Primitive Groups Synchronize Non-uniform Maps of Extreme Ranks

João Araújo

Universidade Aberta, R. Escola Politécnica, 147

1269-001 Lisboa, Portugal

&

Centro de Álgebra, Universidade de Lisboa

1649-003 Lisboa, Portugal, jaraujo@ptmat.fc.ul.pt

Peter J. Cameron

Mathematical Institute

North Haugh, St Andrews KY16 9SS, UK

pjc@mcs.st-andrews.ac.uk

Abstract

Let Ω be a set of cardinality n, G a permutation group on Ω, and $f : \Omega \to \Omega$ a map which is not a permutation. We say that G synchronizes f if the semigroup $\langle G, f \rangle$ contains a constant map.

The first author has conjectured that a primitive group synchronizes any map whose kernel is non-uniform. Rystsov proved one instance of this conjecture, namely, degree n primitive groups synchronize maps of rank $n - 1$ (thus, maps with kernel type $(2, 1, \ldots, 1)$). We prove some extensions of Rystsov's result, including this: a primitive group synchronizes every map whose kernel type is $(k, 1, \ldots, 1)$. Incidentally this result provides a new characterization of imprimitive groups. We also prove that the conjecture above holds for maps of extreme ranks, that is, ranks 3, 4 and $n - 2$.

These proofs use a graph-theoretic technique due to the second author: a transformation semigroup fails to contain a constant map

1

if and only if it is contained in the endomorphism semigroup of a non-null (simple undirected) graph.

The paper finishes with a number of open problems, whose solutions will certainly require very delicate graph theoretical considerations.

1   Introduction

In automata theory, the well-known Černý conjecture states that a synchronizing automaton with n states has a synchronizing word of length $(n-1)^2$. (For many references on the growing bibliography on this problem please see the two websites [21, 23].) Solving this conjecture is equivalent to prove that given a set $S = \{f_1, \ldots, f_m\}$ of transformations on a finite set $\Omega := \{1, \ldots, n\}$, if S generates a constant, then S generates a constant in a length $(n-1)^2$ word on its generators. This conjecture has been established when $\langle S \rangle$ is a semigroup in which all its subgroups are trivial [24]. So it remains to prove the conjecture for semigroups containing non trivial subgroups; the case in which the semigroup contains a permutation group is a particular instance of this general problem. In addition, the known examples witnessing the optimality of the Černý bound contain a permutation among the given set of generators S, so they make it especially interesting to study the cases in which a subset of S generates a permutation group.

Let G be a permutation group on a set Ω with $|\Omega| = n$. We say that G *synchronizes* a map f on Ω if the semigroup $\langle G, f \rangle$ contains a constant map. G is said to be *synchronizing* if G synchronizes every non-invertible transformation on Ω. The *diameter* of a group is the largest diameter of its Cayley graphs. Taking into account the motivation of the considerations above, the ultimate goal is to find a classification of the synchronizing groups and then study those with the largest diameter, since they should assist the generation of a constant with the lowest diligence. But even when we forget about the automata motivation of these problems, the classification of synchronizing groups (a class strictly between primitivity and 2-homogeneity) and the study of their diameters are very interesting questions in themselves, as well as extremely demanding (please see [6, 10, 11, 20, 18]).

Let f be a map on Ω. Recall that the *rank* of f is $|\Omega f|$, and the *kernel* of f is the partition of Ω into the inverse images of points in the image of f; equivalently, the kernel of f is the partition of Ω induced by the equivalence

relation $\{(x, y) \in \Omega \times \Omega \mid xf = yf\}$. The *kernel type* of f is the partition of n given by the sizes of the parts of the kernel. A partition of Ω is *uniform* if all its parts have the same size. We will call a map *uniform* if its kernel is uniform.

We note that, if a transformation semigroup S contains a transitive group G but not a constant function, then the image I of a map f of minimal rank in S is a *G-section* for the kernel of f, in the sense that Ig is a section for $\ker(f)$, for all $g \in G$; in addition, the map f has uniform kernel (see Neumann [20]).

In [6] the conjecture that a primitive group of permutations of Ω synchronizes every non-uniform transformation on Ω was proposed. In 1995 Rystsov [22] proved the following particular instance of this conjecture.

Theorem 1 *A transitive permutation group G of degree n is primitive if and only if it synchronizes every map of rank $n - 1$.*

The goal of this paper is to use a graph-theoretic approach due to the second author to prove the conjecture for maps of extreme rank, that is, their rank either is close to 1 or close to n.

It is worth pointing out that Rystosov's Theorem 1 in fact characterizes primitivity in terms of maps of kernel type $(2, 1, \ldots, 1)$; our first result provides a similar characterization of imprimitivity in terms of maps of kernel type $(k, 1, \ldots, 1)$.

Theorem 2 *Let G be a transitive permutation group on a finite set Ω and let k be given with $k > 1$. Then G is imprimitive with a block of imprimitivity of size at least k if and only if G fails to synchronize some map f with kernel type $(k, 1, 1, \ldots, 1)$.*

This result proves, in particular, that primitive groups synchronize every map with kernel type $(k, 1, 1, \ldots, 1)$.

Our next result concerns synchronization of large rank maps.

Theorem 3 *Let G be a primitive permutation group on a finite Ω, with $|\Omega| > 2$. Then G synchronizes:*

(a) every map of rank $n - 2$;

(b) every idempotent map with kernel type $(3, 2, 1, 1, \ldots, 1)$;

3

(c) every map f with kernel type $(3, 2, 1, 1, \ldots, 1)$, provided there exists $g \in G$ such that $rank(fgf) = rank(f)$.

In the second part of the paper, we turn from maps of large rank to those of small rank, and prove the following theorem. (The first part of this theorem is due to Neumann [20], but we will provide an alternative proof.)

Theorem 4 *Let G be a primitive group of degree $n > 2$.*

(a) G synchronizes every map of rank 2.

(b) G synchronizes every non-uniform map of rank 3 or 4.

The condition that the map is non-uniform in Theorem 4(b) is necessary: the group $S_3 \, \text{wr} \, S_2$ of degree 9 (the automorphism group of the 3×3 grid) is primitive and fails to synchronize a map of rank 3 (for example, the projection of the grid onto a diagonal whose kernel classes are the rows).

In Section 2 we introduce the graph, and some basic results about it, that is going to be our main tool throughout the paper. Section 3 is dedicated to the proof of Theorem 2, Section 4 to the proof of Theorem 3, and Section 5 to the proof of Theorem 4. The paper ends with a number of open problems whose solution will certainly require delicate considerations on graph theory, permutations groups and transformation semigroups.

2   Transformation semigroups and graphs

The critical idea used in this paper is a graph associated to a transformation semigroup, due to the second author. Let S be a transformation semigroup on Ω. Form a graph on the vertex set Ω by joining two vertices v and w if and only if there is no element f of S which maps v and w to the same point. We denote this graph by $\text{Gr}(S)$. Now the following result is almost immediate (*cf.* [12]).

Theorem 5 *Let S be a transformation semigroup on Ω and let $\text{Gr}(S)$ be as above.*

(a) S contains a map of rank 1 if and only if $\text{Gr}(S)$ is null.

(b) $S \leq \text{End}(\text{Gr}(S))$, and $\text{Gr}(\text{End}(\text{Gr}(S))) = \text{Gr}(S)$.

(c) The clique number and chromatic number of $\mathrm{Gr}(S)$ *are both equal to the minimum rank of an element of* S.

Proof Regarding (a), the forward direction is obvious. Conversely, let $f \in S$ be a map of minimal rank, and suppose that $\mathrm{rank}(f) > 1$. For every $x, y \in \Omega f$ we have $xs \neq ys$, for all $s \in S$ (otherwise $\mathrm{rank}(fs) < \mathrm{rank}(f)$ contrary to our assumption). Therefore $\{x, y\}$ is an edge of $\mathrm{Gr}(S)$. It is proved that if S has no constant, then $\mathrm{Gr}(S)$ is not null.

Regarding (b), let $f \in S$ and let $\{x, y\}$ be any edge in $\mathrm{Gr}(S)$; we claim that $\{xf, yf\}$ is an edge in $\mathrm{Gr}(S)$ and hence $f \in \mathrm{End}(\mathrm{Gr}(S))$. In fact, if $\{xf, yf\}$ is not an edge in $\mathrm{Gr}(S)$, then there exists $f' \in S$ such that $xff' = yff'$, that is, $\{x, y\}$ is not an edge of $\mathrm{Gr}(S)$, contradicting our assumptions.

Now we prove that $\mathrm{Gr}(\mathrm{End}(\mathrm{Gr}(S))) \subseteq \mathrm{Gr}(S)$. Let $\{x, y\}$ be an edge in $\mathrm{Gr}(\mathrm{End}(\mathrm{Gr}(S)))$. This means that $xf \neq yf$, for all $f \in \mathrm{End}(\mathrm{Gr}(S))$. But we already proved that $S \leq \mathrm{End}(\mathrm{Gr}(S))$; thus $xf \neq yf$, for all $f \in S$ and hence $\{x, y\}$ is an edge in $\mathrm{Gr}(S)$.

Conversely, to prove that $\mathrm{Gr}(\mathrm{End}(\mathrm{Gr}(S))) \supseteq \mathrm{Gr}(S)$, let $\{x, y\}$ be an edge in $\mathrm{Gr}(S)$. Then for every $f \in \mathrm{End}(\mathrm{Gr}(S))$ the set $\{xf, yf\}$ is an edge of $\mathrm{Gr}(S)$, that is, $xf \neq yf$, for all $f \in \mathrm{End}(\mathrm{Gr}(S))$. Thus $\{x, y\}$ is an edge of $\mathrm{Gr}(\mathrm{End}(\mathrm{Gr}(S)))$ and (b) follows.

Now we prove (c). It is clear that the image of any map f of minimum rank forms a clique of $\mathrm{Gr}(S)$; for if not there would be $x, y \in \Omega f$ and $f' \in S$ such that $xf' = yf'$; thus $\mathrm{rank}(ff')$ would be strictly smaller than $\mathrm{rank}(f)$ and hence f would not be of minimum rank. Let Γ be the complete graph contained in $\mathrm{Gr}(S)$ and whose vertex set is Ωf (for a map f of minimum rank). It is clear that $f : \mathrm{Gr}(S) \mapsto \Gamma$ is a morphism; conversely, $\iota : \Gamma \mapsto \mathrm{Gr}(S)$ such that $\{x, y\}\iota = \{x, y\}$ is a morphism. Thus the complete graph Γ is a core of $\mathrm{Gr}(S)$; it is well known that if a graph has complete core, then the chromatic number of the graph equals its clique number. The result follows.

Note that (a) is a special case of (c), when the minimum rank is 1. $\square$

In particular, if $S = \langle G, f \rangle$ for some group G, then $G \leq \mathrm{Aut}(\mathrm{Gr}(S))$. So, for example, if G is primitive and does not synchronize f, then $\mathrm{Gr}(S)$ is non-null and has a primitive automorphism group, and so is connected.

In this situation, assume that f is an element of minimal rank in S; then the kernel of f is a partition ρ of Ω, and its image A is a G-*section* for ρ (that is, Ag is a section for ρ, for all $g \in G$). Neumann [20], analysing this situation, defined a graph Δ on Ω whose edges are the images under G of

the pairs of vertices in the same ρ-class. Clearly Δ is a subgraph of the complement of $\mathrm{Gr}(S)$, since edges in Δ can be collapsed by elements of S. Sometimes, but not always, Δ is the complement of $\mathrm{Gr}(S)$.

For the sake of completeness we include here a general lemma on primitive groups.

Lemma 6 *Let G be a primitive group:*

(a) *if G contains a transposition (v, w), then G is the symmetric group;*

(b) *if G has degree greater than 5 and contains a double transposition $(v, w)(x, y)$, then G is 2-transitive.*

Proof Regarding (a), suppose G is a primitive group of permutations of $\Omega := \{1, \ldots, n\}$. Define a relation on Ω as follows: for all $x, y \in \Omega$,

$$x \sim y \Leftrightarrow x = y \text{ or } (x, y) \in G.$$

It is clear that $\sim$ is reflexive and symmetric. In addition, if $x \sim y \sim z$, then $(x, y), (y, z) \in G$ and hence $(x, z) = (y, z)(x, y)(y, z) \in G$; thus $\sim$ is an equivalence relation on Ω. The transpositions generate the symmetric groups on the equivalence classes. We claim that there is only one equivalence class; for suppose not and let $(x, y) \in G$ and $A \subset \Omega$ be an equivalence class. Since G is primitive there exists $g \in G$ such that $xg \in A$ and $yg \notin A$. Thus $g^{-1}(x, y)g = (xg, yg) \in G$; thus $xg \sim yg$, a contradiction. It is proved that there is only one equivalence class and it was already shown above that the transpositions generate the symmetric group inside each equivalence class.

Regarding (b), we refer the reader to Example 3.3.1 on p.82 of [14]. $\square$

The next lemma has some interest in itself, but it is very important for the techniques it introduces and that will be used later.

Lemma 7 *Let X be a nontrivial graph and let $G \leq \mathrm{Aut}(X)$ be primitive. Then no two vertices of X can have the same neighbourhood.*

Proof For $a \in X$ denote its neighbourhood by $N(a)$. Suppose that $a, b \in X$, with $a \neq b$, and $N(a) = N(b)$. We are going to use two different techniques to prove that this leads to a contradiction. The first uses the fact that the graph has at least one edge; the second uses the fact that the graph is not complete.

6

First technique. Define the following relation on the vertices of the graph: for all $x, y \in X$,

$$x \equiv y \Leftrightarrow N(x) = N(y).$$

This is an equivalence relation and we claim that $\equiv$ is neither the universal relation nor the identity. The latter follows from the fact that by assumption a and b are different and $N(a) = N(b)$. Regarding the former, there exist adjacent vertices c and d (because X is non-null); now $c \in N(d)$ but $c \notin N(c)$, so $c \not\equiv d$. As G is a group of automorphisms of X it follows that G preserves $\equiv$, a non-trivial equivalence relation, and hence G is imprimitive, a contradiction.

Second technique. Assume as above that we have $a, b \in X$ such that $N(a) = N(b)$. Then the transposition (a, b) is an automorphism of the graph. By the previous lemma, a primitive group containing a transposition is the symmetric group and hence X is the complete graph, a contradiction. $\square$

The two techniques in the previous proof are important because we will use variants on them later.

We conclude this section with a general result about *primitive graphs* (those admitting a vertex-primitive automorphism group), which we will use later in the paper.

Lemma 8 *Let Γ be a non-null graph with primitive automorphism group G, and having chromatic number r. Then Γ does not contain a subgraph isomorphic to the complete graph on $r + 1$ vertices with an edge removed.*

Proof Let c be a colouring of Γ with r colours. Suppose, by contradiction, that the set $\{1, 2, \ldots, r, r + 1\}$ of vertices contains all possible edges except for $\{r, r + 1\}$. Then $\{1, \ldots, r\}$ is a clique, and so contains one vertex of each colour; similarly for $\{1, \ldots, r - 1, r + 1\}$. Since the colors of r and $r + 1$ are different from the colors of $1, \ldots, r - 1$, we conclude that vertices r and $r + 1$ have the same colour. The same conclusion holds for the image of these vertices under any element of G.

Now let Δ be the graph whose edge set is the G-orbit containing $\{r, r+1\}$. Then Δ is G-invariant and non-empty, but is disconnected, since all its edges lie within colour classes of the colouring c. This contradicts the primitivity of G. $\square$

We note that the hypotheses are both necessary: the complete r-partite graph with parts of constant size is vertex-transitive and contains K_{r+1} minus an edge; and every graph occurs as an induced subgraph of some primitive graph as proved in the next result.

Proposition 9 *Every graph is isomorphic to an induced subgraph of a graph with primitive automorphism group.*

Proof First represent the graph as an *intersection graph*, that is, the vertices are subsets of a set E, and two vertices are adjacent if the sets are not disjoint. This was first observed by Szpilrajn-Marczewski [25]; it is most easily done by taking E to be the edge set of the graph, and identifying each vertex with the set of edges incident with it.

Now, by adding extra points each in at most one of the sets, we may assume that all the sets have the same cardinality k.

Now the graph is an induced subgraph of the graph whose vertices are the k-element subsets of an n-set (where we may assume that $n > 2k$), two vertices adjacent if they are not disjoint. The automorphism group of this graph is the symmetric group S_n, in its primitive action on k-sets. □

3   A characterization of imprimitivity

Rystsov's Theorem says that every primitive group synchronizes a map of kernel type $(2, 1, \ldots, 1)$. The next theorem generalizes this result by proving that every primitive group synchronizes a map of kernel type $(k, 1, \ldots, 1)$, for every k such that $|\Omega| \geq k \geq 2$.

In fact, using the graph-theoretic techniques of the preceding section we prove the following characterization of imprimitivity.

Theorem 2 *Let G be a transitive permutation group on a finite set Ω and let k be given with $k > 1$. Then G is imprimitive with a block of imprimitivity of size at least k if and only if G fails to synchronize some map f with kernel type $(k, 1, 1, \ldots, 1)$.*

Proof To prove the theorem in the forward direction, suppose that G is imprimitive, with blocks of size at least k. Let X be the complete multipartite graph whose partite classes are the blocks. Then $G \leq \mathrm{Aut}(X)$. Let A be a subset of a block, with $|A| = k$, and choose $a \in A$. Define f so that $bf = a$

for all $b \in A$ and $xf = x$ for $x \notin A$. Then f is an endomorphism of X (so that f cannot be synchronized by G) with kernel type $(k, 1, 1, \ldots, 1)$.

Conversely, let G and f be as given, and let A be the kernel class of size k of G.

By the general observations of the previous section we know that there is a non-null graph $X = \mathrm{Gr}(\langle G, f \rangle)$ with $\langle G, f \rangle \leq \mathrm{End}(X)$.

Observe that A is an independent set in X, since A is collapsed to a point by the endomorphism f. Thus X is not the complete graph and hence, since X is also not null, we conclude that X is not trivial.

We claim that any two points in A have the same neighbourhood. To see that let $N(x)$ denote the neighbourhood of x. Since $G \leq \mathrm{Aut}(X)$ is transitive, all vertices have the same number of neighbours. Now let $Af = \{z\}$. Then, for any $a \in A$, as $f \in \mathrm{End}(X)$ it follows that f maps $N(a)$ to $N(z)$; since $N(a) \cap A = \emptyset$, f is injective on $N(a)$, and so maps it bijectively to $N(z)$ (recall from above that the transitivity of G implies that $|N(a)| = |N(z)|$). Similarly for another point $b \in A$. But $z \notin N(z)$, so $f^{-1}|_{N(z)}$ is a well defined bijective map from $N(z)$ to $N(a)$, and also to $N(b)$; so these two sets are equal. By Lemma 7 this immediately implies that G is imprimitive.

Now recall the G-congruence $\equiv$ on Ω defined in the proof of Lemma 7: $x \equiv y$ if and only if $N(x) = N(y)$. Since all elements in A have the same neighbourhood, we conclude that A is contained in a single $\equiv$-class. So G is imprimitive, with a system of blocks (the $\equiv$-classes) of size at least k. $\qquad\square$

4 Primitive groups and large rank maps

The aim of this section is to prove the following theorem.

Theorem 3 *Let G be a primitive permutation group on a finite Ω, with $|\Omega| > 2$. Then G synchronizes:*

(a) *every map of rank $n - 2$;*

(b) *every idempotent map with kernel type $(3, 2, 1, 1, \ldots, 1)$;*

(c) *every map f with kernel type $(3, 2, 1, 1, \ldots, 1)$, provided there exists $g \in G$ such that $rank(fgf) = rank(f)$.*

The proof of this theorem will be carried out in a sequence of subsections.

4.1 Proof of Theorem 3(a)

The kernel type of a map of rank $n-2$ is either $(3, 1, 1, \ldots, 1)$ or $(2, 2, 1, \ldots, 1)$. By Theorem 2, a primitive group synchronizes a map with the first kernel type.

   We begin with some general remarks about the case where f is a map with exactly two non-singleton kernel classes A and B, and G is a primitive group which fails to synchronize f.

   We start with a general lemma.

Lemma 10 *Given a primitive group G that does not synchronize a map of kernel type $(p, q, 1, \ldots, 1)$, with $p, q \geq 2$. Let A and B be the non-singleton kernel classes, and $K := A \cup B$. Let $S = \langle G, f \rangle$ and $X = G(S)$. Then there must be at least a path or a cycle of length 4 contained in the non-singleton kernel classes A and B. Moreover, let $S = \langle G, f \rangle$ and $X = \mathrm{Gr}(S)$. Then in the graph X we have that*

   (a) there are no isolated points in K;

   (b) there cannot be two points of A which each have a single neighbour in B, these neighbours being equal.

Proof   The rank of f must be larger than 2 since, by [20] and/or Theorem 4, G synchronizes every rank 2 map; therefore, $A \cup B$ is a proper subset of Ω. We let $S = \langle G, f \rangle$ and $X = \mathrm{Gr}(S)$. Suppose that $Af = x$ and $Bf = y$.
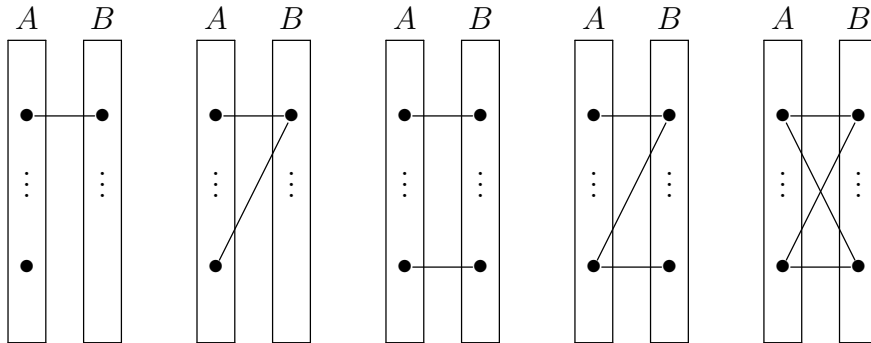

Figure 1: The five possible configurations of the edges in K

10

The graph X is non-trivial and has the primitive group G contained in $\mathrm{Aut}(X)$; so X is connected, and hence there exists at least one edge from $A \cup B$ to its complement (recall that $A \cup B$ is a proper subset of Ω).

Certainly neither A nor B contain edges of X, since f collapses each one of them. So X is not complete.

We claim that the set $K := A \cup B$ must contain an edge of X. For suppose not. Take $a_1, a_2 \in A$. Then $N(a_1) \subseteq X \setminus (A \cup B)$ and f is injective on $X \setminus (A \cup B)$. Thus f maps $N(a_1)$ injectively into $N(x)$. The transitivity of G implies that all neighbourhoods have the same size and hence $N(a_1)f = N(x)$; so does $N(a_2)$. Thus $N(a_1) = N(x)f^{-1} = N(a_2)$, which is impossible in a primitive group (Lemma 7). It follows that K contains an edge and hence $\{x, y\}$ is an edge (since f is an endomorphism of X). Therefore the edges in K must contain one of the five configurations in figure 1. We are going to show that only the last two configurations can happen.

First, we claim that any point of K lies on an edge within this set. For suppose that $a \in A$ does not; then all its neighbours are outside K, and so are mapped bijectively by f; but they are mapped onto $N(x) \setminus \{y\}$, which is smaller than $N(a)$. It is proved that the first configuration in figure 1 cannot occur.

Next we claim that there cannot be two points of A which each have a single neighbour in B, these neighbours being equal. For suppose that a_1 and a_2 are two such points. Then the sets $N(a_1) \setminus B$ and $N(a_2) \setminus B$ are mapped injectively, and hence bijectively, to $N(x) \setminus \{y\}$; so we must have $N(a_1) \setminus B = N(a_2) \setminus B$. But a_1 and a_2 have the same neighbour in B; so their neighbourhoods are equal, which again is impossible in a primitive group (Lemma 7). It is proved that the second configuration in figure 1 cannot occur.

Also, the induced subgraph on K cannot have two connected components each consisting of a single edge. For suppose that $\{a_1, b_1\}$ and $\{a_2, b_2\}$ were such components. As above, we would have $N(a_1) \setminus B = N(a_2) \setminus B$ and, similarly, $N(b_1) \setminus A = N(b_2) \setminus A$. But then the permutation $(a_1, a_2)(b_1, b_2)$ is an automorphism of the graph. However, a primitive group of degree greater than 5 containing such an element must be 2-transitive (by Lemma 6) whereas a non-trivial graph cannot have a 2-transitive automorphism group. $\square$

Now we can prove Theorem 3(a). The kernel type of a map of rank $n - 2$ is either $(3, 1, 1, \ldots, 1)$ or $(2, 2, 1, \ldots, 1)$. By Theorem 2, a primitive group synchronizes a map with the first kernel type.

Let f be a map of kernel type $(2, 2, 1, \ldots, 1)$ and let $S = \langle G, f \rangle$ and $X = \mathrm{Gr}(S)$. Suppose that $Af = x$ and $Bf = y$. By the previous result we already know that $K := A \cup B$ must contain a path or a cycle of length 4. In order to finish the proof we must consider those two cases for the induced subgraph on K: a path or cycle of length 4, when $|A| = 2 = |B|$.

Since $G \leq \mathrm{Aut}(X)$ is transitive, X is regular of valency, say, k. Observe that in each case, the $k-1$ or $k-2$ vertices of $N(a_i) \setminus K$ are mapped injectively to the vertices of $N(x) \setminus \{y\}$, and the $k - 1$ or $k - 2$ vertices of $N(b_i) \setminus K$ to the vertices of $N(y) \setminus \{x\}$.

Now the graph Xf is a subgraph of the induced subgraph of X on Ωf, call it X', say. Then in X' we have removed two vertices, which are incident with either $2k - 1$ or $2k$ edges, according as they are adjacent or not. So X' has at most $e - 2k + 1$ edges, where e is the number of edges of X. We show that this is incompatible with each of our cases except in one situation.

To get a lower bound for the number of edges of Xf, we simply have to calculate the size of the image of the edge set of X under f. (Each edge of X maps to an edge of Xf.) We do this by counting edges collapsed by f.

Consider the case where K induces a path of length 3, say (a_1, b_1, a_2, b_2). Now f collapses the three edges within K to the single edge $\{x, y\}$. It maps the $k-1$ vertices of $N(a_1) \setminus K$ bijectively to $N(x) \setminus \{y\}$, and the $k-2$ vertices of $N(a_2) \setminus K$ injectively inside this set; so $k - 2$ pairs of edges of this form collapse. Similarly $k - 2$ pairs of edges through b_i collapse. So the number of edges of Xf is at least $e - (2 + 2(k - 2)) = e - 2k + 2$, a contradiction.

Now consider the case where K induces a 4-cycle. The neighbours of both a_1 and a_2 outside K are mapped injectively to $N(x) \setminus \{y\}$, so either $k - 2$ or $k - 3$ edges are collapsed, depending on whether the images of these two sets are equal or not. Similarly for b_1 and b_2. Moreover, four edges within K are collapsed to one. So the number of edges of Xf is at least $e - 3 - 2(k - 2) = e - 2k + 1$. This is just possible, but we see that the sets $N(a_1) \setminus K$ and $N(a_2) \setminus K$ must be equal, and similarly $N(b_1) \setminus K = N(b_2) \setminus K$.

Now, if we assume that $A = \{a_1, a_2\}$ and $B = \{b_1, b_2\}$, the equality of the neighbourhoods just proved shows that the permutation $(a_1, a_2)(b_1, b_2)$ is an automorphism of X, a contradiction as before. This finishes the proof of Theorem 3(a). $\qquad\square$

12

4.2   Proof of Theorem 3(b)

As in the previous subsection, we begin with a more general result. Let f be a map with kernel type $(p, q, 1, \ldots, 1)$ (with $p, q > 1$) non synchronized by a primitive group G; let $S = \langle G, f \rangle$ and $X = \mathrm{Gr}(S)$. Suppose, further, that f is an idempotent. We claim that the induced subgraph on $K = A \cup B$ (where A and B are the non-trivial kernel classes) cannot have all possible edges between A and B.

As in the preceding section, we use the fact that Xf is a subgraph of the restriction X' of X to the image of f. Now the fact that f is an idempotent means that the points not in the image of f must consist of $p - 1$ points of A and $q - 1$ points of B; by assumption, the induced subgraph on this set is complete bipartite.

Let e be the number of edges, and k the valency, of X.

In the subgraph X', we lose $p - 1$ vertices of A and $q - 1$ of B, and so $k(p - q + 2)$ edges; but of these, $(p - 1)(q - 1)$ are counted twice. So the number of edges in this graph is

$$e - k(p + q - 2) + (p - 1)(q - 1) \tag{1}$$

Now we consider Xf, and count how many edges collapse to the same place. The pq edges within K collapse to a single edge, so we lose $pq - 1$ edges. The p vertices of A each lie on $k - q$ edges outside K, so at most $(p - 1)(k - q)$ edges are lost; and similarly at most $(q - 1)(k - p)$ edges through vertices in B. Thus the number of edges in Xf is at least

$$e - (pq - 1) - (p - 1)(k - 1) - (q - 1)(k - p) = e - (p + q - 2)k - (p - 1)(q - 1),$$

and this number equals the value found in (1). So all the neighbours of A outside K are mapped to the same set of $k - q$ vertices. This means that any two vertices in A have the same neighbours. Therefore any transposition of two elements in A is an automorphism of X and hence G is the symmetric group (by Lemma 6); but this is impossible, since G does not synchronize f while the symmetric group synchronizes every map.

Now we return to the proof of Theorem 3(b), the case $p = 2$, $q = 3$. Lemma 10, (a) and (b), in the preceding section, shows that there are at least four edges between A and B. One case with four edges is ruled out by having an isolated vertex in B, and another by having two vertices in B each with a single common neighbour in A, these neighbours being the same. The

13

remarks above rule out the complete bipartite graph. The two cases that remain are shown in figure 2.
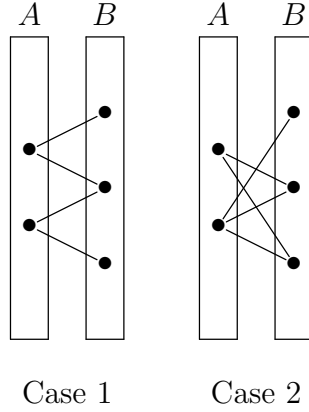

Figure 2: The two (im)possible configurations of the edges in K

Now we count some edges, along the same lines as earlier. The graph induced on Ωf by X omits three vertices, and so, if e denotes the number of edges of X, it has at most $e - 3k + 3$ edges (with equality if the three vertices form a triangle).

We count the edges of Xf by seeing how many edges are identified by f. All the edges within K collapse to a single edge, so we lose 3 or 4 edges. The other collapsed edges are those with one end in K. The neighbours of a vertex in A are mapped injectively to $N(x) \setminus \{y\}$, and the neighbours of a vertex of B to $N(y) \setminus \{x\}$.

Case 1: at most $k - 2$ edges through A, and $(k-1) + (k-2)$ edges through B; thus at most $3k - 2$ identified, at least $e - 3k + 2$ remain.

Case 2: at most $k - 3$ through A, and $(k - 2) + (k - 2)$ through B; thus at most $3k - 3$ identified, at least $e - 3k + 3$ remain.

In Case 2, the fact that we have equality means that the neighbours outside K of the middle and bottom points of B map to the same $k - 2$ points of $N(y) \setminus \{x\}$, so these sets are equal. Thus these two points of B have identical neighbour sets, contradicting primitivity (Lemma 7). So this case cannot occur.

14

Now consider Case 1. Since the bounds differ by one, there are two subcases:

Subcase 1A The number of edges of Xf is $e - 3k + 2$, which means that the neighbours outside K of the two vertices in A map to the same $k - 2$ neighbours of x, and so these two neighbour sets are equal. In this case, the permutation interchanging the two vertices of A and the top and bottom vertices of B is an automorphism, contradicting proper primitivity.

Subcase 1B The number of edges of Xf is $e - 3k + 3$, so the bound is tight. In this case, the three vertices outside the image of f must form a triangle. This cannot happen if f is an idempotent, since then the three vertices outside the image of f lie in K, and cannot form a triangle.

The proof of Theorem 3(b) is complete. $\qquad\qquad\qquad\qquad\square$

4.3   Proof of Theorem 3(c)

The following result is the main observation underlying Theorem 3(c).

Lemma 11 *Let f be a transformation on a finite set Ω and let G be a group of permutations of Ω. If there exists $g \in G$ such that $rank(fgf) = rank(f)$, then there exists an idempotent $e \in \langle f, G \rangle$ such that e and f have the same kernel.*

Proof Pick $g \in G$ such that $\mathrm{rank}(fgf) = \mathrm{rank}(f)$, that is, $|\Omega fgf| = |\Omega f|$.

Since $\langle f, G \rangle$ is finite it follows that there exists a smallest natural n such that $(fg)^n$ belongs to $\{fg, (fg)^2, (fg)^3, \ldots, (fg)^{n-1}\}$. Say $(fg)^n = (fg)^m$, with $m < n$. We claim that $(fg)^{n-m}$ is idempotent.

First, observe that for all natural l we have $\mathrm{rank}((fg)^l) = \mathrm{rank}(f)$. To see this suppose not and pick the smallest i such that $\mathrm{rank}(fg)^i = \mathrm{rank}(f)$, but $\mathrm{rank}(fg)^{i+1} < \mathrm{rank}(f)$. Observe that if $\mathrm{rank}(fg)^i = \mathrm{rank}(f)$, then we also have $\mathrm{rank}(f) = \mathrm{rank}(fg)^i = \mathrm{rank}((fg)^{i-1}f)$ (as a permutation in the end does not change the rank) and hence $\Omega(fg)^{i-1}f = \Omega f$. Now

$$|\Omega(fg)^{i+1}| = |\Omega(fg)^i fg| = |\Omega(fg)^i f| = |\Omega(fg)^{i-1}fgf| = |\Omega fgf|.$$

Thus $|\Omega f| = |\Omega(fg)^i| > |\Omega(fg)^{i+1}| = |\Omega fgf|$, a contradiction with the first sentence of this proof. Thus $\mathrm{rank}(fg)^l = \mathrm{rank}(f)$, for all natural l. In

15

particular, $\mathrm{rank}(fg)^m = \mathrm{rank}(fg)^{n-m} = \mathrm{rank}(f)$. In addition, $\ker(fu) \supseteq \ker(f)$, for every transformation u. Thus $\ker(fg)^m$ and $\ker(fg)^{m-n}$ both contain $\ker(f)$. As their ranks are equal and we are dealing with finite sets, it follows that $\ker(fg)^m = \ker(fg)^{n-m} = \ker(f)$.

Now, $(fg)^m = (fg)^n = (fg)^m (fg)^{n-m}$ implies that for all $x \in \Omega(fg)^m$ we have $x(fg)^{n-m} = x$. In addition, it is obvious that if $u = uv$, then $\Omega u \subseteq \Omega v$; as $(fg)^m = (fg)^m (fg)^{n-m}$ we get that $\Omega(fg)^m \subseteq \Omega(fg)^{n-m}$ and hence equality follows because $\mathrm{rank}(fg)^m = \mathrm{rank}(fg)^{n-m}$. It is proved that $\Omega(fg)^m = \Omega(fg)^{n-m}$ and we already know that $(fg)^{n-m}$ is the identity on $\Omega(fg)^m = \Omega(fg)^{n-m}$. It follows that $(fg)^{n-m}$ is idempotent. In addition, since we already proved that $\ker(fg)^{n-m} = \ker f$ the result follows. $\qquad\square$

Now the proof of Theorem 3(c) is immediate. If we have a group G and a transformation f under the hypothesis of the theorem, then, by the previous lemma, there exists an idempotent $e \in \langle f, G \rangle$ such that $\ker(f) = \ker(e)$. By Theorem 3(b) there exists a constant transformation t such that

$$t \in \langle e, G \rangle (\subseteq \langle f, G \rangle),$$

so that G synchronizes f.

5 Proof of Theorem 4

The aim of this section is to prove the following theorem.

Theorem 4 *Let G be a primitive group of degree $n > 2$.*

(a) G synchronizes every map of rank 2.

(b) G synchronizes every non-uniform map of rank 3 or 4.

Let S be a transformation semigroup on a set of cardinality n which contains a transitive group G. If f is an element of S of minimum rank r, then the image of f is an r-clique in $\mathrm{Gr}(S)$, and the kernel partition is a colouring with r colours, and is uniform (so each part has size n/r).

If h is any element of S, then the rank of h is at least r; we can assume (replacing f by hf if necessary) that the kernel partition of h refines that of f. We begin with a general result asserting that, if G is primitive, then it is not possible for just one part of f to be split by the kernel partition of h.

Theorem 12 *Let S be a transformation semigroup containing a primitive group G, and suppose that the minimum rank of an element of S is r, where $r > 1$. Then there cannot be an element of S with rank greater than r whose kernel partition has $r - 1$ parts of size n/r.*

Proof Let f be an element of rank r in S, and assume that h is an element whose kernel partition consists of $r - 1$ parts of the kernel partition of f and splits the remaining part into at least two.

Let $\Gamma = \mathrm{Gr}(S)$. We need one further observation about Γ. We know that it has clique number r, so the independence number is at most n/r (since Γ is vertex-transitive). So, if B is a part of the kernel partition of f, and v a vertex not in B, then v has at least one neighbour in B (else $B \cup \{v\}$ would be an independent set).

Let $A_2, \ldots, A_r$ be the kernel classes of h of size n/r, and $A_{1,1}, \ldots, A_{1,m}$ be the kernel classes into which the class A_1 of f is split. Let $a_j = A_j h$ and $a_{1,i} = A_{1,i} h$.

For $j, k > 1$, there is an edge between A_j and A_k; and for $j > 1$ and any i, there is an edge between $A_{1,i}$ and A_j. Since h is an endomorphism of Γ, there are edges between a_j and a_k for $j, k > 1$, and between $a_{1,i}$ and a_j for $j > 1$ and all i. Thus the subgraph on $\{a_{1,1}, a_{1,2}, a_2, \ldots, a_r\}$ is a complete graph on $r + 1$ vertices with an edge removed, contradicting Lemma 8. □

Let S be a transformation semigroup containing a primitive group G, and suppose that the minimum rank of an element of S is r, where $r > 1$. If S contains a map h of rank $r + 1$, then either $\mathrm{rank}(hgh) = \mathrm{rank}(h)$, for all $g \in G$, or there exists $g \in G$ such that $\mathrm{rank}(hgh) = r$. The latter case cannot happen since only two kernel blocks of h collapse, and hence h would have $r - 1$ kernel blocks of size n/r, in contradiction with the previous result. The former case implies that h is uniform (by [20]). But, for $r > 1$ it is impossible to have $(a_1, \ldots, a_{r-1}, b_1, b_2)$ and $(a_1, \ldots, a_{r-1}, b_1 + b_2)$ both uniform. We have proved the following corollary.

Corollary 13 *Let S be a transformation semigroup containing a primitive group G, and suppose that the minimum rank of an element of S is r, where $r > 1$. Then S cannot contain an element of rank $r + 1$.*

It is worth observing that this corollary immediately implies the result (proved by Rystsov) that the degree $n > 1$ primitive groups on Ω synchronize the

rank $n - 1$ transformations of Ω. In fact, if $n = 2$, every rank $n - 1$ map is already a constant and the result holds. If $n > 2$, then a rank $n - 1$ map f cannot be uniform and hence, by [20], there exists $g \in G$ such that $\text{rank}(fgf) < \text{rank}(f) = n - 1$. Thus let $n > n - 1 > r_k > \ldots > r_1$ be the possible ranks of the elements in $\langle G, f \rangle$. It is clear that for every $t \in \langle G, f \rangle$ and every $g \in G$ we have $\text{rank}(tgf) \in \{\text{rank}(t), \text{rank}(t) - 1\}$, since the kernel of f does not allow to collapse more than two elements at once. This implies that $r_2 = r_1 + 1$. Thus, by Corollary 13, r_1 cannot be larger that 1 and hence $\langle G, f \rangle$ contains a constant, as claimed.

Proof of Theorem 4   As we have noted, the first part of the theorem is due to P.M. Neumann [20]. But that result can be easily shown using the graph $\text{Gr}(S)$. If the minimal rank of an element in a transformation semigroup S is 2, then $\text{Gr}(S)$ is bipartite, and its automorphism group cannot be primitive (if $n > 2$).

Since an element of minimal rank is uniform, we see that if f is non-uniform of rank 3 then the minimum rank in $\langle G, f \rangle$ is either 1 (so G synchronizes f) or 2 (so G is imprimitive, since primitive groups synchronize rank 2 maps).

Similarly, if f is non-uniform of rank 4 , then the minimum rank in $\langle G, f \rangle$ is 1 (so G synchronizes f), 2 (so G is imprimitive), or 3 (so the preceding corollary gives a contradiction). $\qquad\square$

6   Problems

The major open question regarding the content of this paper is the following problem.

Problem 1 Is it true that every primitive group of permutations of a finite set Ω synchronizes a non-uniform transformation on Ω?

Assuming the previous question has an affirmative answer (as we believe), an intermediate step in order to prove it would be to solve the following set of connected problems:

Problem 2   (a) Remove the word *idempotent* in Theorem 3(b).

(b) Extend Theorem 3(a) to rank $n - 3$.

(c) Prove that a primitive group synchronizes every non-uniform map of rank 5.

(d) Prove that if $S = \langle f, G \rangle$ contains a map of minimal rank r, with $\mathrm{rank}(f) > r > 1$, there can be no map in S of rank $r + 2$.

Observe that if this conjecture is true, then the previous question is immediately also true. To see that, assume the conjecture holds and suppose that f is a rank 5 map. By [20], if $r > 1$, then $r \geq 3$; thus $r \in \{3, 4\}$. Now the conjecture (if true) implies that $r + 2 \neq 5$, thus $r \neq 3$; on the other hand, Corollary 13 implies that $r \neq 4$. This implies (modulo the conjecture) that a rank 5 map f either satisfies $\mathrm{rank}(fgf) = 5$, for all $g \in G$, (and hence f is uniform by [20]), or f is synchronized by any primitive group.

The next class of groups lies strictly between primitive and synchronizing.

Problem 3 Is it possible to classify the primitive groups which synchronize every rank 3 map?

Note that there are primitive groups that do not synchronize a rank 3 map (see the example immediately before Section 2). And there are non-synchronizing groups which synchronize every rank 3 map. Take for example $\mathrm{PGL}(2, 7)$ of degree 28; this group is non-synchronizing, but synchronizes every rank 3 map since 28 is not divided by 3.

Let Ω be a finite set of size n and let G be a non-synchronizing primitive group on Ω. Let $s_1 < s_2 < \ldots < s_m$ be the sequence of all the possible sizes of the G-regular partitions of Ω (that is, for every s_i there exists a partition P of Ω, with $|P| = s_i$, and a set $S \subseteq \Omega$, such that Sg is a section for P, for all $g \in G$). The depth of a group is

$$
\mathrm{d}(G) := \begin{cases} s_2 - s_1 & \text{if } m > 1 \\ \infty & \text{otherwise.} \end{cases}
$$

Let n be a natural number. If there exist non-synchronizing groups of degree n, then define the depth of n as

$$\mathrm{d}(n) := \min\{\mathrm{d}(G) \mid G \text{ is a degree } n \text{ non-synchronizing primitive group}\}.$$

Problem 4 (a) Compute $\mathrm{d}(n)$, for every natural number n admitting degree n primitive non-synchronizing groups.

19

(b) Let G be a degree n non-synchronizing primitive group with sequence $s_1 < s_2 < \ldots < s_m$ as above. Prove that G synchronizes every rank $s_1 + e$ map (acting on the same set as G), where

$$e \in \{1, \ldots, \mathrm{d}(n)\} \cap \{1, \ldots, n-1\}.$$

(Observe that Corollary 13 already implies that this is true for $e = 1$.)

There are very fast algorithms to decide if a given set of permutations generate a primitive group.

Problem 5 Find an efficient algorithm to decide if a given set of permutations generate a synchronizing group.

Problem 6 Formulate and prove analogues of our results for semigroups of linear maps on a vector space. Note that linear maps cannot be non-uniform, but we could ask for linear analogues of results expressed in terms of rank, such as Theorems 1 and 3(a).

Problem 7 Solve the analogue of Problem 6 for independence algebras (for definitions and fundamental results see [1, 2, 3, 4, 5, 7, 8, 9, 13, 15, 16, 17]).

References

[1] J. Araújo. Normal semigroups of endomorphisms of proper independence algebras are idempotent generated. *Proc. Edinburgh Math. Soc.* **45** (2) (2002), 205–217.

[2] J. Araújo. Generators for the semigroup of endomorphisms of an independence algebra. *Algebra Colloq.* **9** (4) (2002), 375–282.

[3] J. Araújo. Idempotent generated endomorphisms of an independence algebra. *Semigroup Forum* **67** (3) (2003), 464–467.

[4] J. Araújo. Lifts for Semigroups of Monomorphisms of an Independence Algebra. *Colloquium Mathematicum.* **97** (2003), 277–284.

[5] J. Araújo. Lifts for Semigroups of Endomorphisms of an Independence Algebra *Colloquium Mathematicum.* **106** (2006), 39–56.

[6] J. Araújo, W. Bentz and P.J. Cameron, Groups Synchronizing a Transformation of Non-Uniform Kernel.

http://arxiv.org/abs/1205.0682

[7] J. Araújo, M. Edmundo and S. Givant. v^*-Algebras, Independence Algebras and Logic. *International Journal of Algebra and Computation* **21** (7) (2011), 1237–1257.

[8] J. Araújo and J. Fountain. The Origins of Independence Algebras *Proceedings of the Workshop on Semigroups and Languages (Lisbon 2002)*, World Scientific, (2004), 54–67

[9] J. Araújo and J.D. Mitchell. Relative ranks in the monoid of endomorphisms of an independence algebra. *Monatsh. Math.* **151** (1) (2007), 1–10.

[10] F. Arnold and B. Steinberg, Synchronizing groups and automata. *Theoret. Comput. Sci.* **359** (2006), no. 1-3, 101–110.

[11] J. Bamberg, N. Gill, T.P. Hayes, H.A. Helfgott, A. Seress and P. Spiga, Bounds on the diameter of cayley graphs of the symmetric group.

http://arxiv.org/pdf/1205.1596.pdf

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

[13] P. J. Cameron and C. Szabó, Independence algebras, *J. London Math. Soc.*, **61** (2000), 321–334.

[14] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics **163**, Springer, New York, 1996.

[15] J. Fountain and A. Lewin. Products of idempotent endomorphisms of an independence algebra of finite rank. *Proc. Edinburgh Math. Soc.* **35** (2) (1992), 493–500.

[16] J. Fountain and A. Lewin. Products of idempotent endomorphisms of an independence algebra of infinite rank. *Math. Proc. Cambridge Philos. Soc.* **114** (2) (1993), 303–319.

[17] V. Gould, Independence algebras. *Algebra Universalis* **33** (1995), 294–318.

[18] H.A. Helfgott and A. Seress, On the diameter of permutation groups, *(to appear on the Annals of Math.)*

http://arxiv.org/abs/1109.3550

[19] I. Levi, R. McFadden, D. McAlister, Groups Associated with Finite Transformation Semigroups. *Semigroup Forum* **61** (2000), 453–467.

[20] P. M. Neumann, Primitive permutation groups and their section-regular partitions. *Michigan Math. J.* **58** (2009), 309–322.

[21] J.-E. Pin, Černý's conjecture.

http://www.liafa.jussieu.fr/~jep/Problemes/Cerny.html

[22] I. Rystsov, Quasioptimal bound for the length of reset words for regular automata. *Acta Cybernet.* **12** (1995), no. 2, 145–152.

[23] A.N. Trahtman, Bibliography, synchronization TESTAS

http://www.cs.biu.ac.il/~trakht/syn.html

[24] A.N. Trahtman, *The Černý Conjecture for Aperiodic Automata*, Discr. Math. & Theoret. Comput. Sci. **9**(2007), (2) 3–10.

[25] Edward Szpilrajn-Marczewski, Sur deux propriétés des classes d'ensembles, *Fund. Math.* **33** (1945), 303-307.