Electronic Journal of Graph Theory and Applications **7** (1) (2019), 31–42

Electronic Journal of Graph Theory and Applications

On the Erdős-Ko-Rado property of finite groups of order a product of three primes

Modjtaba Ghorbani, Mina Rajabi-Parsa

Department of Mathematics, Faculty of Science, Shahid Rajaee Teacher Training University, Tehran, 16785 - 136, I. R. Iran.

mghorbani@sru.ac.ir, mina.rparsa@gmail.com

Abstract

Let G be a subgroup of the symmetric group $\mathbb{S}_n$. Then G has the Erdős-Ko-Rado (EKR) property, if the size of any intersecting subset of G is bounded above by the size of a point stabilizer of G. The aim of this paper is to investigate the EKR and the strict EKR properties of the groups of order pqr, where p, q, r are three prime numbers.

Keywords: Cayley graph, permutation groups, EKR property
Mathematics Subject Classification : 05C35, 05D05
DOI: 10.5614/ejgta.2019.7.1.3

1. Introduction

Let $[n] = \{1, 2, \dots, n\}$, the Erdős-Ko-Rado (EKR) Theorem is based on the largest family of subsets of size r from the set $[n]$ such that the intersection of each pair of subsets is non-empty, see [5]. Let $n \geq 2r$, the size of largest collection is $\binom{n-1}{r-1}$ and in this case, the only collections of this size are the collections of all subsets that contain a fixed element from $[n]$. Suppose $G \leq \mathbb{S}_n$ is a permutation group. A subset S of G is said to be intersecting if for any pair of permutations $\sigma, \tau \in S$ there exists $i \in [n]$ such that $\sigma\tau^{-1}(i) = i$. A group G has the Erdős-Ko-Rado (EKR) property, if for any intersecting subset $S \subseteq G$, $|S|$ is bounded above by the size of the largest point stabilizer in G. The maximal intersecting set is one with maximum size. The group G has the strict EKR property if every maximal intersecting set is the coset of the stabilizer of a point.

Received: 4 September 2017, Revised: 2 September 2018, Accepted: 14 September 2018.

It is clear from the definition that if a group has the strict EKR property then it has the EKR property. A group can have the (strict) EKR property under one action while it fails to have this property under another action. In [3] the author defined a new version of the EKR property. Let the action of G on the set X be transitive. We say this action satisfies the weak EKR property if the cardinality of any intersecting set is bounded above by the cardinality of the stabilizers and G has the weak EKR property, if all transitive actions of G have the weak EKR property.

In 1977 Frankl and Deza [6] proved that $\mathbb{S}_n$ has the EKR property and they conjectured that it has also the strict EKR property, see for more details [4, 9, 12, 20]. In [19] it is shown that $\mathbb{A}_n$ has the strict EKR property and in [20] the EKR property for some Coxeter groups is investigated. Meagher and Spiga [14, 15] stablished that the projective special linear group $PGL_2(q)$ has the strict EKR property, while the projective general linear group $PGL_3(q)$ does not have this property. Ahmadi and Meagher [2] showed the strict EKR property of cyclic, dihedral and Frobenius groups. Recently, they also investigated the EKR property of Mathieu groups and all $2-$transitive groups with degree no more than 20, see [1]. Jalali-Rad and Ashrafi [17] investigated the EKR and the strict EKR properties of the group G, where $G \in \{V_{8n}, U_{6n}, T_{4n}, SD_n\}$. We refer to [5] for background information about the history of this interesting problem. The aim of this paper is to investigate the EKR property of groups of order a product of three primes.

2. Definitions and Preliminaries

Let G be a finite group. A symmetric subset of a group G is a subset $S \subseteq G$, where $e \notin S$ and $S = S^{-1}$. The Cayley graph $\Gamma = \mathrm{Cay(G, S)}$ with respect to S is a graph whose vertex set is $V(\Gamma) = G$ and two vertices $x, y \in V(\Gamma)$ are adjacent if and only if $yx^{-1} \in S$. A symmetric subset by these properties is called a Cayley set or a connection set. It is a well-known fact that a Cayley graph is connected if and only if $G = \langle S \rangle$. Recall that the Cayley graph $\Gamma = \mathrm{Cay(G, S)}$ is normal if S is a symmetric normal subset of G.

A derangement is a permutation with no fixed point. The subset $\mathcal{D}$ of a permutation group is a derangement set if all elements of $\mathcal{D}$ are derangements. Suppose G is a permutation group and $\mathcal{D} \subseteq G$ is a derangement set. The derangement graph $\Gamma_G = \mathrm{Cay}(\mathrm{G}, \mathcal{D})$ has the elements of G as its vertices and two vertices are adjacent if and only if they do not intersect. Since $\mathcal{D}$ is a union of conjugacy classes of G, Γ_G is a normal Cayley graph.

A clique of a graph Γ is a complete subgraph of Γ. A set of vertices of Γ that induces an empty subgraph of Γ is called an independent set. The size of the largest clique and the size of the largest independent set in graph Γ are denoted by $\omega(\Gamma)$ and $\alpha(\Gamma)$, respectively. In particular for any permutation group $G \leq \mathbb{S}_n$, an independent set in Cayley graph Γ is a set of permutations in which every two permutations agree at least on one point.

Let G be a permutation group with derangement graph $\Gamma_G = \mathrm{Cay}(\mathrm{G}, \mathcal{D})$. By these notation, two permutations in G are intersecting if and only if their corresponding vertices are not adjacent in Γ_G. Therefore, the problem of classifying the maximum intersecting subsets of G is equivalent to characterizing the maximum independent sets of vertices in Γ_G.

The group G has the EKR property if and only if

$$\alpha(\Gamma) = \max\{|G_x| \, |x \in G\}. \tag{1}$$

Given a graph Γ, we recall that the independence number of Γ is equal with the clique number of $\bar{\Gamma}$. This means that the Eq.1 can be reformulated as

$$\omega(\bar{\Gamma}) = \max\{|G_x| \mid x \in G\}.$$

For independence and clique numbers of a graph, we have the following result.

Lemma 2.1. *[4] If Γ is a vertex-transitive graph, then $\omega(\Gamma)\alpha(\Gamma) \leq |V(\Gamma)|$. Moreover, equality holds, if every maximum independent set and every maximum clique intersect.*

The group G has the strict EKR property if and only if the cosets of the largest stabilizer of a point in G are the only independent sets of maximum size.

Lemma 2.2. *[2] For any permutation $\sigma \in \mathbb{S}_n$, the cyclic group G generated by σ has the strict EKR property.*

Now, for every $g \in G$, we define a map $\varphi_g : X \longrightarrow X$ by $\varphi_g(x) = xg^{-1}$. Clearly, φ_g is a permutation on X. Moreover, the map $\varphi : G \longrightarrow \mathbb{S}_X$, which is defined by $\varphi(g) = \varphi_g$ for every $g \in G$, is a homomorphism. It is called the permutation presentation of G corresponding to the group action G on X.

Suppose H is a subgroup of G and suppose $X = G/H$ denote to the set of right cosets of H in G. The map $\varphi : G \hookrightarrow S_X$, for every $g \in G$ is the homomorphism $\varphi(g) = \varphi_g$, where for all $a \in G$ we have $\varphi_g(Ha) = Hag^{-1}$. The core of H in G is defined as $\text{cor}_G(H) = \cap_{g\in G} g^{-1}Hg$. We say that H is core-free if $\text{cor}_G(H) = \{e\}$.

For the subgroup $H \leq G$ and $g \in G$, the conjugate of subgroup H in G is denoted by $H^g = g^{-1}Hg$. If $G \leq \text{Sym}(n)$ is a transitive permutation group, then G is called a Frobenius group if it has a non-trivial subgroup H for which $H \cap H^g = \{e\}$, for all $g \in G \setminus H$. The kernel of a Frobenius group G is defined as

$$K = (G \setminus \cup_{g\in G} H^g) \cup \{e\}.$$

It is not difficult to see that the non-identity elements of K are all derangements of G.

Theorem 2.1. *[18] (Frobenius Theorem) Suppose H is a proper non-trivial subgroup of G such that for all $g \in G \setminus H$:*

$$H \cap g^{-1}Hg = \{e\}.$$

Let $K = G \setminus \cup_{g\in G} g^{-1}(H \setminus \{e\})g$, then

$$K \lhd G,\ G = KH \ and \ H \cap K = \{e\}.$$

Proposition 2.1. *[2] Let $G = KH$ be a Frobenius group with kernel K. Then G has the EKR property. Furthermore, G has the strict EKR property if and only if $|H| = 2$.*

Let us to show the direct product of two groups G, H by $G \times H$.

Corollary 2.1. *[2] Suppose $G_1 \leq Sym(n_1), ..., G_k \leq Sym(n_k)$ and $G = G_1 \times \cdots \times G_k$ then G_i $(1 \leq i \leq k)$ has the (strict) EKR property if and only if G has the $(strict)$ EKR property.*

Theorem 2.2. *[3] Let G be a finite group which is either nilpotent or a subgroup of a direct product of groups of squrae-free order. Then G has the weak EKR property.*

3. Main results

In this section, we study the EKR property of groups of order a product of three primes. Let p be a prime number and $p > q$, where $q|p-1$. A non-abelian group of order pq has the following presentation:

$$F_{p,q} = \langle a, b : \ a^p = b^q = e, b^{-1}ab = a^u \rangle,$$

where u is an element of order q in multiplicative group $\mathbb{Z}_p^*$, see [11].

It is not difficult to see that this group is a Frobenius group and hence by Proposition 2.1, it has the EKR property.

3.1. Groups of order pqr

Let $p > q > r$ be three prime numbers, in [7] the structures of all groups of order pqr are verified as follows:

- $G_1 = \mathbb{Z}_{pqr}$,
- $G_2 = F_{p,qr}(qr|p-1)$,
- $G_3 = \mathbb{Z}_r \times F_{p,q}(q|p-1)$,
- $G_4 = \mathbb{Z}_p \times F_{q,r}(r|q-1)$,
- $G_5 = \mathbb{Z}_q \times F_{p,r}(r|p-1)$,
- $G_{5+d} = \langle a, b, c : a^p = b^q = c^r = e, ab = ba, c^{-1}bc = b^u, c^{-1}ac = a^{v^d} \rangle$, where $r|p-1, q-1, q|p-1, o(u) = r$ in $\mathbb{Z}_q^*$ and $o(v) = r$ in $\mathbb{Z}_p^*$ $(1 \leq d \leq r-1)$.

By Theorem 2.2, every group of order pqr (similarly every group of order p^3) has the weak EKR property and thus it has the EKR property. So we investigate the strict EKR property of them.

Theorem 3.1. *Group $G = G_{5+d}$ $(1 \leq d \leq r-1)$ is a Frobenius group.*

Proof. Let $H = \langle c \rangle$ and $K = \langle a, b \rangle$. Let $g = a^i b^j c^k \in G \setminus H$ and suppose that $H \cap g^{-1}Hg \neq \{e\}$. So there exist $1 \leq l, t \leq r-1$ such that $c^{-k}b^{-j}a^{-i}c^t a^i b^j c^k = c^l$. Hence $c^{-k+t}a^{-v^t i+i}b^{j-u^t j}c^k = c^l$ and so $c^t a^{v^k(i-v^t i)}b^{u^k(j-u^t j)} = c^l$. This yields that

$$\begin{cases} i - v^t i \equiv 0 \ (mod\ p) \\ j - u^t j \equiv 0 \ (mod\ q) \\ t = l \end{cases}$$

and so $i = j = 0$, which means that $g \in H$, a contradiction. Hence, $H \cap H^g = \{e\}$ and Theorem 2.1 implies that G is a Frobenius group. $\square$

Let $p, q \neq 2$, by Lemma 2.2, Proposition 2.1, Corollary 2.1 and Theorem 3.1 we conclude the following theorem.

Theorem 3.2. *Among all groups of order pqr only the group G_1 has the strict EKR property.*

3.2. Groups of order p^2q

According to [16] the structures of groups of order p^2q, where $p < q$ are as follows:

- $L_1 = \mathbb{Z}_{p^2q}$,
- $L_2 = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$,
- $L_3 = \mathbb{Z}_p \times F_{q,p}$ $(p|q-1)$,
- $L_4 = F_{q,p^2}$ $(p^2|q-1)$,
- $L_5 = \langle a, b : a^{p^2} = b^q = e, a^{-1}ba = b^u,\ u^p \equiv 1\ (mod\ q)\rangle$ $(p^2|q-1)$

and the structures of groups of order p^2q where, $p > q$ are as follows:

- $Q_1 = \mathbb{Z}_{p^2q}$,
- $Q_2 = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$,
- $Q_3 = \mathbb{Z}_p \times F_{p,q}$ $(q|p-1)$,
- $Q_4 = \langle a, b : a^q = b^{p^2} = 1, a^{-1}ba = b^{\alpha},\ \alpha^q \equiv 1\ (mod\ p^2)\rangle$ $(q|p-1)$,
- $Q_5 = \langle a, b, c \mid a^q = b^p = c^p = 1, a^{-1}ba = c, a^{-1}ca = b^{-1}c^{2\alpha}, bc = cb,$ $(\alpha + \sqrt{\alpha^2 - 1})^q = 1\ (mod\ p)\ \rangle,\ (q|p+1), \alpha^2 - 1$ is not perfect square.
- $Q_{5+i} = \langle a, b, c \mid a^q = b^p = c^p = 1, a^{-1}ba = b^{\beta}, a^{-1}ca = c^{\beta^i}, bc = cb,\ \beta^q \equiv 1\ (mod\ p)\rangle$ $(q|p-1),\ i = 1, 2, 3, \ldots, \frac{q-1}{2}$ *and* $q - 1$.

Lemma 3.1. *Groups $L_1, \cdots, L_4$ have the EKR property.*

Proof. By Lemma 2.2, every cyclic group has the EKR property and thus L_1 has the EKR property. The group L_4 is a Frobenius group and it has the EKR property. Also, by Proposition 2.1 and Corollary 2.1, L_2 and L_3 have the EKR property. □

Lemma 3.2. *No subgroup of $L = L_5$ is core-free.*

Proof. It is not difficult to see that all non-conjugate subgroups of L are $K_1 = \langle e\rangle$, $K_2 = \langle a^p\rangle$, $K_3 = \langle a\rangle$, $K_4 = \langle b\rangle$, $K_5 = \langle a^p, b\rangle$ and $K_6 = L$. We have $N_L(K_2) = L$, so K_2 is a normal subgroup of L. Also by Sylow theorem, K_4 is a normal subgroup of L. Since $[L : K_5] = p$ and p is the smallest prime number that divides the order of group, K_5 is normal subgroup of L. Let s be an arbitary integer, then $b^{-s}a^ib^s = a^ib^{s(1-u^i)}$ which yields that K_3 is not core-free. □

Lemma 3.2 implies that the action of L on the set $\{1, 2, \cdots, p^2q\}$ is faithful. In the following, by $\bar{u}$ we mean u in modula q.

Lemma 3.3. *Suppose $L = L_5$ and $H = \{e\}$. The permutation peresentation of generetors of L are*

$$\begin{aligned} a^{-1} &= (1, 2, \cdots, p^2)(p^2+1, p^2+q+\overline{u}-1, \ \cdots, p^2q-q+\overline{u^{p^2-1}}-1)\cdots \\ &\quad (p^2+q, p^2+2q+\overline{u}-2, \cdots, p^2+\overline{u^{p^2-1}})\cdots(p^2q, p^2q+\overline{(q-1)u}, \cdots, \\ &\quad p^2q-2q+2+\overline{(q-1)u^{p-1}}), \\ b &= (1, p^2+q-1, \cdots, p^2+1)(2, p^2+2q-2, \cdots, p^2+q)\cdots(p^2, pq, \cdots, \\ &\quad p^2q-q+2). \end{aligned}$$

Proof. Assign a labeling to the elements of L/H as follows:

$$\begin{aligned} H &\to 1, Ha \to 2, \cdots, Ha^{p^2-1} \to p^2, \\ Hb &\to p^2+1, \cdots, Hb^{q-1} \to p^2+q-1, \\ Hab &\to p^2+q, \cdots, Hab^{q-1} \to p^2+2q-2, \\ Ha^2b &\to p^2+2q-1, \cdots, Ha^{p^2-1}b^{q-1} \to p^2q. \end{aligned}$$

With regards to the relations of L and the action of L on the set of right cosets L/H, we have $\varphi_{a^{-1}}(Ha^ib^j) = Ha^{i+1}b^{uj}$ and $\varphi_b(Ha^ib^j) = Ha^ib^{j-1}$. Indeed, the permutation presentation of a^{-1} is composed of q cycles of order p^2 and the permutation presentation of b is composed of p^2 cycles of order q. □

Lemma 3.4. *The group $L = L_5$ has the EKR property.*

Proof. First, we show that any non-identity element in L has no fixed point. Assume that

$$a^{-i}b^j(Ha^rb^s) = Ha^rb^s, (1 \le i, r \le p^2, 1 \le j, s \le q).$$

Hence $a^{-i}b^j(Ha^rb^s) = a^{-i}(Ha^rb^{s+j}) = Ha^{r+i}b^{u^i(s+j)} = Ha^rb^s$, then

$$\begin{cases} i+r \equiv r \ (mod\, p^2) \\ u^i(s+j) \equiv s \ \ (mod\, q) \end{cases}.$$

Thus, $i \equiv 0(mod\ p^2)$ and $j \equiv 0(mod\ q)$. Consequently, $\mathcal{D}_L = L - \{e\}$, so the derangement graph $\Gamma_L = \mathrm{Cay}(\mathrm{L}, \mathcal{D}_\mathrm{L})$ is a complete graph and this completes the proof. □

Theorem 3.3. *Suppose G is a group of order p^2q, where $p < q$. Then G has the EKR property.*

Proof. Use Lemmas 3.1 and 3.4. □

Theorem 3.4. *Suppose G is a group of order p^2q, where $p > q$. Then G has the EKR property.*

Proof. By Lemma 2.2, Proposition 2.1 and Corollary 2.1, groups Q_1, Q_2, Q_3 have the EKR property. Let $H = \langle a \rangle$ and $K = \langle b \rangle$. It is clear that $K \lhd Q_4$. On the other hand, $|Syl_q(Q_4)| = p^2$ and the intersection of Sylow q-subgroups is trivial. This yields that the group $Q_4 = KH$ is a Frobenius group. By a similar argument we can prove that groups Q_5 and $Q_5 + i$, $(i = 1, 2, 3, \ldots, \frac{q-1}{2}\ and\ q-1)$ are Frobenius groups and by Proposition 2.1, they have the EKR property. □

Corollary 3.1. *A group of order p^2q has the EKR property.*

By Lemma 2.2 and Corollary 2.1, groups L_1, L_2, Q_1 and Q_2 have the strict EKR property. Also, by Lemma 3.4, derangement graph of group L_5 is complete graph and it has the strict EKR property. Let $p, q \neq 2$, by Proposition 2.1 and Corollary 2.1, the other groups of order p^2q do not have the strict EKR property. So we proved the following theorem.

Theorem 3.5. *Among all groups of order p^2q only the groups L_1, L_2, L_5, Q_1 and Q_2 have the strict EKR property.*

3.3. Groups of order p^3

Let p be an odd prime number. Then there are three abelian groups $\mathbb{Z}_{p^3}, \mathbb{Z}_p \times \mathbb{Z}_{p^2}, \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ of order p^3 and two non-abelian groups of order p^3 as follows:

$$\begin{aligned} K_1 &= \langle a, b | a^p = b^{p^2} = e, a^{-1}ba = b^{p+1} \rangle, \\ K_2 &= \langle a, b, c | a^p = b^p = c^p = e, [a, b] = c, [a, c] = [b, c] = e \rangle. \end{aligned}$$

According to Lemma 2.2 and Corollary 2.1, three abelian groups have the strict EKR property. It remains to check the strict EKR property for groups K_1 and K_2. First, consider the group K_1. To do this we have the following lemma.

Lemma 3.5. *Let $H = \langle a \rangle \leq K_1$. Then H is the only core-free subgroup of K_1.*

Proof. The group K_1 has three non-conjugate subgroups of order p, namely $H_1 = \langle e \rangle$, $H_2 = \langle a \rangle$ and $H_3 = Z(K_1)$. It is not difficult to see that H_2 is core free. On the other hand, there are $p+1$ subgroups of order p^2 containing $Z(K_1)$ and we denote them by $H_4, \ldots, H_{p+4}$. All of them are normal in K_1. So for $i \neq 2$, $\mathrm{cor}_G(H_i) = H_i$. □

According to Lemma 3.5, the action of K_1 on the set $\{1, 2, \cdots, p^2\}$ is faithful.

Theorem 3.6. *Let $H = \langle a \rangle \leq K_1$, the permutation peresentation of generators of K_1 are*

$$\begin{aligned} a^{-1} &= (2, (p+1)^2+1, \cdots, (p+1)^{p-1}+1) \cdots (3, 2(p+1)+1, \cdots, 2(p+1)^{p-1} \\ &\quad +1) \cdots (p, (p-1)(p+1)+1, \cdots, (p-1)(p+1)^{p-1}+1), \\ b &= (p^2, p^2-1, \cdots, 1). \end{aligned}$$

Proof. First, consider the labeling $H \rightarrow 1, Hb \rightarrow 2, \cdots, Hb^{p^2-1} \rightarrow p^2$. It is not difficult to see that $\varphi_{a^{-1}}(Hb^i) = Hb^{(p+1)i}$ and $\varphi_b(Hb^i) = Hb^{i-1}$. The permutation presentation of a^{-1} is a product of $p-1$ cycles of order p. Note that b has no fixed point. Since $\varphi_{a^{-1}}(Hb^i) = Hb^i$ if and only if $b^{pi} \in H$, we conclude a^{-1} fixes all points $1, p+1, 2p+1, \cdots, p^2+1$. Thus, every element $a^ib^{tp} (1 \leq i, t \leq p-1)$ has $p+1$ fixed points. □

Theorem 3.7. *The derangement graph $\Gamma_{K_1} = \mathrm{Cay}(\mathrm{K_1}, \mathcal{D}_{\mathrm{K_1}})$ is isomorphic with the graph depicted in Figure 1.*

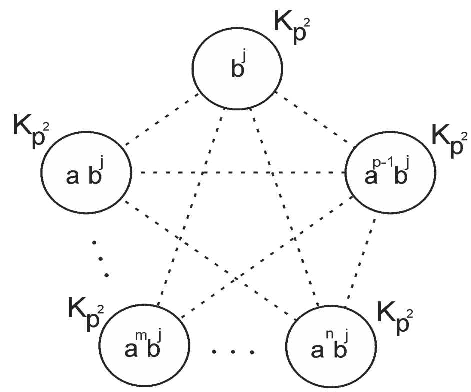

Figure 1. Cayley graph $\Gamma_{K_1} = \mathrm{Cay}(\mathrm{K}_1, \mathcal{D}_{\mathrm{k}_1})$, $(1 \leq j \leq p^2)$.

Proof. The derangement set of Γ_{K_1} is $\mathcal{D}_{K_1} = K_1 - \{e, a^i b^j\}$, where $1 \leq i \leq p-1$ and $j = tp$ $(0 \leq t \leq p-1)$. Hence it is a regular graph and the degree of every vertex is $p^3 - p - (p-1)^2$. Since $a^i b^j$ is adjacent with $a^r b^s$ if and only if $a^r b^{s-j} a^{-i} \in S$ if and only if $a^{r+p-i} b^{(p+1)^{p-i}(s-j)} \in S$, we conclude that $a^i b^j$ is adjacent to $a^r b^s$ if and only if

$$\begin{cases} r \neq i \ (mod\, p) \\ (1-pi)(s-j) \neq tp \ \ (mod\, p^2) \end{cases} or \begin{cases} r = i \ (mod\, p) \\ j \neq s \end{cases} \begin{cases} r \neq i \ (mod\, p) \\ j = s, \end{cases} \tag{2}$$

where $1 \leq t \leq p-1$. The equation $(1-pi)(s-j) \neq tp \ \ (mod\, p^2)$, for every t has only one soloution, where $s \neq tp + j$ which yields Γ_{K_1} has p non-disjoint cliques of order p^2. $\square$

Lemma 3.6. *The independence number of* $\Gamma_{K_1} = \mathrm{Cay}(\mathrm{K}_1, \mathcal{D}_{\mathrm{K}_1})$ *is* p.

Proof. By using Lemma 2.1 and Theorem 3.7 one can see that $\alpha(\Gamma_{K_1}) \leq p$. Since $\langle a \rangle$ is an independent set of Γ_{K_1}, we have $\alpha(\Gamma_{K_1}) = p$. $\square$

By Eq. (2), and permutation peresentation of generators of K_1, we conclude that

$$S = \{e, ab^p, a^2b^p, \cdots, a^{p-1}b^p\}$$

is a maximum independent set in $\Gamma = \mathrm{Cay}(\mathrm{K}_1, \mathrm{S})$. This yields that the group K_1 does not have the strict EKR property.

Lemma 3.7. *Let* $H = \langle a \rangle \leq K_2$*, then* H *is the largest core-free subgroup of* K_2.

Proof. All non-conjugate subgroups of K_2 are $\langle a \rangle$, $\langle b \rangle$, $\langle c \rangle$, $\langle a^i b^j \rangle$ and the number of such subgroups is $p - 1 + 3 = p + 2$. Let us show them by $H_1, \ldots, H_{p+2}$. For $2 \leq i \leq p+2$, $|N_G(H_i)| = p^2$ and $N_G(H_3) = G$. On the other hand, all non-conjugate subgroups of order p^2 are $\langle a^i, b^j \rangle (1 \leq i, j \leq p-1)$ and $\langle b, c \rangle$. Hence, there are $p - 1 + 2 = p + 1$ non-conjugate subgroups of this form. We call them by $G_1, \ldots, G_{p+1}$. For $1 \leq i \leq p+1$, we have $N_G(G_i) = G$. Since for $1 \leq i \leq p+1$, G_i is a normal subgroup of G and $\mathrm{cor}_G(G_i) = G_i$. By the relations in group K_2 we have $b^{-1}a^i b = a^i c^{-i}$ which yields $\mathrm{cor}_{K_2}(H) = \{e\}$. $\square$

According to Lemma 3.7, the action of K_2 on the set $\{1, 2, \cdots, p^2\}$ is faithful.

Theorem 3.8. *Let $H = \langle a \rangle \leq K_2$. The permutation peresentations of generators of K_2 are*

$$\begin{array}{rcl} a^{-1} & = & (2, 2p, \cdots, 3p-2)(3, 3p, \cdots, 4p-4)\cdots(p, p^2, \cdots, p^2-p+2), \\ b & = & (1, p, \cdots, 2)(p+1, p^2-p+2, \cdots, 2p)\cdots(2p-1, p^2, \cdots, 3p-2), \\ c & = & (1, 2p-1, \cdots, p+1)(2, 3p-2, \cdots, 2p)\cdots(p, p^2, \cdots, p^2-p+2). \end{array}$$

Proof. First, asign the following labels to the elements of coset K_2/H.

$$\begin{array}{rcl} H & \rightarrow & 1, Hb \rightarrow 2, \cdots, Hb^{p-1} \rightarrow p, \\ Hc & \rightarrow & p+1, \cdots, Hc^{p-1} \rightarrow 2p-1, \\ Hbc & \rightarrow & 2p, \cdots, Hbc^{p-1} \rightarrow 3p-2, \\ Hb^2c & \rightarrow & 3p-1, \cdots, Hb^{p-1}c^{p-1} \rightarrow p^2. \end{array}$$

With regards to the relations of K_2 and the action of K_2 on the right coset K_2/H, we have $\varphi_{a^{-1}}(Hb^ic^j) = Hb^ic^{i+j}$, $\varphi_b(Hb^ic^j) = Hb^{i-1}c^j$ and $\varphi_c(Hb^ic^j) = Hb^ic^{j-1}$. Indeed, the permutation presentation of a^{-1} is composed of $p-1$ cycles of order p and the permutation presentations of b and c are composed of p cycles of order p. One can see that a^{-1} fixes all points $1, p+1, \cdots 2p-1$ and b, c move all points. □

Theorem 3.9. *The Cayley graph $\Gamma_{K_2} = \mathrm{Cay}(\mathrm{K_2}, \mathcal{D}_{\mathrm{K_2}})$ is isomorphic with the graph depicted in Figure 2.*

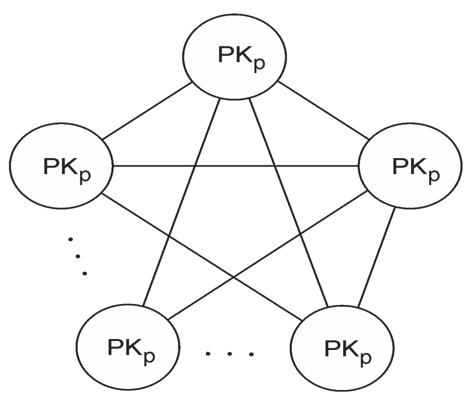

Figure 2. Cayley graph $\Gamma_{K_2} = \mathrm{Cay}(\mathrm{K_2}, \mathcal{D}_{\mathrm{k_2}})$.

Proof. The derangement set of Γ_{K_2} is $\mathcal{D}_{K_2} = K_2 - \{e, a^ic^k\}$, where $1 \leq i \leq p-1$, $0 \leq k \leq p-1$. Hence Γ_{K_2} is a regular graph of degree $p^3 - p(p-1) - 1$. Since $a^ib^jc^k$ is adjacent with $a^rb^sc^t$ if and only if $a^rb^{s-j}a^{-i}c^{t-k} \in \mathcal{D}_{K_2}$ if and only if $a^{r+p-i}b^{s-j}c^{-si+ij+t-k} \in \mathcal{D}_{K_2}$, we conclude that $a^ib^jc^k$ is not adjacent to $a^rb^sc^t$ if and only if $s = j\ (mod\ p)$ and $r \neq i\ (mod\ p)$. By these relations, the derangement graph Γ_{K_2} is composed of p subgraphs $G_1, \cdots, G_p$, where

$G_i \cong pK_p(i = 1, 2, \cdots, p)$ and $pK_p = \cup_{i=1}^{p} K_P$. For two distinct integers $i, j \in [p]$ all vertices of G_i are adjacent with all vertices of G_j. Hence, the Cayley graph $\Gamma_{K_2} = \mathrm{Cay}(\mathrm{K}_2, \mathcal{D}_{\mathrm{K}_2})$ is as depicted in Figure 2 and thus the independence number of Γ_{K_2} is p. □

By the proof of Theorem 3.9 and permutation peresentation of generators of K_2, we conclude that $S = \{e, ac, a^2c, \cdots, a^{p-1}c\}$ is a maximum independent set in $\Gamma = \mathrm{Cay}(\mathrm{K}_2, \mathrm{S})$. Then the group K_2 does not have the strict EKR property.

4. Applications

A Kneser graph denoted by $K_{v:k}$ is the graph with the k-subsets of a v-set as its vertices, where two k-subsets are adjacent if they are disjoint as sets. It is a well-known fact that the independence number of Kneser graph is $\binom{v-1}{r-1}$. For proving this result, we construct an intersecting set whose size is equal with the independence number. The idea of EKR theorem on finite groups is given from above algorithm.

Let $\mathbb{S}_n$ be the set of permutations of $[n]$. A family of $\mathbb{S}_n$ is said to be t-intersecting if any two permutations in the family agree in at least t points. In 1977, Deza and Frankl [6] proved that a 1-intersecting family has size at most $(n-1)!$. In [13] a statistical application of EKR theorem is given.

The other application of EKR theorem can be found in hyper graphs. A hypergraph is a generalization of a graph in which an edge can join any number of vertices. Formally, a hypergraph H is a pair $H = (X, E)$, where X is a set of elements called vertices, and E is a set of non-empty subsets of X called edges. Therefore, E is a subset of $P(X) - \{\phi\}$, where $P(X)$ is the power set of X. The Erdős-Ko-Rado theorem is part of the theory of hypergraphs, specifically, uniform hypergraphs of rank r. A family of sets is a hypergraph, and when all the sets are the same size it is called a uniform hypergraph. Since every set in A has size r, A is an r-uniform hypergraph. Given $n > 2k$, every intersecting k-uniform hypergraph H on n vertices contains a vertex that lies in at most $\binom{n-2}{k-2}$ edges. This result can be viewed as a special case of the degree version of a well-known conjecture of Erdős on hypergraph matchings. In [10], it is proved that given integers n, k, s with $n \geq 3k^2 s$, every k-uniform hypergraph H on n vertices with minimum vertex degree greater than $\binom{n-1}{k-1}$ -$\binom{n-s}{k-1}$ contains s disjoint edges.

Finally, we find the independence number of a Cayley derangement graph constructed by Mathieu group. The Mathieu groups are five sporadic simple groups $M_{11}, M_{12}, M_{22}, M_{23}$ and M_{24} introduced by Mathieu (1861, 1873). They are multiply transitive permutation groups on 11, 12, 22, 23 or 24 objects. They were the first sporadic groups to be discovered. In [1], it is proved that the Mathieu group M_{12} has the EKR property and it is a well-known fact that the stabilizer of a point in M_{12} is M_{11}. Then the independence number of derangement graph of M_{12} is equal with the size of the stabilizer of a point (the size of M_{11}) which is 7920.

References

[1] B. Ahmadi, *Maximum Intersecting Families of Permutations*, Ph.D. thesis. University of Regina, Regina, (2013).

[2] B. Ahmadi and K. Meagher, The Erdős-Ko-Rado property for some permutation groups groups, *Australas. J. Comb.* **61** (1) (2015), 23–41.

[3] M. Bardestani and K. Mallahi-Karai, On the Erdős-Ko-Rado property for finite groups, *J. Algebr. Comb.* **42** (2015), 111–128.

[4] P.J. Cameron and C.Y. Ku, Intersecting families of permutations, *European J. Combin.* **24** (2003), 881-890.

[5] P. Erdős, Chao Ko and R. Rado, Intersection theorems for systems of finite sets, *Quart. J. Math.* **12** (1961), 313-320.

[6] P. Frankl and M. Deza, The maximum number of permutations with given maximal or minimal distance, *J. Combin. Theory Ser. A.* **22** (1977), 352-360.

[7] M. Ghorbani and F. Nowroozi-Larki, Automorphism group of groups of order pqr, *Journal of Algebraic Structures and Their Applications* **1** (2014), 49–56.

[8] M. Ghorbani and M. Rajabi-Parsa, On the spectrum of derangement graphs of order a product of three primes, *Journal of Algebraic Structures and Their Applications* **6** (2019), 81–89.

[9] C. Godsil and K. Meagher, A new proof of the Erdős-Ko-Rado theorem for intersecting families of permutations, *European J. Combin.* **30** (2009), 404-414.

[10] H. Huang and Y. Zhao, Degree versions of the Erdős-Ko-Rado Theorem and Erdős hypergraph matching conjecture, arXiv:1605.07535v1.

[11] G. James and M. Liebeck, *Representation and Characters of Groups*, Cambridge University Press. Cambridge, (1993).

[12] B. Larose and C. Malvenuto, Stable sets of maximal size in Kneser-type graphs, *European J. Combin.* **25** (2004), 657-673.

[13] T.M. Ligget, Extensions of the Erdős-Ko-Rado theorem and a statistical application, *J. Combin. Theory Ser. A* **23** (1977), 15-21.

[14] K. Meagher and P. Spiga, An Erdős-Ko-Rado theorem for the derangement graph of PGL(2, q) acting on the projective line, *J. Combin. Theory Ser. A.* **118** (2011), 532-544.

[15] K. Meagher and P. Spiga, An Erdős-Ko-Rado-type theorem for $PGL3(q)$, *SIAM J. Discrete Math.* **28** (2014), 918-941.

[16] H. Holder, Die Gruppen der ordnungen p^3, pq, pqr, p^4, *Math. Ann. XLIII.* (1893), 371–410.

[17] M. Jalali-Rad and A.R. Ashrafi, Erdős-Ko-Rado properties of some finite groups, *Sib. Electron. Math.* Reports **13** (2016), 1249–1257

[18] J.S. Rose, *A Course on Group Theory*, Cambridge University Press (1978).

[19] C.Y. Ku and T.W.H. Wong, Intersecting families in the alternating group and direct product of symmetric groups, *Electron. J. Combin.* **14** (2007), #R25.

[20] J. Wang and S.J. Zhang, An Erdős-Ko-Rado-type theorem in Coxeter groups, *European J. Combin.* **29** (2008), 1112–1115.