Michigan Math. J. 58 (2009)

Primitive Permutation Groups and Their Section-Regular Partitions

Peter M Neumann

Dedicated to the memory of Donald G. Higman

1. Introduction

The study reported here arises out of a question asked by João Araújo (Lisbon) in an e-mail message of 19 October 2006. Let X be a finite set and let G be a group of permutations of X, that is, a subgroup of $\mathrm{Sym}(X)$. A partition of X as a disjoint union of non-empty pairwise disjoint subsets corresponds to an equivalence relation, and we shall move freely between the two concepts, using ρ to stand either for the relation or for the partition, as context demands. A section (or transversal) of ρ is then a subset S of X that contains precisely one element from each class of ρ. Given a relation ρ and one of its sections S, the two conditions

$$S^g \text{ is a section of } \rho \text{ for all } g \in G, \qquad S \text{ is a section of } \rho^g \text{ for all } g \in G$$

are of course equivalent. A relation ρ for which there exists a section S such that this condition is satisfied will be called *section-regular* relative to G or sometimes *G-regular.* In this language Araújo's question is

> *is it true that if G is primitive on X then there are no non-trivial proper G-regular partitions of X?*

The short answer is no. As usual, however, much lies behind this monosyllable.

The context of the question is this. Call the group G *synchronizing* if $G \neq \{1\}$ and there are no non-trivial proper G-regular partitions of X. Although formally different, this is in effect the same as a definition made by Araújo in his work on semigroups and automata (see Section 6 of this paper). Clearly, if G is intransitive then the partition of X into orbits is section-regular relative to G. Similarly, if G is transitive but imprimitive and ρ is a non-trivial proper G-invariant partition then ρ is section-regular with respect to G. Thus we have the very simple observation that

> *if G is a synchronizing group then G is primitive on X,*

and Araújo's question is whether the converse is true.

This paper describes a preliminary study of the situation. It contains some general analysis, descriptions of a number of examples, a proof that, in quite a strong sense, for most n all primitive groups of degree n are synchronizing, and some

Received July 18, 2007. Revision received February 4, 2008.

notes suggesting further lines of investigation. Although it is far from being a definitive account, I hope that it might be of some use in the theory of semigroups and automata from which the question it treats originally emerged.

ACKNOWLEDGMENT. I am most grateful to Dr Araújo for raising the question, for helpful comments on earlier drafts of this paper, and especially for supplying references and advice in connection with Section 6.

2. Some Analysis

Before describing some examples of primitive groups that are not synchronizing, we analyse section-regular partitions for transitive groups. An equivalence relation ρ will be said to be *uniform* if all its classes have the same cardinality—and then $|\rho|$ will denote this number.

THEOREM 2.1. *Suppose that G is transitive on X. A section-regular partition for G is uniform.*

Proof. Let ρ be a section-regular partition for G with classes $R_1, \dots, R_s$, and let $r_i := |R_i|$ for $1 \le i \le s$. We may suppose that $r_1 \le r_2 \le \cdots \le r_s$. Then

$$|X| = r_1 + r_2 + \cdots + r_s \ge sr_1, \tag{$\star$}$$

and $|X| = sr_1$ only if $r_i = r_j$ for all i and j. Let S be a section of ρ that witnesses its G-regularity and for $1 \le i \le s$ let $x_i \in S \cap R_i$, so that in fact $S \cap R_i = \{x_i\}$ and $S = \{x_1, x_2, \dots, x_s\}$. Let H_i be the stabiliser of x_i in G. By assumption, if $g \in G$ then $|S^g \cap R_1| = 1$ and it follows that

$$G = \bigcup_{i=1}^{s} \bigcup_{y \in R_1} \{g \in G \mid x_i^g = y\}.$$

Thus G is a union of s sets, of which the ith is itself a union of r_1 cosets of H_i. Since G is transitive, $|H_i| = |G|/|X|$ for all i and so we find that

$$|G| \le s \times r_1 \times \frac{|G|}{|X|},$$

that is, $|X| \le sr_1$. It follows that equality holds in ($\star$) and therefore $r_1 = r_2 = \cdots = r_s$, that is, ρ is uniform as the theorem states. □

COROLLARY 2.2. *If G is transitive and ρ is a non-uniform partition then ρ is not section-regular for G.*

This tells us that in quite a strong sense if G is transitive then "most" partitions are not G-regular. In particular, we have the following result.

COROLLARY 2.3. *If G is transitive and $|X|$ is prime then G is a synchronizing group.*

The theorem takes us a first small step toward classifying section-regular partitions ρ for primitive (indeed transitive) groups G. Except in Lemma 2.6, from now on we focus entirely on non-trivial proper uniform partitions ρ of X. We shall maintain the following notation as standard:

$$n := |X|, \quad r := |\rho|, \quad s := |X/\rho|,$$

so that n is the degree of the permutation group G and $n = rs$. Also $r > 1$ since ρ is non-trivial, and $s > 1$ since ρ is a proper partition. The triple (n, r, s) will be called the parameters of G, X, and ρ. The following lemma excludes the possibilities $r = 2$ and $s = 2$ from our further consideration.

Lemma 2.4. *Suppose that G is primitive and ρ is a non-trivial proper G-regular partition of X with parameters (n, r, s). Then $r > 2$ and $s > 2$.*

Proof. Let S be a section of ρ that witnesses its regularity. Suppose first, seeking a contradiction, that $s = 2$. In this case S is an unordered pair and we consider the graph Γ with vertex set X and edge set S^G. This is an orbital graph for Γ (see for example [4, Sec. 1.11; 7, Sec. 3.2; 13, Sec. 2]) and by a famous lemma of D. G. Higman it is connected (see [9, (1.12); 4, Theorem 1.9; 7, Theorem 3.2A; 13, Lemma 3]). Let R_1 and R_2 be the two classes of ρ. Since S^g is a section of ρ for all $g \in G$, if $x \in R_1$ then any path of even length starting from x will end in R_1 and any path of odd length will end in R_2. Therefore Γ is bipartite with R_1 and R_2 as its two parts, and any graph automorphism either fixes each of R_1 and R_2 setwise or interchanges R_1 and R_2. Since Γ admits G as a group of automorphisms, ρ is G-invariant. This contradicts the primitivity of G and proves that our assumption is untenable. That is, $s > 2$.

Suppose now that $r = 2$. Define $S_1 := S$ and $S_2 := X \setminus S$. Then $S_1 \cup S_2$ is a partition σ of X. Since S witnesses the G-regularity of ρ, we find that any equivalence class R of ρ witnesses that σ is G-regular. This, however, contradicts what has just been proved. Therefore $r > 2$. □

Corollary 2.5. *If G is primitive on X and $|X| = 2p$, where p is prime, then G is synchronizing.*

Viewed in the light of a theorem of Helmut Wielandt, this is perhaps not surprising. In [18] he proves that a primitive group of degree $2p$ is almost always 2-transitive. In fact, using CFSG (the classification of the finite simple groups), one can refine his theorem and show that all primitive groups of degree $2p$ are 2-transitive except in case $p = 5$. And it is almost trivial that a 2-transitive group is always synchronizing.

The idea of the proof of Lemma 2.4 can be extended. Given an equivalence relation ρ on X define

$$E_\rho := \{\{x^g, y^g\} \in X^{\{2\}} \mid x \equiv y \pmod{\rho},\ x \neq y,\ g \in G\}$$

and given $S \subseteq X$ define

$$E_S := \{\{x^g, y^g\} \in X^{\{2\}} \mid x, y \in S,\ x \neq y,\ g \in G\}.$$

Here $X^{\{2\}}$ is the set of unordered pairs, that is 2-subsets, from X. Then define Γ_ρ and Γ_S to be the graphs with vertex set X and with edge sets E_ρ and E_S, respectively. It should be clear that $G \leq \mathrm{Aut}(\Gamma_\rho)$ and $G \leq \mathrm{Aut}(\Gamma_S)$. The following simple lemma provides a link with suborbit theory [4, Sec. 1.11; 7, Sec. 3.2; 13, Sec. 2] and hence a means of studying G-regular partitions for primitive groups G. Although I perceive it as a tool for analysing primitive groups, the lemma is formulated in rather general terms. This responds to a question of a referee, whose interest I gratefully acknowledge. Recall that a clique in a graph is a complete subgraph—that is, a set of vertices any two of which are joined by an edge.

LEMMA 2.6. *Suppose that $G \leq \mathrm{Sym}(X)$ and that ρ is a G-regular partition of X as witnessed by a section S. Then*

(1) *S is a largest clique in Γ_S, and*
(2) *if S meets every G-orbit in X, and in particular if G is transitive on X, then every part of ρ is a maximal clique in Γ_ρ.*

Proof. That S is a clique of Γ_S is clear. Let S' be a subset of X with $|S'| > |S|$. Since ρ has $|S|$ parts, there must be one of its parts that contains two distinct members x and y of S'. Then x and y do not both lie in any G-transform of S, and so $\{x, y\}$ is not an edge of Γ_S. Therefore S' is not a clique, and so S is a largest clique in Γ_S.

For (2) suppose that S meets every G-orbit in X and let R be one of the parts of ρ. That R is a clique in Γ_ρ is clear. Let $x \in X \setminus R$. There is a G-translate of S that contains x and without loss of generality this may be assumed to be S itself. Let $y \in R \cap S$ (so that in fact $R \cap S = \{y\}$). If $\{x, y\}$ were an edge of Γ_ρ then there would exist $g \in G$ such that $x^g \equiv y^g \pmod{\rho}$, but this contradicts the fact that S^g is a section of ρ for all $g \in G$. Thus $R \cup \{x\}$ is not a clique in Γ_ρ and it follows that R is a maximal clique. This proves (2). □

We finish this section with an observation of a rather different kind.

OBSERVATION 2.7. *Suppose that G is primitive on X, but has a subgroup K of index 2 that is imprimitive. If ρ is a non-trivial proper K-congruence on Ω then ρ is section-regular with respect to G. In particular, G is not synchronizing.*

Proof. Since ρ is K-invariant but not G-invariant the orbit ρ^G consists of precisely two partitions, ρ_1 and ρ_2. Since G is primitive K is transitive, and ρ_1 and ρ_2, which are K-congruences, are therefore uniform. Then, by a theorem of König (1916), there is a subset S of X that is a section of each of the two members of ρ^G, and therefore ρ is G-regular. König's original statement of his theorem [10, Satz A] is that a regular bipartite graph has a 1-factor, but it is easy to see that this implies the required result (see Hall [8] for the exact form of the result needed here, for comment, and for further references). □

This observation yields a considerable number of primitive non-synchronizing groups, some of which are mentioned explicitly in the next section.

3. Some Examples

This section is devoted to descriptions of some examples of G-regular partitions for primitive groups. As a guide, the reader should bear in mind the O'Nan–Scott taxonomy of finite primitive permutation groups: very roughly, there are those of affine type (having an elementary abelian regular normal subgroup); there are those that have two distinct regular normal subgroups; there are those that are subgroups of wreath products $H \operatorname{wr} \operatorname{Sym}(k)$ in product action, where H is almost simple; there are those with a unique non-abelian minimal normal subgroup but regular subnormal subgroups ("diagonal type"); and there are the almost simple groups. It is a theory much more than merely a theorem and many treatments are available—see [4, Chap. 4; 7, Chap. 4] and the references quoted there. Our first example, which is also the smallest (both in degree and order), is a group of affine type with parameters $(9, 3, 3)$.

Example 3.1. Let V be a vector space of dimension 2 over the field $\mathbb{F}_3$ of size 3. Take X to be V construed as $\mathrm{AG}(2, 3)$, the affine plane over $\mathbb{F}_3$. Recall that affine transformations are permutations of V of the form $f_{A,b}\colon x \mapsto xA + b$, where $A \in \mathrm{GL}(V)$ and $b \in V$. If we take V to be the space of 1×2 row vectors then $\mathrm{GL}(V)$ is the group $\mathrm{GL}(2, 3)$ of 2×2 invertible matrices over $\mathbb{F}_3$, with matrices acting on row vectors by right multiplication.

Let $U := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, so that $U^2 = -I$ and $U^4 = I$. Define $H := \{I, U, U^2, U^3\} = \{\pm I, \pm U\}$. Then H is a cyclic subgroup of $\mathrm{GL}(2, 3)$ of order 4, and, as is easy to see, it is irreducible as linear group—that is, there are no non-zero proper H-invariant subspaces of V. Now define

$$G := \{f_{A,b} \mid A \in H,\ b \in V\}.$$

Thus G is the semidirect product (split extension) of the translation group T by H. Because H is irreducible as a linear group G is primitive as a permutation group. Take ρ_x to be the partition whose classes are the lines parallel to the x-axis. Thus

$$(x_1, y_1) \equiv (x_2, y_2) \pmod{\rho_x} \iff y_1 = y_2.$$

Since ρ_x is preserved by every translation and also by U^2 we find that for all $g \in G$ either $\rho_x^g = \rho_x$ or $\rho_x^g = \rho_y$, where

$$(x_1, y_1) \equiv (x_2, y_2) \pmod{\rho_y} \iff x_1 = x_2.$$

Define $\rho := \rho_x$ and $S := \{(0,0), (1,1), (2,2)\}$, the line with equation $x = y$. Then since S is a section both of ρ_x and of ρ_y, it is a section of ρ^g for all $g \in G$. Thus although G is primitive there is a non-trivial proper G-regular partition of X. Here $n = 9$ and $r = s = 3$. Note that this example can be seen as an instance of Observation 2.7.

Example 3.1 can be considerably generalised. First, taking X to be the affine plane $\mathrm{AG}(2, q)$ over the finite field $\mathbb{F}_q$, we get examples with parameters (q^2, q, q) as follows. The parallel classes of affine lines in X are the points of $\mathrm{PG}(1, q)$, the projective line over $\mathbb{F}_q$, which may be identified with the set Λ_∞ of "points at infinity" on the affine lines. Note that $\mathrm{GL}(2, q)$ maps parallel classes to parallel classes, so it acts on Λ_∞ (as the projective group $\mathrm{PGL}(2, q)$). Take $H \le \mathrm{GL}(2, q)$ such that its action on Λ_∞ is not transitive and has no orbit of size 1. The latter condition is necessary and sufficient to ensure that H is irreducible as linear group, that is as subgroup of $\mathrm{GL}(2,q)$, and therefore that the group $G := T.H$ (where T is the translation group as before) is a primitive subgroup of $\mathrm{Sym}\,X$. Such groups H will always exist if $q > 2$: for example H could be the monomial group consisting of all matrices $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & a \\ b & 0 \end{smallmatrix}\right)$ where $ab \neq 0$. Now let ρ be a parallel class of lines in X and let π_ρ be the corresponding point of the line at infinity Λ_∞. Then $\{\rho^g \mid g \in G\}$ is the set of parallel classes corresponding to the points π_ρ^h for $h \in H$. Since H is not transitive on Λ_∞ there exists a point $\sigma \in \Lambda_\infty$ not in this H-orbit. We take S to be an affine line that has σ as its point at infinity. Then S is a section of ρ^g for all $g \in G$, and so ρ is G-regular.

Examples can also be created from higher-dimensional affine spaces. Let V be a d-dimensional vector space over $\mathbb{F}_q$, where $q > 2$ and $d \geq 2$. Take X to be V construed as the affine space $\mathrm{AG}(d,q)$. For each k in the range $1 \leq k \leq d-1$ there is a primitive subgroup G of $\mathrm{AGL}(d,q)$ for which there is a partition ρ of X into parallel k-dimensional affine subspaces that is section-regular. The group G will be constructed as $T.H$, where T is the translation group and H is a suitable subgroup of $\mathrm{GL}(d,q)$. What is required of H is, first, that it is irreducible as linear group. This ensures that G is primitive as subgroup of $\mathrm{Sym}(X)$. Further requirements on H may be expressed in terms of its action on the $(d-1)$-dimensional projective space Λ_∞ of points at infinity on the affine lines in X. Namely, there should exist a $(d-k-1)$-flat Z of Λ_∞ and an H-orbit Y in the set of $(k-1)$-flats of Λ_∞, every member of which is disjoint from Z. Such groups always exist. For example, the group of $d \times d$ monomial matrices (matrices that have a single non-zero entry in each row and column), which is isomorphic to the wreath product $\mathbb{F}_q^\times \mathrm{\,wr\,} \mathrm{Sym}(d)$, is irreducible (this is one of the points where the condition $q > 2$ is required), and it meets the geometric requirement with Z equal to the set of points at infinity on the affine $(d-k)$-space

$$\left\{(x_1, x_2, \ldots, x_d) \mid x_1 = x_2 = \cdots = x_{k-1} = \sum x_i = 0\right\}$$

and Y equal to the orbit of the set of points at infinity on the k-space

$$\{(x_1, x_2, \ldots, x_d) \mid x_{k+1} = x_{k+2} = \cdots = x_d = 0\}.$$

For $\Pi \in Y$ define ρ_Π to be the partition of X into the corresponding parallel class of k-spaces, and take ρ to be ρ_Π for some $\Pi \in Y$. Take S to be the $(d-k)$-subspace of X corresponding to $Z \subseteq \Lambda_\infty$. Then S will be witness to the G-regularity of ρ. The parameters of this example are (q^d, q^k, q^{d-k}).

Two questions, which we shall not pursue here, arise from these constructions. First, what can be done with affine groups over $\mathbb{F}_2$? And secondly, is it true that if G is a primitive subgroup of $\mathrm{AGL}(d,p)$ (where now p is prime), then every section-regular partition is a parallel class of subspaces?

It is possible to manufacture new examples from old in a very natural way using product actions of wreath products.

EXAMPLE 3.2. Let G_0 be a primitive permutation group on a set X_0, let ρ_0 be a G_0-regular partition of X_0 as witnessed by a section S_0, and let k be a positive integer. Define $G := G_0 \mathrm{\,wr\,} \mathrm{Sym}(k)$ and $X := X_0^k$. Then G has a natural action on

X and this is primitive provided that G_0 is not cyclic of prime order (see for example [4, Thm. 4.5; 7, Lemma 2.7A]). By Corollary 2.3, the condition that G_0 is not cyclic of prime order will certainly be met if ρ_0 is a non-trivial proper partition. Define $\rho := \rho_0^k$, that is,

$$(x_1, \ldots, x_k) \equiv (y_1, \ldots, y_k) \pmod{\rho} \iff x_i \equiv y_i \pmod{\rho_0} \text{ for } 1 \le i \le k,$$

and $S := S_0^k$. One easily checks that S^g is a section of ρ for all $g \in G$, and so ρ is a G-regular partition. If the parameter set of ρ_0 is (n_0, r_0, s_0) then ρ will have parameters (n_0^k, r_0^k, s_0^k).

Next we have examples where the primitive group G has two distinct (necessarily non-abelian and regular) minimal normal subgroups.

Example 3.3. Take $A := \mathrm{Alt}(5)$, the simple group of order 60. Take $X := A$ and $G := A \times A$ acting on X by left and right multiplication, $x^{(a,b)} := a^{-1}xb$. This is the same as the group of "inner affine transformations" of A given by $f_{a,b}\colon x \mapsto x^a b$, where $x^a := a^{-1}xa$. It is well known and easy to prove that, because A is simple, G is primitive on X. Let $B := \mathrm{Alt}(4) \le A$ and take ρ to be the partition of X into right cosets of B. We find that if $g = f_{a,b} \in G$ then ρ^g is the partition of X into right cosets of the conjugate subgroup B^a. Therefore if C is a subgroup of order 5 in A then, thought of as subset of X, C is a section of ρ^g for all $g \in G$, and hence ρ is section-regular for G. Here the parameters are $(60, 12, 5)$, but if the roles of B and C are interchanged then an example with parameters $(60, 5, 12)$ emerges.

This example may obviously be generalised. First, the group A can be any simple group that admits a non-trivial factorisation $A = BC$, where B and C are subgroups such that $B \cap C = \{1\}$. Such factorisations have been catalogued by Liebeck, Praeger, and Saxl [11]. They give section-regular partitions with parameter sets $(|A|, |B|, |C|)$, the first few of which are $(60, 12, 5)$, $(60, 5, 12)$, $(168, 24, 7)$, $(168, 7, 24)$, $(504, 56, 9)$, and $(504, 9, 56)$. Next, for any natural number m, using the wreath product construction of Example 3.2 one may create examples of primitive groups G having two different minimal normal subgroups, each of which is a direct product of m simple groups isomorphic to A, such that G admits non-trivial proper section-regular partitions.

A very slight modification gives examples of groups of diagonal type having a unique minimal normal subgroup. All that is needed is to replace the group G of Example 3.3 with the group $A \operatorname{wr} C_2$ thought of as $(A \times A).\{\pm 1\}$ acting on X (which, recall, was the simple group A) by

$$x^{(a,b,\varepsilon)} := (a^{-1}xb)^{\varepsilon}.$$

The same partition ρ as in Example 3.3 is section-regular for this extended group G. And of course this example may be generalised by using as ingredient an arbitrary factorisable simple group A, and then using the construction of Example 3.2 to create examples of diagonal type and with arbitrarily complicated minimal normal subgroups.

In the next examples the group G is a wreath product in product action. The case where the parameter k is 2 is an instance of the phenomenon treated in Observation 2.7.

EXAMPLE 3.4. Let H be a primitive group (not cyclic of prime order) acting on a set Y, let $k \geq 2$, and let K be a transitive subgroup of $\mathrm{Sym}(k)$. Take $X := Y^k$ and take G to be the wreath product $H \operatorname{wr} K$ acting on X. Thus G is the split extension of H^k by K acting to permute the k factors of the direct power, and G acts on Y^k in the natural way. It is well known and easy to prove (see Example 3.2 for references) that G will be primitive on X—this is where the fact that H is not cyclic of prime order is relevant. For $1 \leq i \leq k$, define ρ_i by the condition

$$(y_1, \ldots, y_k) \equiv (z_1, \ldots, z_k) \pmod{\rho_i} :\Longleftrightarrow y_i = z_i,$$

and let S be the diagonal $\{(y, \ldots, y) \in X \mid y \in Y\}$. If $\rho := \rho_1$ then $\rho^G = \{\rho_1, \ldots, \rho_k\}$ and, since S is a section of ρ_i for every i, it is a section that witnesses the G-regularity of ρ. Here the parameters are (m^k, m^{k-1}, m), where $m := |Y|$.

There are also examples coming from the last of the O'Nan–Scott categories, the class of almost simple groups.

EXAMPLE 3.5. Let q be any prime power and let $G := \mathrm{PGL}(3, q).2$, the extension of the group of invertible 3×3 matrices (modulo scalars) over the field of size q by a cyclic group of order 2 whose generator acts as the inverse-transpose automorphism. This group acts on the set X of flags (incident point-line pairs) of the projective plane $\mathrm{PG}(2, q)$, with inverse transpose acting as a polarity that interchanges points and lines. It is not hard to see that it acts primitively on X. Now take ρ_1 to be the partition of X where two flags are equivalent if they have the same point and ρ_2 the partition where they are equivalent if they have the same line. Clearly, elements of $\mathrm{GL}(3, q)$ preserve each of ρ_1 and ρ_2. But the polarity interchanges points and lines and therefore if $\rho := \rho_1$ then ρ^G has size 2 and so ρ is G-regular by Observation 2.7. In this example the parameters are $((q+1)(q^2+q+1), q+1, q^2+q+1)$; the smallest has $q = 2$ and parameters $(21, 3, 7)$.

EXAMPLE 3.6. Let $G := \mathrm{Sym}(7)$, and let H be its subgroup $C_7.C_6$. This is the normaliser of a Sylow 7-subgroup; it can be thought of as $\mathrm{AGL}(1, 7)$. It is well known that H is maximal in G and therefore G acts primitively on its coset space X. Let $K := \mathrm{Alt}(7) \leq G$ and let $L := K \cap H$. Now L is not maximal in K because it is contained in a group isomorphic to $\mathrm{PSL}(2, 7)$ (which is the same as $\mathrm{SL}(3, 2)$ in its natural action on the seven points of the Fano plane $\mathrm{PG}(2, 2)$). Therefore there is a K-invariant equivalence relation ρ, which must be G-regular by Observation 2.7. Its parameters are $(120, 8, 15)$.

Similar examples to this last one can be made with the symmetric group of prime degree p whenever there exists a non-soluble transitive proper subgroup H of $\mathrm{Alt}(p)$ in which the Sylow p normalisers have order $\frac{1}{2}p(p-1)$. For then the group $\mathrm{AGL}(1,p)$ will be maximal in $\mathrm{Sym}(p)$ (supplement what is to be found in [14, Chap. 10] with an easy consequence of CFSG), so that the action of $\mathrm{Sym}(p)$ on its coset space will be primitive, whereas $\mathrm{AGL}(1,p) \cap \mathrm{Alt}(p)$ is contained in (a conjugate of) H and so is not maximal in $\mathrm{Alt}(p)$. In addition to the example with $p = 7$ described previously there are examples for $p = 11$, where H can be $\mathrm{PSL}(2,11)$ or the Mathieu group M_{11}; for degree 17, with $H = \Sigma\mathrm{L}(2,16)$, the extension of $\mathrm{SL}(2,16)$ by a cyclic group of order 4 acting by field automorphisms; and for degree 23, with H the Mathieu group M_{23}.

Our last classes of examples are of a rather different kind.

Example 3.7. Let m be a composite positive integer, $m = rt$ where $2 \le t < \frac{1}{2}m$. Take G to be $\mathrm{Sym}(m)$ or $\mathrm{Alt}(m)$, and take $X := [1,m]^{\{t\}}$, the set of t-subsets of $[1,m]$ (where $[1,m] := \{1,2,\ldots,m\}$). By a theorem of Zs. Baranyai (see [2] or [3, Chap. 1]), there is a partition ρ of X such that each class of ρ is a partition of $[1,m]$ (into r sets of size t of course). Now take $S := \{x \in X \mid 1 \in x\}$. Clearly, for any $g \in G$, $S^g = \{y \in X \mid 1^g \in y\}$, and, as each class of ρ contains precisely one t-set containing 1^g, S^g is a section of ρ. Thus ρ is section-regular with respect to G. Its parameters are $\left(\binom{m}{t}, r, \binom{m-1}{t-1}\right)$.

4. The Rarity of Primitive Non-synchronizing Groups

Let E_0 be the set of natural numbers n for which there exists a primitive group G of degree n admitting a non-trivial proper section-regular partition—that is, a primitive group that is not synchronizing. Trivially, such a group G cannot be 2-transitive (nor even 2-homogeneous), and therefore $E_0 \subseteq E$, where E is the set of all n for which there exists a primitive group of degree n other than $\mathrm{Sym}(n)$ or $\mathrm{Alt}(n)$. This set E was the subject of a study by Cameron, Neumann, and Teague [6]. They showed that E has density 0. More precisely, they showed that if $e(x)$ is the number of $n \in E$ such that $n \le x$, and $\pi(x)$ is, as usual, the number of prime numbers $\le x$, then

$$e(x) = 2\pi(x) + \left(1+\sqrt{2}\right)\sqrt{x} + O\left(\frac{\sqrt{x}}{\log x}\right),$$

so that $e(x) \sim 2x/\log x$ as $x \to \infty$. One of the contributions $\pi(x)$ comes from prime values of n. By Corollary 2.3 these do not lie in E_0, however. The second contribution $\pi(x)$ comes from numbers $n = p+1$ where p is prime, arising from the groups $\mathrm{PSL}(2,p)$ and $\mathrm{PGL}(2,p)$ in their natural representations on $\mathrm{PG}(1,p)$. These groups are 2-transitive and therefore do not contribute to E_0. The proof of the theorem in [6] therefore yields the following. Defining

$$e_0(x) := |\{n \in E_0 \mid n \le x\}|$$

we have $e_0(x) \le \left(1+\sqrt{2}\right)\sqrt{x} + O\left(\sqrt{x}/\log x\right)$. This is, however, an overestimate for $e_0(x)$. Example 3.4 with $H = \mathrm{Sym}(m)$ and $k = 2$ witnesses that $m^2 \in E_0$ for every $m \ge 3$. Certainly therefore $e_0(x) \ge \sqrt{x} - O(1)$. But the term $\sqrt{2}\sqrt{x}$ in the Cameron–Neumann–Teague theorem comes from binomial coefficients $m(m-1)/2$. Some of these may be realised as the degrees of primitive permutation representations of the groups $\mathrm{PSL}(2,q)$ acting on coset spaces for dihedral subgroups of index $q(q-1)/2$ and $q(q+1)/2$, and some may arise accidentally as degrees of other primitive groups, but mostly they arise from $\mathrm{Alt}(m)$ or $\mathrm{Sym}(m)$ acting on the set of pairs. Thus the following result suggests that perhaps only those binomial coefficients $m(m-1)/2$ in which m is even really contribute to E_0.

LEMMA 4.1. *Let m be an odd integer $2k+1 \geq 5$, let $X := [1,m]^{\{2\}}$, the set of pairs from $[1,m]$, and let G be an at least 4-fold transitive subgroup of $\mathrm{Sym}(m)$, thought of as a subgroup of $\mathrm{Sym}(X)$. Then there are no non-trivial proper G-regular partitions of X, so G is a synchronizing group.*

Proof. Since G is 4-fold transitive on $[1,m]$ it is a rank-3 permutation group on X. That is to say, it has three orbits in X^2: one is the diagonal (known as the "trivial orbital"); another is Δ_1 where

$$\Delta_1 := \{(x,y) \in X^2 \mid x \cap y \text{ is a singleton}\},$$

and the third is Δ_2 where

$$\Delta_2 := \{(x,y) \in X^2 \mid x \cap y = \emptyset\}.$$

Note that Δ_1 and Δ_2 are self-paired in the sense that if $(x,y) \in \Delta_i$ then also $(y,x) \in \Delta_i$. The graphs Γ_1 and Γ_2 that have vertex set X and edge sets Δ_1 and Δ_2 respectively are the two non-trivial orbital graphs of G acting on X. Since Δ_1 and Δ_2 are self-paired we may construe these as undirected graphs.

Now suppose, seeking a contradiction, that there existed a G-regular partition ρ of X, as witnessed by a section S. The edge sets of the graphs Γ_ρ and Γ_S introduced for Lemma 2.6 are disjoint and are unions of G-orbits on pairs. It follows that these graphs must be the orbital graphs Γ_1 and Γ_2. Therefore we look for the maximal cliques in Γ_1 and Γ_2.

It is easy to see that there are two kinds of maximal clique in Γ_1: triangles of the form $\{\{a,b\},\{a,c\},\{b,c\}\}$ and $(m-1)$-cliques of the form $\{\{a,x\} \mid x \neq a\}$. It is equally easy to see that there is just one kind of maximal clique in Γ_2, namely, k-cliques of the form $\{\{a_1,b_1\},\dots,\{a_k,b_k\}\}$, where $a_1,\dots,a_k,b_1,\dots,b_k$ are distinct and hence are all except one of the members of $[1,m]$. By Lemma 2.6 there are three possibilities for the pair (r,s), namely $(3,k)$, $(m-1,k)$, and $(k,m-1)$. In all cases the equation $rs = n = m(m-1)/2 = mk$ is contradicted, however. This proves the lemma. □

As sketched in the paragraph before the statement of the lemma this leads to the following asymptotic result.

THEOREM 4.2. $e_0(x) = \big(1 + 1/\sqrt{2}\big)\sqrt{x} + O(\sqrt{x}/\log x)$.

The proof is very similar to that of the main theorem of [6] and will therefore only be sketched.

We have seen that if $m \geq 3$ then $m^2 \in E_0$ and $m(2m-1) \in E_0$. Coincidences $m_1^2 = m_2(2m_2-1)$ arise only from solutions of the familiar diophantine equation

$u^2 - 2v^2 = -1$, and the theory associated with Pell's Equation tells us that there are $O(\log x)$ of them below a given number $x > 1$. It follows immediately that

$$e_0(x) \geq \big(1 + 1/\sqrt{2}\big)\sqrt{x} - O(\log x).$$

Since $\log x = o(\sqrt{x}/\log x)$ it remains to find an acceptable upper bound for $e_0(x)$.

Define E_1 to be the set of positive integers n for which there is an almost simple primitive non-synchronizing group of degree n (note that the notation here differs from that in [6]). Also, as in [6], define

$$E_2 := \{m^k \mid m, k \in \mathbb{N},\ m \geq 2,\ k \geq 2,\ m^k > 4\},$$

$$E_3 := \{n \in \mathbb{N} \mid \text{there is a non-abelian simple group of order } n\},$$

and define

$$e_i(x) := |\{n \in E_i \mid n \leq x\}|.$$

By the O'Nan–Scott theorem $E_0 \subseteq E_1 \cup E_2 \cup E_3$ and therefore $e_0(x) \leq e_1(x) + e_2(x) + e_3(x)$. It is shown in [6] that $e_2(x) \leq \sqrt{x} + O(\sqrt[3]{x})$ and $e_3(x) \leq O(\sqrt[3]{x})$. It remains therefore to show that $e_1(x) \leq \big(1/\sqrt{2}\big)\sqrt{x} + O(\sqrt{x}/\log x)$.

Following [6] we define E_4 to be the set of natural numbers n for which there exists a primitive permutation group of degree n that is almost simple but not alternating or symmetric, and $e_4(x)$ to be the number of its members less than x. There are three types of group that contribute significantly to E_4. First there are alternating and symmetric groups acting on pairs, but by Lemma 4.1 the only contribution from these to E_0 consists of the binomial coefficients $k(2k-1)$, and these contribute $\big(1/\sqrt{2}\big)\sqrt{x} + O(1)$ to $e_1(x)$. The other two types are the groups $\mathrm{PSL}(2, p)$ or $\mathrm{PGL}(2, p)$ acting on coset spaces of dihedral subgroups of index $p(p-1)/2$ or index $p(p+1)/2$, where p is prime and $p \geq 5$. The numbers $p(p+1)/2$ are already counted among the binomial coefficients $k(2k-1)$; of the others, however, there are at most $\pi\big(\sqrt{2x}\big)$ below x and so their contribution to $e_1(x)$ is at most $O(\sqrt{x}/\log x)$. The contribution to $e_4(x)$ from groups other than these three types is $o(\sqrt{x}/\log x)$. It follows that $e_1(x) \leq \big(1/\sqrt{2}\big)\sqrt{x} + O(\sqrt{x}/\log x)$, as required.

5. Final Comments

Note 5.1. Although Section 3 exhibits many primitive permutation groups that are not synchronizing, so far the only synchronizing primitive groups we have seen are those of prime degree, doubly transitive groups (or, a little more generally, doubly homogeneous groups), and the examples in Lemma 4.1. The method of proof of that lemma should be sufficient to decide of every rank-3 group G whether or not it is synchronizing, and if not, to find all G-regular partitions. Note that the primitive rank-3 groups have been classified modulo CFSG in major works by Kantor and Liebler (almost simple classical groups over finite fields), Liebeck (groups of affine type), and Liebeck and Saxl (most of the rest)—see [12] for context and references. The method of proof of Lemma 4.1 will also deal with the actions of $\mathrm{Sym}(m)$ and $\mathrm{Alt}(m)$ on the set of k-sets from $[1, m]$ for $2 \leq k < m/2$.

Note 5.2. It seems possible that, using the O'Nan–Scott theorem, one might be able to classify the primitive groups G for which there exists a non-trivial proper section-regular partition, and hence, perhaps, all those for which there is no nontrivial proper section-regular partition, that is, those that are synchronizing. I do not propose to embark on such a project, but hope that what I have written here might start someone else off. In particular, it seems possible that the techniques suggested in Section 2 might be enough to classify all possible G-regular partitions for primitive groups G of small rank (say rank ≤ 6) or with parameters (n, r, s) where r is small or s is small (say $r \leq 6$ or $s \leq 6$).

NOTE 5.3. In many cases, when we have found a G-regular partition with parameters (n, r, s) for a primitive group G, we have also found such a partition with parameters (n, s, r). It would be surprising if this always happens. In particular, it would be surprising if the group $\mathrm{PGL}(3, q).2$ of Example 3.5 had a section-regular partition with parameters $((q+1)(q^2+q+1), q^2+q+1, q+1)$. A special case seems particularly interesting and promising as a line of investigation. Consider a pair (ρ, σ) of partitions of X with the property that every σ-class S witnesses G-regularity of R. Then also every ρ-class R will witness that σ is G-regular. Such a pair will be called *sympathetic*. Sympathetic pairs of G-regular partitions appear among the examples of groups of affine type (Example 3.1 and its generalisations) and those described in Example 3.3. The classification of all primitive groups that admit sympathetic pairs of section-regular partitions ought to be significantly easier than the project outlined in Note 5.2, but nevertheless of some interest.

6. Appendix

NOTE 6.1. I am asked by the editors and a referee to say a few words about where Araújo's question comes from. It lies at a couple of steps removed from the problem in the theory of automata from which he actually started. That problem is the so-called Černý Problem. Associated with any finite-state (deterministic) automaton (or semiautomaton, that is, automaton without a designated initial state and without designated accept states) is the semigroup generated by its transition maps. A word in those transition maps is said to be a *reset word* if it sets the machine to one and the same state whatever state it is originally in. An automaton is said to be *synchronizing* if it admits a reset word. The Černý Conjecture is that if an n-state automaton is synchronizing then it admits a reset word of length at most $(n-1)^2$. For accounts of the conjecture and substantial lists of references see [15; 16; 17].

This is, however, a question simply about transformation semigroups, and automata have little to do with it except insofar as they provide context for the origin of the problem and a ready source of applications. Let $T(X)$ denote the full transformation semigroup on a set X of size n. A subsemigroup of $T(X)$ is said to be synchronizing if it contains a constant map. Let U_0 be a subset of $T(X)$, and suppose that the subsemigroup U generated by U_0 is synchronizing. The Černý Conjecture is that there is a word of length at most $(n-1)^2$ in the members of U_0 that is a constant map.

Setting this particular conjecture aside, in the theory of automata and in semigroup theory one seeks as much information as one can get about synchronizing semigroups and their generating sets. Inspired by the problems formulated in [16, p. 338], Araújo had the idea of studying the subgroups G of $\mathrm{Sym}(X)$ with the property that for every t in $T(X) \setminus \mathrm{Sym}(X)$ the semigroup $\langle G, t\rangle$ generated by G together with t is synchronizing. He and others (see [1]) call these "synchronizing groups" and observe that this is equivalent to the definition made in Section 1. For suppose first that G is not a synchronizing group in the latter sense, as is witnessed by a non-trivial proper partition ρ and its section S. Note that then S^g is a section of ρ^h for all $g, h \in G$. Define

$$V := \{t \in T(X) \mid \exists g, h \in G : \mathrm{Im}\, t = S^g,\ \mathrm{Ker}\, t = \rho^h\}.$$

The properties of S and ρ entail that if $t_1, t_2 \in V$ then $\mathrm{Im}(t_1 t_2) = \mathrm{Im}\, t_2$ and $\mathrm{Ker}(t_1 t_2) = \mathrm{Ker}\, t_1$. Therefore V is closed under composition, that is, it is a subsemigroup of $T(X)$. Also it is normalised by G, that is, $g^{-1} t g \in V$ for all $t \in V$, and so VG, the set of all products tg with $t \in V$ and $g \in G$, is a subsemigroup of $T(X)$. It contains no constant maps and so for any $t \in V$, the subsemigroup $\langle G, t\rangle$ of $T(X)$ contains no constant maps.

Conversely, suppose that the group G is synchronizing in the sense defined in Section 1. Let $t \in T(X) \setminus \mathrm{Sym}(X)$, and let t_0 be an element of least rank (that is, with smallest possible image) in $\langle G, t\rangle$. Let $\rho := \mathrm{Ker}\, t_0$ and $S := \mathrm{Im}\, t_0$. If there existed $g \in G$ and distinct elements $x, y \in S$ such that $x^g \equiv y^g \pmod{\rho}$ then we'd have $x^{g t_0} = y^{g t_0}$, and therefore $t_0 g t_0$ would be a member of $\langle G, t\rangle$ of strictly smaller rank than t_0, which is not possible. It follows that S^g is a section of ρ for every $g \in G$, that is, ρ is G-regular. Since ρ is certainly not the trivial relation, it follows that ρ is universal, so t_0 is a constant map. Therefore $\langle G, t\rangle$ is a synchronizing semigroup and G is a synchronizing group in the original sense.

NOTE 6.2. Since this paper was accepted new information has come to my attention.

(1) In their lovely paper [1], Arnold and Steinberg point out that if the permutation module $\mathbb{Q}X$ splits as $T_0 \oplus T_1$, where T_0 is the trivial G-module and T_1 is an irreducible $\mathbb{Q}G$-module, then G is a synchronizing group. This applies to certain groups of affine type; more interestingly, it applies to show that if $2^k - 1$ is a Mersenne prime number, $G = \mathrm{SL}(2, 2^k)$, and X is the coset space of a dihedral subgroup of order $2(2^k + 1)$ then G is a synchronizing group.

(2) Coming from a completely different direction Cameron and Kazanidis [5] have discovered a serendipitous connection with graph theory. In particular, they make considerable progress with the problem of classifying the rank-3 permutation groups that are synchronizing—see Note 5.1.

I am grateful to the editors for permission to update this paper at a late stage.

References

[1] Fredrick Arnold and Benjamin Steinberg, *Synchronizing groups and automata,* Theoret. Comput. Sci. 359 (2006), 101–110.

[2] Zs. Baranyai, *On the factorization of the complete uniform hypergraph,* Infinite and finite sets (Keszthely, 1973), vol. I, Colloq. Math. Soc. János Bolyai, 10, pp. 91–108, North-Holland, Amsterdam, 1975.

[3] Peter J. Cameron, *Parallelisms of complete designs,* London Math. Soc. Lecture Note Ser., 23, Cambridge Univ. Press, Cambridge, 1976.

[4] ———, *Permutation groups,* London Math. Soc. Stud. Texts, 45, Cambridge Univ. Press, Cambridge, 1999.

[5] Peter J. Cameron and P. A. Kazanidis, *Cores of symmetric graphs,* J. Australian Math. Soc. 85 (2008), 145–154.

[6] Peter J. Cameron, Peter M. Neumann, and David N. Teague, *On the degrees of primitive permutation groups,* Math. Z. 180 (1982), 141–149.

[7] John D. Dixon and Brian Mortimer, *Permutation groups,* Grad. Texts in Math., 163, Springer-Verlag, New York, 1996.

[8] P. Hall, *On representatives of subsets,* J. London Math. Soc. 10 (1935), 26–30.

[9] D. G. Higman, *Intersection matrices for finite permutation groups,* J. Algebra 6 (1967), 22–42.

[10] Dénes König, *Über Graphen und ihre Anwendung auf Determinantentheorie und Mengenlehre,* Math. Ann. 77 (1916), 453–465.

[11] Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl, *On factorizations of almost simple groups,* J. Algebra 185 (1996), 409–419.

[12] Martin W. Liebeck and Jan Saxl, *The finite primitive permutation groups of rank three,* Bull. London Math. Soc. 18 (1986), 165–172.

[13] Peter M. Neumann, *Finite permutation groups, edge-coloured graphs and matrices,* Topics in group theory and computation (Proc. Summer School, University College, Galway, 1973), pp. 82–118, Academic Press, London, 1977.

[14] ———, *Permutationsgruppen von Primzahlgrad und verwandte Themen,* Vorlesungen aus dem Mathematischen Institut Giessen, Heft 5, Mathematisches Institut Giessen, Giessen, 1977.

[15] Jean-Éric Pin, *Černý's conjecture,* ⟨www.liafa.jussieu.fr/~jep/Problemes/Cerny.html⟩.

[16] Arto Salomaa, *Generation of constants and synchronization of finite automata,* J. UCS 8 (2002), 332–347.

[17] A. N. Trakhtman, *Synchronization algorithms and Černý conjecture,* ⟨http://www.cs.biu.ac.il/~trakht/syn.html⟩.

[18] Helmut Wielandt, *Primitive Permutationsgruppen vom Grad* $2p$, Math. Z. 63 (1956), 478–485; reprinted and translated in Helmut Wielandt: Mathematische Werke (B. Huppert, H. Schneider, eds.), vol. 1, pp. 64–71, 183–189, de Gruyter, Berlin, 1994.

The Queen's College
Oxford OX1 4AW
United Kingdom

peter.neumann@queens.ox.ac.uk