ELSEVIER

Intersection density of imprimitive groups of degree pq

Angelot Behajaina [a], Roghayeh Maleki [b],
Andriaherimanana Sarobidy Razafimahatratra [b,c,*]

[a] *Department of Mathematics, Technion - Israel Institute of Technology, Haifa, Israel*
[b] *University of Primorska, UP FAMNIT, Glagoljaška 8, 6000 Koper, Slovenia*
[c] *University of Primorska, UP IAM, Muzejski trg 2, 6000 Koper, Slovenia*

A R T I C L E   I N F O

A B S T R A C T

A subset $\mathcal{F}$ of a finite transitive group $G \leq \mathrm{Sym}(\Omega)$ is *intersecting* if any two elements of $\mathcal{F}$ agree on an element of Ω. The *intersection density* of G is the number

$$\rho(G) = \max \left\{ |\mathcal{F}|/|G_\omega| \mid \mathcal{F} \subset G \text{ is intersecting} \right\},$$

where $\omega \in \Omega$ and G_ω is the stabilizer of ω in G. It is known that if $G \leq \mathrm{Sym}(\Omega)$ is an imprimitive group of degree a product of two odd primes $p > q$ admitting a block of size p or two complete block systems, whose blocks are of size q, then $\rho(G) = 1$.

In this paper, we analyze the intersection density of imprimitive groups of degree pq with a unique block system with blocks of size q based on the kernel of the induced action on blocks. For those whose kernels are non-trivial, it is proved that the intersection density is larger than 1 whenever there exists a cyclic code C with parameters $[p, k]_q$ such that any codeword of C has weight at most $p - 1$, and under some additional conditions on the cyclic code, it is a proper rational number. For those that are quasiprimitive, we reduce the cases to almost simple groups containing $\mathrm{Alt}(5)$ or a projective special linear group. We give some examples where the latter has

* Corresponding author at: University of Primorska, UP FAMNIT, Glagoljaška 8, 6000 Koper, Slovenia.
  E-mail address: sarobidy@phystech.edu (A.S. Razafimahatratra).

intersection density equal to 1, under some restrictions on p and q.

1. Introduction

All groups considered in this paper are finite. Given a finite set Ω, we let $\mathrm{Sym}(\Omega)$ be the symmetric group of Ω. A set $\mathcal{F} \subset \mathrm{Sym}(\Omega)$ is *intersecting* if for any $g, h \in \mathcal{F}$, there exists $\omega \in \Omega$ such that $\omega^g = \omega^h$. We are interested in studying the largest intersecting sets in finite permutation groups. Problems of this nature have been studied since the late 70s with the paper of Deza and Frankl [5] on the size and the possible structures of the largest intersecting sets in the symmetric group $\mathrm{Sym}(n)$ with its natural action on $\{1, 2, \ldots, n\}$. Deza and Frankl proved that if $\mathcal{F} \subset \mathrm{Sym}(n)$ is intersecting, then $|\mathcal{F}| \leq (n-1)!$. Later, Cameron and Ku [4], independently, Larose and Malvenuto [16], proved that equality holds if and only if $\mathcal{F}$ is a coset of a stabilizer of a point of $\mathrm{Sym}(n)$. Consequently, the maximum intersecting sets in $\mathrm{Sym}(n)$ are cosets of a stabilizer of a point.

A natural question is then whether similar results to the one on the symmetric group hold for general transitive permutation groups. Unfortunately, the answer to this question is negative. To see this, consider the alternating group $G = \mathrm{Alt}(4)$ acting on left cosets of $H = \langle (1\ 2) \rangle$ by left multiplication. This action is transitive and its point stabilizers have size 2, however, the Klein group $K = \langle (1\ 2), (3\ 4) \rangle$ is an intersecting set of size 4.

In [17], a measure for intersecting sets in transitive groups was introduced. Formally, the *intersection density* of a transitive group $G \leq \mathrm{Sym}(\Omega)$ is the rational number

$$\rho(G) := \max \left\{ \rho(\mathcal{F}) \mid \mathcal{F} \subset G \text{ is intersecting} \right\},$$

with $\rho(\mathcal{F}) := |\mathcal{F}|/|G_\omega|$ for any intersecting set $\mathcal{F}$, where G_ω is the point stabilizer of $\omega \in \Omega$ in G. The study of the intersection density parameter in transitive groups has recently drawn the attention of many researchers [1,12–14,22,23,25,26,24,28,30]. One of the major results about the intersection density of a group was proved in [25]. It was proved that the largest possible value of the intersection density of a group acting transitively on Ω, with $|\Omega| \geq 3$, is $\frac{|\Omega|}{3}$ and this upper bound is sharp since it is attained by the groups given in [25, Theorem 5.1].

The study of the intersection density of the transitive group $G \leq \mathrm{Sym}(\Omega)$, as we will see later in Section 2, is equivalent to the study of the cocliques of a certain Cayley graph Γ_G called the derangement graph of G. The clique-coclique [8] bound states that[1] $\alpha(\Gamma_G)\omega(\Gamma_G) \leq |G|$. The knowledge of cocliques in Γ_G can therefore be used to give an upper bound on certain complex structures on G arising from coding theory, provided

---

[1] $\alpha(\Gamma_G)$ and $\omega(\Gamma_G)$ denote respectively the maximum size of cocliques and cliques in Γ_G.

that G is highly transitive. First recall that $\mathcal{F} \subset G$ is called k-*intersecting* if there exist distinct $\omega_1, \omega_2, \ldots, \omega_k \in \Omega$ such that $\omega_i^g = \omega_i^h$ for any $g, h \in \mathcal{F}$ and $1 \leq i \leq k$. Let $\Omega^{(k)}$ be the set of all k-tuples of Ω with pairwise distinct entries. It is not hard to see that a k-intersecting set of $G \leq \mathrm{Sym}(\Omega)$ is exactly an intersecting set of $G \leq \mathrm{Sym}(\Omega^{(k)})$, provided that G is also k-transitive, that is, it is transitive on $\Omega^{(k)}$. For any two permutations $g, h \in G$, define $\mathrm{d}(g, h) = |\Omega| - \left| \left\{ \omega \in \Omega \; : \; \omega^g = \omega^h \right\} \right|$ to be the distance between g and h. A $\mathrm{PC}(G, k)$ *permutation code* of a transitive group $G \leq \mathrm{Sym}(\Omega)$ is a subset $S \subset G$ such that $\mathrm{d}(g, h) \geq k$, for any two elements $g, h \in G$. A $\mathrm{PC}(G, k)$ permutation code is in fact a clique in the derangement graph of $G \leq \mathrm{Sym}\left(\Omega^{(|\Omega|-k+1)}\right)$. If $\Gamma_G^{(|\Omega|-k+1)}$ is the derangement graph of $G \leq \mathrm{Sym}\left(\Omega^{(|\Omega|-k+1)}\right)$, then by using the clique-coclique bound on $\Gamma_G^{(|\Omega|-k+1)}$, we obtain a general upper bound on the maximum size of a $\mathrm{PC}(G, k)$ permutation code. This yields an upper bound which is not tight in general [2,7] and the classification of multiply transitive groups forces k to be large, unless G is equal to the full symmetric group $\mathrm{Sym}(\Omega)$ or the alternating group $\mathrm{Alt}(\Omega)$. A more general approach to permutation codes arising from permutation groups is given in [3].

The overwhelming majority of the works on the intersection density of transitive groups focus on trying to classify the transitive groups whose intersection densities are equal to 1 or whose largest intersecting sets are cosets of a point stabilizer. For instance, Meagher, Spiga and Tiep [26] proved that any finite 2-transitive group has intersection density 1. In [17,25], works on transitive groups that have large intersection densities were initiated.

Another interesting problem is to study the intersection density of groups with fixed degrees. It was conjectured in [25, Conjecture 6.6] that if G is a transitive group of degree a product of two distinct primes $q < p$, then $\rho(G) = 1$ if p and q are odd, and $\rho(G) \leq 2$ if $q = 2$. The latter was proved in [28]. In [14], Hujdurović et al. proved further that the intersection density of such groups is either 1 or 2; if it is equal to 2, then the group is a split extension of an elementary abelian 2-group. In [12], Hujdurović et al. gave an elegant construction of transitive groups disproving the conjecture when p and q are both odd. They provided a family of imprimitive groups of degree pq ($q < p$ are odd primes) whose intersection densities are equal to q.

Although [25, Conjecture 6.6 (3)] is false, it is natural to ask about the possible values of the intersection density of transitive groups of degree a product of two distinct odd primes $p > q$. When G is primitive of degree pq, the third author proved in [29] that $\rho(G) = 1$ for several families. It is in fact conjectured in [29, Conjecture 9.1] that all primitive groups of degree a product of two odd primes have intersection densities equal to 1. Imprimitive groups of degree pq that admit a block system with blocks of size p have intersection density equal to 1 (see [12]). It was also proved in [29] that any imprimitive group of degree a product of two odd primes with at least two (imprimitivity) block systems has intersection density equal to 1. The objective of this paper is to study the intersection density of the remaining families of imprimitive groups of degree a product of two primes p and q (where $p > q$), i.e., those with a unique block system of size q. To this end, for any $n \geq 2$, we define the set

$$\mathcal{I}_n := \{\rho(G) \mid G \text{ is transitive of degree } n\}.$$

The set $\mathcal{I}_n$, for $n \geq 2$, was first introduced in [25]. For any prime p, we have $\mathcal{I}_p = \{1\}$ since any transitive group of prime degree contains a regular subgroup, which implies that its intersection density is equal to 1 (see Lemma 2.1). For any odd prime p, it follows from [14] that $\mathcal{I}_{2p} = \{1, 2\}$. When p and q are two distinct odd primes ($q < p$), it is known that any transitive group $G \leq \mathrm{Sym}(\Omega)$ of degree pq admits a semiregular element of order p [19]. Using this fact, one can prove that $\rho(G) \leq q$, for any transitive group of degree pq (see Lemma 2.1). This upper bound is sharp since the transitive groups given in [12] attain it. Apart from these few results, very little is known about the set $\mathcal{I}_{pq}$.

Henceforth, we will assume that $p > q$ are odd primes and $G \leq \mathrm{Sym}(\Omega)$ is imprimitive of degree pq admitting a unique block system $\mathcal{B}$ with blocks of size q. Let $\overline{G} \leq \mathrm{Sym}(\mathcal{B})$ be the induced action of G on $\mathcal{B}$ and denote the kernel of the canonical epimorphism $G \to \overline{G}$ by $\mathrm{Ker}(G \to \overline{G})$. If G is *quasiprimitive*, i.e., all its non-trivial normal subgroups are transitive, then $\mathrm{Ker}(G \to \overline{G})$ is trivial since it is intransitive. Conversely, if $\mathrm{Ker}(G \to \overline{G})$ is trivial, then a non-trivial normal subgroup of G is transitive, otherwise its orbits would form a block system of G (see Lemma 2.2) and, by uniqueness of $\mathcal{B}$, this normal subgroup would be trivial. Hence, G is quasiprimitive if and only if $\mathrm{Ker}(G \to \overline{G})$ is trivial. Consequently, we shall distinguish the two cases whether $\mathrm{Ker}(G \to \overline{G})$ is trivial or not.

The first part of this paper focuses on the case where the kernel of the induced action is trivial (i.e., the quasiprimitive cases). We first reduce the quasiprimitive cases to groups containing one of two almost simple groups. Since this reduction is an easy exercise that follows from the classification of the transitive groups of prime degree, due to Burnside in 1900, we only state it as a remark.

Remark 1.1. If $G \leq \mathrm{Sym}(\Omega)$ is an imprimitive quasiprimitive of degree a product of two odd primes $p > q$, then G is an almost simple group with socle equal to

(i) $\mathrm{Alt}(5)$ admitting a transitive action of degree 3×5,
(ii) $\mathrm{PSL}_2(11)$ admitting a transitive action of degree 5×11, or
(iii) $\mathrm{PSL}_d(r^{d^m})$ admitting a transitive action of degree pq, for some $d \geq 2$, $m \geq 0$, and a prime number r such that $p = \frac{r^{d^{m+1}} - 1}{r^{d^m} - 1}$.

A discussion regarding this result is given in Section 3 for sake of completeness. The groups in (i) and (ii) in Remark 1.1 have intersection densities equal to 1 via `Sagemath` [31]. Hence, the remaining minimal cases for the quasiprimitive case are the imprimitive actions of $\mathrm{PSL}_d(r^{d^m})$, of degree a product of two odd primes. These groups are extremely difficult to deal with and we believe that new techniques are required to determine their intersection density in general. We present a case where the intersection density of such groups can be computed using the known techniques in the literature. This result is a particular case of Remark 1.1(iii) where $m = 0$ and $d = r$, and in this case, there is a

unique imprimitive permutation representation of degree pq of $\mathrm{PSL}_r(r)$, where $p = \frac{r^r - 1}{r - 1}$ and $q = r$.

Theorem 1.2. *For any odd prime q, if $p = \frac{q^q - 1}{q - 1}$ is a prime, then the intersection density of the imprimitive representation of $\mathrm{PSL}_q(q)$ of degree pq is 1.*

Based on computational results, we make the following conjecture.

Conjecture 1.3. *If G is a quasiprimitive group of degree pq, then $\rho(G) = 1$.*

The remaining results of the paper are about the non-quasiprimitive cases, i.e., when $\mathrm{Ker}(G \to \overline{G})$ is non-trivial. Our next result is stated as follows.

Theorem 1.4. *Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive group of degree pq admitting a unique block system $\mathcal{B}$ whose blocks are of size q. Suppose that $H = \mathrm{Ker}(G \to \overline{G})$ is non-trivial. Let N be a minimal normal subgroup of G contained in H.*

- *(i) If N is non-abelian, then $\rho(G) = 1$.*
- *(ii) If N is abelian and H admits a derangement, then $\rho(G) = 1$.*

The counterexamples to [25, Conjecture 6.6 (3)] given in [14] are based on the existence of certain cyclic codes (see §4.2 for the basic definitions). In this paper, we also prove a certain converse to their construction.

Theorem 1.5. *Let G be a group as in Theorem 1.4. Moreover, assume that G is minimally transitive with intersection density $\rho(G) = q$. Then, there is a $[p, k]_q$ cyclic code C such that the Hamming weight $w(\mathbf{c})$ is at most $p - 1$ for all $\mathbf{c} \in C$.*

These two results imply that if $\mathrm{Ker}(G \to \overline{G})$ is non-trivial and $\rho(G) > 1$, then G is an extension of a certain derangement-free elementary abelian q-group. We conjecture the following based on computational results via `Sagemath` [31].

Conjecture 1.6. *Assume that $\mathrm{Ker}(G \to \overline{G})$ is non-trivial. If $\overline{G}$ is 2-transitive, then $\rho(G) = 1$. If $\overline{G} = C_p \rtimes C_k < \mathrm{AGL}_1(p)$, then $\rho(G) \in \{1\} \cup \left\{ \frac{q}{d} : d \mid k \text{ and } d \leq q \right\}$.*

This conjecture is hard as far as we know. With additional restrictions on the odd primes p and q, we prove that $\mathcal{I}_{pq}$ contains a proper rational number.

Theorem 1.7. *If q and $p = \frac{q^k - 1}{q - 1}$ are odd primes such that $k < q$, then $\frac{q}{k} \in \mathcal{I}_{pq}$.*

This paper is organized as follows. In Section 2, we provide the necessary background to prove the main results. The proof of Theorem 1.2 and a discussion about Remark 1.1 are given in Section 3. In Section 4, we prove Theorem 1.4 and Theorem 1.5. We give

the proof of Theorem 1.7 in Section 5, and in Section 6, we give a conjecture (see Conjecture 6.1) that encompasses all the possibilities for the set $\mathcal{I}_{pq}$, for any values of p and q.

2. Background results

In this section, we review some basics on transitive groups (§2.1 and §2.2) and codes (§2.3), that are needed in this work.

2.1. Transitive groups

Throughout this section, we let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive group.

2.1.1. Intersection density

The standard technique to study the intersection density of a transitive group is to transform the problem into a graph theoretical one. Recall that if K is a group and $S \subset K \setminus \{1\}$ is a subset such that $x \in S$ implies $x^{-1} \in S$, then the Cayley graph $\mathrm{Cay}(K, S)$ is the graph whose vertex set is K and $x, y \in K$ are adjacent if $yx^{-1} \in S$. It is well known that $\mathrm{Cay}(K, S)$ is connected if and only if $\langle S \rangle = K$. Furthermore, the number of components of $\mathrm{Cay}(K, S)$ is equal to $[K : \langle S \rangle]$. Given a permutation group K, the *derangement graph* of K, denoted by Γ_K, is the graph $\mathrm{Cay}(K, \mathrm{Der}(K))$, where $\mathrm{Der}(K) = \{k \in K \mid k \text{ is a derangement}\}$. If $\mathrm{Der}(K) = \varnothing$, then Γ_K is the empty graph, i.e., without edges. If K is transitive of degree at least 2, then $\mathrm{Der}(K) \neq \varnothing$ by [15], and so Γ_K has at least one edge.

Recall that an *independent set* or a *coclique* in a graph is a subgraph in which no two vertices are adjacent. The size of the largest cocliques in a graph X is called the *independence number* and is denoted by $\alpha(X)$. It is not hard to see that given a transitive group $G \leq \mathrm{Sym}(\Omega)$, a subset $\mathcal{F} \subset G$ is intersecting if and only if $\mathcal{F}$ is a coclique in Γ_G. Consequently, we have $\rho(G) = \alpha(\Gamma_G)/|G_\omega|$, for $\omega \in \Omega$.

We recall the following bound on the intersection density of a transitive group.

Lemma 2.1. *[29, Corollary 4.2] Let $H \leq \mathrm{Sym}(\Omega)$ be a transitive group and K be a subgroup of H with k orbits of the same size. Then, we have $\rho(H) \leq \rho(K)k$.*

2.1.2. Imprimitive groups

In this part, we further assume that $G \leq \mathrm{Sym}(\Omega)$ is imprimitive. Recall that $S \subset \Omega$ is a *block (of imprimitivity)* of G if $S^g \cap S = \varnothing$ or $S^g = S$, for all $g \in G$. It is clear that $\{\omega\}$ for $\omega \in \Omega$ and the set Ω are always blocks of the group G; we call such blocks *trivial*. If G admits a block S such that $1 < |S| < |\Omega|$, then we say that the group G is *imprimitive*. In this case, we know the collection of subsets given by $\mathcal{B} = \{S^g \mid g \in G\}$ forms a partition of Ω, that is invariant by the action of G. Such a G-invariant partition of Ω is called a *(complete) block system*. We recall the following result.

Lemma 2.2 *(Theorem 1.6A [6]). If $N \trianglelefteq G$, then the orbits of N form a G-invariant partition of Ω. That is, $\{\omega^N \mid \omega \in \Omega\}$ is a G-invariant partition of Ω.*

Note that in Lemma 2.2 if $N = 1$ or N is transitive, then the corresponding block systems are $\{\{\omega\} \mid \omega \in \Omega\}$ or $\{\Omega\}$, respectively. That is, they consist of trivial blocks.

Recall that a subgroup $K \leq G$ is *semiregular* if its stabilizers are trivial. Moreover, an element $g \in G$ is called *semiregular* if $\langle g \rangle \leq G$ is semiregular. Therefore, it is clear that any derangement $g \in G$ of prime order is semiregular. Next, we recall the following lemma (see [14, Lemma 3.1]).

Lemma 2.3. *Let G be a transitive group admitting a semiregular subgroup K whose orbits form a G-invariant partition $\mathcal{B}$. Let $\overline{G}$ be the induced action of G on $\mathcal{B}$. Then, we have $\rho(G) \leq \rho(\overline{G})$.*

2.1.3. The subgroup generated by non-derangements

In this section, we briefly describe the structure of the subgroup generated by the non-derangements in a transitive group. We assume that $G \leq \mathrm{Sym}(\Omega)$ is a transitive group, where Ω is a finite set. Define

$$\mathrm{F}(G) := \langle \bigcup_{\omega \in \Omega} G_\omega \rangle. \tag{1}$$

In other words, $\mathrm{F}(G)$ is the subgroup generated by all permutations with at least one fixed point (i.e., the non-derangements). It is not hard to see that $\mathrm{F}(G) \trianglelefteq G$ since the point stabilizers are conjugate. If $\mathrm{F}(G) = \{1\}$, then each point stabilizer of G is trivial, thus G is regular. If $\mathrm{F}(G) \neq \{1\}$, then its orbits form a block system (see Lemma 2.2).

If $\mathrm{F}(G) < G$, then the complement of the derangement graph Γ_G is $\overline{\Gamma}_G = \mathrm{Cay}(G, G \setminus (\mathrm{Der}(G) \cup \{1\}))$. As $\langle G \setminus (\mathrm{Der}(G) \cup \{1\}) \rangle = \mathrm{F}(G)$ is a proper subgroup of G, we can see that $\overline{\Gamma}_G$ is disconnected. The number of components of $\overline{\Gamma}_G$ is equal to $[G : \mathrm{F}(G)]$ since $\overline{\Gamma}_G$ is also a Cayley graph. Switching to the complement, we conclude that Γ_G is a *join* (see [9, pg 21] or [32] for the definition) of $[G : \mathrm{F}(G)]$ copies of the complement of $\overline{\Gamma}_G$ that contains 1, that is, the graph $\Gamma_{\mathrm{F}(G)} = \mathrm{Cay}(\mathrm{F}(G), \mathrm{F}(G) \cap \mathrm{Der}(G))$. From this explanation, the following proposition follows.

Proposition 2.4. *The graph Γ_G is complete multipartite if and only if $\mathrm{F}(G)$ is intersecting.*

If $\mathrm{F}(G) = G$, then the graph Γ_G is not a join anymore. We recall the following result, whose proof can be found in [25].

Proposition 2.5. *[25, Lemma 2.3] A subgroup $H \leq G$ is intersecting if and only if it is derangement-free.*

2.2. The transitive groups of degree pq

In this section, we categorize the types of transitive groups of degree a product of two odd primes for a better analysis of their intersection density. Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive group of degree a product of two odd primes $p > q$. Let m be the number of block systems of G. In [18], Lucchini proved that if $m \geq 2$, then $m = 2$ or $m = p + 1$ and G has at most one block system with blocks of size p. It was proved in [12] that if G admits a block of size p, then $\rho(G) = 1$. If $m \geq 2$, then it was also shown in [29] that $\rho(G) = 1$. Therefore, we only need to consider the cases where G admits only trivial blocks or a unique block system where the blocks are of size q. Consequently, G is one of the following types.

(I) **Quasiprimitive types**: every non-trivial normal subgroup of G is transitive. These groups can be further subdivided into the following.

    (a) **Primitive types:** G only admits trivial blocks. Some groups of this type have been proved to have intersection density 1 in [29].

    (b) **Quasiprimitive types admitting non-trivial blocks:** G admits a block system whose blocks are of size q and whose kernel of the induced action on blocks is trivial.

(II) **Genuinely imprimitive types:** G admits a block system with blocks of size q whose kernel of the induced action on the blocks is non-trivial.

2.3. Cyclic codes

Let $n \geq 1$ be a positive integer and q be a prime number. The *Hamming weight* of $\mathbf{c} \in \mathbb{F}_q^n$, denoted by $w(\mathbf{c})$, is the number of non-zero entries of $\mathbf{c}$. We also define $Z(\mathbf{c}) = n - w(\mathbf{c})$. The standard non-degenerate symmetric bilinear form $\langle \cdot, \cdot \rangle$ on $\mathbb{F}_q^n$ is given by:

$$\langle \mathbf{c}, \mathbf{d} \rangle = c_1 d_1 + \cdots + c_n d_n,$$

for all $\mathbf{c} = (c_1, \ldots, c_n), \mathbf{d} = (d_1, \ldots, d_n) \in \mathbb{F}_q^n$. The symmetric group on $\{0, \ldots, n-1\}$, which is denoted by S_n, acts on $\mathbb{F}_q^n$ as follows:

$$\mathbf{c}^\gamma = (c_{0^\gamma}, \ldots, c_{(n-1)^\gamma}),$$

for $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ and $\gamma \in S_n$.

Now let C be an $[n, k]_q$ *linear code* C over $\mathbb{F}_q$, that is, a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$. The dual $C^\perp$ of C with respect to $\langle \cdot, \cdot \rangle$ is called *the dual code* of C. For any $\gamma \in S_n$, we let $C^\gamma := \{\mathbf{c}^\gamma \mid \mathbf{c} \in C\}$. The *permutation automorphism group* of C is

Table 1
The remaining simply primitive groups of degree pq.

Soc(G)	(p, q)	action	Information
$\mathrm{P\Omega}^{\varepsilon}_{2d}(2)$	$\left(2^d - \varepsilon, 2^{d-1} + \varepsilon\right)$	singular	$\varepsilon = 1$ and d is a Fermat prime
		1-spaces	$\varepsilon = -1$ and $d - 1$ is a Mersenne prime
$\mathrm{PSL}_2(p)$	$(p, \frac{p+1}{2})$	cosets of D_{p-1}	$p \geq 13$ and $p \equiv 1 \pmod{4}$
$\mathrm{PSL}_2(q^2)$	$\left(\frac{q^2+1}{2}, q\right)$	cosets of $\mathrm{PGL}_2(q)$	
$\mathrm{PSL}_2(61)$	$(61, 31)$	cosets of $\mathrm{Alt}(5)$	

$$\mathrm{PAut}(C) = \{\gamma \in S_n \mid C^{\gamma} = C\}.$$

Clearly, $\mathrm{PAut}(C) = \mathrm{PAut}(C^{\perp})$.

From now on, we assume that C is *cyclic*, that is, the *cyclic shift* $\sigma = (0, 1, \ldots, n-1)^{-1}$ is in $\mathrm{PAut}(C)$, or equivalently,

$$(c_0, \ldots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, \ldots, c_{n-2}) \in C.$$

In this case, it is well known that C admits a so-called *parity-check polynomial* $h(t) = \sum_{i=0}^{k} a_i t^i \in \mathbb{F}_q[t]$, which is a divisor of $t^n - 1$. The polynomial $g(t) = \frac{t^n - 1}{h(t)}$ is called the *generator polynomial* of C. Moreover, we have the following description:

$$C = \Big\{(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n \mid a_0 c_{i+k} + a_1 c_{i-1+k} + \ldots + a_k c_i = 0,$$
$$\text{for } i \in \{0, 1, \ldots, n - k - 1\}\Big\}.$$

Given $\mathbf{c} \in C$, the *minimal polynomial* $f = \sum_{i=0}^{\ell-1} b_i t^i + t^{\ell} \in \mathbb{F}_q[t]$ *of* $\mathbf{c}$ is the monic irreducible polynomial with least degree that is annihilated by $\mathbf{c}$, that is,

$$b_0 c_{i+\ell} + b_1 c_{i-1+\ell} + \ldots + b_{\ell-1} c_{i+1} + c_i = 0,$$

for all $i \in \{0, 1, \ldots, p - \ell - 1\}$. Note that such a polynomial always exists and divides $h(t)$ since $h(t)$ is annihilated by $\mathbf{c}$ (see [27]).

3. Quasiprimitive types

In this section, we assume that G is a quasiprimitive group. Clearly, its *socle* $\mathrm{Soc}(G)$ (i.e., the subgroup generated by all minimal normal subgroups) is transitive. One can then reduce the study of the intersection density of G by considering its socle, since the latter is transitive. The socles of primitive groups of degree pq were classified by Marušič and Scapellato in [21]. In [29], it was proved that the socles of primitive groups have intersection density 1, except possibly for the ones given in Table 1.

It is in fact conjectured that the groups in Table 1 all have intersection density equal to 1.

Table 2
Socles of transitive groups of prime degree p.

Line	$\mathrm{Soc}(G)$	Comments
1	C_p	p is prime
2	$\mathrm{Alt}(p)$	p is prime
3	$\mathrm{PSL}_2(11)$	degree 11 (equivalently, acting on cosets of $\mathrm{Alt}(5)$)
4	M_{11}	of degree 11
5	M_{23}	of degree 23
6	$\mathrm{PSL}_d(r^{d^m})$	$d \geq 2$ and $p = \frac{r^{d^{m+1}}-1}{r^{d^m}-1}$ where r is a prime

3.1. A discussion regarding Remark 1.1

Assume that G is a quasiprimitive group which admits a unique block system $\mathcal{B}$ with blocks of size q. Recall that $\mathrm{Ker}(G \to \overline{G})$ is trivial. Consequently, the group $\overline{G}$ acts transitively and faithfully on $\mathcal{B}$. Further, if $\omega \in \Omega$ and $B \in \mathcal{B}$ contains ω, then G_ω is a subgroup of $\overline{G}_B = G_{\{B\}}$ of index q, where $G_{\{B\}}$ is the setwise stabilizer of B in G. In other words,

$$[G : G_{\{B\}}] = p \text{ and } [G_B : G_\omega] = q. \tag{2}$$

A consequence of the Classification of Finite Simple Groups is that all transitive groups of prime degree can be classified in terms of their socles. Since G is isomorphic to $\overline{G}$ which is transitive of degree p, the socle of G is one of the groups in Table 2.

We now give an analysis of the intersection density of the groups in Table 2.

- The group C_p in line 1 cannot be transitive of degree pq. Hence, it cannot be quasiprimitive.
- For the group $\mathrm{PSL}_2(11)$ in line 3, the only possibilities for q are $3, 5$, and 7. The point stabilizer $\mathrm{Alt}(5)$ of $\mathrm{PSL}_2(11)$ does not have any subgroup of index in $\{3, 7\}$. The alternating group $\mathrm{Alt}(4)$ has index 5 in $\mathrm{Alt}(5)$. This gives rise to a transitive action of $\mathrm{PSL}_2(11)$ of degree 55, whose intersection density is 1.
- Similarly, the Mathieu group M_{11} in line 4 cannot have a quasiprimitive action of degree $q \times 11$, for any $q \in \{3, 5, 7\}$ since the point stabilizer of M_{11} in its natural action does not admit a subgroup satisfying (2).
- The Mathieu group M_{23} in line 5 admits two transitive actions of degree 11×23, both of which are primitive. There are no other quasiprimitive actions of degree a product of two odd primes.

The remaining groups in Table 2 are considered separately.

Lemma 3.1. *For any $n \geq 5$ and for any odd prime $q < n$, the group $\mathrm{Alt}(n)$ does not admit a transitive action of degree $n \times q$, unless $(n, q) = (5, 3)$.*

Proof. The point stabilizer of $\mathrm{Alt}(n)$ in its natural action on $\{1, 2 \ldots, n\}$ is $\mathrm{Alt}(n-1)$. If $K \leq \mathrm{Alt}(n-1)$ such that $[\mathrm{Alt}(n-1) : K] = q$ is an odd prime, then $\mathrm{Alt}(n-1)$ acts transitively on $\mathrm{Alt}(n-1)/K$ by left multiplication. If $n \geq 6$, then the group $\mathrm{Alt}(n-1)$ is simple, so the kernel of this action of $\mathrm{Alt}(n-1)$ is trivial. Consequently, $\mathrm{Alt}(n-1)$ embeds into $\mathrm{Sym}(\mathrm{Alt}(n-1)/K)$ and so $\frac{(n-1)!}{2} \leq q!$, which is impossible. If $n = 5$, the kernel of $\mathrm{Alt}(n-1) = \mathrm{Alt}(4)$ contains the Klein group $C_2 \times C_2$ which is of index 3 in $\mathrm{Alt}(4)$. Hence, $\mathrm{Alt}(5)$ admits a transitive action of degree 15. $\quad\square$

A direct consequence of the above lemma is that the group $\mathrm{Alt}(p)$ in line 2 of Table 2 admits a transitive action of degree $p \times q$ only when $(p, q) = (5, 3)$. This action is quasiprimitive and its intersection density can be easily verified to be equal to 1 via `Sagemath`.

Therefore, an imprimitive quasiprimitive group of degree pq is an almost simple group containing $\mathrm{Alt}(5)$ (transitive of degree 15), $\mathrm{PSL}_2(11)$ (transitive of degree 55) or the groups in line 6 of Table 2.

3.2. Proof of Theorem 1.2

Before proving the main result, let us first determine the point stabilizer of $\mathrm{PSL}_k(\ell)$ in its natural action of degree p. Let p be an odd prime such that $p = \frac{\ell^k - 1}{\ell - 1}$ where $\ell = r^{k^m}$, for some prime number r. Let q be an odd prime less than p and assume that $\mathrm{PSL}_k(\ell)$ admits an imprimitive action of degree pq, where the projective space $\mathrm{PG}_{k-1}(\ell)$ of the vector space $\mathbb{F}_\ell^k$ is a complete block system. In order for $p = \frac{\ell^k - 1}{\ell - 1}$ to be a prime, k must be a prime number and $\gcd(k, \ell - 1) = 1$. The latter implies that $\mathrm{PSL}_k(\ell) = \mathrm{SL}_k(\ell)$. A matrix in $\mathrm{SL}_k(\ell)$ that fixes the 1-dimensional subspace $\langle e_1 \rangle$, where $e_1 \in \mathbb{F}_\ell^k$ is the vector whose first entry is 1 and 0 elsewhere, is of the form

$$\left[\begin{array}{c|ccccc} \det(B)^{-1} & a_1 & a_2 & \ldots & a_{k-1} \\ \hline \mathbf{0} & & & B & \end{array} \right] \tag{3}$$

where $B \in \mathrm{GL}_{k-1}(\ell)$ and $[a_1 \; a_2 \; \ldots \; a_{k-1}]^T \in \mathbb{F}_\ell^{k-1}$. If $\mathrm{SL}_k(\ell)$ admits a quasiprimitive action of degree pq for some odd $q < p$, then by (2) the subgroup consisting of all elements of the form (3) admits a subgroup of index q.

For the remainder of this section, we consider the groups in line 6 of Table 2 for $m = 0$ and $r = k = q$. Recall that a *Singer subgroup* of $\mathrm{PSL}_n(s)$, for any prime power s, is a cyclic subgroup of order $\frac{s^n - 1}{s - 1} \gcd(n, s - 1)$. Let T be a Singer subgroup of $\mathrm{PSL}_k(\ell)$. Since $\gcd(k, \ell - 1) = 1$, a Singer subgroup of $\mathrm{PSL}_k(\ell) = \mathrm{SL}_k(\ell)$ is a regular subgroup of order p. Let $\varphi \in \mathrm{Aut}(\mathbb{F}_{\ell^k}/\mathbb{F}_\ell)$ be the Frobenius automorphism of the field $\mathbb{F}_{\ell^k}$. As detailed in [10, pg. 497], an element of $\langle \varphi \rangle$ can be viewed as an invertible matrix over $\mathbb{F}_{\ell^k}$ and the latter induces a collineation of $\mathrm{PG}_{k-1}(\ell)$. Let $\langle \psi \rangle$ be the group determined by these collineations. By [10], the normalizer of T in $\mathrm{PSL}_k(\ell)$ is given by

$$T \rtimes \langle \psi \rangle \cong C_p \rtimes C_k. \tag{4}$$

Moreover, $T \rtimes \langle \psi \rangle$ is a Frobenius group by [10, Theorem 2.10]. By [20, Lemma 2.6] and the fact that $k = q$, the subgroup $T \rtimes \langle \psi \rangle \cong C_p \rtimes C_q$ is a regular subgroup of $\mathrm{PSL}_k(\ell)$. By Lemma 2.1, we conclude that $\rho(\mathrm{PSL}_q(\ell)) = 1$.

4. Proofs of Theorem 1.4 and Theorem 1.5

4.1. Proof of Theorem 1.4

Throughout this section, we assume that $G \leq \mathrm{Sym}(\Omega)$ is transitive of degree pq, where $p > q$ are two odd primes. In addition, we suppose that $\mathcal{B} = \{B_1, B_2, \ldots, B_p\}$ is the unique block system of G and $H = \mathrm{Ker}(G \to \overline{G})$ is non-trivial. Let N be a minimal normal subgroup of G contained in H.

Theorem 4.1. *If N is non-abelian, then $\rho(G) = 1$.*

Proof. Since $N \neq 1$ and q is prime, N is transitive on each block in $\mathcal{B}$. By [6, Theorem 4.3.A (3)], N is a direct product of isomorphic non-abelian simple groups, that is, we can write

$$N = S_1 \times S_2 \times \ldots \times S_k, \ (k \geq 1), \tag{5}$$

and there exists a simple group S such that $S_i \cong S$ for all $i \in \{1, 2, \ldots, k\}$.

We identify H (and thus N) as a subgroup of $\mathrm{Sym}(q)^p$. For $1 \leq j \leq p$, let N_j be the restriction of N to the j-th block B_j and denote by $\pi_j : N \twoheadrightarrow N_j \leq \mathrm{Sym}(q)$ the canonical restriction. Recall that, by a result due to Burnside, the subgroup N_j is a simple group for any $j \in \{1, 2, \ldots, p\}$. If K is any subgroup of N, we define

$$\mathrm{Supp}(K) = \{j \in \{1, \ldots, p\} \mid \pi_{j_{|K}} \neq 1\}.$$

Moreover, if K is a simple normal subgroup of N, then $\pi_{j_{|K}} : K \to N_j$ is an isomorphism for all $j \in \mathrm{Supp}(K)$. Let $i \in \{1, \ldots, k\}$. Set

$$J_i = \mathrm{Supp}(S_i) = \{j \in \{1, \ldots, p\} \mid \pi_{j_{|S_i}} : S_i \to N_j \text{ is an isomorphism}\}.$$

Fact 1: *We claim that $J_i \neq \varnothing$, for any $i \in \{1, 2, \ldots, k\}$.*

It is clear that there exists $j \in \{1, \ldots, p\}$ such that $\pi_j(S_i) \neq 1$. Since π_j is surjective and $S_i \trianglelefteq N$, we have $\pi_j(S_i) \trianglelefteq N_j$, and so $\pi_j(S_i) = N_j$, as N_j is simple. Now, since $\mathrm{Ker}(\pi_{j_{|S_i}})$ is a proper normal subgroup of S_i, we conclude that $\mathrm{Ker}(\pi_{j_{|S_i}}) = 1$. Therefore $j \in J_i$.

Fact 2: *We claim that*

$$\bigcup_{i=1}^{k} J_i = \{1, \ldots, p\}, \tag{6}$$

therefore, all N_j are non-abelian.

Let $j \in \{1, 2, \ldots, p\}$. By definition, $\pi_{j|_N} = \pi_j \neq 1$, so there exists $i \in \{1, 2, \ldots, k\}$ such that $\pi_{j|_{S_i}} \neq 1$, or equivalently, $j \in J_i$. Therefore, we have $\{1, \ldots, p\} = \mathrm{Supp}(N) \subset \bigcup_{i=1}^{k} J_i$. The other inclusion is obvious.

Fact 3: *We claim that $J_i \cap J_{i'} = \varnothing$ when $i \neq i'$.*

Suppose that $J_i \cap J_{i'} \neq \varnothing$, and pick $j \in J_i \cap J_{i'}$. Since S_i and $S_{i'}$ commute when viewed as subgroups of the direct product in (5), $N_j = \pi_j(S_i)$ and $N_j = \pi_j(S_{i'})$ also commute, and so N_j is abelian, which is a contradiction. Hence,

$$J_i \cap J_{i'} = \varnothing \text{ whenever } i \neq i'. \tag{7}$$

Fact 4: *We claim that $|J_i|$ does not depend on i.*

Let $i, i' \in \{1, \ldots, k\}$. Since G is transitive and N is normal, there exists $g \in G$ such that $\mathrm{Supp}(gS_ig^{-1}) \cap \mathrm{Supp}(S_{i'}) \neq \varnothing$. Since $gS_ig^{-1} \trianglelefteq N$ and $S_{i'} \trianglelefteq N$, either $gS_ig^{-1} \cap S_{i'} = 1$ or $gS_ig^{-1} = S_{i'}$. In the first case, gS_ig^{-1} and $S_{i'}$ commute, which implies that, for $j \in \mathrm{Supp}(gS_ig^{-1}) \cap \mathrm{Supp}(S_{i'})$, N_j is abelian. Hence, we get a contradiction. Therefore, we must have $gS_ig^{-1} = S_{i'}$. Since g permutes the blocks, the latter implies that

$$|J_i| = |\mathrm{Supp}(S_i)| = |\mathrm{Supp}(gS_ig^{-1})| = |\mathrm{Supp}(S_{i'})| = |J_{i'}|.$$

Consequently, there exists a positive integer m such that

$$|J_i| = m, \quad \text{for all } i \in \{0, 1, \ldots, k\}. \tag{8}$$

Therefore, by (6), (7), and (8) we have $km = p$. As p is prime, we either have $k = 1$ or $k = p$.

Fact 5: *N admits a derangement which is a product of p q-cycles.*

Assume that $k = 1$. Notice that $\mathrm{Supp}(N) = \{1, \ldots, p\}$, and that, $\pi_j : N \to N_j$ is an isomorphism, for all $j \in \{1, \ldots, p\}$. Since q divides $|N|$, there exists a permutation $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_p) \in N \setminus \{1\}$ of order q (viewed as an element of $\mathrm{Sym}(q)^p$). Therefore, σ_j is a q-cycle or 1, for any $j \in \{1, 2, \ldots, p\}$. However, for $j \in \{1, \ldots, p\}$, the map π_j is injective, so we have

$$1 = \pi_j(1, \ldots, 1) \neq \pi_j(\sigma) = \sigma_j.$$

Hence, all σ_j are q-cycles, and so σ is a product of p q-cycles. In other words, σ is a semiregular element of N.

Next, assume that $k = p$. Since $m = 1$, each S_i is a subgroup of the i-th factor $\mathrm{Sym}(q)$. Therefore,

$$\{S_1, \ldots, S_p\} = \{N_1, \ldots, N_p\}.$$

As each N_i is transitive on the block B_i, for any $i \in \{1, 2, \ldots, p\}$, N_i admits an element of order q. From this we deduce that $N = S_1 \times \ldots \times S_p$ admits an element which is a product of p q-cycles, i.e., a semiregular element.

Fact 6: *The intersection density of G is equal to* 1.

Since N admits a semiregular element of order q and $N \leq H$, we conclude by Lemma 2.3 that $\rho(G) \leq \rho(\overline{G})$. Since $\overline{G}$ is transitive of prime degree, we have $\rho(\overline{G}) = 1$, which implies $\rho(G) = 1$. $\square$

This proves Theorem 1.4 (i). For the remainder of this section, we consider the case when N is an elementary abelian q-group. Before proving the next result, we recall the following lemma, whose proof is straightforward.

Lemma 4.2. *Let $\sigma = (0, \ldots, q - 1)$. The normalizer of $\langle \sigma \rangle$ in $\mathrm{Sym}(q)$ is*

$$N_{\mathrm{Sym}(q)}(\langle \sigma \rangle) = \left\{ \tau_{a,i} = \begin{pmatrix} 0 & 1 & \cdots & q-1 \\ a & a+i & \cdots & a+(q-1)i \end{pmatrix} \mid 0 \leq a \leq q-1, 1 \leq i \leq q-1 \right\}.$$

Moreover, the derangements in $N_{\mathrm{Sym}(q)}(\langle \sigma \rangle)$ are exactly $\sigma, \sigma^2, \ldots, \sigma^{q-1}$.

Theorem 4.3. *Assume that N is an elementary abelian q-group and H contains a derangement x, then $\rho(G) = 1$.*

Proof. We claim that x is necessarily a product of p q-cycles. First, we identify H as a subgroup of $\mathrm{Sym}(q)^p \leq \mathrm{Sym}(\Omega)$. For $1 \leq i \leq p$, let $\pi_i : \mathrm{Sym}(q)^p \twoheadrightarrow \mathrm{Sym}(q)$ be the i-th projection. Since $1 \neq N \trianglelefteq G$ and G acts transitively on Ω, we get $\pi_i(N) \neq 1$ $(1 \leq i \leq p)$ and $\pi_i(N)$ is an elementary abelian q-group of $\mathrm{Sym}(q)$. Such a subgroup of $\mathrm{Sym}(q)$ has to be cyclic. Therefore, there is a q-cycle ℓ_i $(1 \leq i \leq p)$ such that $\pi_i(N) = \langle \ell_i \rangle$.

Write $x = (x_1, \ldots, x_p) \in \mathrm{Sym}(q)^p$, where x_i belongs to the i-th factor $\mathrm{Sym}(q)$. Now let $1 \leq i \leq p$. Since $N \trianglelefteq H$ and $x \in H$, we get

$$\langle \ell_i \rangle = \pi_i(N) = \pi_i(xNx^{-1}) = \pi_i(x)\pi_i(N)(\pi_i(x))^{-1} = x_i\langle \ell_i \rangle x_i^{-1}.$$

Therefore, $x_i \in N_{\mathrm{Sym}(q)}(\langle \ell_i \rangle)$. Since x_i is a derangement, x_i is a q-cycle by Lemma 4.2. Consequently, x is a product of p q-cycles. It is not hard to see that x is a semiregular element such that the set of orbits of $\langle x \rangle$ coincide with $\mathcal{B}$. Therefore, $\rho(G) \leq \rho(\overline{G}) = 1$ by Lemma 2.3. $\square$

4.2. Proof of Theorem 1.5

First, we recall the construction from [14]. Let C be a $[p,k]_q$ cyclic code satisfying

$$Z(\mathbf{c}) > 0 \quad \text{for all } \mathbf{c} \in C. \tag{9}$$

Consider $\Omega = \mathbb{Z}_q \times \mathbb{Z}_p$. Let α be the permutation of Ω given by $\alpha : (i,j) \mapsto (i, j+1)$, and for $\mathbf{c} = (c_0, c_1, \ldots, c_{p-1}) \in C$, we let $\beta_{\mathbf{c}}$ be the permutation of $\mathbb{Z}_q \times \mathbb{Z}_p$ such that $\beta_{\mathbf{c}} : (i,j) \mapsto (i + c_j, j)$. Now, define $S = \{\beta_{\mathbf{c}} \mid \mathbf{c} \in C\}$, $H(C) := \langle S \rangle$, and $G(C) := \langle S \cup \{\alpha\} \rangle$. It is clear that $G(C)$ is transitive on Ω and $H(C) \trianglelefteq G(C)$. The orbits of $H(C)$ are of the form $B_j = \mathbb{Z}_q \times \{j\}$, for $0 \leq j \leq p-1$. We note that for any $\mathbf{c}, \mathbf{c}' \in C$, we have

$$\beta_{\mathbf{c}}\beta_{\mathbf{c}'} = \beta_{\mathbf{c}+\mathbf{c}'}. \tag{10}$$

A straightforward computation, using (10), proves that

$$\mathrm{F}(G(C)) = H(C).$$

Moreover, $H(C)$ is derangement-free since $Z(\mathbf{c}) > 0$, for all $\mathbf{c} \in C$. Hence, $\Gamma_{G(C)}$ is a complete p-partite graph and therefore $\rho(G(C)) = q$. Consequently, we have the following result.

Theorem 4.4 ([14]). *If C is a $[p,k]_q$ cyclic code such that $Z(\mathbf{c}) > 0$, for all $\mathbf{c} \in C$, then there exists an imprimitive group $G(C)$ whose intersection density is equal to q.*

Below, we give a proof of Theorem 1.5, which in a certain sense, gives a converse to Theorem 4.4.

Theorem 4.5. *Let $G \leq \mathrm{Sym}(\Omega)$ be a degree pq ($p > q$ odd primes) transitive group admitting a unique block system $\mathcal{B}$ whose blocks are of size q. Assume that the kernel $H = \mathrm{Ker}(G \to \overline{G})$ is nontrivial and G is minimally transitive with intersection density $\rho(G) = q$. Then, there is a $[p,k]_q$ cyclic code C such that the Hamming weight $w(\mathbf{c})$ is not equal to p, for all $\mathbf{c} \in C$.*

Proof. Since $H = \mathrm{Ker}(G \to \overline{G})$ is nontrivial, there exists a minimal normal subgroup N of G contained in H. By Theorem 1.4, N is an elementary abelian q-group and H is derangement-free. Now let g be a derangement of order p, which exists by [19]. Since $\langle N, g \rangle$ is transitive and G is minimally transitive, we deduce that $N = H$. Now we are going to construct a $[p,k]_q$ ($k = \log_q(|N|)$) cyclic code C with the property that $Z(\mathbf{c}) > 0$, for all $\mathbf{c} \in C$.

Relabel the blocks of $\mathcal{B}$ by $B_0, \ldots, B_{p-1}$ in order to obtain $g(B_j) = B_{j+1}$, for $0 \leq j \leq p-1$ and $g(B_{p-1}) = B_0$. Consequently, we may identify N with a subgroup $\langle \sigma_0 \rangle \times \cdots \times \langle \sigma_{p-1} \rangle$, for some q-cycles $\sigma_j \in \mathrm{Sym}(B_j)$. Moreover, we may assume that $g\sigma_j g^{-1} =$

σ_{j+1} for $0 \leq j \leq p-1$. Now write $B_0 = \{b_{0,0}, \ldots, b_{q-1,0}\}$ and suppose that $\sigma_0 = (b_{0,0} \ \ldots \ b_{q-1,0})$. For $0 \leq i \leq q-1$ and $0 \leq j \leq p-1$, let $b_{i,j} = b_{i,0}^{g^j}$. In this case, we have $B_j = \{b_{0,j}, \ldots, b_{q-1,j}\}$, for all $0 \leq j \leq p-1$. A direct computation shows that $\sigma_j = (b_{0,j} \ \ldots \ b_{q-1,j})$, for all $0 \leq j \leq p-1$. Consider the group isomorphism $\Psi : (a_0, \ldots, a_{p-1}) \in \mathbb{F}_q^p = \mathbb{Z}_q^p \mapsto (\sigma_0^{a_0}, \ldots, \sigma_{p-1}^{a_{p-1}}) \in \langle\sigma_0\rangle \times \cdots \times \langle\sigma_{p-1}\rangle$. In this situation $C = \Psi^{-1}(N)$ is a $[p, k]_q$-cyclic code, where $k = \log_q(|N|)$.

The map $\varphi : b_{i,j} \in \Omega \mapsto (i, j) \in \mathbb{Z}_q \times \mathbb{Z}_p$ is a bijection. By identifying $b_{i,j}$ and (i, j), we deduce an action of C on $\mathbb{Z}_q \times \mathbb{Z}_p$ as follows:

$$(i, j)^{\Psi(\mathbf{c})} := (i + c_j, j), \text{ for } \mathbf{c} = (c_0, c_1, \ldots, c_{p-1}) \in C.$$

For $\mathbf{c} = (c_0, c_1, \ldots, c_{p-1}) \in C$, the element $\Psi(\mathbf{c}) \in N$ admits a fixed point, so there exists $(i, j) \in \mathbb{Z}_q \times \mathbb{Z}_p$ such that $(i, j)^{\Psi(\mathbf{c})} = (i, j)$. Hence, we have $c_j = 0$. It follows that $Z(\mathbf{c}) > 0$ for all $\mathbf{c} \in C$. $\quad\square$

Remark 4.6. The minimal transitivity condition in Theorem 4.5 is not necessary. However, one can check that, this condition allows us to recover the structure of G from the constructed code C. Indeed, in this case, G is permutation equivalent to the group $G(C)$.

5. Proof of Theorem 1.7

In this section, we prove Theorem 1.7. Our proof relies on the existence of certain cyclic codes. Now, let p and q be two odd primes such that $p = \frac{q^k - 1}{q - 1}$ for some prime k. Recall that k is the smallest positive integer such that $q^k = 1 \pmod{p}$. Recall also that $\Phi_p(t)$ is the product of $\frac{\phi(p)}{k} = \frac{p-1}{k}$ monic irreducible polynomials over $\mathbb{F}_q$ of degree k. Hence, the splitting field of $\Phi_p(t)$ is $\mathbb{F}_{q^k}$.

Let $Z \subset \{x \in \mathbb{F}_{q^k} \mid x^p = 1\}$. The *cyclic code with defining zeroes Z* is the cyclic code

$$C_{q,k}(Z) = \left\{(c_0, c_1, \ldots, c_{p-1}) \in \mathbb{F}_q^p \mid \sum_{i=0}^{p-1} c_i x^i = 0, \text{ for all } x \in Z\right\}.$$

Since $\gcd(p, q) = 1$, the map $\varphi : \{0, 1, \ldots, p-1\} \to \{0, 1, \ldots, p-1\}$ given by:

$$i^\varphi = qi \pmod{p}$$

belongs to S_p. Let $\mathbf{c} = (c_0, c_1, \ldots, c_{p-1}) \in C_{q,k}(Z)$ and $x \in Z$. If we denote $\mathbf{c}(x) = c_0 + c_1 x + \ldots + c_{p-1}x^{p-1}$, we have

$$\mathbf{c}^\varphi(x) = \mathbf{c}(x^{q^{k-1}}) = \mathbf{c}(x)^{q^{k-1}} = 0.$$

This is equivalent to saying that $\mathbf{c}^\varphi \in C_{q,k}(Z)$. In other words, $\varphi \in \mathrm{PAut}(C_{q,k}(Z))$. The permutation automorphism φ is called the *Frobenius automorphism* of $C_{q,k}(Z)$.

Moreover, since k is the smallest positive integer such that $q^k = 1 \pmod{p}$, the order of φ is k. See [11] for details.

5.1. An extension from the Frobenius permutation automorphism

Let ζ be any root of $\Phi_p(t)$ with minimal polynomial $g(t) \in \mathbb{F}_q[t]$. The generator polynomial of $C_{q,k}(\{\zeta\})$ is clearly $g(t)$, and so $C_{q,k}(\{\zeta\})$ is a $[p, p-k]_q$ cyclic code. Now, let $C = C_{q,k}(\{\zeta\})^\perp$ be the dual code of $C_{q,k}(\{\zeta\})$. Observe that $\mathrm{PAut}(C) = \mathrm{PAut}(C_{q,k}(\{\zeta\}))$ and C is a $[p, k]_q$ cyclic code.

Next, we consider the group $K = \langle \sigma, \varphi \rangle \le \mathrm{PAut}(C)$, where σ is the cyclic shift and φ is the Frobenius automorphism. By noting that $j^{\varphi^{-1}\sigma\varphi} = j + q \pmod{p}$ for any $j \in \{0, \ldots, p-1\}$, we conclude that $\varphi^{-1}\sigma\varphi = \sigma^q$. In other words, φ normalizes σ. Moreover, since p and q are distinct primes, we have $\langle \sigma \rangle \cap \langle \varphi \rangle = \{id\}$. Therefore, $K = \langle \sigma \rangle \rtimes \langle \varphi \rangle \cong C_p \rtimes C_k$.

Let α and $\beta_\mathbf{c}$ for $\mathbf{c} \in C$ be the permutations of $\Omega_{p,q} = \mathbb{Z}_q \times \mathbb{Z}_p$ defined in the paragraph before Theorem 4.4. Recall that $H(C)$ is the subgroup generated by $\{\beta_\mathbf{c} \mid \mathbf{c} \in C\}$ and $G(C) = H(C) \rtimes \langle \alpha \rangle$. In addition, we define the permutation ψ of $\Omega_{p,q}$ by $(i,j)^\psi = (i, j^\varphi)$, where φ is the Frobenius automorphism of C. For any $(i,j) \in \Omega_{p,q}$ and $\mathbf{c} \in C$, we have

$$\begin{cases} (i,j)^{\psi^{-1}\alpha\psi} & = (i,j)^{\alpha^q} \\ (i,j)^{\psi^{-1}\beta_\mathbf{c}\psi} & = \left(i + v_{j^{\varphi^{-1}}}, j\right) = (i,j)^{\beta_{\mathbf{c}^{\varphi^{-1}}}}. \end{cases}$$

As $\varphi \in \mathrm{PAut}(C)$, we conclude that ψ normalizes $G(C)$. In particular, if we let $M(C) := \langle G(C), \psi \rangle$, noting that $G(C) \cap \langle \psi \rangle = \{id\}$, we have $M(C) = H \rtimes (\langle \alpha \rangle \rtimes \langle \psi \rangle) \cong \mathbb{F}_q^k \rtimes (C_p \rtimes C_k)$. We note that ψ fixes any $(i,0)$ for $i \in \mathbb{Z}_q$, so ψ fixes the block $\mathbb{Z}_q \times \{0\}$ pointwise.

5.2. The derangement graph of $M(C)$

In this section, we will study the derangement graph of $M(C)$ defined in the previous section. The group $M := M(C) = H \rtimes (\langle \alpha \rangle \rtimes \langle \psi \rangle)$ acts imprimitively on $\Omega_{p,q}$ with block system $\mathcal{B} = \{\mathbb{Z}_q \times \{j\} \mid j \in \{0, 1, \ldots, p-1\}\}$. For any $j \in \{0, 1, \ldots, p-1\}$, we let $B_j := \mathbb{Z}_q \times \{j\}$. We also prove the following theorem.

Theorem 5.1. *The intersection density of $M(C)$ is equal to $\max(1, \frac{q}{k})$.*

We begin with the following easy lemma.

Lemma 5.2. *If $t \in \{1, \ldots, k-1\}$, then $q^t - 1$ is invertible modulo p.*

Proof. This follows from the fact that k is the smallest positive integer such that $p \mid q^k - 1$. $\square$

Lemma 5.3. *For $s \in \{0, \ldots, p-1\}$ and $t \in \{0, \ldots, k-1\}$ such that $\alpha^s \psi^t \neq 1$, we have*

$$\alpha^s \psi^t \text{ fixes a block } \Leftrightarrow \alpha^s \psi^t \text{ fixes a unique block } \Leftrightarrow t \neq 0. \tag{11}$$

Moreover, if $\alpha^s \psi^t$ fixes $B \in \mathcal{B}$, then $\alpha^s \psi^t$ fixes B pointwise.

Proof. For $j \in \{0, \ldots, p-1\}$ we have $B_j^{\alpha^s \psi^t} = B_{q^t(j+s)}$. If $t = 0$, then the element $\alpha^s \psi^t = \alpha^s$ fixes no block, since $s \neq 0$. Now assume $t \neq 0$. By Lemma 5.2, $q^t - 1$ is invertible modulo p. Hence, $\alpha^s \psi^t$ fixes a block B_j if and only if $q^t(j + s) = j$, or equivalently, $j \equiv (q^t - 1)^{-1} \pmod{p}$. Therefore, we get (11). The last statement is straightforward. $\quad\square$

5.2.1. Structure of Γ_M

In this section, we determine the structure of the derangement graph of M using the lexicographic product. Given two graphs $X = (V(X), E(X))$ and $Y = (V(Y), E(Y))$, the *lexicographic product* $X[Y]$ is the graph whose vertex set is $V(X) \times V(Y)$ and two vertices (x, y) and (u, v) are adjacent in $X[Y]$ if $x \sim_X u$ or $x = u$ and $y \sim_Y v$.

Recall that ψ fixes the elements of the block $\mathbb{Z}_q \times \{0\}$ pointwise. Since $M = H \rtimes (\langle \alpha \rangle \rtimes \langle \psi \rangle)$, an element of M is of the form $h\alpha^s \psi^t$, for some $h \in H$, $s \in \{0, 1, \ldots, p-1\}$ and $t \in \{0, 1, \ldots, k-1\}$.

Let us find the structure of the derangement graph of M. The point stabilizer $H_{(i,j)}$, for $(i, j) \in \Omega_{p,q}$, is crucial to the structure of this graph. We note that H acts transitively on each element of $\mathcal{B}$. Therefore, $[H : H_{(i,j)}] = q$.

Now, we decompose the derangement graph of M into cosets of the subgroup H. The cosets M/H partition M. Therefore, the derangement graph Γ_M can also be partitioned into $[M : H]$ parts where each part is a coclique of size $|H|$ (H is intersecting). We shall describe the edges of Γ_M by describing the edges between H and another coset of H in M.

We define $H^{(t)} := \{H\alpha^s \psi^t \mid 0 \leq s \leq p-1\}$, for $0 \leq t \leq k-1$. We note that any coset of H in M is in $\bigcup_{t=0}^{k-1} H^{(t)}$ and the latter is a pairwise disjoint union.

Assume that $Hy \in H^{(t)}$ and $Hz \in H^{(t')}$ for $t, t' \in \{0, 1, \ldots, k-1\}$. By definition, for $h_1, h_2 \in H$ we have

$$h_1 y \sim h_2 z \Leftrightarrow h_1 \sim h_2 z y^{-1}.$$

Consequently, we may only consider the adjacency between H and Hzy^{-1}. Assume that $Hzy^{-1} \in H^{(t)}$ for some $t \in \{0, 1, \ldots, k-1\}$. That is, there exists $s \in \{0, 1, \ldots, p-1\}$ such that $Hzy^{-1} = H\alpha^s \psi^t$. Let $\Gamma_M[\alpha^s \psi^t]$ be the subgraph of Γ_M induced by $H \cup H\alpha^s \psi^t$.

- If $t = 0$, then $B^{\alpha^s \psi^t} \neq B$ for any $B \in \mathcal{B}$ (see (11)), unless $s = 0$. If $s \neq 0$ and $t = 0$, then for any $(i, j) \in \Omega_{p,q}$, we have

$$(i, j)^{n\alpha^s} \neq (i, j)^{n'},$$

for any $n, n' \in H$. Therefore, all the possible edges between H and $H\alpha^s$ occur and so

$$\Gamma_M[\alpha^s] = K_{|H|,|H|} \text{ for any } s \in \{1, 2, \ldots, p-1\}, \tag{12}$$

where $K_{|H|,|H|}$ is the complete bipartite graph with parts of equal size $|H|$.

- By (11), if $t \neq 0$, then there exists a unique $B \in \mathcal{B}$ such that $B^{\alpha^s \psi^t} = B$, and moreover, $\alpha^s \psi^t$ fixes B pointwise. Assume without loss of generality that this block B is $B_\ell = \mathbb{Z}_q \times \{\ell\}$, for some $\ell \in \mathbb{Z}_p$. Let $\beta_{\mathbf{c}} \in H$, where $\mathbf{c} = (c_0, c_1, \ldots, c_{p-1}) \in C$ and $c_\ell \neq 0$ (i.e., $\langle \beta_{\mathbf{c}} \rangle$ is transitive on B). The subgroup $\langle \beta_{\mathbf{c}} \rangle = \{id, \beta_{\mathbf{c}}, \beta_{\mathbf{c}}^2, \ldots, \beta_{\mathbf{c}}^{q-1}\}$ is a right transversal of $H_{(0,\ell)}$ in H, that is, $\left| \langle \beta_{\mathbf{c}} \rangle \cap H_{(0,\ell)} y \right| = 1$ for any $y \in H$. Now we will see that we can precisely determine the edges of $\Gamma_M[\alpha^s \psi^t]$.

  The subgroup H is partitioned by the cosets $\left(H_{(0,\ell)} \beta_{\mathbf{c}}^l \right)_{l=0,1,\ldots,q-1}$. Now, we determine the edges between $H_{(0,\ell)} \beta_{\mathbf{c}}^l$ and $H_{(0,\ell)} \beta_{\mathbf{c}}^{l'} \alpha^s \psi^t$, for $l, l' \in \{0, 1, \ldots, q-1\}$. Assume that $(i', j') \in B' = B_{\ell'}$, where $\ell' \neq \ell$. Since $\alpha^s \psi^t$ only fixes B and $H_{(0,\ell)} \beta_{\mathbf{c}}^l \subset H$ which is the kernel of the action on $\mathcal{B}$, we know that for any $l, l' \in \{0, 1, \ldots, q-1\}$

$$(i', j')^{H_{(0,\ell)} \beta_{\mathbf{c}}^{l'} \alpha^s \psi^t} \cap B' = \varnothing \text{ and } (i', j')^{H_{(0,\ell)} \beta_{\mathbf{c}}^l} \subset B'.$$

In other words, no elements of $H_{(0,\ell)} \beta_{\mathbf{c}}^l$ can intersect an element of $H_{(0,\ell)} \beta_{\mathbf{c}}^{l'} \alpha^s \psi^t$ outside of B. Let us examine the possible elements of B on which two permutations from the two cosets can intersect. Since $H_{(0,\ell)}$ fixes B pointwise, if $l = l'$ and $(i, \ell) = (0, \ell)^{\beta_{\mathbf{c}}^l}$, then for any $z, z' \in H_{(0,\ell)} = H_{(i,\ell)}$ we have

$$(0, \ell)^{z' \beta_{\mathbf{c}}^{l'} \alpha^s \psi^t} = \left((0, \ell)^{z' \beta_{\mathbf{c}}^{l'}} \right)^{\alpha^s \psi^t} = (0, \ell)^{z' \beta_{\mathbf{c}}^{l'}} = (0, \ell)^{\beta_{\mathbf{c}}^{l'}} = (0, \ell)^{\beta_{\mathbf{c}}^l} = (i, \ell)$$

$$(0, \ell)^{z \beta_{\mathbf{c}}^l} = (0, \ell)^{\beta_{\mathbf{c}}^l} = (i, \ell).$$

In other words, any permutation in $H_{(0,\ell)} \beta_{\mathbf{c}}^{l'} \alpha^s \psi^t$ intersects any permutation in $H_{(0,\ell)} \beta_{\mathbf{c}}^l$.

If $l \neq l'$, then $\beta_{\mathbf{c}}^l \beta_{\mathbf{c}}^{-l'}$ does not have a fixed point in B since $\langle \beta_{\mathbf{c}} \rangle$ is a right transversal of $H_{(0,\ell)}$ in H. For any $z, z' \in H_{(0,\ell)}$, we have

$$(i, \ell)^{z \beta_{\mathbf{c}}^l} = (i, \ell)^{\beta_{\mathbf{c}}^l}$$

$$(i, \ell)^{z' \beta_{\mathbf{c}}^{l'} \alpha^s \psi^t} = (i, \ell)^{z' \beta_{\mathbf{c}}^{l'}} = (i, \ell)^{\beta_{\mathbf{c}}^{l'}} \neq (i, \ell)^{\beta_{\mathbf{c}}^l}.$$

Consequently, no permutation in $H_{(i,j)} \beta_{\mathbf{c}}^l$ can intersect any permutation of $H_{(i,j)} \beta_{\mathbf{c}}^{l'} \alpha^s \psi^t$, for $l \neq l'$. In summary, for any $t \neq 0$ the graph induced by

$$\begin{cases} H_{(0,\ell)} \beta_{\mathbf{c}}^l \cup H_{(0,\ell)} \beta_{\mathbf{c}}^{l'} \alpha^s \psi^t \text{ is a coclique} & \text{if } l = l' \\ H_{(0,\ell)} \beta_{\mathbf{c}}^l \cup H_{(0,\ell)} \beta_{\mathbf{c}}^{l'} \alpha^s \psi^t \text{ is complete bipartite} & \text{if } l \neq l'. \end{cases} \tag{13}$$

Let K_q^2 be the complete bipartite graph $K_{q,q}$. In addition, let $\widetilde{K}_q^2$ be the graph obtained from K_q^2 by removing q vertex-disjoint edges, i.e., a perfect matching. Combining (12) and (13), we conclude that

$$\Gamma_M[\alpha^s \psi^t] = \begin{cases} K_q^2[\Gamma_{H_{(0,\ell)}}] & \text{if } t = 0 \\ \widetilde{K}_q^2[\Gamma_{H_{(0,\ell)}}] & \text{otherwise.} \end{cases}$$

From this, the adjacency in Γ_M between $H\alpha^s\psi^t$ and $H\alpha^{s'}\psi^{t'}$ is completely determined by the values of $t - t'$. If $t = t'$, then the subgraph induced by $H\alpha^s\psi^t \cup H\alpha^{s'}\psi^{t'}$, where $s \neq s'$, in Γ_M is isomorphic to $\Gamma_M[\alpha^{s-s'}]$ and therefore it is isomorphic to $K_q^2[\Gamma_{H_{(0,\ell)}}]$. If $t \neq t'$, then the subgraph induced by $H\alpha^s\psi^t \cup H\alpha^{s'}\psi^{t'}$ in Γ_M is isomorphic to $\Gamma_M[\alpha^{s-q^{t'-t}s'}\psi^{t'-t}]$, and so it is isomorphic to $\widetilde{K}_q^2[\Gamma_{H_{(0,\ell)}}]$.

5.2.2. Proof of Theorem 5.1

Let $\mathcal{F}$ be a coclique of Γ_M. Without loss of generality, we may assume that $id \in \mathcal{F}$ since we can always multiply $\mathcal{F}$ by the inverse of one of its elements and obtain another intersecting set.

First assume that $\mathcal{F}$ is not contained in H. For any $t \in \{0, 1, \ldots, k-1\}$, we define $\mathcal{F}_t = \mathcal{F} \cap \left(\bigcup_{s=0}^{p-1} H\alpha^s\psi^t \right)$.

Claim 1: *For any $t \in \{1, \ldots, k-1\}$, we have $|\mathcal{F}_t| \leq \frac{|H|}{q}$.*

Indeed, from the structure of Γ_M, $\mathcal{F}_t$ is contained in $H\alpha^s\psi^t$ for some $s \in \{0, \ldots, p-1\}$. Now let $g = \beta_{\mathbf{c}}\alpha^s\psi^t \in \mathcal{F}_t$. Since $g \not\sim_{\Gamma_M} id$, there exists $(i,j) \in \Omega_{p,q}$ such that $(i,j) = (i,j)^g$, that is, $(i,j) = (i + c_j, q^t(j + s))$. From Lemma 5.2, $j = -(q^t - 1)^{-1}s$ and $c_j = 0$. Therefore, there are at most $\frac{|H|}{q}$ possible choices for $\mathbf{c}$, and so $|\mathcal{F}_t| \leq \frac{|H|}{q}$.

Claim 2: *We have $|\mathcal{F}_0| \leq \frac{|H|}{q}$.*

Indeed, $\mathcal{F}_0$ is contained in $H\alpha^s$ for some $s \in \{0, \ldots, p-1\}$. The identity element id is non-adjacent to every element of $\mathcal{F}_t$ and no element in $H\alpha^s$ has a fixed point for $s \in \{1, \ldots, p-1\}$, hence $s = 0$ and $\mathcal{F}_0 \subset H$. Consider $u \in \mathcal{F} \setminus H \neq \varnothing$ and write $u^{-1} = \beta_{\mathbf{c}'}\alpha^{s'}\psi^{t'}$. Now let $h = \beta_{\mathbf{c}} \in \mathcal{F}_0$. Since $h \not\sim u$, there exists $(i,j) \in \Omega_{p,q}$ such that $(i,j) = (i,j)^{hu^{-1}} = (i,j)^{\beta_{\mathbf{c}+\mathbf{c}'}\alpha^{s'}\psi^{t'}}$. Note that $t' \neq 0$ since $\beta_{\mathbf{c}+\mathbf{c}'}\alpha^{s'}$ fixes no point when $s' \neq 0$. The same argument as in Claim 1 proves that there are at most $\frac{|H|}{q}$ choices for $\mathbf{c} + \mathbf{c}'$ and thus for $\mathbf{c}$. Therefore, $|\mathcal{F}_0| \leq \frac{|H|}{q}$.

We conclude that

$$|\mathcal{F}| = \sum_{t=0}^{k-1} |\mathcal{F}_t| \leq \frac{k|H|}{q}.$$

Moreover, this bound is sharp since it is attained by the coclique $\bigcup_{t=0}^{k-1} H_{(1,0)}\psi^t$. Hence, we have

$$\rho(\mathcal{F}) \leq \frac{\frac{k|H|}{q}}{\frac{|M|}{pq}} = 1.$$

Finally, assume that $\mathcal{F}$ is contained in H. Then, it is clear that $|\mathcal{F}| \leq |H|$ and so

$$\rho(\mathcal{F}) \leq \frac{|H|}{\frac{|M|}{pq}} = \frac{|H|pq}{|H|pk} = \frac{q}{k}.$$

The latter is clearly attained by H. Consequently, we have $\rho(M) = \max(1, \frac{q}{k})$. Moreover, a maximum coclique of Γ_M is either a coset of H or is of the form

$$\bigcup_{t=0}^{k-1} H_{(0,0)} \beta_{\mathbf{c}}^{l_t} \alpha^{s_t} \psi^t,$$

for the sequences $(l_t)_{t=0,1,\ldots,k-1} \subset \{0, 1, \ldots, q-1\}$ and $(s_t)_{t=0,1,\ldots,k-1} \subset \{0, 1, \ldots, p-1\}$.

This completes the proof of Theorem 5.1.

5.3. Proof of Theorem 1.7

The group $M(C)$ acts imprimitively on $\Omega_{p,q}$ with block system $\mathcal{B} = \{\mathbb{Z}_q \times \{j\} \mid j \in \{0, 1, \ldots, p-1\}\}$. By Theorem 5.1, $\rho(M(C)) = \max(1, \frac{q}{k})$. In particular, if $p = \frac{q^k - 1}{q - 1}$ such that $k < q$, then $\rho(M(C)) = \frac{q}{k}$ is a rational number.

6. Future work

In this paper, we studied the intersection density of imprimitive groups of degree a product of two odd primes $p > q$. For transitive groups of degree pq admitting a unique block system with blocks of size q, as well as non-trivial normal subgroups, we proved Theorem 1.4 and Theorem 1.7. In addition, we proved that if $G \leq \mathrm{Sym}(\Omega)$ is imprimitive and quasiprimitive of degree pq, then G is an almost simple group containing $\mathrm{Alt}(5)$ or a projective special linear group. The former has intersection density 1 and we conjectured in Conjecture 1.3 that the latter also has intersection density 1. If Conjecture 1.3 is true, then we will obtain that $\mathcal{I}_{pq} = \{1\}$ if and only if there exists no $[p, k]_q$ cyclic code C such that $Z(\mathbf{c}) > 0$, for any $\mathbf{c} \in C$. It is likely that Conjecture 1.3 is too hard for the proof techniques that are available in the literature.

Combining [29, Conjecture 9.1], Conjecture 1.6, and Conjecture 1.3, we make the following conjecture.

Conjecture 6.1. *For any two odd primes $p > q$, we have*

(i) $\mathcal{I}_{pq} = \{1\}$ *if and only if there exists no $[p, k]_q$ cyclic codes C such that $Z(\mathbf{c}) > 0$, for any $\mathbf{c} \in C$.*

(ii) If C is a $[p, k]_q$ cyclic code such that $Z(\mathbf{c}) > 0$, for $\mathbf{c} \in C$, and $\sigma \in \mathrm{PAut}(C)$ is the cyclic shift automorphism, then

$$\mathcal{I}_{pq} = \left\{ \tfrac{q}{k} \mid \mathrm{N}_{\mathrm{PAut}(C)}(\langle \sigma \rangle) \text{ admits an element of order } k < q \right\} \cup \{1\}.$$

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgment

References

[1] A. Behajaina, R. Maleki, A.T. Rasoamanana, A.S. Razafimahatratra, 3-setwise intersecting families of the symmetric group, Discrete Math. 344 (8) (2021) 112467.
[2] S. Bereg, P.J. Dukes, A lower bound on permutation codes of distance $n - 1$, Des. Codes Cryptogr. 88 (1) (2020) 63–72.
[3] P.J. Cameron, Permutation codes, Eur. J. Comb. 31 (2) (2010) 482–490.
[4] P.J. Cameron, C.Y. Ku, Intersecting families of permutations, Eur. J. Comb. 24 (7) (2003) 881–890.
[5] M. Deza, P. Frankl, On the maximum number of permutations with given maximal or minimal distance, J. Comb., Ser. A 22 (3) (1977) 352–360.
[6] J.D. Dixon, B. Mortimer, Permutation Groups, vol. 163, Springer Science & Business Media, 1996.
[7] P. Dukes, N. Sawchuck, Bounds on permutation codes of distance four, J. Algebraic Comb. 31 (2010) 143–158.
[8] C. Godsil, K. Meagher, Erdős-Ko-Rado Theorems: Algebraic Approaches, Cambridge University Press, 2016.
[9] F. Harary, Graph Theory, Addison-Wesley, 1969.
[10] M.D. Hestenes, Singer groups, Can. J. Math. 22 (3) (1970) 492–513.
[11] H.D. Hollmann, Nonstandard linear recurring sequence subgroups in finite fields and automorphisms of cyclic codes, arXiv preprint, arXiv:0807.0595, 2008.
[12] A. Hujdurović, K. Kutnar, B. Kuzma, D. Marušič, Š. Miklavič, M. Orel, On intersection density of transitive groups of degree a product of two odd primes, Finite Fields Appl. 78 (2022) 101975.
[13] A. Hujdurović, K. Kutnar, D. Marušič, Š. Miklavič, On maximum intersecting sets in direct and wreath product of groups, Eur. J. Comb. 103 (2022) 103523.
[14] A. Hujdurović, K. Kutnar, D. Marušič, Š. Miklavič, Intersection density of transitive groups of certain degrees, Algebraic Combin. 5 (2) (2022) 289–297.
[15] C. Jordan, Recherches sur les substitutions, J. Math. Pures Appl. 17 (1872) 351–367.
[16] B. Larose, C. Malvenuto, Stable sets of maximal size in Kneser-type graphs, Eur. J. Comb. 25 (5) (2004) 657–673.

[17] C.H. Li, S.J. Song, V. Pantangi, Erdős-Ko-Rado problems for permutation groups, arXiv preprint, arXiv:2006.10339, 2020.

[18] A. Lucchini, On imprimitive groups with small degree, Rend. Semin. Mat. Univ. Padova 86 (1991) 131–142.

[19] D. Marušič, On vertex symmetric digraphs, Discrete Math. 36 (1) (1981) 69–81.

[20] D. Marušič, R. Scapellato, Characterizing vertex-transitive pq-graphs with an imprimitive automorphism subgroup, J. Graph Theory 16 (4) (1992) 375–387.

[21] D. Marušič, R. Scapellato, Classifying vertex-transitive graphs whose order is a product of two primes, Combinatorica 14 (2) (1994) 187–201.

[22] K. Meagher, An Erdős-Ko-Rado theorem for the group $PSU(3, q)$, Des. Codes Cryptogr. 87 (4) (2019) 717–744.

[23] K. Meagher, A.S. Razafimahatratra, The Erdős-Ko-Rado theorem for 2-pointwise and 2-setwise intersecting permutations, Electron. J. Comb. 28 (4) (2021) 4–10.

[24] K. Meagher, A.S. Razafimahatratra, Some Erdős-Ko-Rado results for linear and affine groups of degree two, Art Discrete Appl. Math. (2022).

[25] K. Meagher, A.S. Razafimahatratra, P. Spiga, On triangles in derangement graphs, J. Comb., Ser. A 180 (2021) 105390.

[26] K. Meagher, P. Spiga, P.H. Tiep, An Erdős–Ko–Rado theorem for finite 2-transitive groups, Eur. J. Comb. 55 (2016) 100–118.

[27] H. Niederreiter, Weights of cyclic codes, Inf. Control 34 (2) (1977) 130–140.

[28] A.S. Razafimahatratra, On complete multipartite derangement graphs, Ars Math. Contemp. 21 (1) (2021) 1–07.

[29] A.S. Razafimahatratra, On the intersection density of primitive groups of degree a product of two odd primes, J. Comb., Ser. A 194 (2023) 105707.

[30] P. Spiga, The Erdős-Ko-Rado theorem for the derangement graph of the projective general linear group acting on the projective space, J. Comb., Ser. A 166 (2019) 59–90.

[31] The Sage Developers, SageMath, the sage mathematics software system (version 10.2), https://www.sagemath.org, 2023.

[32] A.A. Zykov, On some properties of linear complexes, Mat. Sb. 66 (2) (1949) 163–188.