www.combinatorics.ir

Transactions on Combinatorics
ISSN (print): 2251-8657, ISSN (on-line): 2251-8665
Vol. 8 No. 1 (2019), pp. 15-40.

www.ui.ac.ir

ON PROBLEMS CONCERNING FIXED-POINT-FREE PERMUTATIONS AND ON THE POLYCIRCULANT CONJECTURE – A SURVEY

MAJID AREZOOMAND*, ALIREZA ABDOLLAHI AND PABLO SPIGA

Communicated by Bijan Taeri

Abstract. Fixed-point-free permutations, also known as derangements, have been studied for centuries. In particular, depending on their applications, derangements of prime-power order and of prime order have always played a crucial role in a variety of different branches of mathematics: from number theory to algebraic graph theory. Substantial progress has been made on the study of derangements, many long-standing open problems have been solved, and many new research problems have arisen. The results obtained and the methods developed in this area have also effectively been used to solve other problems regarding finite vertex-transitive graphs. The methods used in this area range from deep group theory, including the classification of the finite simple groups, to combinatorial techniques. This article is devoted to surveying results, open problems and methods in this area.

1. History and motivations

A permutation g of a set Ω is said to be a *derangement* if it has no fixed-point on Ω, equivalently for each $\alpha \in \Omega$, $\alpha^g \neq \alpha$. The problem of counting the number of derangements of a finite set originates in the game of thirteen (*jeu du treize*, in French) and was proposed in 1708 by Montmort at the end of his book [70, p.185] as a teasing question, see [75]:

"Suppose a player has a deck of 13 cards numbered "$1, 2, \ldots, 13$". After shuffling, he or she draws one card at a time, without replacement, counting out loud as each card is drawn: "$1, 2, \ldots, 13$". The

MSC(2010): Primary: 20B25; Secondary: 05E18.
Keywords: Derangements, Polycirculant Conjecture, Transitive group.
Received: 25 August 2018, Accepted: 25 December 2018.
*Corresponding author.

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

.

player wins if he or she can go through the entire deck, never drawing a card bearing the number just called. What is the player's probability of winning?"

The game of thirteen has also been called *rencontres* [3, 27], *coincidences* [82], *Montmort's matching problem* [75] and *hat-check problem* [77].

In 1710, in a letter to Johann Bernoulli, Montmort gave the solution to the problem and claimed that he had found the general solution of the game for any deck of cards, but (he said) it would be too long to give all the details. A nephew of Johann Bernoulli, Nikolaus Bernoulli in 1711, in a letter to Montmort, solved the problem in general again. Both letters are reprinted in [71], pp. 303–307 and pp. 308–314, respectively; for more details, see [71] or [82]. In the general case, the shuffled deck corresponds to a permutation $g \in \mathrm{Sym}(n)$, n being the number of cards in the deck, and the player wins if and only if g is a derangement. Therefore $\mathbb{P}(n)$, the probability of winning, is simply the proportion of derangements in $\mathrm{Sym}(n)$. In other words, $\mathbb{P}(n) = \Delta(\mathrm{Sym}(n))/n!$, where $\Delta(\mathrm{Sym}(n))$ denotes the number of derangements in $\mathrm{Sym}(n)$. Montmort, in the second edition of his book [71, p. 301], using the inclusion-exclusion principle proved that $\mathbb{P}(n) = \sum_{j=0}^{n}(-1)^j/j!$. In particular, $\mathbb{P}(n)$ approaches $1/e$ as n approaches infinity or equivalently, $\Delta(\mathrm{Sym}(n))$ is the nearest integer to $n!/e$, see also [4, Corollary 2.7]. For the history, for various appearances of the problem in the theory of probability and for some modern versions see [2, 17, 20, 25, 42, 53, 54, 69, 82, 84].

In 1872, Camille Jordan, when studying Mathieu groups, proved the existence of fixed-point-free elements in a transitive action of a group on a finite set of cardinality at least 2:

Theorem 1.1. (Jordan's theorem)([47, Théorème I]) *Let G be a group acting transitively on a finite set Ω with at least 2 elements. Then there exists an element of G acting on Ω without fixed points.*

As a direct consequence of Jordan's theorem, we obtain that, if H is a proper subgroup of a finite group G, then G cannot be the union of the G-conjugates of H. Indeed, this observation can be deduced from Jordan's theorem applied to the action of G on the right cosets of H. Actually, the standard proof of Jordan's theorem is a simple counting argument that proves this latter fact: indeed, since H has at most $|G : H|$ conjugates and since each conjugate of H contains the identity of G, we have

$$\left|\bigcup_{g\in G} H^g\right| \leq |G : H|(|H| - 1) + 1 = |G| - (|G : H| - 1) < |G|.$$

Hence another way to state Jordan's theorem is

"Every proper subgroup of a finite group G does not meet at least one G-conjugacy class".

It is interesting to observe that, an easy application of the HNN-extension (Higman-Neumann-Neumann-extension) shows that there are infinite groups such that every two non-identity elements are conjugate; therefore, Jordan's theorem fails for infinite groups. For further examples see [2, 7]. Actually, Jordan's theorem incarnates in several different formulations and Jean-Pierre Serre, in his fabulous article [78], surveys some of these equivalent statements. For instance, in the context of character theory, Jordan's

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

theorem can be restated as "There exist two characters of G which are distinct but have the same restriction to H" [78, Theorem 4"].

Since certain permutation groups act as symmetry groups of combinatorial and geometric structures, deeper results on fixed-point-free elements provide useful tools for investigating these structures. The latter often occurs in finite geometry and algebraic geometry, for a survey see [20, 78], but applications are also known in number theory [26, 78], combinatorial set theory [14], in the study of maps between varieties over finite fields [41], and in random generation of groups [20]. Derangements are also useful in studying probabilistic generation [40] and for bounding convergence rates of random walks on finite groups [19]. The existence of a fixed-point-free element in a vertex-transitive graph is very useful in studying some problems in graph theory such as the existence of Hamiltonian cycles and Hamiltonian paths (see [1] and [62, 63], respectively), and for constructing vertex-transitive graphs [66]. In the rest of this introductory section we review some of these appearances proposing, in some cases, some problems.

1.1. **Proportion of fixed-point-free elements.** Results on fixed-point-free elements and their motivations come from a variety of different fields. A good example is given by the *number field sieve*. It all begun with an algorithm factoring integers of the form $r^e - s$, where r, e and $|s|$ are positive integers and $r, |s|$ are not too large. Broadly speaking, the correctness and the implementation of this algorithm depends on arithmetic in an algebraic number field, combined with more traditional sieving techniques. This algorithm is known as the "number field sieve" and for a brief description of the algorithm and several aspects of its implementation, we refer the reader to [55, pp. 11–42].

The importance of fixed-point-free permutations in this area arises from an observation of H. W. Lenstra Jr from 1991, who realized that the algorithm for factoring polynomials over an algebraic number field given in [85] could turn out to be useful in the number field sieve algorithm [55, Proposition 9.1, p. 73], provided that some good estimates on the number of fixed-point-free elements can be given. With this motivation in mind, H. W. Lenstra Jr asked M. A. Cohen about the proportion of fixed-point-free elements of a finite transitive permutation group. This question has spurred some interesting research, starting with the pioneering work of Cohen:

Theorem 1.2. (Cohen's theorem)([55, Lemma 9.2, p. 74]) *Let G be a finite group acting transitively on Ω with $|\Omega| \geq 2$. Then there are at least $\frac{|G|}{|\Omega|}$ elements of G acting without fixed points on Ω.*

Let G be a transitive permutation group on a finite set Ω and let $\delta(G) := |\Delta(G)|/|G|$ be the proportion of fixed-point-free elements of G, where $\Delta(G)$ is the set of fixed-point-free elements of G. Observe that $\Delta(G)$ is inverse-closed (that is, $g^{-1} \in \Delta(G)$ for every $g \in \Delta(G)$) and that $\Delta(G)$ is a union of G-conjugacy classes. By Jordan's theorem, $\delta(G) > 0$ when $|\Omega| \geq 2$. Moreover, by Cohen's theorem, $\delta(G) \geq 1/|\Omega|$ when $|\Omega| \geq 2$. Recall that the *rank* of a transitive permutation group is the number of orbits of its point-stabilizers. In 1992, using a rather clever counting argument involving permutation characters, Cameron and Cohen improved Cohen's theorem [13]:

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

Theorem 1.3. (Cameron-Cohen lower bound)([13, Proposition]) *Let G be a transitive permutation group of degree n and rank r, with $n \geq 2$. Then $\delta(G) \geq (r-1)/n$ with equality if and only if G is a Frobenius group of order $n(n-1)/(r-1)$ and with kernel of order n.*

Actually, Cameron and Cohen have proved something slightly finer, bounding $\delta(G)$ in terms of the degree n, the rank r and the minimal degree d. Recall that the *minimal degree* of G is the minimum number of points moved by any non-identity element of G. Namely, Cameron and Cohen have proved that $\delta(G) \geq \frac{r-1}{n-d} - \frac{d(n-1)}{(n-d)|G|}$, with equality if and only if each element of G fixes at least $n-d$ or at most 1 point [13, Theorem]. In 2008, using probabilistic techniques, Diaconis et al. reproved the lower bound in Theorem 1.3 and found an upper bound on $\delta(G)$ tends to 1 whenever the rank of G tends to infinity [20]:

Theorem 1.4. ([20, Theorem 3.1]) *Let G be a finite transitive permutation group of degree n and rank r, with $n \geq 2$. Then*

$$\frac{r-1}{n} \leq \delta(G) \leq 1 - \frac{1}{r}.$$

It is clear that, when G is a regular permutation group, we have $r = n = |G|$ and $\delta(G) = 1 - \frac{1}{n}$. In 2015, Guralnick et al. [39] reproved the above upper bound using only the Cauchy-Schwartz inequality and observed that this is a sharp bound:

Theorem 1.5. ([39, Theorem 1]) *Let G be a finite transitive permutation group of rank r. Then $\delta(G) \leq 1 - 1/r$. Furthermore, $\delta(G) = 1 - 1/r$ if and only if G acts regularly.*

Let G be a transitive permutation group on Ω. In 1993, Boston et al. calculated $\delta(G)$ for several families of transitive groups [4]. For instance, using the inclusion-exclusion method, they obtained the basic equality

$$|\Delta(G)| = \sum_{i=0}^{|\Omega|} (-1)^i \sum_{\substack{Y \subseteq \Omega \\ |Y|=i}} |G_{(Y)}|,$$

where $G_{(Y)}$ is the pointwise stabilizer of $Y \subseteq \Omega$. With this equality, they easily obtained an exact formula for $\delta(G)$ whenever G is a sharply k-transitive group. We recall that G is *k-transitive*, if G acts transitively on the set of k-tuples of distinct elements of Ω. Moreover, G is *sharply k-transitive*, if G acts regularly on the set of k-tuples of distinct elements of Ω.

Theorem 1.6. ([4, Theorem 2.3]) *Let G be a sharply k-transitive group of degree n. Then*

$$\delta(G) = \sum_{j=0}^{k-1} \frac{(-1)^j}{j!} + \sum_{j=k}^{n} \frac{(-1)^j \binom{n}{j}}{|G|}.$$

We summarize below some other results from [4], which follow from Theorem 1.6.

Theorem 1.7. *Let G be a transitive group of degree n.*

(1) *If G acts regularly, then $\delta(G) = 1 - \frac{1}{n}$;*

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

(2) $\delta(G) = \frac{1}{n}$ *if and only if* G *is sharply 2-transitive;*
(3) *if* G *is sharply 3-transitively, then* $\delta(G) = \frac{1}{2} - \frac{1}{2n}$*;*
(4) *if* $G = \mathrm{Sym}(n)$*, then* $\delta(G) = \sum_{j=0}^{n} \frac{(-1)^j}{j!}$*;*
(5) *if* $G = \mathrm{Alt}(n)$ *and* $n \geq 3$*, then* $\delta(G) = \sum_{j=0}^{n-2} \frac{(-1)^j}{j!} + \frac{(-1)^{n-1}2(n-1)}{n!}$.

Since the degree of every sharply 2-transitive group is a power of a prime, by Theorem 1.7(2), the equality $\delta(G) = \frac{1}{n}$ is achieved only for prime power degrees. When n is not a prime power, Boston et al. [4, pages 3263 and 3274] suggested first to calculate $\min\{\delta(G) \mid G \text{ is transitive of degree } n\}$, second to find the next possible lower bound for $\delta(G)$ if $\delta(G) > 1/n$ and, third to classify the permutation groups attaining the optimal bounds. This problem was solved by Guralnick and Wan in 1997 using the classification of the finite simple groups [41]:

Theorem 1.8. ([41, Theorem 1.3]) *Let* G *be a transitive permutation group of degree* n*. Then one of the following holds:*

(1) G *is a Frobenius group of order* $n(n-1)$*, with* n *a prime power, and* $\delta(G) = \frac{1}{n}$.
(2) G *is a Frobenius group of order* $n(n-1)/2$*, with* n *an odd prime power, and* $\delta(G) = \frac{2}{n}$.
(3) $(G, n, \delta(G)) \in \{(\mathrm{Sym}(4), 4, 3/8), (\mathrm{Sym}(5), 5, 11/30), (\mathrm{Alt}(5), 5, 2/5), (\mathrm{Alt}(5), 6, 1/3), (\mathbb{Z}_2, 2, 1/2)$ *or* $(\mathbb{Z}_3, 3, 2/3)\}$.
(4) $\delta(G) > 2/n$.

Boston et al. [4, Section 7, Problem 2] and Shalev [39, p. 199] independently conjectured that there exists a constant $\epsilon > 0$ such that, for every finite simple transitive permutation group G, $\delta(G) > \epsilon$. This conjecture turned out to stimulate deep group theoretic questions regarding finite simple groups and algebraic groups. Only very recently, Fulman and Guralnick have proved this conjecture in a series of papers [28, 29, 30, 31]. Actually, by focussing on certain finite simple groups of small degree, Boston et al. suggested that one might take $\epsilon = 2/7$ in the statement of their conjecture; however, this is not true. Tim Burness has observed that the group ${}^2F_4(2)$ has a transitive permutation representation of degree 2925 with the proportion of derangements equal to $89/325 < 2/7$. Nevertheless, Fulman and Guralnick have proved that, with possibly finitely many exceptions, the proportion of derangements in every finite simple transitive permutation group G is at least 0.016 [31, Theorem 1.1]. We believe that the papers of Fulman and Guralnick are not the last words on the proportion of derangements in simple transitive groups. For instance, for practical purposes it might be interesting to explicitly determine the "finitely many exceptions" above.

Problem 1.9. *Determine the simple transitive groups* G *with* $\delta(G) \leq 2/7$.

Again for practical purposes, it would be interesting to sharpen the bounds on $\delta(G)$ for some natural actions, for example the parabolic actions of simple groups of Lie type (these improved bounds might play a role in the investigation of the cocliques of maximum size in the derangement graph of a group, as already observed in [67, 68]).

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

1.2. **Actions with the same set of fixed-point-free elements.** Let G be a finite group with two transitive permutation representations on the sets Ω_1 and Ω_2, respectively. It is interesting from a purely theoretical reason to investigate when G has the same set of fixed-point-free elements on both Ω_1 and Ω_2. We find this question important on its own, however it arises naturally in algebraic number theory. Groups having two distinct actions with the same set of derangements can be used to construct different algebraic number fields with some arithmetical similarities, see for instance Čebotarev's density theorem [50] and the work of Perlis [73].

Observe that if the permutation character π_1 of G on Ω_1 equals the permutation character π_2 of G on Ω_2, then G has the same set of fixed-point-free elements in both actions. We recall that, answering a question of Wielandt, Guralnick and Saxl have given examples of finite groups with two actions, with one being primitive and the other being imprimitive, and having equal permutation characters. In particular, these examples point out that the permutation character of a group does not detect whether the action is primitive, therefore neither the set of fixed-point-free elements detects whether the action is primitive.

At the time of this writing, there are not many known examples of groups having two distinct primitive actions having the same set of fixed-point-free elements, see [79].

Problem 1.10. *Determine the finite primitive groups G having two distinct primitive actions having the same set of fixed-point-free elements.*

Consulting the known examples, it is remarkable that, if we denote by π_1 and by π_2 the permutation characters, then either $\pi_1 = \pi_2$, or $\pi_1 - \pi_2$ is a genuine character, or $\pi_2 - \pi_1$ is a genuine character (with genuine character we mean a linear combination with positive integer coefficients of irreducible complex characters).

Problem 1.11. *Let G be a group having two distinct primitive actions having the same set of fixed-point-free elements. Let π_1 and π_2 be the permutation characters for these two actions. Show that either $\pi_1 = \pi_2$, or $\pi_1 - \pi_2$ is a genuine character, or $\pi_2 - \pi_1$ is a genuine character.*

We recall that in [79, Theorem 10] this problem is reduced to the class of almost simple groups.

1.3. **Fixed-point-free elements of p-power order.** Another natural line of research concerning derangements is whether there are any restrictions on the possible orders of derangements. In 1960, J. R. Isbell, stimulated by some work in the context of game theory, made a rather intriguing conjecture on derangements [45]. First, we recall the research that inspired Isbell's conjecture. An *n-player simple game* on a set Ω with n elements is a pair $(\Omega, \mathcal{P})$, where $\mathcal{P}$ is a set of subsets of Ω (called winning coalitions) which is closed under taking supersets and contains one of each complementary pair of subsets. For a concrete example, the reader might think of the stakeholders of a company. A game $(\Omega, \mathcal{P})$ is said to be *homogeneous* if there exists a transitive subgroup of $\mathrm{Sym}(\Omega)$ preserving the elements of $\mathcal{P}$, that is, the automorphism group of the game $\{g \in \mathrm{Sym}(\Omega) \mid X^g = X, \forall X \in \mathcal{P}\}$ is transitive

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

on Ω. This is a natural "fairness" condition for a game. The problem of determining the existence of a homogeneous game with n players was studied in [45]. Indeed, it was proved in [45] that there exists a homogeneous game on a set Ω of size n if and only if there exists a transitive subgroup of $\mathrm{Sym}(n)$ with no fixed-point-free element of 2-power order. So, the existence of a homogeneous game on n players is equivalent to a problem in permutation group theory. It was conjectured by Isbell in [45] that there exists a function $f : \mathbb{N} \to \mathbb{N}$ such that, if $n = 2^a \cdot b$, where $a > f(b)$, then every transitive permutation group of degree n contains a derangement of 2-power order. In particular, this conjecture claims that if $n = 2^a \cdot b$ and a is big with respect to b, then a homogeneous game on n players does not exist. Intuitively, if the 2-part dividing the degree n is preponderant, then every transitive permutation group of degree n contains a derangement of 2-power order. Moving away from the original problem, Cameron [10, 11] has generalized Isbell's conjecture to any prime number. (Although this generalization is due to Cameron, this more general statement is still referred to Isbell.)

Conjecture 1.12. (Isbell's conjecture) *For every prime p, there is a function $f_p : \mathbb{N} \to \mathbb{N}$ such that, if $n = p^r s$ with $r \geq f(s)$, then a transitive group of degree n must contain a fixed-point-free element of p-power order.*

Cameron [10] has proposed a natural approach for proving Isbell's conjecture and it is worth noting that his approach would prove an even stronger result. Namely, Cameron has conjectured that, for every prime p, there is a function $f_p : \mathbb{N} \to \mathbb{N}$ such that, if $r \geq f(s)$, then every permutation p-group having at most s orbits each of size at least p^r must contain a fixed-point-free element. Again, intuitively, if a p-group has a small number of orbits and if each orbit is large, then the p-group contains a fixed-point-free permutation. The veracity of Isbell's conjecture will immediately follow from the veracity of Cameron's conjecture applied to the Sylow p-subgroup of the transitive group of degree n. Surprisingly, Cameron's conjecture turned out to be incorrect for every prime $p > 2$, see [18, 80], but it remains an open problem for the prime $p = 2$. Remarkably, Cameron's conjecture has not been refuted, yet, for the prime $p = 2$. Therefore, Cameron's approach to Isbell's conjecture could still be successful for the original statement of Isbell's conjecture.

Derangements of prime-power order have played a significant role also in number theory. Here the story begins in 1981 when, Fein et al. [26], using the full force of the classification of the finite simple groups proved that every transitive permutation group of degree at least 2 contains a derangement of prime-power order (no classification-free proof is known for this result):

Theorem 1.13. (Fein-Kantor-Schacher's theorem)([26, Theorem 1]) *Let G be a finite group acting transitively on a set Ω with $|\Omega| \geq 2$. Then there exists an element of prime-power order in G acting on Ω without fixed points.*

Surprisingly, the proof of Theorem 1.13 gives no information on the primes r such that G contains a derangement of r-power order. As a consequence of the above theorem, Fein et al. proved that there are no global fields $L \supset K$ with $B(L/K)$ finite, where $B(L/K)$ denotes the subgroup of the Brauer group

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

$B(K)$ of K consisting of those Brauer classes of finite-dimensional central simple K-algebras which are split by L [26, Corollary 4].

Fein et al. have constructed a finite transitive group with no derangement of prime order (we also give some examples later in the paper). Therefore, while every transitive permutation group admits a derangement of prime-power order, the same result is not true if "prime-power" is replaced by "prime" in Theorem 1.13, see [26, p.41]. Finite transitive permutation groups with no derangements of prime order are called **elusive** in [15], and from now on they are the main focus of this survey article.

1.4. **Fixed-point-free elements of prime order and the Polycirculant Conjecture.** In 2006, Isaacs et al. studied transitive permutation groups in which all derangements are involutions. They proved that these groups are either elementary abelian 2-groups or Frobenius groups having an elementary abelian 2-group as kernel [44, Corollary 3.2]. They also considered the analogous problem for abstract groups, and classified groups G with a proper subgroup H such that every element of G not conjugate to an element of H is an involution [44, Theorem 3.3]. For some character-theoretic analogues to the results in [44], see [5]. Recently, generalizing the results in [44] for the class of primitive groups, Burness and Tong-Viet proved that, every finite primitive permutation group with the property that the order of every derangement is a p-power, for some fixed prime p, is either almost simple or affine [9, Theorem 1].

In 1981, Marušič asked whether there exists a vertex-transitive digraph without a non-identity automorphism having all of its orbits of the same length [59, Problem 2.4]. By powering a group element up, the existence of such an automorphism (which is usually called *semiregular*) is equivalent to the existence of a fixed-point-free automorphism of prime order. In 1988, independently, the above problem was again proposed by Jordan [48]. In the 15th British combinatorial conference, in 1995, Klin proposed a more general question in the context of 2-closed groups, which we now recall.

Let G be a permutation group on Ω, following Wielandt [86, Definition 5.3], the 2-closure $G^{(2)}$ of G is the subset of $\mathrm{Sym}(\Omega)$ consisting of all permutations σ such that, for every $\omega, \omega' \in \Omega$ there exists $g \in G$ (which may depend upon ω, ω') with $\omega^\sigma = \omega^g$ and $\omega'^\sigma = \omega'^g$. It is straightforward to prove that $G^{(2)}$ is a subgroup of $\mathrm{Sym}(\Omega)$ and it is actually the largest subgroup of $\mathrm{Sym}(\Omega)$ having the same orbits as G in its natural coordinate-wise action on the Cartesian product $\Omega \times \Omega$. The group G is said to be 2-closed if $G = G^{(2)}$. Now, we can state Klin's question:

"Is there a 2-closed transitive permutation group containing no fixed-point-free element of prime order?"

Note that the automorphism group of any graph or digraph is 2-closed and hence Klin's question is indeed more general than the original Marušič-Jordan question. Moreover, every 2-closed group is the automorphism group of an edge-coloured digraph, but not every transitive 2-closed group is the automorphism group of a graph or digraph, see [15]. Therefore, Klin's question is genuinely a generalization of the Marušič-Jordan question. Broadly speaking, Klin's question is a graph colored version of the Marušič-Jordan question.

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

A graph admitting a fixed-point-free automorphism of prime order is called *polycirculant*, see for example [72, Section 6.9], so it is customary to refer to the conjecture that no 2-closed transitive permutation group is elusive as the *Polycirculant Conjecture*.

Conjecture 1.14. *(Polycirculant Conjecture) There is no 2-closed elusive transitive permutation group.*

We refer the reader to [51] for a short survey on polycirculant graphs. In the rest of this paper, we discuss some recent developments and possible future directions of the Polycirculant Conjecture. First we collect some basic facts about elusive groups.

2. Elusive groups

Recall that a finite transitive permutation group G on a set Ω is called elusive if G has no fixed-point-free element of prime order, see [15]. The name elusive has been chosen to suggest the belief that such groups are rare, although, to the best of our knowledge the term "rare" has never been formally quantified in any reasonable form. Thus we propose the following:

Problem 2.1. *Show that there exists a slow growing function $f : \mathbb{N} \to \mathbb{N}$ such that, for every $n \in \mathbb{N}$, the number of elusive permutation groups of degree n (up to conjugacy in $\mathrm{Sym}(n)$) is at most $f(n)$.*

For the number theoretic applications in [26], it was necessary to prove that a finite transitive group has a fixed-point-free element of prime-power order. In the context of derangements, this is the first time that an important result was proved using the classification of the finite simple groups (CFSG). Here we give a sketch of the proof of Theorem 1.13 for highlighting how the CFSGs was used (nowadays, this type of argument is fairly common and stardard):

Sketch of the proof of Theorem 1.13. Assume that the theorem is false and, among all transitive groups G of degree d with Theorem 1.13 being false, choose one such example with d as small as possible. Then with the degree d being fixed, choose G of degree d with Theorem 1.13 being false and with $|G|$ as small as possible. By considering the action of G on its systems of imprimitivity, we deduce (from the minimality of d) that G is primitive. As every non-identity normal subgroup of G is transitive, we deduce (from the minimality of $|G|$) that G is a non-abelian simple group.

Now, by invoking the classification of the finite simple groups, one proceeds to eliminate potential counterexamples to the theorem by a case by case verification. In this analysis, some number-theoretic results such as Bertrand's postulate (for the Alternating groups) and the existence of Zsigmondy primes (for the Lie type groups) are essential. We give a for instance: suppose $G = \mathrm{Alt}(n)$ with its natural primitive action on the set of uniform partitions of $\{1, \ldots, n\}$ into b parts of cardinality a (here, $n = ab$). In this action the stabilizer of a point is isomorphic to the wreath product $\mathrm{Sym}(a) \wr \mathrm{Sym}(b)$. Now, from Bertrand's postulate there exists a prime p with $n/2 < p < n$. Since p does not divide the order of $\mathrm{Sym}(a) \wr \mathrm{Sym}(b)$, we see that every p-element of G fixes no point. □

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

It was observed in [26] that the above theorem is not true if "prime-power" is replaced by "prime". Here, we report the example given in [26] of a transitive permutation group with no derangements of prime order. This provides the first example of an elusive group. Recall that a prime number p is said to be a *Mersenne prime* if $p = 2^\ell - 1$, for some $\ell \in \mathbb{N}$.

Example 2.2. Let p be a Mersenne prime, let G be the affine group $\mathrm{AGL}_1(p^2)$ consisting of all the permutations of the field $\mathrm{GF}(p^2)$ with p^2 elements of the form

$$t_{a,b} : x \mapsto ax + b,$$

where $a \in \mathrm{GF}(p^2)\setminus\{0\}$ and $b \in \mathrm{GF}(p^2)$ and let H be the subgroup of G consisting of the transformations $t_{a,b}$ where $a, b \in \mathrm{GF}(p)$.

The action of G on the left cosets of H gives rise to a transitive permutation group of degree $|G : H| = p(p+1)$.

Let q be a prime divisor of $p(p+1)$. Since p is a Mersenne prime, $q \in \{2, p\}$. Since G has only one conjugacy class of elements of order p and only one conjugacy class of elements of order 2, and since $t_{-1,1}$ and $t_{1,1}$ are elements of H of order 2 and p, respectively, we deduce that G has no fixed-point-free element of prime order. Thus G is elusive.

It is proved in [46, 49] that the above elusive group is not 2-closed: in line with the Polycirculant Conjecture.

Clearly, every transitive subgroup of an elusive group is elusive. Cameron et al. [15] give several constructions of such groups. We collect here some of them:

(1) Let p be a Mersenne prime and consider the action of $\mathrm{AGL}_2(p)$ on the set of $p(p+1)$ lines of the 2-dimensional affine plane. Then every transitive subgroup of $\mathrm{AGL}_2(p)$ whose Sylow p-subgroup is the translation group of $\mathrm{AGL}_2(p)$ is elusive. In particular, Example 2.2 falls into this category.

(2) $\langle (1,7,11)(2,12,10)(6,8,9), (1,3,12,9,7,4,10,8)(2,6,11,5)\rangle \cong \mathrm{AGL}_1(9)$,
$\langle (2,7)(4,11)(6,10)(8,12), (1,6,11,9)(2,10)(3,7)(4,5,8,12)\rangle \cong M_{11}$,
$\langle (1,6,12,8)(2,9,7,3,10,5,11,4), (1,10,2,7,12)(3,4,8,6,9)\rangle \cong M_{10}$,
$\langle (1,9)(2,6,12,4)(3,10,8,7)(5,11), (1,6,11,9,7,4,12,8)(2,3,10,5)\rangle \cong \mathrm{A\Gamma L}_1(9)$,
$\langle (1,3,12,8)(2,6,7,9)(4,11)(5,10), (1,2)(3,4,8,6)(5,9)(7,12,11,10)\rangle \cong M_9$,
as permutation groups on $\{1,\dots,12\}$. One checks that these are the only elusive groups of degree 12.

(3) The groups with structure $7^3 : (3^{1+2} : Q_8)$ and $7^3 : (3^{1+2} : \mathrm{SL}_2(3))$ with point stabilizers $7^2 : (3^2 : 2)$ and $7^2 : (3^2 : 6)$, respectively, acting on 84 points. Here, 3^{1+2} is the non-abelian group of order $3^3 = 27$ and exponent 3, and Q_8 is the quaternion group of order 8.

It is intriguing to observe that all of these examples are built from Mersenne primes. Despite the fact that we are not able to formalize what we precisely mean by "built", we ask the following.

Problem 2.3. *Are there elusive groups having order not divisible by any Mersenne prime?*

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

2.1. **Elementary properties of elusive groups.** In this section we collect some elementary properties of elusive groups. We give some of the proofs for completeness.

Lemma 2.4. *Let H and K be subgroups of G and let Ω be the set of right cosets of H in G. Then*

(1) *K is faithful on Ω if and only if, for all $k \in K \setminus \{1\}$, the conjugacy class k^G of k in G is not contained in H.*
(2) *K is transitive on Ω if and only if, for all $x \in G$, $K \cap Hx \neq \emptyset$.*
(3) *If K is a transitive permutation group on Ω, then K is elusive on Ω if and only if, for each $k \in K$ of prime order, $k^G \cap H \neq \emptyset$.*

Proof. It is similar to [64, Lemma 2.1]. □

Corollary 2.5. *Let G be a transitive permutation group on Ω and let $\omega \in \Omega$. Then G is elusive on Ω if and only if every G-conjugacy class of elements of prime order meets G_ω. In particular, if for every prime divisor p of $|\Omega|$, G_ω has an element of order p and G has only one conjugacy class of cyclic subgroups of order p, then G is an elusive group.*

Proof. It is a direct consequence of Lemma 2.4 (3). □

In what follows we denote by $\mathbf{Z}(X)$ the centre of the group X and by $\pi(X)$ the set of prime divisors of the order of X.

Lemma 2.6. *Let G be an elusive group on a finite set Ω with $|\Omega| > 1$. Then*

(1) *G contains no transitive subgroup H with $\mathbf{Z}(H) \neq 1$. In particular, $\mathbf{Z}(G) = 1$.*
(2) *G contains no Hall subgroup H such that $\mathbf{Z}(H) \neq 1$ and with $|\Omega|$ dividing $|H|$, cf.* [76, Lemma 2.1.2].
(3) *$|\Omega|$ is not a prime power, cf.* [59, Proposition 3.2].
(4) *$|\Omega| \neq mp$, where p is a prime and $1 \leq m \leq p$, cf.* [59, Theorem 3.4].
(5) *$\pi(G) = \pi(G_\alpha)$ for all $\alpha \in \Omega$, cf.* [38, Lemma 2.1].
(6) *$|G|$ is not square-free.*
(7) *G contains no normal subgroups $N \neq 1$ such that $N_\alpha = 1$, for some $\alpha \in \Omega$.*
(8) *G contains no normal subgroups N with at most two orbits and $\mathbf{Z}(N) \neq 1$, cf.* [38, Lemma 2.3].

Proof. (1) Let H be a transitive subgroup of G and, arguing by contradiction, assume that $\mathbf{Z}(H) \neq 1$. Let $x \in \mathbf{Z}(H) \setminus \{1\}$ with x having prime order. Then there exists $\alpha \in \Omega$ such that $\alpha^x \neq \alpha$. For every $\beta \in \Omega$, there exists $g_\beta \in H$ such that $\beta = \alpha^{g_\beta}$. Hence $\beta^x = \alpha^{g_\beta x} = \alpha^{x g_\beta} \neq \alpha^{g_\beta} = \beta$, which means that x is fixed-point free, that is, G is not elusive on Ω, a contradiction.

(2) Again, we argue by contradiction and we let H be a Hall subgroup of G such that $\mathbf{Z}(H) \neq 1$ with $|\Omega|$ dividing $|H|$. By (1), it is enough to prove that H is transitive on Ω. Since H is a Hall subgroup of G, $\gcd(|H|, |G : H|) = 1$. Let $\alpha \in \Omega$. As $|\Omega|$ divides $|H|$, we obtain that $\gcd(|H|, |G_\alpha|) = |H|/|\Omega|$. Since $|H_\alpha|$ divides $\gcd(|H|, |G_\alpha|)$, we get $|H_\alpha| \leq |H|/|\Omega|$; this implies $|\alpha^H| \geq |\Omega|$. Hence $\alpha^H = \Omega$, that is, H is transitive on Ω and by (1), G is not elusive, a contradiction.

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

(3) Assume $|\Omega| = p^k$, for some prime number p and some integer k. Let P be a Sylow p-subgroup of G. Now, $|\Omega|$ divides $|P|$ and $\mathbf{Z}(P) \neq 1$. Therefore, applying (2) with H replaced by P, we obtain a contradiction.

(4) By (3), the result is clear whenever $m = 1$ or $m = p$. So we may assume that $|\Omega| = mp$, where $2 \leq m \leq p-1$. Let P be a Sylow p-subgroup of G. Then P has m orbits of length p on Ω. Furthermore, for each $\alpha \in \Omega$ and $x \in P$, $x^p \in G_\alpha$. Thus $x^p \in \bigcap_{\alpha\in\Omega} G_\alpha = 1$ and hence $x^p = 1$. Thus every non-identity element of P has order p. As G is elusive, G has no fixed-point-free element of order p. So, for all $x \in P \setminus \{1\}$, $|\mathrm{Fix}_\Omega(x)|$ is a non-zero multiple of p, where $\mathrm{Fix}_\Omega(x) = \{\alpha \in \Omega \mid \alpha^x = \alpha\}$. Now, using the Orbit Counting Lemma, we obtain

$$m = \frac{1}{|P|}\sum_{x\in P} |\mathrm{Fix}_\Omega(x)| \geq \frac{1}{|P|}(mp + (|P|-1)p) = p\frac{m+|P|-1}{|P|} \geq p,$$

which is a contradiction.

(5) Clearly, $\pi(G_\alpha) \subseteq \pi(G)$. Suppose, towards a contradiction, that there exists $p \in \pi(G) \setminus \pi(G_\alpha)$. Then there exists $x \in G$ of order p which does not belong to any G-conjugate of G_α, that is, x does not belong to any point-stabilizer of G on Ω. Hence x is fixed-point-free, a contradiction.

(6) Suppose, arguing by contradiction, that $|G|$ is square-free. Since $|\Omega| > 1$, we get $\pi(G_\alpha) \neq \emptyset$ and $\pi(G) \neq \pi(G_\alpha)$ for all $\alpha \in \Omega$. Hence (5) implies that G is not elusive, a contradiction.

(7) Suppose G has a normal subgroup $N \neq 1$ such that $N_\alpha = 1$, for some $\alpha \in \Omega$. Since N is a normal subgroup of G and G is transitive, we get $N_\beta = 1$, for all $\beta \in \Omega$. Thus every non-identity element of N is fixed-point-free, a contradiction.

(8) Suppose, towards a contradiction, that N is a normal subgroup of G with at most two orbits and $\mathbf{Z}(N) \neq 1$. By (1), N has exactly two orbits, say α^N and β^N. Since $\mathbf{Z}(N)$ is a characteristic subgroup of N, $\mathbf{Z}(N) \trianglelefteq G$. Hence, by (7), we have $(\mathbf{Z}(N))_\alpha \neq 1$. Observe that, if $z \in \mathbf{Z}(N) \setminus \{1\}$ fixes one of α or β (say α), then z fixes all elements of the orbit containing α and z acts fixed-point-freely on the remaining orbit.

Since G is transitive, there exists $g \in G$ with $\alpha^g = \beta$. Let $x \in (\mathbf{Z}(N))_\alpha$ having order p. Then x fixes all elements of α^N and $x^g = g^{-1}xg \in \mathbf{Z}(N)$ fixes all elements of $(\alpha^N)^g = (\alpha^g)^N = \beta^N$. Hence $xx^g \in \mathbf{Z}(N)$ has order p and is fixed-point-free, a contradiction. □

2.2. **Elusive groups of restricted degree.** In 1998, Marušič and Scapellato proved that every vertex-transitive digraph of order $2p^2$, p a prime number, admits a semiregular automorphism of order p [64]. The proof of the latter also holds for transitive 2-closed permutation groups [15, p. 326]. We give the proof for completeness. In the next result, given a permutation group X (or a permutation x) on Ω and an X-invariant (or x-invariant) subset Δ of Ω, we denote by X^Δ (respectively, x^Δ) the permutation group induced by X on Δ.

Theorem 2.7. *Every transitive 2-closed permutation group of degree $2p^2$, p a prime number, is not elusive.*

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

Proof. We argue by contradiction and we let G be an elusive 2-closed transitive permutation group on a set Ω with $|\Omega| = 2p^2$, for some prime p, and we let P be a Sylow p-subgroup of G. Then P has two orbits of length p^2, say A and B, by [87, Theorem 3.4']. Let $\alpha \in \mathbf{Z}(P)$ be of order p. As G is elusive, α is not a derangement. Thus, replacing A by B if necessary, we may assume that α^A is a derangement and $\alpha^B = 1$. Then, by [21, Exercise 1.6.21], there exists a subgroup Q of P with Q^B isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Assume first that $Q^B = \langle \sigma^B \rangle \cong \mathbb{Z}_{p^2}$. So σ^B is a p^2-cycle (a cycle of length p^2). If σ^A is also a p^2-cycle, then σ^p is a fixed-point free element of G of order p, contradicting the fact that G is elusive. If σ^A is not a p^2-cycle, then $(\sigma^p)^A = 1$ and $\sigma^p\alpha$ is a fixed-point-free element of G of order p, contradicting the fact that G is elusive.

We may now assume that $Q^B \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Then there are elements $\gamma, \delta \in Q$ such that $\langle \gamma, \delta \rangle^B = Q^B$ and both γ^B and δ^B are derangements of order p. Suppose first that one of γ^A and δ^A, say γ^A, is not a p^2-cycle. If $\gamma^A = 1$, then $\gamma\alpha$ is a derangement of G of order p, a contradiction. Hence γ^A has order p and, moreover, γ has some fixed points in A. Then γ^A fixes each of the orbits $A_0, A_1, \ldots, A_{p-1}$ of $\langle \alpha \rangle$ in A. Let $B_0, B_1, \ldots, B_{p-1}$ be the orbits of $\langle \gamma \rangle$ in B. Note that $\alpha^{B_j} = 1$ for each j. On the other hand, B_j is an orbit of $\langle \gamma \rangle$ and $A_i^\gamma = A_i$ for each i. Now we define the permutation $\pi \in \mathrm{Sym}(\Omega)$ by the rule

$$v \mapsto v^\pi = \begin{cases} v^\alpha & \text{if } v \in A, \\ v^\gamma & \text{if } v \in B. \end{cases}$$

Since α and γ are derangements of order p on A and B, respectively, we conclude that π is a derangement of order p on Ω. We show that $\pi \in G$, from which we obtain a contradiction because G is elusive.

Let $A_i = a_i^{\langle \alpha \rangle}$ and $B_i = b_i^{\langle \gamma \rangle}$, $i = 1, \ldots, p$. Let $\Delta = (u, w)^G$ be an orbital of G (an orbit of G in its natural action on $\Omega \times \Omega$). Let $x \in A_i$ and $y \in B_j$, for some i and j. If $(x, y) \in \Delta$, then $A_i \times B_j \subseteq \Delta$. To see this, let $x' \in A_i$ and $y' \in B_j$ be arbitrary. Then $x' = x^{\alpha^k}$ and $y' = y^{\gamma^r}$ for some integers k, r. Since $\alpha^k \in G$ fixes y, we have $(x', y) = (x^{\alpha^k}, y) = (x, y)^{\alpha^k} \in \Delta$. On the other hand, $\gamma^r \in G$ implies that $(x^{\gamma^r}, y') = (x, y)^{\gamma^r} \in \Delta$. Since $A_i^\gamma = A_i$, $x^{\gamma^r} \in A_i$. Repeating the above argument, we get $(x', y') \in \Delta$, which yields $A_i \times B_j \subseteq \Delta$. With an entirely similarly argument, we see that, if $(y, x) \in \Delta$, then $B_j \times A_i \subseteq \Delta$.

Now let $g \in G$ be arbitrary. Before concluding the proof of our claim, we make four rather immediate observations:

(i): If $u^g, w^g \in A$, then $u^{g\pi} = u^{g'}$ and $w^{g\pi} = w^{g'}$, where $g' = g\alpha \in G$.

(ii): If $u^g, w^g \in B$, then $u^{g\pi} = u^{g'}$ and $w^{g\pi} = w^{g'}$, where $g' = g\gamma \in G$.

(iii): If $u^g \in A$ and $w^g \in B$, then $u^g \in A_i$ and $w^g \in B_j$ for some $i, j \in \{1, \ldots, p\}$. Since $u^{g\pi} = u^{g\alpha} \in A_i$ and $w^{g\pi} = w^{g\gamma} \in B_j$, by the argument in the previous paragraph, we get $(u^{g\pi}, w^{g\pi}) \in \Delta$.

(iv): If $u^g \in B$ and $w^g \in A$, then $u^g \in B_j$ and $w^g \in A_i$ for some $i, j \in \{1, \ldots, p\}$. With an argument similar to the case above, we have $(u^{g\pi}, w^{g\pi}) \in \Delta$.

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

Thus in all of the cases we have $(u^g, w^g)^\pi \in \Delta$. As g is arbitrary, we have $\Delta^\pi = \Delta$. Now, since Δ is arbitrary, we have $\pi \in G^{(2)}$. Now $G^{(2)} = G$ implies that $\pi \in G$, and our claim is finally proven.

We are now left with the case where both γ^A and δ^A are p^2-cycles. If $\langle \gamma^A \rangle = \langle \delta^A \rangle$, then $\gamma^A = (\delta^i)^A$ for some i. Thus $(\gamma\delta^{-i})^A = 1$. Since $(\gamma\delta^{-i})^B$ has order p, the permutation $\alpha\gamma\delta^{-i}$ is a derangement of G of order p, a contradiction. Assume now that $\langle \gamma^A \rangle \neq \langle \delta^A \rangle$. Since $\langle \gamma^A \rangle \neq \langle \delta^A \rangle$, $\gamma^A(\delta^{-1})^A \neq 1$. Let $x, y \in A$ such that $x^\gamma = y$. Since δ^A is a p^2-cycle, $x^{\delta^i} = y$ for some $i \in \{1, \ldots, p^2 - 1\}$. Hence $\gamma\delta^{-i}$ fixes x. Also $\langle \gamma^A \rangle \neq \langle \delta^A \rangle$ implies that $\gamma^A(\delta^{-i})^A \neq 1$. Since $\gamma\delta^{-i}$ is a p-element and $\langle \gamma^A(\delta^{-i})^A \rangle$ is a subgroup of the symmetric group on A having degree p^2, we conclude that $\gamma^A(\delta^{-i})^A$ has order p. Since $\langle \delta, \gamma\delta^{-i} \rangle^B = Q$, where both δ^B and $(\gamma\delta^{-1})^B$ are derangements of order p, we may now apply the argument in the case either γ^A or δ^A was not a p^2-cycle, by replacing γ with $\gamma\delta^{-i}$. Then the permutation π, defined by the rule $v^\pi = v^\alpha$ if $v \in A$ and $v^\pi = v^{\gamma\delta^{-i}}$ if $v \in B$, is a fixed-point-free element of G of order p, which completes the proof. □

The following theorem answers the analogous natural question: what can we say about transitive groups of degree $2pq$, where p and q are distinct odd primes?

Theorem 2.8. ([89, Theorem 1.3]) *Let G be a transitive permutation group of degree $2pq$, where p and q are distinct odd primes. Then G is not elusive.*

In fact Theorem 2.8 is a consequence of the following theorem.

Theorem 2.9. ([89, Lemma 4.1]) *Let G be an elusive permutation group of degree pqr, where p, q, r are prime numbers with $p > q > r$, and let N be a minimal normal subgroup of G. Then N is an elementary abelian p-group and each N-orbit has length p. Moreover $p - 1 = qt$ for some even integer t with $r > t$.*

It is conjectured that there are no elusive permutation groups of square-free degree, [89, Conjecture 1.1]. However, if such groups exist, then they satisfy the following properties:

Theorem 2.10. ([89, Theorem 1.2],[23, Theorem 4.1]) *Let G be an elusive group on a finite set Ω with $|\Omega|$ square-free. Then*

(1) *every minimal normal subgroup N of G is elementary abelian and all N-orbits are of length a prime divisor of $|\Omega|$, and*
(2) *G is not 2-closed.*

From this result, there is a question that naturally arises: "Are there 2-closed elusive groups having a minimal normal subgroup such that the length of all of its orbits is a fixed prime?" Actually, we already have an answer to this question and, in our opinion, this answer is one of the main contributions towards the veracity of the Polycirculant Conjecture. Indeed, let Γ be a vertex-transitive graph with mp vertices, where p is a prime number, and let N be a normal subgroup of $\mathrm{Aut}(\Gamma)$ having an orbit of length p. Then Γ admits a semiregular element of order p, by [22, Lemma 2]. It is noted in [24, Remark 3.6] that the proof of [22, Lemma 2] works as well for digraphs. Since every 2-closed permutation group

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

is the intersection of the automorphism groups of its orbital digraphs, with some work based on [22, 24] one may prove the following theorem:

Theorem 2.11. ([24, Remark 3.6]) *If G is a 2-closed elusive group, then G has no normal subgroup having an orbit of prime length.*

Let G be a group acting transitively on a set Ω. A non-empty subset Δ of Ω is called a *block* for G if, for each $g \in G$, $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$. Clearly, Ω and singletons $\{\omega\}$, for $\omega \in \Omega$, are blocks for every transitive group on Ω. These blocks are called *trivial blocks*. If Δ is a block for G, then $\{\Delta^g \mid g \in G\}$ is a G-invariant partition of Ω and is called the *system of imprimitivity* containing Δ. A transitive group is called *primitive* if it has no non-trivial blocks; otherwise it is called *imprimitive*. By [21, Theorem 1.6A], orbits of a non-identity normal subgroup N of a transitive group G form a system of imprimitivity for G. Furthermore, if G is a primitive permutation group, then N is also transitive. More generally, a permutation group is said to be *quasiprimitive* if all of its non-identity normal subgroups are transitive.

Theorem 2.12. ([24, Corollary 4.9]) *Let n be a positive integer such that $\gcd(n, \varphi(n)) = 1$, where φ is Euler's totient function. Suppose that every quasiprimitive group of composite degree m dividing n is either the alternating group $\mathrm{Alt}(m)$ or the symmetric group $\mathrm{Sym}(m)$. Then no group of degree n is elusive.*

2.3. **Elusive groups admitting a minimal normal transitive subgroup.** Clearly, every primitive group is quasiprimitive while not all quasiprimitive groups are primitive: consider the action of any nonabelian simple group on the cosets of a nonmaximal subgroup. In 2003, Giudici studied an even more general class of permutation groups (including primitive and quasiprimitive groups); those which have a transitive minimal normal subgroup:

Theorem 2.13. ([32, Theorems 1.1 and 1.2]) *Let G be an elusive group on a set Ω. If G has a minimal normal and transitive subgroup N, then it is the unique minimal normal subgroup of G, $G \cong M_{11} \wr K$ acting with its product action on $\Omega = \Delta^k$ for some $k \geq 1$, where M_{11} is the Mathieu group with its action of degree 12, K is a transitive subgroup of $\mathrm{Sym}(k)$ and $|\Delta| = 12$. Moreover, G is primitive and G is not 2-closed.*

In our opinion, Theorem 2.13 is the main result supporting the veracity of the Polycirculant Conjecture.

As the following theorem shows, every 2-closed almost simple transitive permutation group confirms the Polycirculant Conjecture.

Theorem 2.14. ([32, Theorem 1.4],[15, Theorem 5.5]) *Let G be an almost simple elusive group. Then G is either M_{11} or $M_{10} \cong A_6.2$ acting on 12 points and G is not 2-closed.*

By [21, Theorem 4.2A], every transitive minimal normal subgroup of an elusive group G is the unique minimal normal subgroup of G. Hence Theorem 2.13 and [21, Lemma 2.7A] imply that every elusive

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

group having a transitive minimal normal subgroup is quasiprimitive and in fact it is primitive. Another direct consequence of Theorem 2.13 is that every minimal normal subgroup to a counterexample of the Polycirculant Conjecture must be intransitive. Therefore every 2-closed primitive or quasiprimitive permutation group satisfies the Polycirculant Conjecture. Giudici and Xu extended this result to biquasiprimitive groups in [34]. (A *biquasiprimitive* permutation group is a transitive permutation group for which every non-identity normal subgroup has at most two orbits and there is some normal subgroup with precisely two orbits.)

Theorem 2.15. ([34, Theorem 1.4]) *Let G be a finite biquasiprimitive elusive permutation group on Ω and let $\alpha \in \Omega$. Then one of the following holds:*

(1) $G = M_{10}$ *and* $|\Omega| = 12$;

(2) $G = M_{11}^k \rtimes K \leq M_{11} \wr \mathrm{Sym}(k)$ *and* $G_\alpha \cong \mathrm{PSL}(2,11)^k \rtimes K'$, *where k is a positive integer, $K' \leq K \leq \mathrm{Sym}(k)$ such that K is transitive, $|K : K'| = 2$, and $K \setminus K'$ contains no elements of order 2;*

(3) $G = M_{11}^k \rtimes K \leq M_{11} \wr \mathrm{Sym}(k)$ *and* $G_\alpha \cong (\mathrm{PSL}(2,11)^{k/2} \times M_{11}^{k/2}) \rtimes K'$, *where k is an even positive integer, $K' \leq K \leq \mathrm{Sym}(k)$ such that K is transitive and K' is intransitive, $|K : K'| = 2$ and $K \setminus K'$ contains no elements of order 2.*

Moreover, each group G in (1)–(3) is biquasiprimitive and elusive, G is not 2-closed, and $G^{(2)}$ contains a fixed-point-free element of order 3.

In the following lemma, we study imprimitive elusive groups. Note that this lemma generalizes [15, Theorem 4.1 (a)].

Lemma 2.16. *Let G be an imprimitive permutation group on a set Ω, let Σ be a system of imprimitivity of non-trivial blocks and let K be the kernel of the action of G on Σ.*

(1) *If G/K contains a fixed-point-free element of prime order p on Σ, then there exists $g \in G$ of order a power of p such that gK is of order p and is fixed-point-free on Σ.*

(2) *If one of the following holds, then G contains a fixed-point-free element of order p on Ω:*
   (*a*) $\gcd(|K|, p) = 1$,
   (*b*) $|\Delta| < p$, *where* $\Delta \in \Sigma$.

Proof. The first part is proved in [89, Lemma 2.3]. Hence we prove the second part. Let $g^p = k \in K$ and let the order of k be n. If $\gcd(|K|, p) = 1$, then $\gcd(n, p) = 1$ and g^n has order p. Furthermore, $g^n K$ is fixed-point-free on Σ, which implies that g^n is a fixed-point-free element of prime order on Ω. This proves (*a*).

Now assume $|\Delta| < p$, where $\Delta \in \Sigma$. Clearly g is fixed-point-free on Ω. We claim that $g^p = 1$. Let $\Sigma = \{\Delta_1, \ldots, \Delta_t\}$, where $\Delta_1 = \Delta$. Since $g^p \in K$ and g is of p-power order, $\langle g^p \rangle$ acts on each Δ_i fixing each of its elements, which means that $g^p = 1$. This completes the proof. □

The following result is slightly more technical, but it plays a crucial role in a number of investigations. Broadly speaking, it brings the "global" primitive/quasiprimitive hypothesis used in Theorem 2.13 to a

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

"local" hypothesis. First some terminology. Let G be a transitive permutation group on Ω, let $\omega \in \Omega$, let $\Sigma \subseteq \Omega \setminus \{\omega\}$ be a G_ω-orbit and let $\sigma \in \Sigma$. Now, $(\omega, \sigma)^G = \{(\omega^g, \sigma^g) \mid g \in G\}$ is an orbital graph and this is said to be self-paired if $(\omega, \sigma)^G = (\sigma, \omega)^G$, that is, (ω, σ) and (σ, ω) are in the same G-orbit for the action of G on the cartesian product $\Omega \times \Omega$. Observe that this definition does not depend upon $\sigma \in \Sigma$. When the orbital graph $(\omega, \sigma)^G$ is self-paired, we say for simplicity that the suborbit Σ is self-paired. Finally, as customary, we denote by G_ω^Σ the permutation group induced by G_ω in its action on Σ.

Theorem 2.17. ([34, Theorem 1.3]) *Let G be a finite transitive permutation group on Ω and let $\omega \in \Omega$. Suppose that there exists a self-paired orbit Σ of G_ω on $\Omega \setminus \{\omega\}$ such that G_ω^Σ is quasiprimitive. Then $G^{(2)}$ is not elusive.*

It would be very interesting to remove the condition on Σ being self-paired in Theorem 2.17.

Problem 2.18. *Remove the condition on Σ being self-paired in Theorem 2.17.*

Cameron et al., using Wielandt's Dissection Theorem [86, Theorem 6.5], proved the following lemma. Observe that the hypothesis of this lemma holds for elementary abelian p-groups such that their point-stabilizers have codimension 1. Recall that a group is called *half-transitive* if all of its orbits have the same length.

Lemma 2.19. ([15, Theorem 5.3]) *Let G be a half-transitive permutation group with orbits O_i having the following properties:*

(1) *the action of G on each O_i is regular,*

(2) *if $\alpha_i \in O_i$ and $\alpha_j \in O_j$ for $i \neq j$ then either $G_{\alpha_i} = G_{\alpha_j}$ or $G_{\alpha_i} G_{\alpha_j} = G$.*

Then $G^{(2)}$ is not elusive.

It is proved in [51, Proposition 3] that, if every Sylow subgroup of the automorphism group of a vertex-transitive graph Γ is cyclic, then Γ has a semiregular automorphism. It is not hard to show that if each Sylow subgroup of a finite group G is cyclic, then G is supersolvable, see [74, Theorem 10.26]. In the following lemma we generalize [51, Proposition 3]. Observe that every supersolvable group has a non-trivial cyclic normal subgroup.

Lemma 2.20. *Let G be a finite transitive permutation group on a set Ω. If G has a non-identity cyclic normal subgroup, then G is not elusive. In particular, if G is supersolvable then it is not elusive.*

Proof. Let H be a non-identity cyclic normal subgroup of G, let $p \in \pi(H)$ and let $K = \langle x \rangle$ be the unique subgroup of H of order p. Then, for all $\alpha \in \Omega$, $K_\alpha = 1$ or $K_\alpha = K$. If for all $\alpha \in \Omega$ we have $K = K_\alpha$, then $K = 1$, which is a contradiction. So $K_\alpha = 1$, for some $\alpha \in \Omega$. Let $\beta \in \Omega$ be arbitrary. Then $\beta = \alpha^g$ for some $g \in G$. Since K is a characteristic subgroup of H, $K \trianglelefteq G$ and so $K_\beta = g^{-1} K_\alpha g = 1$, which means that K is a semiregular subgroup and so G contains a fixed-point-free element of order p. □

Since every supersolvable group is a solvable group, as a generalization of [51, Problem 2], a natural line of research on the Polycirculant Conjecture is the following problem:

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

Problem 2.21. *Which finite transitive solvable permutation groups are not elusive?*

Some partial answers to the above problem, are given in [60].

3. Constructions of elusive groups

As we already noted in the introduction, the first family of elusive groups was constructed in [26] in 1981. Also note that, for each integer $k \geq 1$, there exist elusive groups of degrees 12^k and $2 \cdot 12^k$ by Theorems 2.13 and 2.15, respectively. In 2002, several constructions of elusive groups are given in [15]. One can construct some new elusive groups from old ones as the following theorem shows:

Theorem 3.1. ([15, Theorem 4.1]) (Product construction) (1) *If G is elusive on Ω and $\mathcal{B}$ is a system of imprimitivity such that G acts faithfully on $\mathcal{B}$, then G is elusive on $\mathcal{B}$.*
(2) *If G is elusive on Ω and H is a transitive subgroup of G, then H is also elusive on Ω.*
(3) *If G_1 and G_2 are elusive on Ω_1 and Ω_2 respectively, then $G_1 \wr G_2$ and $G_1 \times G_2$ with their natural imprimitive actions, are elusive on $\Omega_1 \times \Omega_2$.*
(4) *If G is elusive on Ω, $|G|$ is odd and $|\Omega| = n$, then $2^{n-1} \rtimes G$ is elusive on $2 \times \Omega$ (see also Theorem 3.2).*
(5) *If G is elusive on Ω, then $G \wr \mathrm{Sym}(n)$ with its natural product action is elusive on Ω^n for every $n \geq 2$.*
(6) *If H is elusive in its action on the right cosets of K in H and if G is a non-split extension of H of prime index, then G is elusive in its action on the right cosets of K in G.*

Some elusive affine groups may be constructed via the following theorem:

Theorem 3.2. ([15, Theorem 3.1]) (Coprime affine construction) *Let G be a subgroup of $\mathrm{GL}(V)$ for some finite vector space V, and suppose that G has order prime to the characteristic of V. Let H be a subgroup of G, and let W be an H-invariant proper subspace of V. Then the action of $V \rtimes G$ on the right cosets of $W \rtimes H$ is elusive if and only if the following hold:*

(1) *the images of W by G cover V, that is, $V = \bigcup_{g \in G} W^g$, and*
(2) *every conjugacy class of elements of prime order in G meets H.*

The degree of the elusive group constructed in Theorem 3.2 is $|V : W||G : H|$. Keeping the notations and the hypothesis of Theorem 3.2, it is proved in [15, Theorem 3.2] that, for every $m \geq 1$, there exists an elusive group of degree $|V : W|^m|G : H|$. Thus, for each Mersenne prime p and for each $m \geq 1$, there exists an elusive group of degree $p^m(p + 1)$: this is a generalization of the first construction of elusive groups in [26]. Moreover, combining other elusive groups via Theorems 3.1 and 3.2, it is possible to show that, for each $m \geq 1$, there exists an elusive group of degree $7^m \cdot 12$. Furthermore, the authors of [15] have shown that there exists an elusive group of degree $p^m.2^n$, for every Mersenne prime p, and for all positive integers m and n with $2^n > p$.

Note that Theorem 3.2 does not hold when the characteristic of V divides $|G|$, see [33, p. 2721]. In some sense, the non-coprime case of Theorem 3.2 is the following:

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

Theorem 3.3. ([33, Theorem 2.2]) (Non-coprime affine construction) *Let G be a subgroup of $\mathrm{GL}(V)$ for some finite vector space V over a field of characteristic p, and suppose that p divides $|G|$. Let H be a subgroup of G and let W be an H-invariant proper subspace of V. Then the action of $V \rtimes G$ on the set of right cosets of $W \rtimes H$ is elusive if and only if*

(1) *the images of W by G cover V;*
(2) *every conjugacy class of elements of prime order in G meets H; and*
(3) *for each element vh of order p of G, with $v \in V$ and $h \in H$, there is an image U of W under G which is fixed by h and such that vh fixes some coset of U.*

There are elusive groups that cannot be constructed from old ones using one of the procedures we have described thus far. For instance, see [33, Example 3.4] for the first example of an elusive group G with an elementary abelian minimal normal subgroup N such that the stabilizer in N of a point is not a hyperplane and G is not permutation isomorphic to a wreath product in product action.

The following construction of elusive groups is given in [33] and is called the *priming construction*. Let $G = V \rtimes \langle a \rangle$ be an elusive permutation group of degree $p^s l$ with point stabilizer $H = U \rtimes \langle b \rangle$, where

(1) V is a finite-dimensional vector space over the finite field $\mathrm{GF}(p)$ with p elements,
(2) a is an element of $\mathrm{GL}(V)$ with order k coprime to p,
(3) U is a codimension s subspace of V whose stabilizer in $\langle a \rangle$ is $\langle b \rangle$.

Let r be a prime which divides k. Let $V' = \bigoplus_{i=1}^{r} V_i$, where $V_i = V$ for each i, and let g be the linear transformation in $\mathrm{GL}(V) \wr \mathrm{Sym}(r)$ of the vector space V' given by $(1, \ldots, 1, a)\tau$ where $\tau = (123...r)$ permutes the r copies of V. Next let $U' = U \oplus \bigoplus_{i=1}^{r-1} V_i$. Then U' is M-invariant where $M = \langle (b, \ldots, b) \rangle$. Finally, let $G^* = V' \rtimes \langle g \rangle$ and $H^* = U' \rtimes M$. Then the action of G^* on the set of right cosets of H^* is elusive of degree $p^s lr$ [33, Theorem 2.6].

We observe that, using the priming construction, in [33] Giudici has found a rich family of new degrees of elusive groups:

Theorem 3.4. (1) *Let $p = 2^\ell - 1$ be a Mersenne prime and let $q_1, \ldots, q_r$ be distinct odd primes dividing $p - 1$. Then, for every $k \geq 1$, $n \geq l$ and $j_1, \ldots, j_r \geq 0$, there exists an elusive group of degree $p^k \cdot 2^n \cdot q_1^{j_1} \cdots q_r^{j_r}$, see* [33, Theorem 1.1].
(2) *Let p be a Mersenne prime. Then there exists an elusive group of degree $2p(p+1)$, see* [33, Theorem 3.3].

Note that the degree $2p(p+1)$ are already provided by the examples of [15].

Giudici proved that the only elusive groups of degree up to 30 are five groups of degree 12 together with nineteen groups of degree 24 and none of them are 2-closed [33]. Furthermore, he proved that all the elusive constructions in his paper [33] are not 2-closed and their 2-closures are not elusive and so do not provide counterexamples for the Polycirculant Conjecture.

As we mentioned before, for every Mersenne prime p, $\mathrm{AGL}_1(p^2)$ acting on the set of $p(p+1)$ lines of the affine plane $\mathrm{AG}_2(p)$ is an elusive group. Giudici et al. called any transitive subgroup of the elusive

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

group $\mathrm{AGL}_1(p^2)$ an *FKS-group*, [35]. Note that any FKS-group G is elusive. Furthermore, $G = N \rtimes G_1$ where N is a minimal normal elementary abelian p-subgroup of G and G_1 is cyclic. Also N has $p+1$ orbits of length p. In general, it is proved that any elusive group with the above abstract structure can be constructed from FKS-groups:

Theorem 3.5. ([35, Theorem 1.1]) *Let G be an elusive permutation group such that $G = N \rtimes G_1$ where N is an elementary abelian minimal normal subgroup and G_1 is cyclic. Then G can be obtained by repeatedly applying priming construction to an FKS-group.*

Finally, we remark that using coding theory, Dobson et al., constructed several new elusive groups from old ones in [24, Section 3].

Problem 3.6. *Let us denote by $\mathcal{N}$ the positive integers n such that there exists an elusive group of degree n. What is the density of $\mathcal{N}$ in $\mathbb{N}$?*

3.1. **p-elusive and strongly p-elusive groups.** Let G be a transitive permutation group on a finite set Ω and let p be a prime divisor of $|\Omega|$. Then G is said to be *p-elusive* if it does not contain a derangement of order p. Similarly, G is said to be *strongly p-elusive* if it does not contain a derangement of p-power order, see [8]. Since G is elusive if and only if it is p-elusive for each prime p dividing $|\Omega|$, p-elusive groups are useful to prove or disprove (or simply to investigate) the Polycirculant Conjecture. All p-elusive and strongly p-elusive almost simple primitive groups with socle an alternating or sporadic group are determined in [8, Theorems 1.1 and 1.4]. Then the p-elusive almost simple primitive groups with socle a classical group are studied in detail in [7]. The study of p-elusivity for almost simple classical groups completed in [6].

Problem 3.7. *Which almost simple primitive groups with socle a group of Lie type are p-elusive?*

Another natural line of research on the Polycirculant Conjecture stems from the definition of p'-elusive groups: for a prime p, a finite transitive permutation group on Ω is called *p'-elusive* if $|\Omega|$ has a prime divisor different from p, and G does not contain a derangement of prime order q with $q \neq p$. The structure of $2'$-elusive quasiprimitive and biquasiprimitive permutation groups has been studied in [7].

4. Vertex-transitive digraphs confirming the conjecture

In this section, we review some results on vertex-transitive graphs which confirm the Polycirculant Conjecture. Roughly speaking, so far there are four main strategiest for attacking the Polycirculant Conjecture: specializing the order, specializing the valency, specializing some property on the automorphism group of the graph and specializing some well-behaved families of graphs.

4.1. **Orders.** We have discussed some results in this direction earlier in the paper. The automorphism group of any Cayley digraph admits a regular subgroup. So Cayley digraphs admit semiregular automorphisms. Since the automorphism group of any digraph is a 2-closed group, if for some integer n

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

every 2-closed transitive permutation group of degree n admits a semiregular element, then every vertex-transitive digraph of order n admits a semiregular automorphism. For example, every vertex-transitive digraph of p^k, mp, $2p^2$ or of square-free order, where p is a prime and $1 \leq m \leq p$ admits a semiregular automorphism, by Lemma 2.6 (3), Lemma 2.6 (4), Theorem 2.7 and Theorem 2.10, respectively. Also recently, Marušič proved that every vertex-transitive graph of order $3p^2$, where p is a prime, admits a semiregular automorphism [61, Theorem 1]. It seems that the natural next problems are the following:

Problem 4.1. *Which vertex-transitive graphs of order qp^k, where p and q are primes and k is an integer, admit a semiregular automorphism?*

A partial answer to the above problem is given in [60, Theorem 2.4 and Corollary 2.5].

Problem 4.2. *Which vertex-transitive graphs of order $p(p+1)$, p a prime, admit a semiregular automorphism?*

Problem 4.3. *Which vertex-transitive graphs of order n where n has only one square admit a semiregular automorphism?*

4.2. **Valencies.** In 1998, Marušič et al. proved that every cubic vertex-transitive graph admits a semiregular automorphism [64, Theorem 3.3]. The proof allows the possibility that the semiregular automorphism has order 2 or 3. Cameron et al. proved that every cubic vertex-transitive graph admits a semiregular automorphism of order greater than 2, see [16, Theorem 3]. They also proved that if Γ is a connected cubic G-vertex-transitive graph and G is a 2-group of exponent n, then G admits a semiregular element of order n, see [16, Theorem 7]. In later work, Spiga proved that the maximal order of a semiregular element in the automorphism group of a cubic vertex-transitive graph Γ does not tend to infinity as the number of vertices of Γ tends to infinity [81], a negative answer to a conjecture proposed in [16]. In some sense, this suggests that the order of the putative semiregular elements might be very small, even when the number of vertices of the graph is arbitrarily large. Despite this negative answer to the conjecture in [16], Li [57, Theorem 1.1] has proved that every connected cubic vertex-transitive graph admits a large semiregular subgroup, confirming a conjecture of Cameron-Sheehan [12, Problem BCC17.12].

In 2007, Dobson et al., proved that every vertex-transitive graph of valency $p+1$, p an odd prime, admitting a transitive $\{2,p\}$-group of automorphisms, has a semiregular automorphism, see [23, Theorem 4.2]. From this it is easy to deduce that every quartic vertex-transitive graph admits a semiregular automorphism [23, Theorem 1.1].

In 2015, Giudici et al. proved that every vertex-transitive group of automorphisms of a connected graph of valency four contains a semiregular automorphism [38, Theorem 1.1]. They also proved that every finite vertex-transitive digraph of out-valency at most three admits a semiregular automorphism [38, Corollary 1.3]. The problem for valency 5 is still open:

Problem 4.4. *Which vertex-transitive graphs of valency 5 admit a semiregular automorphism?*

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

In 2014, Giudici et al. proved that any edge-transitive regular graph of valency at most four admits a semiregular element [37, Theorem 1.2 and Corollary 1.4].

Although the Polycirculant Conjecture for valency 5 for vertex-transitive graphs is still open, an immediate corollary of Theorem 4.6 below yields that every arc-transitive graph of prime valency admits a semiregular automorphism. Moreover every finite 2-arc-transitive graph admits a semiregular automorphism [34, Corollary 1.2]. Xu in 2008 proved that every arc-transitive graph with valency pq, p and q two primes, having a nonabelian minimal normal subgroup of automorphisms admits a semiregular automorphism [88, Theorem 1.1]. Also it is proved that every arc-transitive graph of valency $2p$ admits a semiregular automorphism [36]. Finally, Verret [83, Theorem 1.2] has proved that arc-transitive graphs of valency 8 do admit semiregular automorphisms: 8 was the smallest valency not covered by earlier results.

Problem 4.5. *Which arc-transitive graphs of valency pq, where p and q are primes, contain a semiregular automorphism? In particular, which arc-transitive graphs of valency 9 contain semiregular automorphism?*

4.3. **Special actions.** Recall that a vertex-transitive graph Γ is called quasiprimitive if any non-identity normal subgroup of $\mathrm{Aut}(\Gamma)$ is transitive on the vertex set. By [32, Theorem 1.2] (Theorem 2.13) any primitive and any quasiprimitive graph admits a semiregular automorphism. Since edge-primitive graphs are vertex-quasiprimitive or vertex-biquasiprimitive, by Theorems 2.13 and 2.15, every vertex-transitive, edge-primitive graph has a semiregular automorphism. Also all vertex-transitive bipartite graphs, where the only system of imprimitivity is given by their bipartition, have a semiregular automorphism.

A graph Γ is called *G-locally quasiprimitive* if $G \leq \mathrm{Aut}(\Gamma)$ and for each $v \in V(\Gamma)$, the vertex-stabilizer G_v acts quasiprimitively on the set $\Gamma(v)$ of vertices adjacent to v. Each vertex-transitive 2-arc-transitive graph is a locally-quasiprimitive graph. We refer the reader to [58] for some properties of locally-quasiprimitive graphs. One of the important steps towards a possible complete solution to the Polycirculant problem is proved in the following theorem:

Theorem 4.6. ([34, Theorem 1.1]) *Let Γ be a finite graph with a group G of automorphisms such that G is vertex-transitive and locally-quasiprimitive. Then Γ has a nonidentity semiregular automorphism.*

4.4. **Special infinite families.** With an ad-hoc argument, the Polycirculant Conjecture was proved for distance-transitive graphs in [52].

Clearly, every prime order automorphism of a Cayley digraph is semiregular. In an attempt to generalize this obvious observation, generalized Cayley graphs were introduced in [65]. Here we recall the definition. Let G be a group, let $S \subseteq G$ and let $\alpha \in \mathrm{Aut}(G)$ satisfying:

(i): $\alpha^2 = 1$,
(ii): $(g^{-1})^\alpha g \notin S$, for every $g \in G$, and
(iii): for every $g, h \in G$ with $(h^{-1})^\alpha g \in S$, we have $(g^{-1})^\alpha h \in S$.

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

The *generalized Cayley graph* $X = \mathrm{GC}(G, S, \alpha)$ on G with respect to the ordered pair (S, α) is the graph with vertex set G, with two vertices g and h being adjacent if and only if $(h^{-1})^{\alpha} g \in S$. If $\alpha = 1$ then X is the Cayley graph of G with respect to S. Hence every Cayley graph is a generalized Cayley graph, but the converse is not true by [65, Proposition 3.2]. It is proved in [43, Theorem 3.4] that every generalized Cayley graph admits a semiregular automorphism.

Acknowledgments

This research was financially supported by Iran National Science Foundation: INSF and University of Isfahan.

References

[1] B. Alspach, Lifting Hamilton cycles of quotient graphs, *Discrete Math.*, **78** (1989) 25–36.

[2] A. Barbour, L. Holst and S. Janson, *Poisson approximation*. Oxford Science Publications. Clarendon Press, Oxford University Press, New York, 1992.

[3] E. Baticle, Le problème des rencontres, *Comptes Rendus Acad. Sci. Paris*, **209** (1936) 724–726 and 1891–1892.

[4] N. Boston, W. Dabrowski, T. Foguel, P. J. Gies, J. Leawitt, D. T. Ose and D. A. Jackson, The proportion of fixed-point-free elements of a transitive permutation group, *Comm. Algebra*, **21** (1993) 3259–3275.

[5] D. Bubboloni, S. Dolfi and P. Spiga, Finite groups whose irreducible characters vanish only on p-elements, *J. Pure Appl. Algebra*, **213** (2009) 370–376.

[6] T. C. Burness and M. Giudici, Locally elusive classical groups, *Israel J. Math.*, **225** (2018) 343–402.

[7] T. C. Burness and M. Giudici, *Classical Groups, Derangements and Primes*, Australian Mathematical Society lecture series 25, Cambridge University Press, 2016.

[8] T. C. Burness, M. Giudici and R.A. Wilson, Prime order derangements in primitive permutation groups, *J. Algebra*, **341** (2011) 158–178.

[9] T. C. Burness and H. P. Tong-Viet, Primitive permutation groups and derangements of prime power order, *Manuscripta Math.*, **150** (2015) 225–291.

[10] P. J. Cameron, Permutation Groups, *London Mathematical Society Student Text*, **45**, Cambridge University Press, Cambridge, 1999.

[11] P. J. Cameron, *Some open problems on permutation groups*, in: Groups, Combinatorics and Geometry, Durham, 1990, in: London Math. Soc. Lecture Note Ser., **165**, Cambridge Univ. Press, Cambridge, 1992 340–350.

[12] P. J. Cameron (ed.), Problems from the Seventeenth British Combinatorial Conference, *Discrete Math.*, **231** (2001) 469–478.

[13] P. J. Cameron and M. A. Cohen, On the number of fixed point free elements in a permutation group, A collection of contributions in honour of Jack van Lint, *Discrete Math.*, **106/107** (1992) 135–138.

[14] P. J. Cameron, P. Frankl and W. M. Kantor, Intersecting families of finite sets and fixed-point-free 2-elements, *European J. Combin.*, **10** (1989) 149–160.

[15] P. J. Cameron, M. Giudici, G. A. Jones, W. M. Kantor, M. H. Klin, D. Marušič and L. A. Nowitz, Transitive permutation groups without semiregular subgroups, *J. London Math. Soc.*, **66** (2002) 325–333.

[16] P. J. Cameron, J. Sheehan and P. Spiga, Semiregular automorphisms of vertex-transitive cubic graphs, *European J. Combin.*, **27** (2006) 924–930.

[17] S. Chatterjee, P. Diaconis and E. Meckes, Exchangeable pairs and Poisson approximation, *Probab. Surv.*, **2** (2005) 64–106.

[18] E. Crestani and P .Spiga, Fixed-point-free elements in p-groups, *Israel J. Math.*, **180** (2010) 413–424.

[19] P. Diaconis, *Group representations in probability and statistics*, Lecture Notes Monograph Series 11, Institute of Mathematical Statistics, Hayward, CA 1988.

[20] P. Diaconis, J. Fulman and R. Guralnick, On fixed points of permutations, *J. Algebraic Combin.*, **28** (2007) 189–218.

[21] J. D. Dixon, B. Mortimer, *Permutation groups*, Springer-Verlag, New York, 1996.

[22] E. Dobson, Isomorphism problem for Cayley graphs of $\mathbb{Z}_p^3$, *Discrete Math.*, **147**(1995) 87–94.

[23] E. Dobson, A. Malnič, D. Marušič and L. A. Nowitz, Minimal normal subgroups of transitive permutation groups of square-free degree, *Discrete Math.*, **307** (2007) 373–385.

[24] E. Dobson and D. Marušič, On semiregular elements of solvable groups, *Comm. Algebra*, **39** (2011) 1413–1426.

[25] L. Euler, Calcul de la probabilité dans le jeu de rencontre, *Mém. Acad. Sci. Berlin*, **7** (1753) 255–270.

[26] B. Fein, W. M. Kantor and M. Schacher, Relative Brauer groups II, *J. Reine Angew. Math.*, **328** (1981) 39–57.

[27] M. Frèchet, A note on the "problḿe des rencontres", *American Mathematical Monthly*, **46** (1939) 501.

[28] J. Fulman and R. Guralnick, *Derangements in simple and primitive groups*, in Groups, combinatorics, and geometry: Durham 2001, World Scientific Publishing, 2003 99–121.

[29] J. Fulman, R. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements, *Amer. Math. Soc.*, **364** (2012) 3023–3070.

[30] J. Fulman and R. Guralnick, Derangements in subspace actions of finite classical groups, *Trans. Amer. Math. Soc.*, **364** (2017) 2521–2572.

[31] J. Fulman and R. Guralnick, *Derangements in finite classical groups for actions related to extension field and imprimitive subgroups and the solution of the Boston-Shalev conjecture*, preprint.

[32] M. Giudici, Quasiprimitive groups with no fixed point free elements of prime order, *J. London Math. Soc. (2)*, **67** (2003) 73–84.

[33] M. Giudici, New constructions of groups without semiregular subgroups, *Comm. Algebra*, **35** (2007) 2719–2730.

[34] M. Giudici and J. Xu, All vertex-transitive locally-quasiprimitive graphs have a semiregular automorphism, *J. Algebr. Comb.*, **25** (2007) 217–232.

[35] M. Giudici and S. Kelly, Characterizing a family of elusive permutation groups, *J. Group Theory*, **12** (2009) 95–105.

[36] M. Giudici and G. Verret, *Semiregular automorphisms in arc-transitive graphs of valency* $2p$, in preparation.

[37] M. Giudici, P. Potočnik and G. Verret, Semiregular automorphisms of edge-transitive graphs, *J. Algebr. Comb.*, **40** (2014) 961–972.

[38] M. Giudici, L. Morgan, P. Potocnik and G. Verret, Elusive groups of automorphisms of digraphs of small valency,*European J. Combin.*, **64** (2015) 1–9.

[39] R. Guralnick, I. M. Isaacs and P. Spiga, On a relation between the rank and the proportion of derangements in finite transitive permutation groups, *J. Combin. Theory Ser. A*, **136** (2015) 198–200.

[40] R. Guralnick, M. Liebeck, J. Saxl and A. Shalev, Random generation of finite simple groups, *J. Algebra* **219** (1999) 345–355.

[41] R. Guralnick and D. Wan, Bounds for fixed point free elements in a transitive group and applications to curves over finite fields, *Israel J. Math.*, **101** (1997) 255–287.

[42] A. Hald, *A History of Probability and Statistics and Their Applications Before 1750*, Wiley, New York, 1990.

[43] A. Hujdurovič, K. Kutnar and D. Marušič, Vertex-transitive generalized Cayley graphs which are not Cayley graphs, *European J. Combin.*, **46** (2015) 45–50.

[44] I. M. Isaacs, T. M. Keller and M. L. Lewis, A. Moreto, Transitive permutation groups in which all derangements are involutions, *J. Pure Appl. Algebra*, **207** (2006) 717–724.

[45] J. R. Isbell, Homogeneous games, II, *Proc. Amer. Math . Soc.*, **11** (1960) 159–161.

[46] G. Jones and M. Klin, *On polycirculant graphs and groups*, University of Southampton, Preprint N340, 2000.

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

[47] C. Jordan, Recherches sur les substitutions, *J. Liouville*, **17** (1872) 351–367

[48] D. Jordan, Eine Symmetrieeigenschaft von Graphen, in: Graphentheorie und ihre Anwendungen, *Dresdner Reihe Forsch.*, **9** (1988) 17–20.

[49] M. Klin, *On transitive permutation groups without semi-regular subgroups*, ICM 1998: International Congress of Mathematicians, Berlin, 18-27 August 1998. Abstracts of short communications and poster sessions, 1998.

[50] N. Klingen, *Arithmetical Similarities–Prime Decomposition and Finite Group Theory*, Oxford Sci. Publ., Oxford Univ. Press, Oxford,1998.

[51] K. Kutnar and D. Marušič, Recent trends and future directions in vertex-transitive graphs, *Ars Math. Contemp.*, **1** (2008) 112–125.

[52] K. Kutnar and P. Šparl, Distance-transitive graphs admit semiregular automorphisms, *European J. Combin.*, **31** (2010) 25–28.

[53] J. H. Lambert, Examen d'une espéce de superstition ramenée au calcul des probabilités, *Nouveau Mém. Acad. Roy. Sci. et Belle-Lettres de Berlin*, (1773) 411–420.

[54] P. S. de Laplace, *Théorie Analytique des Probabilités*, Paris, 1812.

[55] A. K. Lenstra, H. W. Lenstra, Jr., *The development of the number field sieve*, Lecture Notes in Mathematics 1554, Springer-Verlag, Berlin, 1993.

[56] A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse and J. M. Pollard, The factorization of the ninth Fermat number, *Math. Comp.*, **61** (1993) 319–349.

[57] C. H. Li, Semiregular automorphisms of cubic vertex-transitive graphs, *Proc. Amer. Math. Soc.*,**136** (2008) 1905–1910.

[58] C. H. Li, C. E. Praeger, A. Venkatesh and S. Zhou, Finite locally-quasiprimitive graphs, *Discrete Math.*, **246** (2002) 197–218.

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

[60] D. Marušič, Semiregular automorphisms in vertex-transitive graphs with a solvable group of automorphisms, *Ars Math. Contemp.*, **13** (2017) 461–468.

[61] D. Marušič, Semiregular automorphisms in vertex-transitive graphs of order $3p^2$, *Electron. J. Combin.*, **25** (2018).

[62] D. Marušič and T. D. Parsons, Hamiltonian paths in vertex-symmetric graphs of order $5p$, *Discrete Math.*, **42** (1982) 227–242.

[63] D. Marušič and T. D. Parsons, Hamiltonian paths in vertex-symmetric graphs of order $4p$, *Discrete Math.*, **43** (1983) 91–96.

[64] D. Marušič and R. Scapellato, Permutation groups, vertex-transitive digraphs and semiregular automorphisms, *European . J. Combin.*, **19** (1998) 707–712.

[65] D. Marušič, R. Scapellato and N. Zagaglia Salvi, Generalized Cayley graphs, *Discrete Math.*, **102** (1992) 279–285.

[66] B. D. McKay and G .F. Royle, The transitive graphs with at most 26 vertices, *Ars Combin.*, **30** (1990) 161–176.

[67] K. Meagher, P. Spiga and P. H.Tiep, An Erdős-Ko-Rado theorem for finite 2-transitive groups, *European J. Combin.*, **55** (2016) 100–118.

[68] K. Meagher and P. Spiga, An Erdős-Ko-Rado theorem for the derangement graph of $\mathrm{PGL}_3(q)$ acting on the projective plane, *SIAM J. Discrete Math.*, **28** (2014) 918–941.

[69] A. de Moivre, *The Doctrine of Chances*, Third Edition, Millar, London, 1756. Reprinted by Chelsea, New York, 1967.

[70] P. R. Montmort, *Essay d'Analyse sur les Jeux de Hazard*, Paris, Jacque Quillau, 1708.

[71] P. R. Montmort, *Essay d'Analyse sur les Jeux de Hazard*, Second edition, Paris, Jacque Quillau 1713.

[72] T. Pisanski and B. Servatius, *Configurations from a graphical viewpoint*, Birkhäuser Advanced Texts Basler Lehrbücher Series, Birkhäuser Boston Inc., Boston, 2013.

[73] R. Perlis, On the equation $\zeta_K(s) = \zeta_K(s)$, *J. Number Theory*, **9** (1977) 342–360.

[74] J. S. Rose, *A course on group theory*, Cambridge University Press, Cambridge, 1978.

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585

[75] G. R. Sanchis, Swapping Hats: A Generalization of Montmort's Problem, *Mathematics Magazine*, **71** (1998) 53–57.

[76] R. Scapellato, *Vertex-transitive graphs and digraphs*, Graph symmetry: Algebraic methods and applications, Kluwer Academic Publisher, Netherlands, 1997 319–378.

[77] R. Scoville, The Hat-Check Problem, *The American Mathematical Monthly*, **73** (1966) 262–265.

[78] J-P. Serre, On a theorem of Jordan, *Bull. Amer. Math. Soc.*, **40** (2003) 429–440.

[79] P. Spiga, Permutation characters and fixed-point-free elements in permutation groups, *J. Algebra*, **299** (2006) 1–7.

[80] P. Spiga, Permutation 3-groups with no fixed-point-free elements, *Algebra Colloq.*, **20** (2013) 383–394.

[81] P. Spiga, Semiregular elements in cubic vertex-transitive graphs and the restricted Burnside problem, *Math. Proc. Cambridge Philos. Soc.*, **157** (2014) 45–61.

[82] L. Takács, The problem of coincidences, *Arch. Hist. Exact Sci.*, **21** (1979-1980) 229–244.

[83] G. Verret, Arc-transitive graphs of valency 8 have a semiregular automorphism, *Ars Math. Contemp.*, **8** (2015) 29–34.

[84] E. Waring, *An Essay on the Principles of Human Knowledge*, Cambridge, 1794.

[85] P. J. Weingberger and L. P. Rothschild, Factoring polynomials over algebraic number fields, *ACM Trans. Math. Software*, **2** (1976) 335–350.

[86] H. W. Wielandt, *Permutation groups through invariant relations and invariant functions*, Lecture Notes, Ohio State University, 1969. Also publised in: Wielandt, Helmut, Mathematische Werke (Mathematical works), **1** Group theory, Walter de Gruyter & Co., Berlin, 1994 237–296.

[87] H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1966.

[88] J. Xu, Semiregular automorphisms of arc-transitive graphs with valency pq, *European J. Combin.*,**29** (2008) 622–629.

[89] J. Xu, On elusive permutation groups of square-free degree, *Comm. Algebra*, **37** (2009) 3200–3206.

Majid Arezoomand

Department of Engineering, University of Larestan, 74317-16137, Lar, Iran

Email: arezoomand@lar.ac.ir

Alireza Abdollahi

Department of Mathematics, University of Isfahan, 81746-73441, Isfahan, Iran

Email: a.abdollahi@math.ui.ac.ir

Pablo Spiga

Dipartimento di Matematica e Applicazioni, University of Milano-Bicocca, Via Cozzi 55, 20125, Milan, Italy

Email: pablo.spiga@unimib.it

DOI: http://dx.doi.org/10.22108/toc.2018.112665.1585