads to contributions from $\pm\mathbf{c}$, …, $\pm 6\mathbf{c}$ of at most $2(1 + 1/2^3 + \cdots + 1/6^3)/(3 \cdot 3 \cdot 15)$. This is the largest possible from such $\mathbf{c}$; when combined with the quantity from Proposition 2 with $A = 30$ and $B = 1000$, this yields a bound of approximately 0.0298.

Lemma 1 with $A = 1000$ and $B = 16000$ leads to 0.0556.

Lemma 1 with $B = 2A$ for $A = 16000$ and successive doublings, as long as $B < p/6$, gives at most 0.0088.

Lemma 1 with $p/12 < A < p/6$ and $B = (p-1)/2$, for which we can take $C = 4/p$ and $D = \log p$, gives at most 0.0165.

The total $0.0298 + 0.0556 + 0.0088 + 0.0165 = 0.1107$ is less than $1/8$.

We treat primes $12000 < p < 96000$ with first bound exactly as above and modified second bound with $A = 1000$ and $B = [p/6]$. The third bound is omitted, and the fourth is modified to $A = [p/6]$, $B = (p-1)/2$, $C = 1/(2[p/6])$, and

$$D = \frac{1}{2} + 2\Big(\sum_{j=1}^{[\frac{p}{6}]}\frac{1}{3j} + \sum_{j=[\frac{p}{6}]+1}^{\frac{p-1}{2}}\frac{1}{2j}\Big).$$

On a case-by-case basis this is checked to yield a total of less than $1/8$.

4. Main theorem

We come to the statement of the main theorem.

Theorem 2. *Let p be an odd prime and $\mathbf{v} \in (\mathbf{Z}/p\mathbf{Z})^3$ a vector with nonzero coordinates, such that no pair of coordinates sums to zero. Then, except in the case $p = 7$ and $\mathbf{v} = \pm(1, 2, 4)$ up to permutation of coordinates, there always exists a scalar multiple of $\mathbf{v}$ whose coordinates lie in $\{1, \dots, (p-1)/2\}$.*

For primes less than 12000 the main theorem is checked by an exhaustive search.

Assuming $p > 12000$, by the bounds in Section 3 we only need to check the cases

(i) $\mathbf{v}$ may be scaled to a vector with two coordinates in $\{\pm 1, \dots, \pm 2000\}$,
(ii) no scalar multiple of $\mathbf{v}$ has two coordinates in $\{\pm 1, \dots, \pm 2000\}$, but $\mathbf{v} \perp \mathbf{c}$ for some $\mathbf{c}$ appearing in the list in (2).

Any $\mathbf{v}$ as in (i) may be further scaled so that two coordinates in $\{\pm 1, \dots, \pm 2000\}$ are, viewed as integers in that set, relatively prime. The third coordinate is represented by an integer of absolute value at most $(p-1)/2$. After permuting and possibly multiplying by -1, we may suppose the coordinates to be ordered, in absolute value,

in weakly ascending order with final coordinate positive. Case (i) therefore may be restated:

(i′) $\mathbf{v}$ is scalar multiple of a vector in $(\mathbf{Z}/p\mathbf{Z})^3$, reduction of $(a,b,c) \in \mathbf{Z}^3$ with $|a| \le |b| \le c \le (p-1)/2$, such that a, b, c have no common prime factor and

$$\begin{cases} |b| \le 2000, & \text{when } \gcd(a,b) = 1, \\ c \le 2000, & \text{when } \gcd(a,b) > 1. \end{cases}$$

The treatment of both cases will make use of the following elementary result.

Lemma 2. *Let A and E be positive integers and γ a positive real number, such that there exist positive integers B and M with*

$$\frac{1}{\gamma} \le M \le \min\Big(\frac{A+1}{B+1}, \sqrt{E}\Big) \qquad \text{and} \qquad \frac{1-\gamma}{2B} + \frac{1}{[E/M]} \le \frac{\gamma}{2} - \frac{1}{2E}.$$

Let a, b, $c \in \mathbf{Z}$ with $\max(|a|,|b|) \le |c|$. If there is no nontrivial $\mathbf{Z}$-linear relation among a, b, c with coefficients of absolute value at most A and no nontrivial $\mathbf{Z}$-linear relation among any two of a, b, c with coefficients of absolute value at most E, then for every pair of closed intervals I, $J \subset \mathbf{R}$ of length γ, we have

$$\big(\mathbf{Z}\big(\frac{a}{c}, \frac{b}{c}\big) + \mathbf{Z}^2\big) \cap I \times J \ne \emptyset.$$

Proof. Without loss of generality we have $\gcd(a,b,c) = 1$. So, the subgroup G of $(\mathbf{Q}/\mathbf{Z})^2$ generated by $(a/c, b/c)$ has order $|c|$. As well, a/c generates a subgroup of $\mathbf{Q}/\mathbf{Z}$ of order $> E$. Translating by a point with first coordinate close to the midpoint of I, we are reduced to proving the assertion under the assumption that

$$[-\delta, \delta] \subset I,$$

where $\delta = \gamma/2 - 1/2E$. The assertion is clear if J contains an integer point on the vertical axis, so we suppose the contrary. After translating vertically by an integer and possibly multiplying by -1, we obtain

$$J = [t, t+\gamma] \qquad \text{with} \qquad 0 < t \le \frac{1-\gamma}{2}.$$

We cover the unit square by rectangles of height $1/M$ and width $1/N$, where N is the largest integer with $MN < |c|$. We have $|c| > E$, so $N \ge [E/M]$. By the pigeonhole principle, there exists

$$0 \ne (u,v) \in \mathbf{Z}\big(\frac{a}{c}, \frac{b}{c}\big) + \mathbf{Z}^2$$

with

$$|u| < \frac{1}{N}, \qquad 0 \le v < \frac{1}{M}.$$

We assume that (u,v) is taken with $|u|$ as small as possible.

If $v \ge B|u|$ then we let $s = [t/v]$, and we have:

$$sv \le t, \qquad t \le (s+1)v \le t + v \le t + \gamma,$$

and

$$s|u| \le s\frac{v}{B} \le \frac{t}{B}, \qquad (s+1)|u| \le \frac{t}{B} + |u| \le \frac{1-\gamma}{2B} + \frac{1}{[E/M]} \le \delta.$$

Now suppose $v < B|u|$. This means that we have

$$u = \frac{a'}{c}, \qquad v = \frac{b'}{c},$$

with $1 \le |a'| \le M$ and $|b'| \le B|a'| - 1$. Let $g = \gcd(a', b')$. Notice that $g \mid c$: if there is prime p with, say, $p^i \,\|\, c$, $p^j \,\|\, g$, $j > i$, then using $\gcd(p, p^{-i}c) = 1$ we see that the subgroup of G generated by $(a'/c, b'/c)$ contains $(p^{-1}a'/c, p^{-1}b'/c)$, contradicting the minimality of $|u|$. Now the index of the subgroup of G generated by $(a'/c, b'/c)$ is g. In particular, $(ga/c, gb/c)$ lies in this subgroup. There is thus a nontrivial linear relation

$$b'a - a'b = mc$$

with $|m| \le a' + b'$. Since $M + BM - 1 \le A$, we have a contradiction. □

We record some parameters satisfying the first hypothesis of Lemma 2:

$$\gamma = 1/3,\ A = 14,\ E = 42 \qquad \text{and} \qquad \gamma = 1/25,\ A = E = 2000.$$

Proof of the main theorem. By the remarks above, it suffices to verify the assertion for $p > 12000$ and $\mathbf{v}$ as in case (i′) or as in case (ii).

Suppose $\mathbf{v}$ is given by some (a, b, c) as in (i′). When a and b are positive the assertion is obvious, so we suppose at least one of a and b is negative. We let $\delta = |b|/12000$ and define

$$\begin{cases} I = \left[\delta, \frac{1}{2}\right],\ J = \left[\delta, \frac{1}{2}\right], & \text{when } a < 0 \text{ and } b < 0, \\ I = \left[\delta, \frac{1}{2}\right],\ J = \left[0, \frac{1}{2} - \delta\right], & \text{when } a < 0 \text{ and } b > 0, \\ I = \left[0, \frac{1}{2} - \delta\right],\ J = \left[\delta, \frac{1}{2}\right], & \text{when } a > 0 \text{ and } b < 0. \end{cases}$$

Consider an interval $[t_0, t_0 + \varepsilon]$ in

$$\{t \in \mathbf{R} \,|\, (t(a, b) + \mathbf{Z}^2) \cap I \times J \neq \emptyset\}. \tag{3}$$

If $c \ge 1/\varepsilon$ then the set (3) contains some rational number ℓ/c with $\ell \in \mathbf{Z}$. It follows that the set

$$\left\{t \in \mathbf{R} \,|\, (t(a, b, c) + \mathbf{Z}^3) \cap \left[0, \frac{1}{2}\right]^3 \neq \emptyset\right\} \tag{4}$$

contains the interval with left endpoint ℓ/c of length

$$\min\left(\frac{1}{2c}, \frac{1}{12000}\right).$$

The length is always at least $1/p$. So whenever $c \ge 1/\varepsilon$ for some ε as above the assertion is valid.

For every a and b, not both positive, with $a + b \neq 0$ and $|a| \le |b| \le 2000$, we can determine the largest value of ε that occurs and thereby determine $c_0 = 1/\varepsilon$, taken to be at most 2000 in case $\gcd(a, b) > 1$, such that the verification of case (i′) for given a and b is reduced to checking (by directly computing the set (4)) the finitely many cases

$$|b| \le c < c_0.$$

Some speedup is gained by appealing to Lemma 2 with $\gamma = 1/3$, $A = 14$, $E = 42$ for most a and b (all except (a, b) proportional to some $(\pm a_0, \pm b_0)$ with $a_0,\ b_0 \in \{1, \dots, 42\}$); for the values of c for which the hypothesis of the lemma is satisfied, the above argument (where, we observe, the intervals I and J have length $\ge 1/3$) establishes the assertion for all $p > 12000$.

Case (ii) is treated with Lemma 2, applied with $\gamma = 1/25$, $A = E = 2000$; the condition in (ii) on pairs of coordinates guarantees applicability to any pair of coordinates of $\mathbf{v}$ together with p. For each $\mathbf{c}$ in the list in (2), the condition $\mathbf{v} \perp \mathbf{c}$ ensures that some coordinate of $\mathbf{v}$ is a linear combination of the other two, with coefficients that are integers, small in magnitude. For each pair of coefficients that arises we examine

the graph of the corresponding linear function $(\mathbf{R}/\mathbf{Z})^2 \to \mathbf{R}/\mathbf{Z}$ and identify a component of the intersection with $[0,1/2]^3$ whose projection to the first two coordinates contains a square of side length at least $1/25$. □

5. Motivating problem

The choice of main theorem was guided by a recent result of Bergh [2] on algebraic orbifolds, spaces which are close to nonsingular algebraic varieties but where the local structure is as a nonsingular affine variety with specified finite subgroup of the automorphism group. So, for instance, we might have complex affine 2-space with $(x,y) \mapsto (-x,-y)$. If we forget the orbifold structure and just examine the orbits of complex points, then we are looking at the singular variety defined by the equation $uv - w^2 = 0$ in affine 3-space. Bergh proves that a general algebraic orbifold can be transformed by well-defined simple operations to one which remains nonsingular after forgetting the orbifold structure. The method of proof is to reduce the problem to one in toric geometry, where the orbifold is not arbitrary but of a specific form given by combinatorial data.

Let n be a positive integer, and let $\mathbf{u}_1, \ldots, \mathbf{u}_n \in \mathbf{Z}^n$ be a collection of linearly independent vectors; their $\mathbf{Z}$-span is a sublattice N' of $N = \mathbf{Z}^n$ of finite index. The dual vectors $\mathbf{u}_1^\vee, \ldots, \mathbf{u}_n^\vee$ span a lattice M' containing $M = N^\vee$ (again, of finite index). Given a field k, the polynomial ring $k[X_1, \ldots, X_n] = k[\mathbf{N} \cdot \mathbf{u}_1^\vee + \cdots + \mathbf{N} \cdot \mathbf{u}_n^\vee]$ admits a natural coaction by the Hopf algebra $k[M'/M]$, with coinvariant ring

$$k[(\mathbf{Q}_{\geq 0} \cdot \mathbf{u}_1^\vee + \cdots + \mathbf{Q}_{\geq 0} \cdot \mathbf{u}_n^\vee) \cap M]. \tag{5}$$

The goal is to reach a situation where the ring (5) is again a polynomial ring; then each $\mathbf{u}_i$ is a multiple d_i of a vector in N such that, taken together, these form a $\mathbf{Z}$-basis of N. When k is algebraically closed of characteristic zero, we can translate this situation into geometry: affine n-space over k is acted upon diagonally by a product of finite cyclic groups (groups of roots of unity), and the space of orbits is again affine n-space. The goal is achieved using two kind of combinatorial operations, corresponding to two kinds of geometric operations used in Bergh's destackification algorithm: (i) star subdivision, which involves replacing $\mathbf{u}_i$ by $\mathbf{u}_1 + \cdots + \mathbf{u}_n$ (this is done for each i, leading to n new instances of the basic combinatorial set-up), and (ii) root operation, replacing each $\mathbf{u}_i$ by a positive integer scalar multiple $d_i\mathbf{u}_i$.

Let us suppose we wish to destackify an algebraic orbifold over a field k of positive characteristic. Bergh's destackification is applicable in the *tame* setting: the characteristic of k should not divide the order of the stabilizer group of any point. Interestingly, the result after transformation is no longer generally an algebraic orbifold but rather an object known as a *tame Artin stack* [1]. In the combinatorial set-up, tameness corresponds to the requirement that $\mathrm{char}(k)$ does not divide the order of M'/M. When operation (ii) is performed with $\mathrm{char}(k)$ dividing some d_i, we leave the realm of algebraic orbifolds and must call upon the theory of tame Artin stacks. Suppose, for instance, $\mathrm{char}(k) = 2$ and we have $n = 2$, $\mathbf{u}_1 = (1,0)$, $\mathbf{u}_2 = (-2,3)$, so M'/M has order 3. Then the algorithm could start by applying operation (ii) with $d_1 = 2$ and $d_2 = 1$. (The precise first step in the algorithm depends on further data known as a "distinguished structure", which we ignore for this discussion.)

A natural question is the extent to which destackification is possible if we work only with algebraic orbifolds, or in combinatorial terms, if we restrict operation (ii) by requiring $\mathrm{char}(k)$ not to divide any d_i. Suppose $\mathrm{char}(k) = 2$, with arbitrary n and

$\mathbf{u}_i$ equal to the ith standard basis element for $i = 1, \ldots, n-1$ and

$$\mathbf{u}_n = (-a_1, \ldots, -a_{n-1}, p)$$

for some odd prime p, with $a_i \in \{1, \ldots, p-1\}$ for $i = 1, \ldots, n-1$. (This is in some sense the general case, up to $\mathbf{Z}$-linear change of coordinates, for order p stabilizer.) Bergh's algorithm, simplified as in the previous paragraph, would start by applying operation (ii) with $d_i \in \{1, \ldots, p-1\}$ for all i and

$$(d_1, \ldots, d_n) \qquad \text{a scalar multiple of} \qquad (a_1, \ldots, a_{n-1}, 1)$$

in $(\mathbf{Z}/p\mathbf{Z})^n$. So we are led to ask whether some scalar multiple of $(a_1, \ldots, a_{n-1}, 1)$ has odd coordinates when represented with positive integer coordinates less than p. Equivalently (multiplying by -1), we ask for even coordinates, or (relating by a factor of 2), we ask for the coordinates to be in $\{1, \ldots, (p-1)/2\}$.

References

[1] D. Abramovich, M. Olsson, and A. Vistoli, *Tame stacks in positive characteristic*, Ann. Inst. Fourier (Grenoble) 58 (2008), 1057–1091.

[2] D. Bergh, *Functorial destackification of tame stacks with abelian stabilisers*, Compositio Math. 153 (2017), 1257–1315.

[3] J. H. H. Chalk, *The number of solutions of congruences in incomplete residue systems*, Canad. J. Math. 15 (1963), 291–296.

[4] T. Cochrane, *The distribution of solutions to equations over finite fields*, Trans. Amer. Math. Soc. 293 (1986), 819–826.

[5] M. Fujiwara, *Distribution of rational points on varieties over finite fields*, Mathematika 35 (1988), 155–171.

[6] L. J. Mordell, *On the number of solutions in incomplete residue sets of quadratic congruences*, Arch. Math. (Basel) 8 (1957), 153–157.

[7] G. Myerson, *The distribution of rational points on varieties defined over a finite field*, Mathematika 28 (1981), 153–159.

[8] R. A. Smith, *The distribution of rational points on hypersurfaces defined over a finite field*, Mathematika 17 (1970), 328–332.

[9] I. M. Vinogradov, *Elements of number theory*, Dover Publications, New York, 1954.

Institut für Mathematik, Universität Zürich, Winterthurerstrasse 190, CH-8057 Zürich, Switzerland

E-mail address: andrew.kresch@math.uzh.ch