Permutations destroying arithmetic structure

Veselin Jungić
Department of Mathematics
Simon Fraser University
Burnaby, Canada
vjungic@sfu.ca

Julian Sahasrabudhe
Department of Mathematics
Simon Fraser University
Burnaby, Canada
jds16@sfu.ca

Submitted: Dec 19, 2012; Accepted: Mar 24, 2015; Published: Apr 14, 2015
Mathematics Subject Classifications: 05C88, 05C89

Abstract

Given a linear form $C_1X_1 + \cdots + C_nX_n$, with coefficients in the integers, we characterize exactly the countably infinite abelian groups G for which there exists a permutation f that maps all solutions $(\alpha_1, \ldots, \alpha_n) \in G^n$ (with the α_i not all equal) to the equation $C_1X_1+\cdots+C_nX_n = 0$ to non-solutions. This generalises a result of Hegarty about permutations of an abelian group avoiding arithmetic progressions. We also study the finite version of the problem suggested by Hegarty. We show that the number of permutations of $\mathbb{Z}/p\mathbb{Z}$ that map all 4-term arithmetic progressions to non-progressions, is asymptotically $e^{-1}p!$.

Keywords: Pattern Avoidance; Additive Combinatorics

1 Introduction

Hegarty [8] characterized the countably infinite abelian groups for which there exists a bijection mapping arithmetic progressions to non-arithmetic progressions. He also considered other problems regarding permutations f of an abelian group that ruin arithmetic structures. In particular, for large enough N, he gave a construction of a permutation of $\mathbb{Z}/N\mathbb{Z}$ that mapped all 4-term progressions to non-progressions.

In the sequel we address the following problem. If G is a countably infinite abelian group and $C_1, C_2, \ldots, C_n \in \mathbb{Z}$, under what conditions does there exist a bijection $f : G \to G$ such that, for any $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in G^n$, with the α_i not all equal, if $\sum_{i=1}^n C_i\alpha_i = 0$ then $\sum_{i=1}^n C_if(\alpha_i) \neq 0$? We obtain Hegarty's result as a special case of our result for $C_1 = C_2 = 1$ and $C_3 = -2$.

We also continue Hegarty's investigations in the finite setting. We show that the number of permutations that map 4-term progressions to non-progressions in $\mathbb{Z}/p\mathbb{Z}$, (p a prime) is asymptotically $e^{-1}p!$

2 Breaking linear forms in countably infinite abelian groups

For this section we take G to be a countably infinite abelian group and $L(X_1,\dots,X_n) = C_1X_1 + \cdots C_nX_n$ to be a linear form with integer coefficients.

Before stating our main result, Theorem 1, we introduce the following terms. We say that $(\alpha_1,\dots\alpha_n) \in G$ is a *proper* solution to the linear equation $C_1X_1 + \cdots + C_nX_n = 0$ if the $C_1\alpha_1 + \cdots + C_n\alpha_n = 0$ and the elements $\alpha_1, \alpha_2, \dots, \alpha_n$ are not all equal. A solution is called *improper* otherwise. We say that a permutation f of G *breaks* the linear form $L(X_1,\dots,X_n)$ *over* G if all proper solutions to $L(X_1,\dots,X_n) = 0$ over G get mapped to non-solutions of $L(X_1,\dots,X_n) = 0$. That is, f breaks L over G if f is a permutation of G such that if $(\alpha_1,\dots,\alpha_n) \in G^n$ is a proper solution to $L(X_1,\dots,X_n) = 0$ then $(f(\alpha_1),\dots,f(\alpha_n))$ is not a solution. We call a linear form $L = C_1X_1 + \cdots + C_nX_n$ *minimal* if $\sum_{i\in[n]} C_i = 0$ and $\sum_{i\in B} C_i \neq 0$ for any nonempty proper subset B of $[n]$. For example, the linear form $X_1+X_2-2X_3$ is minimal, while the linear form $X_1+X_2-X_3-X_4$ is not.

We remark that, for the purposes of breaking the linear form $L = C_1X_1 + \cdots + C_nX_n$ over G, it is natural to assume that $\sum_{i\in[n]} C_i = 0$. For if $\sum_{i\in[n]} C_i = A \neq 0$ then for any $g \in G$, with the order of g not dividing A, the bijection $f(x) = x + g$ breaks the linear form L. Also note that if L is such that $\sum_{i\in[n]} C_i = 0$ but L is not minimal then, for some nonempty proper subset B of $[n]$,

$$\sum_{i\in B} C_i = \sum_{i\in[n]\setminus B} C_i = 0.$$

It follows that for any bijection $f : G \to G$ and any $t, t' \in G$,

$$t\sum_{i\in B} C_i + t'\sum_{i\in[n]\setminus B} C_i = f(t)\sum_{i\in B} C_i + f(t')\sum_{i\in[n]\setminus B} C_i = 0$$

and f does not break L. Hence the question of what groups have a permutation breaking L is only interesting for minimal linear forms.

Let $L = C_1X_1 + \cdots + C_nX_n$ be a minimal linear form, let $\mathcal{B}$ be the set of all non-empty proper subsets of $[n]$, and let $\sum_{\mathcal{B}} = \{\sum_{i\in B} C_i : B \in \mathcal{B}\}$. For $m \in \mathbb{N}$, let Ω_m denote the m-torsion subgroup of G, i.e., the subgroup of G consisting of all elements that have order that divides m. We can now state the main result of this section.

Theorem 1. *The minimal linear form L is breakable over a countably infinite abelian group G if and only if for any $\beta \in \sum_{\mathcal{B}}$ the quotient group $G/\Omega_{|\beta|}$ is infinite.*

We need the following definition in the course of the proof of Theorem 1. We say that a group G has the $(q_1,\dots,q_n)$-property, where the q_i are integers, if for any finite set $A \subset G$ there exists some $g \in G$ so that $q_ig \notin A$ for all $i = 1,\dots,n$. The following four lemmas give some sufficient conditions under which a group G has the $(q_1,\dots,q_n)$-property.

Lemma 2. *If H_1 has the $(q_1,\dots,q_n)$-property and H_2 has the $(r_1,\dots,r_m)$-property then $G = H_1 \times H_2$ has the $(q_1,\dots,q_n,r_1,\dots r_m)$-property.*

Proof. Suppose that H_1 has the $(q_1,\dots,q_n)$-property and H_2 has the $(r_1,\dots,r_m)$-property. Let A be a finite subset of $G = H_1 \times H_2$ and let A_1 and A_2 denote the projections of A onto H_1, H_2 respectively. Since H_1 has the $(q_1,\dots,q_n)$-property there is $g_1 \in H_1$ so that $q_ig_1 \notin A_1$ for $i = 1,\dots,n$. Similarly, there is $g_2 \in H_2$ so that $r_ig_2 \notin A_2$ for all $i = 1,\dots,m$. Hence $q_i(g_1 \times g_2) = q_ig_1 \times q_ig_2 \notin A$ for $i = 1,\dots,n$ and $r_i(g_1 \times g_2) \notin A$ for $i = 1,\dots,m$. □

Lemma 3. *If $|lcm(q_1,\dots,q_n)G| = \infty$ then G has the $(q_1,\dots,q_n)$-property.*

Proof. Suppose, for a contradiction, that there exists a finite set A so that for every $g \in G$ we have $q_ig \in A$ for some $i \in [n]$. Now write $\mathrm{lcm}(q_1,\dots,q_n) = kq_i$ so we have $\mathrm{lcm}(q_1,\dots,q_n)g = kq_ig = ka$ for some $a \in A$. Hence $|\mathrm{lcm}(q_1,\dots,q_n)G| < \infty$, a contradiction. □

Lemma 4. *If G has an element of infinite order then G has the $(q_1,\dots,q_n)$-property for any non-zero integers $q_1,\dots q_n$.*

Proof. Suppose that G has an element of infinite order. Then G has a subgroup $H \cong \mathbb{Z}$. Since $\mathrm{lcm}(q_1,\dots,q_n)H$ is a subgroup of $\mathrm{lcm}(g_1,\cdots,g_n)G$, from $|\mathrm{lcm}(q_1\cdots q_n)H| = \infty$ it follows that $|\mathrm{lcm}(g_1,\dots,g_n)G| = \infty$, and we appeal to Lemma 3. □

In the proof of the next lemma we will use the following notation. For a positive integer n and a prime p, let $\nu_p(n)$ denote the largest integer k for which $p^k|n$.

Lemma 5. *Let G be an abelian group and let $q_1,\dots,q_n$ be integers. If $|G/\Omega_{q_i}| = \infty$ for all $i \in [n]$ then G has the $(q_1,\dots,q_n)$-property.*

Proof. We argue by induction on n. If $n = 1$, assume for a contradiction that for every $g \in G$ we have $q_1g \in A$, for some finite set A. Thus, it follows that $qG \subseteq A$. But, since A is finite and $qG \cong G/\Omega_{|q_1|}$, a contradiction follows.

Now assume that $n > 1$. By Lemma 4, we may assume that every element of G has finite order. Thus G admits the decomposition

$$G \cong \bigoplus_{p\ prime} T_p,$$

where T_p denotes the subgroup of elements of G that have order a power of p.

Note that

$$q_i\left(\bigoplus_{p\ prime} T_p\right) = \bigoplus_{p\ prime} q_iT_p,$$

for all $i \in [n]$. We remark that, for all $i \in [n]$, $|q_iG| = |G/\Omega_{q_i}| = \infty$.

If there are infinitely many primes p such that T_p is non-trivial, then we may write $G \cong H_1 \times H_2$, with $H_1 = \bigoplus_p T_p$, where p ranges over all primes p that divide at least one of the q_i's and $H_2 = \bigoplus_p T_p$, where p ranges over all primes that divide none of the q_i's. Since $|H_2| = \infty$ and since $\mathrm{lcm}(q_1, \ldots q_n)H_2 \cong H_2$ it follows that $|\mathrm{lcm}(q_1, \ldots q_n)H_2| = \infty$. By Lemma 3, H_2 has the $(q_1, \ldots, q_n)$-property and consequently G has the $(q_1, \ldots, q_n)$-property.

Suppose that there are only finitely many primes p such that $T_p \neq \{e\}$. Then $G \cong \bigoplus_{j=1}^k T_{p_j}$, for some primes $p_1, \ldots, p_k$, and $q_iG \cong \bigoplus_{j=1}^k q_iT_{p_j}$ for all $i \in [n]$. This together with $|q_iG| = \infty$ implies that for each q_i there is some prime p_j for which $|q_iT_{p_j}| = \infty$. Let $f : \{q_1, \ldots, q_n\} \to \{p_1, \ldots, p_k\}$ be a function such that $|q_iT_{f(q_i)}| = \infty$ for all $i \in [n]$.

We distinguish two cases.

If f is not a constant function we partition $\{p_1, \ldots, p_k\} = R \cup S$ so that $f(\{q_1, \ldots, q_n\}) \cap R \neq \emptyset$ and $f(\{q_1, \ldots, q_n\}) \cap S \neq \emptyset$. Next we define $H_1 = \bigoplus_{p_j \in R} T_{p_j}$ and $H_2 = \bigoplus_{p_j \in S} T_{p_j}$ and note that $|q_iH_1| = \infty$ for $f(q_i) \in R$ and $|q_iH_2| = \infty$ for $f(q_i) \in S$. By induction, H_1 has the $(q_i)_{f(q_i) \in R}$-property and H_2 has the $(q_i)_{f(q_i) \in S}$-property. By Lemma 2 it follows that G has the $(q_1, \ldots, q_n)$-property.

If f is a constant function then there is a prime p for which $|q_iT_p| = \infty$ for all $i \in [n]$. We write $G \cong T_p \times H$ and assume that q_1 is such that $\nu_p(q_1)$ is maximum over $\{q_1, \ldots, q_n\}$. From $\mathrm{lcm}(q_1, \ldots, q_n)T_p \cong q_1T_p$ it follows that $|\mathrm{lcm}(q_1, \ldots, q_n)T_p| = \infty$. By Lemma 3, T_p has the $(q_1, \ldots, q_n)$ property and therefore G has the $(q_1, \ldots, q_n)$ property. □

The proof of Theorem 1 follows.

Proof. We define a permutation $f : G \to G$ in a "back-and-forth" manner. Let $G = \{x_1, x_2, \ldots\}$ be an enumeration of G. We start the recursion by setting $f(x_1) = x_1$. We now define f in stages. At stage t we have the following:

1. The function f has been defined on a finite set D_t that contains $x_1, \ldots, x_t$.

2. The function f^{-1} has been defined on a finite set D'_t that contains $x_1, \ldots, x_t$.

3. There are no proper pairs of solutions $(\alpha_1, \ldots, \alpha_n)$, $(f(\alpha_1), \ldots, f(\alpha_n))$, with $\alpha_i \in D_t$.

4. f is a bijection $f : D_t \to D'_t$.

Assuming inductively, that the above hold for the first t stages we proceed to stage $t+1$ and show that we can preserve the above properties. At stage $t+1$ we choose the smallest value in the enumeration of $G \setminus D_t$, say x_k, for which the function f has not yet been defined. We want to choose a value for $f(x_k)$ among $G \setminus f(D_t)$ such that no proper solutions are mapped to solutions. To this end, for each $I \in \mathcal{B}$ we define

$$A_I = \left\{ -\sum_{i \in I} C_i a_i : a_i \in f(D_t) \right\}$$

and then set

$$A = \bigcup_{I \in \mathcal{B}} A_I$$

It is clear that A is a finite set. Thus $A \cup f(D_t)$ is a finite set. By Lemma 5, G has the $(q : q \in \sum_{\mathcal{B}})$-property and, consequently, has the $(q : q \in \sum_{\mathcal{B}} \cup \{1\})$-property. It follows that we can find a $g \in G$ such that $qg \notin A \cup f(D_t)$ for every $q \in \sum_{\mathcal{B}} \cup \{1\}$. We define $f(x_k) = g$. We now check the desired properties. First observe that $f(x_k) \notin f(D_t)$. Now suppose that there is some proper solution $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ to the linear equation $L(X_1, \ldots, X_n) = 0$ for which $f(\alpha_i)$ is defined for $i = 1, \ldots, n$. We may assume that x appears among $\alpha_1, \ldots, \alpha_n$ as previous elements are left unaltered by the choice of $f(x_k)$. Hence we may define $S \subset [n]$ to be the non-empty, proper subset of indices i for which $\alpha_i = x$. Now suppose that $(f(\alpha_1), \ldots, f(\alpha_n))$ is a solution to the equation $L(X_1, \ldots, X_n) = 0$. In this case we have

$$0 = \sum_{i=1}^{n} C_i f(\alpha_i) = \sum_{i \in S} C_i g + \sum_{i \notin S} C_i f(\alpha_i)$$

and hence

$$g \left(\sum_{i \in S} C_i \right) = - \sum_{i \notin S} C_i f(\alpha_i) \in A,$$

a contradiction.

We now take the smallest element of $G \setminus (D_t \cup \{g\})$ for which the value of f^{-1} is not yet defined and then argue exactly as above with the role of f^{-1} taking the place of f. Notice that since f breaks L if and only f^{-1} breaks L the argument is indeed identical.

The above defines a bijection on G that satisfies the desired properties. This proves one direction of the argument.

Conversely suppose that for some $B \in \mathcal{B}$ and $\beta = \sum_{i \in B} C_i$ the factor group $G/\Omega_{|\beta|}$ is finite. Let $f : G \to G$ be a bijection. Since G is infinite, the cosets of $\Omega_{|\beta|}$ are infinite. This, together with the fact that $G/\Omega_{|\beta|}$ is finite, implies that there are $t, t' \in G$, $t \neq t'$, such that t and t' belong to the same coset of $\Omega_{|\beta|}$ and that $f(t)$ and $f(t\prime)$ belong to the same coset of $\Omega_{|\beta|}$. For each $i \in [n]$ we define

$$\alpha_i = \begin{cases} t & \text{if} \quad i \in B \\ t' & \text{if} \quad i \in [n] \backslash B \end{cases}$$

and observe that

$$\sum_{i \in [n]} C_i \alpha_i = t \sum_{i \in B} C_i + t' \sum_{i \in [n] \backslash B} C_i = \beta(t - t') = 0$$

and $\sum_{i \in [n]} C_i f(\alpha_i) = \beta(f(t) - f(t')) = 0$. Therefore, the bijection f does not break the linear form $L = C_1 X_1 + \cdots + C_n X_n$. □

We obtain the result of Hegarty [8] as a special case of Theorem 1.

Corollary 6. *(Hegarty) Let G be a countably infinite abelian group, then there exists a 3-term arithmetic progression avoiding permutation of G if and only if G/Ω_2 is infinite.*

3 Permutations avoiding 4-term arithmetic progressions

In what follows, we restrict ourselves to the study of the groups $\mathbb{Z}/p\mathbb{Z}$ where p is a prime. We also assume that $p > 3$ in all that follows. We are interested in the problem of estimating the number of permutations of $\mathbb{Z}/p\mathbb{Z}$ that map 4-term progressions to non-progressions. Let $\alpha(p)$ denote the number of such permutations. We show that

$$\lim_{p\to\infty} \frac{\alpha(p)}{p!} = e^{-1}.$$

To show this we note that the quantity $\frac{\alpha(p)}{p!}$ is the same as the probability that a permutation of $f \in \mathbb{Z}/p\mathbb{Z}$, sampled uniformly at random, maps all 4-term progressions to non-progressions. We then estimate this probability by showing that the random variable that counts the number of 4-term progression preserved by f is asymptotically Poisson. This is done by the "method of moments".

In what follows, we consider all 4-term progressions as ordered quadruples $(x, x+d, x+2d, x+3d)$ and define

$$A_p = \{(x, x+d, x+2d, x+3d) : x, d \in \mathbb{Z}/p\mathbb{Z}, d \neq 0\}.$$

For a permutation f of $\mathbb{Z}/p\mathbb{Z}$, we abuse notation slightly and define $f((a,b,c,d)) = (f(a), f(b), f(c), f(d))$. We are interested in permutations f for which

$$(a,b,c,d) \in A_p \Rightarrow (f(a), f(b), f(c), f(d)) \notin A_p.$$

It is easy to check that this agrees with the equational definition of a permutation that *avoids* 4-term progressions given by Hegarty [8].

We now sample a permutation $f \in \mathbb{Z}/p\mathbb{Z}$ uniformly at random and consider the random variable X, that counts the number of progressions that are mapped to a progression by f. More precisely,

$$X = \sum_{P\in A_p} \mathbf{1}\left(f(P) \in A_p\right).$$

Following standard notation, for $k \in \mathbb{N}$ we write $(X)_k = X(X-1)\cdots(X-k+1)$ and call $\mathbb{E}((X)_k)$ the kth *factorial moment* of X. In what follows, we show that the random variable X is asymptotically Poisson by way of the following well-known lemma. See, for example, Theorem 1.22 in [3].

Lemma 7. *Suppose that X_n is a sequence of non-negative, integer valued, random variables and that λ is a real number. If for each k we have $\mathbb{E}((X_n)_k) \to \lambda^k$ as $n \to \infty$ then X_n weakly converges to a random variable $\tilde{X}$ that is Poisson distributed with parameter λ. In other words, for every non-negative integer l*

$$\mathbb{P}\left(X_n = l\right) \to \mathbb{P}\left(\tilde{X} = l\right) = e^{-\lambda}\frac{\lambda^l}{l!}$$

as $n \to \infty$.

To estimate the moments we require the following simple lemma. Let Q be a non-empty set of 4-tuples (a, b, c, d) where a, b, c, d are distinct elements of a finite ground set V. For some fixed ordering of the ground set $V = \{x_1, \ldots, x_n\}$ of Q, we say that an element $x_i \in V$ is *fixed with respect to* Q (or if it clear that we are speaking of Q we shall simply say *fixed*) if there is a quadruple $(a, b, c, d) \in Q$ with one of a, b, c, d equal to x_i and two more of a, b, c, d among $\{x_1, \ldots, x_{i-1}\}$. We call an element $x_i \in V$ *free with respect to* Q (or simply *free*) if it is not fixed.

Lemma 8. *If Q is a non-empty set of 4-tuples of distinct elements of a finite ground set V such that every element of V appears in some quadruple of Q then one of the following holds.*

1. *There exists an ordering of the ground set $V = \{x_1, \ldots, x_n\}$ so that the number of fixed elements of V is strictly greater than the number of free elements*

2. *Every element of V is contained in at most one quadruple of Q.*

Proof. Choose a linear ordering π of the ground set uniformly at random over all possible orderings. Define the random variable Y as the number of x_i that are fixed by Q, with respect to the ordering. We write

$$Y = \sum_{i=1}^{n} \mathbf{1}\left(x_i \text{ is fixed in the ordering } \pi\right).$$

Now if $q_i \in Q$ is an arbitrarily chosen quadruple that x_i appears in, we have

$$\mathbb{P}\left(x_i \text{ is fixed in the ordering } \pi\right) \geqslant \mathbb{P}\left(\text{at least 2 coordinates of } q_i \text{ appear before } x_i\right) = \frac{1}{2}$$

where the last equality holds by symmetry and the fact that

$$\mathbb{P}\left(\geqslant 2 \text{ coordinates of } q_i \text{ appear before } x_i\right) + \mathbb{P}\left(\geqslant 2 \text{ coordinates of } q_i \text{ appear after } x_i\right) = 1.$$

Now assume that there exists some x_i that appears in more than one quadruple (i.e. we have excluded alternative 1 of the Lemma). In this case, it is easy to check that

$$\mathbb{P}\left(x_i \text{ is fixed}\right) > \frac{1}{2}.$$

Thus we have the strict inequality

$$\mathbb{E}(Y) = \sum_{i=1}^{n} \mathbb{P}\left(x_i \text{ is fixed in the ordering }\right) > \frac{n}{2}.$$

Since Y is integer-valued there must be some choice of π for which the number of fixed x_i exceeds the number of free x_i by at least 1. This completes the proof of the lemma. □

We define the notion of isomorphism between two sets of quadruples in a natural way. We say that Q, Q' are isomorphic if there exists a bijection ϕ between the grounds sets of Q, Q' so that $\phi((a,b,c,d)) \in Q'$ if and only if $(a,b,c,d) \in Q$. We will also use the notation $Q \cong Q'$ if Q, Q' are isomorphic.

We are now in a position to estimate the kth factorial moment of X.

Lemma 9. *Let $k \in \mathbb{N}$ and suppose that X is the random variable, as defined above, that counts the number of 4-term progressions that are mapped to 4-term progressions by f, a permutation sampled uniformly at random over all permutations of $\mathbb{Z}/p\mathbb{Z}$, then*

$$\mathbb{E}((X)_k) = 1 + o(1).$$

Proof. Let f be a permutation of $\mathbb{Z}/p\mathbb{Z}$, sampled uniformly at random over all permutations of $\mathbb{Z}/p\mathbb{Z}$. For a progression $P \in A_p$ we define $E(P)$ to be the event "$f(P) \in A_p$". Hence we may express the kth factorial moment as

$$\mathbb{E}((X)_k) = k! \sum_{\{P_{i_1},\dots,P_{i_k}\} \in A_p^{(k)}} \mathbb{P}\{E(P_{i_1}) \cap \dots \cap E(P_{i_k})\}.$$

To estimate the value of $\mathbb{E}((X)_k)$ we split the sum up according to isomorphism classes of the $\{P_{i_1},\dots,P_{i_k}\}$ and then estimate the probability that a given configuration of progressions $\{P_{i_1},\dots,P_{i_k}\}$ gets mapped to a collection of progressions by f.

We have

$$\mathbb{E}((X)_k) = k! \sum_{Q} \sum_{\{P_{i_1},\dots,P_{i_k}\} \cong Q} \mathbb{P}\{E(P_{i_1}) \cap \dots \cap E(P_{i_k})\}$$

where the outer sum runs over a collection of representatives from each isomorphism class. Crucially, we note that there are only finitely many such isomorphism classes. Our main contribution will come from configurations where every point is contained in at most one quadruple. We call this configuration Q_0. Hence the above is equal to

$$k! \sum_{Q \neq Q_0} \sum_{\{P_{i_1},\dots,P_{i_k}\} \cong Q} \mathbb{P}\{E(P_{i_1}) \cap \dots \cap E(P_{i_k})\} + k! \sum_{\{P_{i_1},\dots,P_{i_k}\} \cong Q_0} \mathbb{P}\{E(P_{i_1}) \cap \dots \cap E(P_{i_k})\}.$$

To estimate the first sum, we fix some Q, and consider it on some fixed (abstract) ground set $V = \{x_1,\dots,x_l\}$. Let $\mathrm{Free}(Q)$ denote the number of free x_is and $\mathrm{Fixed}(Q)$ denote the number of fixed x_is. We start with the question: how many terms are in the following sum?

$$\sum_{\{P_{i_1},\dots,P_{i_k}\} \cong Q} \mathbb{P}\{E(P_{i_1}) \cap \dots \cap E(P_{i_k})\}$$

This is the same as asking for the number of subsets of A_p of size k that are isomorphic to Q. We let S_i be the number of maps $\phi : \{x_1 \dots, x_i\} \to \mathbb{Z}/p\mathbb{Z}$ such that there *exists* some isomorphism $\tilde{\phi}$ between Q and a subset of A_p that is identical to ϕ when restricted to $\{x_1,\dots,x_i\}$. We will call a map such as ϕ a *partial isomorphism.* Notice that S_l is an upper bound for the number of subsets of A_p that are isomorphic to Q - the quantity that we want to estimate.

We now proceed to bound S_l. We do this by way of two simple observations. First we have the trivial bound

$$S_i \leqslant S_{i-1}p$$

as there are at most p choices for x_i once $x_1, \ldots x_{i-1}$ have been chosen. More carefully, we observe that if x_i is a *fixed* element with respect to Q then we have the sharper bound.

$$S_i \leqslant 12S_{i-1}$$

To see this, we count the number of ways of extending a fixed partial isomorphism ϕ on $x_1, \ldots, x_{i-1}$ of Q to a partial isomorphism ϕ' on $x_1, \ldots, x_i$. Since x_i is fixed there are two other elements x_j, x_k among $x_1, \ldots, x_{i-1}$ that appear in a 4-tuple with x_i. Since this 4-tuple must eventually get mapped to a member of A_p we must ensure that $\phi'(x_i)$ is contained in a progression with x_j, x_k. Finally, note that $\phi(x_j), \phi(x_k)$ are are mutually contained in $\binom{4}{2} = 6$ tuples of A_p. Hence there are at most $6 \cdot 2 = 12$ possible choices for $\phi(x_j)$. The claim follows.

Inductively applying these estimates, we arrive at the following estimate on S_l.

$$S_l \leqslant 12^l p^{\text{Free}(Q)} \leqslant 12^{4k} p^{\text{Free}(Q)}$$

Where the last inequality follows as $l \leqslant 4k$. Hence the number of terms in the sum under consideration is at most $12^{4k}p^{\text{Free}(Q)}$.

We now turn to estimate the quantity $\mathbb{P}(E(P_{i_1}) \cap \ldots \cap E(P_{i_k}))$ for $\{P_{i_1}, \ldots, P_{i_k}\} \cong Q$. In particular, we claim that

$$\mathbb{P}(E(P_{i_1}) \cap \ldots \cap E(P_{i_k})) \leqslant \frac{6^{4k}}{p^{\text{Fixed}(Q)}}(1 + o(1)).$$

We prove this in a way very similar to the above. We fix $\{P_{i_1}, \ldots, P_{i_k}\} \cong Q$ on the ground set $\{y_1, \ldots, y_l\} \subseteq \mathbb{Z}/p\mathbb{Z}$. We may assume that we chose the ordering of $\{y_1, \ldots, y_l\}$ so that the map sending x_i to y_i, $i = 1, \ldots, l$, is an isomorphism of Q and $\{P_{i_1}, \ldots, P_{i_k}\}$.

Now we define the event E_i for $i = 1, \ldots, l$ to be the event: "there exists *some* isomorphism $\theta : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ of $\{P_{i_1}, \ldots, P_{i_k}\}$ that agrees with f on $x_1, \ldots, x_i$". Thus

$$\mathbb{P}(E(P_1) \cap \ldots \cap E(P_k)) = \mathbb{P}(E_l) = \mathbb{P}(E_l \mid E_{l-1})\mathbb{P}(E_{l-1} \mid E_{l-2}) \cdots \mathbb{P}(E_2 \mid E_1).$$

We bound each term $\mathbb{P}(E_i \mid E_{i-1})$ trivially by 1 if y_i is free and by $\frac{6}{p-i}$ if y_i is fixed. After noting that $p \to \infty$ and $l \leqslant 4k$, the claim follows.

Putting the above together, it follows that

$$\sum_{\{P_{i_1}, \ldots, P_{i_k}\} \cong Q} \mathbb{P}\{E(P_{i_1}) \cap \ldots \cap E(P_{i_k})\} \leqslant Cp^{\text{Free}(Q) - \text{Fixed}(Q)}.$$

Since, by Lemma 8, we may work with some ordering on the ground set A of Q that has more fixed elements than free elements, the above sum is bounded by C/p, for some constant C (which depends on k). And since there are only finitely many isomorphism classes, we have

$$\sum_{\{P_{i_1},\dots,P_{i_k}\}\cong Q} \mathbb{P}\{E(P_{i_1})\cap\ldots\cap E(P_{i_k})\} \leqslant \frac{C'}{p}.$$

Where the C' is a constant that depends on k, but not p. That is, the contribution from the $Q \ncong Q_0$ terms in the sum that represents $\mathbb{E}((X)_k)$ is negligible.

We now need to determine the contribution from the main term $Q \cong Q_0$. Let us first count the number of ways of choosing a set of 4-term progressions of $\mathbb{Z}/p\mathbb{Z}$ that have no common elements. We claim that there are

$$\frac{1}{k!}\prod_{i=1}^{k}(p(p-1)-O(ip)) = \frac{p^{2k}}{k!} - o(1)$$

such sets. To see this, observe that there are $|A_p| = p(p-1)$ ways of choosing the first set. Then after we have chosen i sets to be in our collection, there are $O(ip)$ sets of A_p that share an element with the previously chosen sets. Hence there are $p(p-1)-O(ip)$ choices for the $(i+1)$th set. We then must divide by $k!$, to remove the order from our choice.

To determine $\mathbb{P}\{E(P_{i_1})\cap\cdots\cap E(P_{i_k})\}$ we use a trick. We realize the uniform probability measure on the space of permutations (henceforth $\mathbb{P}_\pi$) as the probability measure uniform on all functions (henceforth $\mathbb{P}_f$) $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ *conditioned* on the event "$f(0),\dots,f(p-1)$ are distinct" . Before we begin the calculation, note that without loss we may assume that the elements appearing in $P_{i_1},\dots P_{i_k}$ are exactly $x_1,\dots,x_{4k}$. We have

$$\begin{aligned}\mathbb{P}_p\{E(P_{i_1})\cap\cdots\cap E(P_{i_k})\} &= \mathbb{P}_f\{E(P_{i_1})\cap\cdots\cap E(P_{i_k})|f(0),\dots,f(p-1)\text{ distinct}\}\\ &= \mathbb{P}_f\{E(P_{i_1})\cap\cdots\cap E(P_{i_k})|f(x_1),\dots,f(x_{4k})\text{ are distinct}\}\\ &= \frac{\mathbb{P}_f\{E(P_{i_1})\cap\cdots\cap E(P_{i_k})\}}{\mathbb{P}_f\{x_1,\dots,x_{3k}\text{ are distinct}\}} = \frac{1}{p^{2k}}(1+o(1)),\end{aligned}$$

where the second equality holds by independence and the basic property of conditional probability $\mathbb{P}(E|A\cap B) = \mathbb{P}(E|A)$ if B is independent of E. The last equality holds by the fact that $\mathbb{P}_f\{x_1,\dots,x_{3k}\text{ are distinct}\} = (1-o(1))$ as p tends to infinity while k is fixed. Putting this estimate together with our earlier estimate on the number of distinct sums gives

$$\sum_{\{P_{i_1},\dots,P_k\}\cong Q_0} k!\,\mathbb{P}\{\mathbf{P}_{i_1}\cap\cdots\cap\mathbf{P}_{i_k}\} = 1+o(1).$$

Hence, we have shown

$$\mathbb{E}((X)_k) = (1+o(1)) + \frac{C}{p} = 1 + o(1),$$

as desired. □

Our main result of this section follows.

Theorem 10. *Let p be a prime and let $\alpha(k,p)$ be the number of permutations of $\mathbb{Z}/p\mathbb{Z}$ that avoid k-term arithmetic progressions. Then*

1. $\lim_{p\to\infty} \frac{\alpha(k,p)}{p!} = 1$ *if* $k > 4$ *,*

2. $\lim_{p\to\infty} \frac{\alpha(4,p)}{p!} = e^{-1}$*, and*

3. $\lim_{p\to\infty} \frac{\alpha(3,p)}{p!} = 0.$

Proof. We sample a permutation f of $\mathbb{Z}/p\mathbb{Z}$ uniformly at random and let $X_{k,p}$ denote the random variable that counts the number of k-term progressions that f maps to k-term progressions. It is also useful to define for $k \geqslant 2$ the set $A_{k,p}$ of all (ordered) arithmetic progressions $(x, x{+}d, x{+}2d, \ldots, (k{-}1)d)$, where $x, d \in \mathbb{Z}/p\mathbb{Z}$ and $d \neq 0$. Before proceeding we need an easy calculation.

For $2 \leqslant k < p$, let $P = (x, x+d, \ldots, x+(k-1)d) \in A_{k,p}$ and let $E(P)$ be the event "$f(P) \in A_{k,p}$". We observe that

$$\mathbb{P}\{E(P)\} = \frac{1}{(p-2)(p-3)\cdots(p-k+1)}.$$

To see this, first note that if $P \in A_{2,p}$ then $\mathbb{P}\{E(P)\} = 1$. Now for $k \geqslant 3$ we may expand the quantity $\mathbb{P}\{E(P)\}$ as

$$\mathbb{P}\left\{E(P)|f(x,\ldots,x+(k-2)d) \in A_{(k-1),p}\right\}\mathbb{P}\left\{f(x,\ldots,x+(k-2)d) \in A_{(k-1),p}\right\}.$$

Now notice that

$$\mathbb{P}\left\{E(P)|f(x,\ldots,x+(k-2)d) \in A_{(k-1),p}\right\} = (p-(k-1))^{-1},$$

as the values of $f(x), f(x+d)$ determine a unique value that $f(x+(k-1))$ must take in order for $E(P)$ to hold. Since this value is not among $f(x), f(x+d), \ldots, f(x+(k-2)d)$, as $k > p$ and p is prime and since the value is sampled uniformly among all values $\mathbb{Z}/p\mathbb{Z} \setminus \{f(x), f(x+d), \ldots, f(x+(k-2)d)\}$ the equality follows. The calculation now follows by induction.

To proceed with the proof of the theorem, we write

$$\frac{\alpha(k,p)}{p!} = \mathbb{P}(X_{k,p} = 0).$$

In the case $k > 4$, we have

$$1 - \frac{\alpha(k,p)}{p!} = \mathbb{P}\left(X_{k,p} \geqslant 1\right) \leqslant \mathbb{E}(X_{k,p}) \leqslant |A_{k,p}|\mathbb{P}\left\{E(P)\right\} \leqslant \frac{C}{p} \to 0.$$

where $P \in A_{k,p}$ is arbitrary and we have used the formula for $\mathbb{P}\left\{E(P)\right\}$ obtained above. In the case $k = 4$ we have

$$\frac{\alpha(k,p)}{p!} = \mathbb{P}\left(X_{k,p} = 0\right) \to e^{-1},$$

by applying Lemma 7 along with our moment calculations, Lemma 9.

The third item in the theorem can be established by a standard second moment calculation. To do this we note that $\mathbb{E}(X_{3,p}) = \frac{1}{p-2}|A_{k,p}| = (1 + o(1))p$ and claim that $\mathbb{E}(X_{3,p}^2) - (\mathbb{E}(X_{3,p}))^2 \leqslant Cp$, where C is an absolute constant. To see this, we write

$$\mathbb{E}(X_{3,p}^2) = \sum_{P,P' \in A_{3,p}} \mathbb{P}\left\{E(P) \cap E(P')\right\} = \sum_{P \in A_{3,p}} \mathbb{P}\left\{E(P)\right\} + \sum_{P \neq P' \in A_{3,p}} \mathbb{P}\left\{E(P) \cap E(P')\right\}.$$

We now claim that each term in the second sum is at most $(p-6)^{-2}$. To see this note that since P, P' have at most two elements in common, there exists x appearing in P and not appearing in P' and y appearing in P' and not appearing in P. To calculate $\mathbb{P}\left\{E(P) \cap E(P')\right\}$, first expose the elements appearing in the tuples P, P' that are not x, y. As, P, P' are progressions, there will be at most one choice for each x, y among the remaining $\leqslant p - 6$ elements of $\mathbb{Z}/p\mathbb{Z}$ such that the event $E(P) \cap E(P')$ holds. As this choice is uniform, the bound follows.

Now since

$$\mathbb{E}(X_{3,p})^2 = \sum_{P,P' \in A_{k,p}} \mathbb{P}\left\{E(P)\right\}\mathbb{P}\left\{E(P')\right\},$$

we may express the quantity $\mathbb{E}(X_{3,p}^2) - \mathbb{E}(X_{3,p})^2$ as

$$\sum_{P \in A_{3,p}} \mathbb{P}\left\{E(P)\right\} - \mathbb{P}\left\{E(P)\right\}^2 + \sum_{P \neq P' \in A_{3,p}} \mathbb{P}\left\{E(P) \cap E(P')\right\} - \mathbb{P}\left\{E(P)\right\}\mathbb{P}\left\{E(P')\right\}.$$

Now, using the observation we have just made, and the formula for $\mathbb{P}\left\{E(P)\right\}$ that we have obtained above, we have

$$\mathbb{P}\left\{E(P) \cap E(P')\right\} - \mathbb{P}\left\{E(P)\right\}\mathbb{P}\left\{E(P')\right\} \leqslant \frac{1}{(p-6)^2} - \frac{1}{(p-2)^2} \leqslant \frac{C}{p^3}$$

While we may bound terms in the first sum more crudely,

$$\mathbb{P}\left\{E(P)\right\} - \mathbb{P}\left\{E(P)\right\}^2 \leqslant \frac{1}{p}$$

It follows that

$$\mathbb{E}(X_{3,p}^2) - \mathbb{E}(X_{3,p})^2 \leqslant C|A_{k,p}|p^{-1} + C|A_{k,p}|^2p^{-3} \leqslant C'p,$$

as claimed.

We now use this claim with Chebyshev's inequality to finish the proof of Theorem 10. We have

$$\begin{aligned}\frac{\alpha(3,p)}{p!} &= \mathbb{P}(X_{3,p}=0) \leqslant \mathbb{P}(|X_{3,p}-p/2| \geqslant p/2) \leqslant 4\frac{\mathrm{Var}(X_{3,p})}{p^2} \\ &= 4\frac{\left(\mathbb{E}(X_{3,p}^2)-\mathbb{E}(X_{3,p})^2\right)}{p^2} \leqslant \frac{C'}{p} \to 0,\end{aligned}$$

as $p \to \infty$. This completes the proof. □

4 Open questions

Perhaps the most interesting open question is whether or not there exists a permutation $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ that avoids 3-term progressions. Hegarty [8] has conjectured that such permutations exist for $N \neq 2, 3, 5, 7$.

Let us also note that the type of question explored in this paper is related to a question about the existence of a map (not necessarily a permutation) $f : \mathbb{N} \to \mathbb{N}$ that maps arithmetic progressions to non-arithmetic progressions with $|f(n) - f(n+1)| < C$, where C has no dependence on n. This question originated in a different but equivalent formulation in the setting of infinite words [2, 4, 5, 6, 7, 9]. The question of the existence of such a map is open and appears to be quite difficult.

Acknowledgements

The authors would like to thank the anonymous referee for a careful reading of the paper and many helpful suggestions.

References

[1] Noga Alon, Joel Spencer. *The probabilistic method.* Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons, New York, second edition, 2000.

[2] Hayri Ardal, Tom Brown, Veselin Jungić, Julian Sahasrabudhe. On Additive and Abelian Complexity in Infinite Words. *Integers, Electron. J. Combin. Number Theory.* 12 :#A21, 2012.

[3] Béla Bollobás. *Random graphs.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, second edition, 2001.

[4] Tom Brown, Veselin Jungić, Andrew Poelstra. On 3-term double arithmetic progressions. *Integers, Electron. J. Combin. Number Theory* , 14 :#A43, 2014.

[5] Allan Freedman. Sequences on sets of four numbers. to appear in *INTEGERS: Elect. J. Combin. Number Theory.*

[6] Jaroslaw Grytczuk. Thue type problems for graphs, points, and numbers. *Discrete Math.* 308: 4419–4429, 2008.

[7] Lorenz Halbeisen, Norbert Hungerbühler. An application of van der Waerden's theorem in additive number theory. *INTEGERS: Elect. J. Combin. Number Theory.* 0: #A7, 2000.

[8] Peter Hegarty. Permutations avoiding arithmetic patterns. *The Electronic Journal of Combinatorics* , 11 :#R39, 2004.

[9] G. Pirillo, S. Varricchio, On uniformly repetitive semigroups, *Semigroup Forum* 49:125–129, 1994.

[10] A. F. Sidorenko. *An infinite permutation without arithmetic progressions.* Discrete Math. 69:211, 1988.