Vertex transitive graphs G with $\chi_D(G) > \chi(G)$ and small automorphism group

Niranjan Balachandran[*], Sajith Padinhatteeri[†], and Pablo Spiga[‡]

Abstract

For a graph G and a positive integer k, a vertex labelling $f : V(G) \to \{1, 2 \ldots, k\}$ is said to be k-distinguishing if no non-trivial automorphism of G preserves the sets $f^{-1}(i)$ for each $i \in \{1, \ldots, k\}$. The distinguishing chromatic number of a graph G, denoted $\chi_D(G)$, is defined as the minimum k such that there is a k-distinguishing labelling of $V(G)$ which is also a proper coloring of the vertices of G. In this paper, we prove the following theorem: Given $k \in \mathbb{N}$, there exists an infinite sequence of vertex-transitive graphs $G_i = (V_i, E_i)$ such that

1. $\chi_D(G_i) > \chi(G_i) > k$,
2. $|\mathrm{Aut}(G_i)| = O_k(|V_i|)$, where $\mathrm{Aut}(G_i)$ denotes the full automorphism group of G_i.

In particular, this answers a problem raised in [1].

Keywords: Distinguishing Chromatic Number, Vertex transitive graphs, Cayley Graphs.

2010 AMS Classification Code: 05C15, 05D40, 20B25, 05E18.

1 Introduction

Let G be a graph. An automorphism of G is a permutation φ of the vertex set $V(G)$ of G such that, for any $x, y \in V(G)$, $\varphi(x), \varphi(y)$ are adjacent if and only x, y are adjacent. The automorphism group of a graph G, denoted by $\mathrm{Aut}(G)$, is the group of all automorphisms of G. A graph G is said to be vertex transitive if, for any $u, v \in V(G)$, there exists $\varphi \in \mathrm{Aut}(G)$ such that $\varphi(u) = v$.

Given a positive integer r, an r-coloring of G is a map $f : V(G) \to \{1, 2, \ldots, r\}$ and the sets $f^{-1}(i)$, for $i \in \{1, 2 \ldots, r\}$, are the color classes of f. An automorphism $\varphi \in \mathrm{Aut}(G)$ is said to fix

*Department of Mathematics, Indian Institute of Technology Bombay, Mumbai, India. email: niranj@math.iitb.ac.in

†Department of Mathematics, Indian Institute of Technology Bombay, Mumbai, India. email: sajith@math.iitb.ac.in

‡Dipartimento Di Matematica E Applicazioni, University of Milano-Bicocca, Milano Italy, Email: pablo.spiga@unimib.it

a color class C of f if $\varphi(C) = C$, where $\varphi(C) = \{\varphi(v) : v \in C\}$. A coloring of G, with the property that no non-trivial automorphism of G fixes every color class, is called a distinguishing coloring of G.

Collins and Trenk in [5] introduced the notion of the distinguishing chromatic number of a graph G, which is defined as the minimum number of colors needed to color the vertices of G so that the coloring is both proper and distinguishing. Thus, the distinguishing chromatic number of G is the least integer r such that the vertex set can be partitioned into sets $V_1, V_2, \ldots, V_r$ such that each V_i is independent in G, and for every non-trivial $\varphi \in \mathrm{Aut}(G)$ there exists some color class V_i with $\varphi(V_i) \neq V_i$. The distinguishing chromatic number of a graph G, denoted by $\chi_D(G)$, has been the topic of considerable interest recently (see for instance, [1, 2, 3, 4]).

One of the many questions of interest regarding the distinguishing chromatic number concerns the contrast between $\chi_D(G)$ and the cardinality of $\mathrm{Aut}(G)$. For instance, the Kneser graphs $K(n,r)$ have very large automorphism groups and yet, $\chi_D(K(n,r)) = \chi(K(n,r))$ for $n \geq 2r+1$, and $r \geq 3$ (see [2]). The converse question is compelling: Are there infinitely many graphs G_n with 'small' automorphism groups and satisfying $\chi_D(G_n) > \chi(G_n)$?

The question as posed above is not actually interesting for two reasons. First, for all even n, $\chi_D(C_n) > \chi(C_n) = 2$ and $|\mathrm{Aut}(C_n)| = 2n$, where C_n is the cycle of length n. Second, if one stipulates that G also has arbitrarily large chromatic number, then here is a construction for such a graph. Start with a rigid graph G with a leaf vertex x and having large chromatic number (one can obtain this by minor modifications to a random graph, for instance); then, blow up the leaf vertex x to a new disjoint set X whose neighbor in the new graph $\widetilde{G}$ is the same as the neighbor of x in G. In fact one can arrange for $\chi_D(\widetilde{G}) - \chi(\widetilde{G})$ to be as large as one desires. Furthermore, since $|\mathrm{Aut}(\widetilde{G})| = |X|!$, this provides examples of graphs for which the automorphism groups are relatively 'small' in terms of the order of the graph.

In the example above, the fact that $\chi_D(G)$ is larger than $\chi(G)$ is accounted for by a 'local' reason, and that is what makes the problem stated above not very interesting. However, if one further stipulates that the graph is vertex-transitive, then the same question is highly non-trivial. In [1], the first and second authors constructed families of vertex-transitive graphs with $\chi_D(G) > \chi(G) > k$ and $\mathrm{Aut}(G)| = O(|V(G)|^{3/2})$, for any given k. In this paper, we improve upon that result:

Theorem 1. *Given $k \in \mathbb{N}$, there exists an infinite family of graphs $G_n = (V_n, E_n)$ satisfying:*

1. $\chi_D(G_n) > \chi(G_n) > k$,
2. *G_n is vertex transitive and $|\mathrm{Aut}(G_n)| < 2k|V_n|$.*

Our family of graphs consists of Cayley graphs. To recall the definition, let A be a group and let S be an inverse-closed subset of A, i.e., $S = S^{-1}$, where $S^{-1} := \{s^{-1} : s \in S\}$. The Cayley graph $\mathrm{Cay}(A,S)$ is the graph with vertex set A and the vertices u and v are adjacent in $\mathrm{Cay}(A,S)$ if and only if $uv^{-1} \in S$.

We start with a brief description of the graphs of our construction. For q, an odd prime, let $\mathbb{F}_q^n$ denote the n-dimensional vector space over $\mathbb{F}_q$. Our graphs shall be Cayley graphs $\mathrm{Cay}(\mathbb{F}_q^n, S)$ for some suitable inverse-closed set $S \subset \mathbb{F}_q^n$ which is obtained by taking a union of a certain collection of lines in $\mathbb{F}_q^n$ and then deleting the zero element of $\mathbb{F}_q^n$. More precisely, let $\mathcal{H}_0 := \{(x_1, x_2, \ldots, x_{n-1}, 0) : x_i \in \mathbb{F}_q, 1 \leq i \leq n-1\}$ and let $\mathbf{0}$ denote the element $(0, \ldots, 0) \in \mathbb{F}_q^n$. For each line (1-dimensional subspace of $\mathbb{F}_q^n$) $\ell \subset \mathbb{F}_q^n$ satisfying $\ell \cap \mathcal{H}_0 = \{\mathbf{0}\}$, pick ℓ independently with probability 1/2 to form the random set $\widetilde{S}$. Our connection set S for the Cayley graph $\mathrm{Cay}(\mathbb{F}_q^n, S)$ is defined by $S := \{v \in \mathbb{F}_q^n : v \in \ell \text{ for some } \ell \in \widetilde{S}\} \setminus \{\mathbf{0}\}$. Our main theorem states that with high probability, $G_{n,S} := \mathrm{Cay}(\mathbb{F}_q^n, S)$ satisfies the conditions of Theorem 1.

To show that these graphs have 'small' automorphism groups, we prove a stronger version of Theorem 4.3 of [6] in this particular context, which is also a result of independent interest.

Theorem 2. *Let q be a prime power, let n be a positive integer with $n \geq 2$ and let G be the additive group of the n-dimensional vector space $\mathbb{F}_q^n$ over the finite field $\mathbb{F}_q$ of cardinality q, and let $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$ be the multiplicative group of the field $\mathbb{F}_q$ with its natural group action on G by scalar multiplication, and write $K := \mathbb{F}_q^n \rtimes \mathbb{F}_q^*$. If S is a subset of G with $K \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$, then either*

(i) $\mathrm{Aut}(\mathrm{Cay}(G, S)) = K$, *or*

(ii) *there exists $\varphi \in \mathrm{Aut}(\mathrm{Cay}(G, S)) \setminus K$ with φ normalizing G.*

The rest of the paper is organized as follows. We start with some preliminaries in Section 2 and then include the proofs of Theorems 1 and 2 in the next section. We conclude with some remarks and some open questions.

2 Preliminaries

We begin with a few definitions from finite geometry. For more details, one may see [13, 14]. By $PG(n, q)$ we mean the Desarguesian projective space obtained from the affine space $AG(n+1, q)$.

Definition 3. A cone with vertex $A \subset PG(k, q)$ and base $B \subset PG(n-k-1, q)$, where $PG(k, q) \cap PG(n-k-1, q) = \emptyset$, is the set of points lying on the lines connecting points of A and B.

Definition 4. Let V be an $(n+1)$-dimensional vector space over a finite field $\mathbb{F}$. A subset S of $PG(V)$ is called an $\mathbb{F}_q$-linear set if there exists a subset U of V that forms an $\mathbb{F}_q$-vector space, for some $\mathbb{F}_q \subset \mathbb{F}$, such that $S = \mathcal{B}(U)$, where

$$\mathcal{B}(U) := \{\langle u \rangle_{\mathbb{F}} : u \in U \setminus \{\mathbf{0}\}\}$$

and where $\langle u \rangle_{\mathbb{F}}$ denotes the projective point of $PG(V)$, corresponding to the vector u of $U \subset V$.

Further details about $\mathbb{F}_q$-linear sets can be found in [14], for instance.

The projective space $PG(n, q)$ can be partitioned into an affine space $AG(n, q)$ and a hyperplane at infinity, denoted by H_∞.

Definition 5. Following [13], we say that a set of points $U \subset AG(n,q)$ determines the direction $d \in H_\infty$, if there is an affine line through d meeting U in at least two points.

We now state the main theorem of [13] which will be relevant in our setting.

Theorem 6. *Let $U \subset AG(n, \mathbb{F}_q), n \geq 3, |U| = q^k$. Suppose that U determines at most $\frac{q+3}{2}q^{k-1} + q^{k-2} + \cdots + q^2 + q$ directions and suppose that U is an $\mathbb{F}_p$-linear set of points, where $q = p^h$, $p > 3$ prime. If $n-1 \geq (n-k)h$, then U is a cone with an $(n-1-h(n-k))$-dimensional vertex at H_∞ and with base a $\mathbb{F}_q$-linear point set $U_{(n-k)h}$ of size $q^{(n-k)(h-1)}$, contained in some affine $(n-k)h$-dimensional subspace of $AG(n,q)$.*

We end this section by recalling another result that appears in [6] as Theorem 4.2.

Theorem 7. *Let G be a permutation group on Ω with a proper self-normalizing abelian regular subgroup. Then $|\Omega|$ is not a prime power.*

3 Proofs of the Theorems

In this section we prove Theorems 1 and 2 starting with the proof of Theorem 2. We believe that this result is only the tip of an iceberg: its current statement has been tailored to the context of our setting, and uses some ideas that appear in [6, Section 3] and [9].

Proof of Theorem 2. We suppose that (**i**) does not hold, that is, K is a proper subgroup of $\mathrm{Aut}(\mathrm{Cay}(G,S))$; we show that (**ii**) holds. Write $\Gamma := \mathrm{Cay}(G,S)$.

Let B be a subgroup of $\mathrm{Aut}(\Gamma)$ with $K < B$ and with K maximal in B. Suppose that $K \lhd B$. As G is characteristic in K, we get $G \lhd B$. In particular, every element φ in $B \setminus K$ satisfies (**ii**).

Suppose then that K is not normal in B. Since K is maximal in B and $G \lhd K$, we have $\mathbf{N}_B(G) = K$. Suppose that there exists $b \in B \setminus K$ such that $L := \langle G, G^b \rangle$ (the smallest subgroup of B containing G and G^b) satisfies $L \cap K = G$. We claim that we are now in the position to apply [6, Theorem 4.2] (and implicitly some ideas from [9]). Indeed, as $\mathbf{N}_L(G) = \mathbf{N}_B(G) \cap L = K \cap L = G$, L is a transitive permutation group on the vertices of Γ with a proper regular self-normalizing abelian subgroup G. (Observe that G is a proper subgroup of L because $b \notin \mathbf{N}_B(G) = K$.) From [6, Theorem 4.2], $|G|$ is not a prime power, which is a contradiction because $|G| = q^n$, see also Theorem 7. This proves that, for every $b \in B \setminus K$, we have $\langle G, G^b \rangle \cap K > G$.

Fix $b \in B \setminus K$. Now, G and G^b are abelian and hence $G \cap G^b$ is centralized by $\langle G, G^b \rangle$. From the preceding paragraph, there exists $k \in \langle G, G^b \rangle \cap K$ with $k \notin G$. Observe now that $K = \mathbb{F}_q^n \rtimes \mathbb{F}_q^*$ is a Frobenius group with kernel $G = \mathbb{F}_q^n$ and complement $\mathbb{F}_q^*$. Therefore, k acts by conjugation fixed-point-freely on $G \setminus \{\mathbf{0}\}$. As k centralizes $G \cap G^b$, we deduce $|G \cap G^b| = 1$.

Let $C := \bigcap_{x \in B} K^x$ be the core of K in B. As $G \cap G^b = 1$, $K \cap K^b$ has no non-identity q-elements. Therefore $C \cap G = 1$. As $C \lhd B$ and $C \leq K$, C is a normal subgroup of the Frobenius group K intersecting its kernel on the identity. This yields $C = 1$.

Let Ω be the set of right cosets of K in B. From the paragraph above, B acts faithfully on Ω. Moreover, as K is maximal in B, the action of B on Ω is primitive. Therefore B is a finite primitive group with a solvable point stabilizer K. In [11], Li and Zhang have explicitly determined such primitive groups: these are classified in [11, Theorem 1.1] and [11, Tables I–VII]. Now, using the terminology in [11], a careful (but not very difficult) case-by-case analysis on the tables in [11] shows that B is a primitive group of affine type, that is, B contains an elementary abelian normal r-subgroup V, for some prime r. For this analysis it is important to keep in mind that the stabilizer K is a Frobenius group with kernel the elementary abelian group $G \cong \mathbb{F}_q^n$ and $n > 1$.

Let $|V| = r^t$. Now, the action of B on Ω is permutation equivalent to the natural action of $B = V \rtimes K$ on V, with V acting via its regular representation and with K acting by conjugation. Observe that $q \neq r$, because K acts faithfully and irreducibly as a linear group on V and hence K contains no non-identity normal r-subgroups. Observe further that $|B| = |V||K| = r^t \cdot q^n \cdot (q-1)$.

We are finally ready to reach a contradiction and to do so, we go back studying the action of B on the vertices of Γ. Observe that B is solvable because V is solvable and so is $B/V \cong K$. We write $B_{\mathbf{0}}$ for the stabilizer in B of the vertex $\mathbf{0}$ of Γ. As G acts regularly on the vertices of Γ, we obtain $B = B_{\mathbf{0}}G$ and $B_{\mathbf{0}} \cap G = 1$. In particular, $|B_{\mathbf{0}}| = r^t \cdot (q-1)$. Observe that $B_{\mathbf{0}}$ is a Hall Π-subgroup of the solvable group B, where Π is the set of all the prime divisors of $q-1$ together with the prime r. As V is a Π-subgroup, from the theory of Hall subgroups (see for instance [7], Theorem 3.3), V has a conjugate contained in $B_{\mathbf{0}}$. Since $V \lhd B$, we have $V \leq B_{\mathbf{0}}$. This is clearly a contradiction because V is normal in B, but $B_{\mathbf{0}}$ is core-free in B being the stabilizer of a point in a transitive permutation group. $\square$

For the next lemma, recall that $\mathcal{H}_0 := \{(x_1, \ldots, x_{n-1}, 0) : x_i \in \mathbb{F}_q \text{ for each } i \in \{1, \ldots, n-1\}\}$. In what follows, $G_{n,S}$ will denote the Cayley graph $\mathrm{Cay}(\mathbb{F}_q^n, S)$ and $S = \widetilde{S} \setminus \{\mathbf{0}\}$ for some set $\widetilde{S} = \bigcup_{\ell \in \mathcal{L}} \ell$, where $\mathcal{L}$ is a collection of lines in $\mathbb{F}_q^n$ with each $\ell \in \mathcal{L}$ satisfying $\ell \cap \mathcal{H}_0 = \{\mathbf{0}\}$.

Lemma 8. *$\chi(G_{n,S}) = q$.*

Proof. Observe that each line that belongs to the set S gives rise to a clique of size q in the graph $G_{n,S}$. Therefore $\chi(G_{n,S}) \geq q$. On the other hand, for a fixed $v \in S$, the partition $(C_\lambda)_{\lambda \in \mathbb{F}_q}$, where $C_\lambda := \{w + \lambda v : w \in \mathcal{H}_0\}$, of the vertex set $\mathbb{F}_q^n$ is a proper coloring of the graph $G_{n,S}$. Indeed, for any $u, v \in C_\lambda$, we have $u - v = w \notin S$, so the sets C_λ are independent in $G_{n,S}$ for each $\lambda \in \mathbb{F}_q$. $\square$

Lemma 9. *Assume that q is prime. Let $\widetilde{S}$ be the random set corresponding to a union of lines ℓ in $\mathbb{F}_q^n$ with $\ell \cap \mathcal{H}_0 = \{\mathbf{0}\}$ and where each $\ell \in \mathbb{F}_q^n$ is chosen independently with probability $\frac{1}{2}$; and let $S = \widetilde{S} \setminus \{\mathbf{0}\}$. Then*

$$\mathbb{P}\left(\chi_D(G_{n,S}) > q\right) \geq 1 - \exp\left(-\frac{q^{n-3}}{4}\right).$$

Proof. First, note that $\mathbb{E}(|S|) = \frac{q^{n-1}}{2}$, so taking $\delta = \frac{1}{q}$ and $\mu = \mathbb{E}(|S|)$ in the Chernoff bound (see (2.6) on page 26 of [10]) we obtain

$$\mathbb{P}\left(|S| < \frac{q^{n-1} - q^{n-2}}{2}\right) \leq \exp\left(-\frac{q^{n-3}}{4}\right).$$

In particular, with probability at least $1 - \exp(-q^{n-3}/4)$, we have $|S| > \frac{q^{n-1}-q^{n-2}}{2}$. We may thus assume $|S| > \frac{q^{n-1}-q^{n-2}}{2}$ in what follows.

We claim that every color class in a proper q-coloring of $G_{n,S}$ is an affine hyperplane of $\mathbb{F}_q^n$. To see why, let $C_1, \ldots, C_q$ be independent sets in $G_{n,S}$ witnessing a proper q-coloring of $G_{n,S}$. Fix $v \in S$ and consider the line $\ell_v := \{\lambda v : \lambda \in \mathbb{F}_q\}$ along with its translates $\ell_v + w := \{\lambda v + w : \lambda \in \mathbb{F}_q\}$, for $w \in \mathcal{H}_0$. Each set $\ell_v + w$ is a clique of size q in $G_{n,S}$, and these cliques partition the vertex set of $G_{n,S}$, so in particular each C_i contains at most one vertex from each of these translates $\ell_v + w$. Consequently, $|C_i| \le q^{n-1}$ for all $i \in \{1, \ldots, q\}$. By size considerations, it follows that $|C_i| = q^{n-1}$ for each $i \in \{1, \ldots, q\}$.

Consider a color class C. Suppose C determines at least $\frac{q+3}{2}q^{n-2} + q^{n-3} + \cdots + q^2 + q + 1$ directions. Then if $\langle C \rangle$ denotes the set of all affine lines intersecting at least two points in C, we have $|\langle C \rangle| + |S| > 1 + q + \cdots + q^{n-1}$, so $\langle C \rangle \cap S \neq \emptyset$. However, this contradicts the assumption that C is an independent set in $G_{n,S}$. Therefore C determines at most $\frac{q+3}{2}q^{n-2} + q^{n-3} + \cdots + q^2 + q$ directions. Since q is prime, by Corollary 10 in [13], it follows that C is an $\mathbb{F}_q$-linear set. Hence, by Theorem 6, the color class C is a cone with an $n-2$ (projective) dimensional vertex $\mathcal{V}$ at H_∞ and an affine point u_1 as base. In particular, the affine plane corresponding to the $\mathbb{F}_q$-subspace spanned by $\mathcal{V}$ passing through the affine point u_1 is contained in C. Since $|C| = q^{n-1}$, it follows that C is this affine hyperplane, and this proves the claim.

To complete the proof, observe that for each $\lambda \in \mathbb{F}_q^* \setminus \{1\}$, the map $\varphi_\lambda(x) = \lambda x$, $x \in \mathbb{F}_q^n$ fixes each color class. Moreover, φ_λ fixes the set S and $\varphi_\lambda(u) - \varphi_\lambda(v) = \varphi_\lambda(u - v)$, so φ_λ is a non-trivial automorphism which fixes each color class. Therefore $\chi_D(G_{n,S}) > q$. $\square$

Lemma 10. *If $n \ge 5$ and $q \ge 5$ is prime, then $\mathrm{Aut}(G_{n,S}) \cong \mathbb{F}_q^n \rtimes \mathbb{F}_q^*$ with probability at least $1 - 2^{(-\frac{q^{n-1}}{3})}$.*

Proof. Since $G_{n,S}$ is a Cayley graph on the additive group $G = \mathbb{F}_q^n$, by Theorem 2, either $\mathrm{Aut}(G_{n,S}) = K \cong \mathbb{F}_q^n \rtimes \mathbb{F}_q^*$ or there exists $\varphi \in \mathrm{Aut}(G_{n,S}) \setminus K$ with φ normalizing $G = \mathbb{F}_q^n$. We show that with probability at least $1 - 2^{(-\frac{q^{n-1}}{3})}$, there is no φ satisfying the latter condition.

Suppose $\varphi \in \mathrm{Aut}(G_{n,S})$ normalizes $\mathbb{F}_q^n$. If $a = \varphi(\mathbf{0})$ and $\lambda_a : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is the right translation via a, then $\lambda_a^{-1}\varphi$ is an automorphism of $G_{n,S}$ normalizing $\mathbb{F}_q^n$ and with $(\lambda_a^{-1}\varphi)(\mathbf{0}) = (\lambda_a^{-1})(\varphi(\mathbf{0})) = (\lambda_a^{-1})(a) = a - a = \mathbf{0}$. Therefore, without loss of generality, we may assume that $\varphi(\mathbf{0}) = \mathbf{0}$. Since S is the neighbourhood of $\mathbf{0}$ in $G_{n,S}$, we get $\varphi(S) = S$. Moreveor, since φ acts as a group automorphism on $\mathbb{F}_q^n$, we have $\varphi \in \mathrm{GL}_n(q)$.

Now, for $\varphi \in \mathrm{GL}_n(q)$, let E_φ denote the event $\varphi(S) = S$. Let $\mathcal{L}$ denote the set of all lines ℓ with $\ell \cap \mathcal{H}_0 = \emptyset$. Also, let $\mathrm{Orb}_\varphi(\ell) = \{\ell, \varphi(\ell), \varphi^2(\ell), \ldots, \varphi^k(\ell)\}$ where $\varphi^{k+1}(\ell) = \ell$. Then

$$\mathbb{P}(E_\varphi) \le \prod_{i=1}^{N_\varphi} 2^{1-|\mathrm{Orb}_\varphi(\ell_i)|} = 2^{N_\varphi - |\mathcal{L}|},$$

where N_φ denotes the number of distinct orbits of φ in $\mathcal{L}$. Setting $\mathcal{G} = GL(n,q) \setminus \{\lambda I : \lambda \in \mathbb{F}_q^*\}$, we have

$$\mathbb{P}\left(\bigcup_{\varphi\in\mathcal{G}} E_\varphi\right) \le \sum_{\varphi\in\mathcal{G}} \mathbb{P}(E_\varphi) \le 2^{-|\mathcal{L}|}\sum_{\varphi\in\mathcal{G}} 2^{N_\varphi}. \tag{1}$$

Let $F_\varphi := |\{\ell \in \mathcal{L} : \varphi(\ell) = \ell\}|$ and $F := \max_{\varphi\in\mathcal{G}} F_\varphi$. Now $N_\varphi \le F + \frac{|\mathcal{L}|-F}{2} = \frac{F+|\mathcal{L}|}{2}$. Thus, it suffices to give a suitable upper bound for F. Towards that end, we note that, if $F_\varphi = F$ for $\varphi \in \mathcal{G}$, then every line ℓ fixed by φ corresponds to an eigenvector of φ. If $\mathcal{E}_1, \mathcal{E}_2 \ldots, \mathcal{E}_k$ denote the eigenspaces of φ for some distinct eigenvalues $\lambda_1, \ldots, \lambda_k$, then

$$F_\varphi \le \sum_{i=1}^{k}\left(\binom{\dim \mathcal{E}_i}{1}_q - \binom{\dim(\mathcal{E}_i \cap \mathcal{H}_0)}{1}_q\right) \le q^{n-2}+1.$$

Similarly, we have $|\mathcal{L}| = \binom{n}{1}_q - \binom{n-1}{1}_q = q^{n-1}$, and so by (1), we have

$$\mathbb{P}\left(\bigcup_{\varphi\in\mathcal{G}} E_\varphi\right) \le |\mathcal{G}|2^{\frac{F-|\mathcal{L}|}{2}} < q^{n^2}2^{-\left(\frac{q^{n-1}-q^{n-2}-1}{2}\right)} < 2^{-\left(\frac{q^{n-1}}{3}\right)},$$

for $q \ge 5$, $n \ge 6$. ◻

Computations and estimates similar to the ones presented in the proof of Lemma 10 have been proved useful in a variety of problems, see for instance [1], [8] and [12, Section 6.4].

Proof of Theorem 1. Given $k \in \mathbb{N}$ with $k \ge 4$, pick a prime number q with $k < q < 2k$. Consider the random graph $G_{n,S}$ of the group $\mathbb{F}_q^n$ as constructed above. By Lemmas 9 and 10, with positive probability, the graph $G_{n,S}$ satisfies the statements of both lemmas, and hence satisfies the conclusions of Theorem 1. ◻

4 Concluding Remarks

- We observe that, for S chosen randomly as in the proof of our result, the distinguishing chromatic number of $G_{n,S}$ is $q+1$ with high probability. Indeed, consider the q-coloring C described in Lemma 8. Re-color the vertex $\mathbf{0}$ using an additional color. Then the coloring described by the partition $C' = C \cup \{\mathbf{0}\}$ is a proper, distinguishing coloring of $G_{n,S}$ with $q+1$ colors. In fact, C' is clearly proper, and to show that it is distinguishing, consider $\varphi \in \mathrm{Aut}(G_{n,S}) = \mathbb{F}_q^n \rtimes \mathbb{F}_q^*$ (by Lemma 10) that fixes every color class. Write $\varphi(x) = \lambda x + b$ with $\lambda \in \mathbb{F}_q^*, b \in \mathbb{F}_q^n$. Since φ fixes the color class containing $\mathbf{0}$, we have $b = \mathbf{0}$. Also, x and λx cannot be in same color class unless $\lambda = 1$. Therefore φ is the identity automorphism.
  It is interesting to determine if one can obtain families of vertex-transitive graphs with $\chi_D(G) > \chi(G)+1$, with 'small' automorphism groups and with $\chi(G)$ being arbitrarily large. In fact, for $k \in \mathbb{N}$, there is no known family of vertex-transitive graphs for which $\chi_D(G) > \chi(G)+1 > k$ and $|\mathrm{Aut}(G)| = O(|V(G)|^{O(1)})$. It is plausible that Cayley graphs over certain groups may provide the correct constructions.

- Theorem 1 establishes, for any fixed k, the existence of vertex-transitive graphs $G_n = (V_n, E_n)$ with $\chi_D(G_n) > \chi(G_n) > k$ and with $|\mathrm{Aut}(G_n)| < 2k|V_n|$. It would be interesting to obtain a similar family of graphs that satisfy with $\chi_D(G_n) > \chi(G_n) > k$ and with $|\mathrm{Aut}(G_n)| \leq C|V_n|$, for some absolute constant C.

Acknowledgments

The first and second authors would like to thank Ted Dobson for useful discussions.

References

[1] N. Balachandran and S. Padinhatteeri. $\chi_D(G)$, $|Aut(G)|$ and a variant of the motion lemma. *Ars Math. Contemp.*, 12(1), 2016.

[2] Z. Che and K. L. Collins. The Distinguishing Chromatic Number of Kneser Graphs. *Electron. J. Combin.*, 20(1), 2013.

[3] J. Choi, S. G. Hartke, and H. Kaul. Distinguishing chromatic number of cartesian products of graphs. *SIAM J. Discrete Math.*, 24(1):82–100, 2010.

[4] K. L. Collins, M. Hovey, and A. N. Trenk. Bounds on the distinguishing chromatic number. *Electron. J. Combin*, 16, 2009.

[5] K. L. Collins and A. N. Trenk. The distinguishing chromatic number. *Electron. J. Combin*, 13, 2006.

[6] E. Dobson, P. Spiga, and G. Verret. Cayley graphs on abelian groups. *Combinatorica*, 4:1–23, 2015.

[7] K. Doerk and T. O. Hawkes. *Finite Soluble Groups.* De Gruyter Expositions in Mathematics 4, 1992.

[8] S. Guest and P. Spiga. Finite primitive groups and regular orbits of group elements. *Trans. Amer. Math. Soc.*, 369(2):997–1024, 2017.

[9] E. Jabara and P. Spiga. Abelian carter subgroups in finite permutation groups. *Arch. Math. (Basel)*, 101:301–307, 2013.

[10] S. Janson, T. Łuczak, and A. Ruciński. *Random Graphs.* John Wiley & Sons, Inc.,New York, 2000.

[11] C. H. Li and H. Zhang. The finite primitive groups with soluble stabilizers, and the edge-primitive s-arc transitive graphs. *Proc. Lond. Math.Soc.*, 103:441–472, 2011.

[12] P. Potočnik, P. Spiga, and G. Verret. Asymptotic enumeration of vertex-transitive graphs of fixed valency. *J. Combin. Theory Ser. B*, 122:221–240, 2017.

[13] L. Strome and P. Sziklai. Linear point sets and Rédei type k-blocking sets $PG(n, q)$. *J. Algebraic Combin.*, 14:221–228, 2001.

[14] G. V. Voorde. *Blocking sets in finite projective spaces and coding theory*. PhD thesis, Ghent University, 2010.