Groups Synchronizing a Transformation of Non-Uniform Kernel

João Araújo Wolfram Bentz Peter J. Cameron

May 31, 2014

Abstract

Suppose that a deterministic finite automata $A = (Q, \Sigma)$ is such that all but one letters from the alphabet Σ act as permutations of the state set Q and the exceptional letter acts as a transformation with non-uniform kernel. Which properties of the permutation group G generated by the letters acting as permutations ensure that A becomes a synchronizing automaton under every possible choice of the exceptional letter (provided the exceptional letter acts as a transformation of non-uniform kernel)? Such permutation groups are called *almost synchronizing*. It is easy to see that an almost synchronizing group must be primitive; our conjecture is that every primitive group is almost synchronizing.

Clearly every synchronizing group is almost synchronizing. In this paper we provide two different methods to find non-synchronizing, but almost synchronizing groups. The infinite families of examples provided by the two different methods have few overlaps.

The paper closes with a number of open problems on group theory and combinatorics.

2010 *Mathematics Subject Classification*: 68Q15, 68Q70, 20B15, 20B25, 20B40, 20M20, 20M35.

Keywords: Algebraic theory of languages and automata; Complexity classes; Computational methods; Finite automorphism groups of algebraic, geometric, or combinatorial structures; Primitive groups; Pseudo-cores; Semigroups in automata theory; Semigroups of transformations; Synchronizing automata.

1 Introduction

Imagine that you are in a dungeon consisting of a number of interconnected caves, all of which appear identical. Each cave has a number of one-way doors of different colors through which you may leave; these lead to passages to other caves. There is one more door in each cave; in one cave the extra door leads to freedom, in all the others to instant death. You have a map of the dungeon with the escape door identified, but you do not know in which cave you are. If you are lucky, there is a sequence of doors through which you may pass which take you to the escape cave from any starting point. The example below shows this.

In the example, the sequence (BLUE, RED, BLUE, BLUE) always brings you to cave number 3. In this situation we say that the dungeon (in fact a finite deterministic automaton) admits a *synchronizing* word (or a *reset* word) and in general we are interested in the following question: for a given finite deterministic automaton, does there exist a synchronizing word?

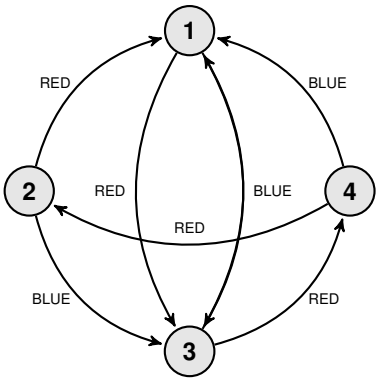

Figure 1: The Dungeon

These type of situations appear in many different contexts. For example, from time to time software enters a faulty state. To recover from this state, many systems use some kind of backward error recovery approach, such as resetting the computer or restarting a database from a checkpoint. However, this is not always possible; as an extreme illustration of this, consider the programmable and autonomous computing machine made out of biomolecules introduced by Benenson, Paz-Elizur, Adar, Keinen, Livneh and Shapiro in the 2001 issue of *Nature* [5]. For such cases, a more interesting approach consists in doing forward error recovery: something that can bring the process to a known state, irrespective of its current state. Yet another example is the concept of *self-stabilization* in distributed systems introduced in Dijkstra's seminal paper [12]. For instructive illustrations of the practical usefulness of synchronization please see [1, 24] and also the talk [25]; for the fast growing bibliography on the topic we refer the reader to the websites [19, 22].

There exist efficient algorithms to decide whether a given automaton admits a synchronizing word or not, or for obtaining relatively short synchronizing words (see for example [13, 24]). In addition, Berlinkov proved that a random automaton with n states and any fixed non-singleton alphabet is synchronizing with high probability [6]. In this paper we take the stand of [3, 18], that is, we are interested in the groups that together with any non-invertible transformation generate a constant.

Our results hence amount to establishing corresponding properties of groups (see below), which are of interest in their own right, but also for the original study of automata. For example, the well-known Černý conjecture states that a synchronizing automaton with n states has a synchronizing word of length at most $(n-1)^2$. This conjecture has been established in the special case that the transformation semigroup of the automaton is aperiodic [23], that is a semigroup in which all subgroups are trivial. So it remains to prove the conjecture for semigroups in which the subgroups are not trivial; the case in which there exists a permutation group is a particular case of this general problem. In addition, the known examples witnessing the Černý bound contain a permutation so they make it especially interesting to study the automata whose transition contains a permutation group. Finally, if our main conjecture is true we will have highly efficient decision algorithms for the situation of multiple automata with the same underlying permutation group.

For a natural n, let S_n and T_n be, respectively, the symmetric group and the full trans-

formation monoid on the set $X = \{1, \ldots, n\}$. We say that a group $G \leq S_n$ synchronizes a transformation $t \in T_n \setminus S_n$ if the semigroup $\langle G, t\rangle$ contains a constant map.

In this paper we adopt an approach similar to [3, 18], which concern groups that synchronize any non-invertible transformation $t \in T_n \setminus S_n$. A group $G \leq S_n$ is said to be non-synchronizing if there exists a partition P of the set X and a section S such that, for all $g \in G$, Sg is a section for P. Such a section is said to be G-regular and it is proved in [18] that any partition admitting a G-regular section must be uniform (that is, all its blocks have the same size). A group that is not non-synchronizing is said to be synchronizing; a synchronizing group $G \leq S_n$ synchronizes every non-invertible transformation $t \in T_n$. (This result was first proved by the first author [2] and was included in [18].)

A synchronizing group must be primitive ([2, 3, 18]), that is, given any set $S = \{x, y\} \subseteq X$, and given any partition of X into two blocks $P = \{P_1, P_2\}$, there exists a permutation $g \in G$ such that Sg is a section (or transversal, or cross-section) for the partition P. In addition, if we have a singular map t such that $\mathrm{rank}(t) > 1$ and a primitive group G, that together with t does not generate maps of rank lower than t, then G is non-synchronizing, and the kernel of t (that is, the set of pairs of states (x, y) such that $xt = yt$) induces a uniform partition [18].

Based on this result, we ask the following question: is it true that a primitive group G synchronizes every map t whose kernel is non-uniform? We call such groups *almost synchronizing*. Our conjecture is that every primitive group is almost synchronizing, but such a proof will likely require the (yet to be done) classification of the transitive synchronizing groups.

In this paper we provide two methods to find non-synchronizing but almost synchronizing groups. For the first method, we introduce an hierarchy in the class of non-synchronizing groups and prove that the first level of that hierarchy, what we call *parameter* 2 *non-synchronizing groups*, are almost synchronizing (provided they satisfy a weak extra condition that holds for all parameter 2 non-synchronizing groups we know); in addition we prove that there are infinitely many parameter 2 non-synchronizing groups. We hope that this approach can be generalized for the parameter k non-synchronizing but almost synchronizing groups (for $k > 2$).

In the second method we use a totally orthogonal approach, much more combinatorial, and based on some recent results by Godsil and Royle [16]. Again we prove that this method leads to infinite families of almost synchronizing groups, with little overlap with the groups found using the first method.

2 First method: notation and preliminary results

In this paper we make the global assumption that $G \leq S_n$ is a primitive group.

Before introducing our notation, we would like to make two observations. First, we observe that an almost synchronizing group is primitive. If G is imprimitive, then it fails to synchronize a map t which collapses one block of imprimitivity into one single point in that block, and is the identity elsewhere. This map is not uniform. In addition G, together with t, cannot generate a constant since the rank of any map in this semigroup will be at least the number of imprimitivity blocks.

The second observation is that in fact we do not really need that the transition semigroup of an automaton contains a group of permutations, in order to be able to apply the results of groups of permutations. For example, suppose $K = g_1 a_1 g_2 a_2 \ldots g_k a_k g_{k+1}$ is a constant map generated by singular maps and permutations (a_i are the singular maps and g_i are the permutations) . We

claim that we can generate a constant map using only conjugates of the singular maps. In fact,

$$K = g_1 a_1 g_2 a_2 \dots g_k a_k g_{k+1} = a_1^{g_1} a_2^{g_1 g_2} a_3^{g_1 g_2 g_3} \dots a_k^{g_1 g_2 \cdots g_k} g_1 g_2 \dots g_k g_{k+1},$$

(where $a^g = gag^{-1}$). Thus $a_1^{g_1} a_2^{g_1 g_2} a_3^{g_1 g_2 g_3} \dots a_k^{g_1 g_2 \cdots g_k}$ is also a constant, and is generated by conjugates of the a_i. Therefore, if we know that a given group G together with any singular map generates a constant, then we know that any set of singular maps whose normalizer contains G, also generates a constant. (The normalizer of a set S of transformations on X is the group of permutations g of X such that $s^g \in \langle S \rangle$, for all $s \in S$.)

Given a set $S \subseteq X$ with $1 < |S| < n$, we define a graph Γ_S on the vertex set X by the rule that two distinct vertices x and y are adjacent if and only if there is an element $g \in G$ with $\{x, y\}g \subseteq S$. Following the standard convention, the complement of Γ_S will be denoted $\overline{\Gamma}_S$; we will denote adjacency in $\overline{\Gamma}_S$ by $\sim$. The neighborhood of an element x in $\overline{\Gamma}_S$ will be denoted by $\overline{\Gamma}_S(x) := \{y \mid x \sim y\}$ and the closed neighborhood of x in $\overline{\Gamma}_S$ will be denoted by $\overline{\Gamma}_S[x] := \{x\} \cup \{y \mid x \sim y\}$. Clearly the graph $\overline{\Gamma}_S$ is G-invariant (that is, it is an edge-disjoint union of orbital graphs for G), and hence is vertex-transitive; and S is an independent set in $\overline{\Gamma}_S$.

Lemma 1 *Suppose that T is a clique in $\overline{\Gamma}_S$ which meets every G-translate of S. Then*

$$\bigcap_{x \in T} \overline{\Gamma}_S[x] = T.$$

Proof: The hypothesis that T meets every G-translate of S is equivalent to saying that $|S| \cdot |T| = n$; so T is a maximal clique of $\overline{\Gamma}_S$. Clearly T is contained in the intersection on the left; if the intersection contained an additional point z, then $T \cup \{z\}$ would be a clique, a contradiction. ■

Let S and T be as in the previous lemma. We define the parameter $m(S, T)$ to be the smallest number m such that the intersection of the closed neighbourhoods of *any* m points of T in $\overline{\Gamma}_S$ is equal to T. Said otherwise, $m(S, T)$ is one more than the maximum number of neighbours in T of any point outside T in the graph $\overline{\Gamma}_S$. Clearly $m(S, T) \leq |T|$. Moreover, $m(S, T) \geq 2$. For suppose that $m(S, T) = 1$. Then $T = \overline{\Gamma}_S[x]$ for any $x \in S$; so T is a connected component of $\overline{\Gamma}_S$, contradicting the assumed primitivity of G.

The following lemma is immediate from the definitions.

Lemma 2 *Suppose that $m(S, T) = 2$. Then the G-invariant graph $\overline{\Gamma}_S$ has the property that every point x has a neighbourhood $\overline{\Gamma}_S(x)$ having a connected component which is a complete graph. In particular, if $\overline{\Gamma}_S$ is edge-transitive, then $\overline{\Gamma}_S(x)$ is a disjoint union of complete graphs.*

In order to formulate our main theorem, we recall some definitions. A partition P of X is a *non-synchronizing partition* for G if there is a subset S of X such that $|S \cap T| = 1$ for every part T of P. The set S is called a *G-regular section* for P. It follows from earlier remarks that a group G is non-synchronizing if and only if it has a non-synchronizing partition.

We define a parameter $m(G)$ as follows: $m(G)$ is the maximum of $m(S, T)$, over all pairs for which T is a part of a non-synchronizing partition P for which S is a G-regular section. Note that such a set T is indeed a clique in Γ_S satisfying $|S| \cdot |T| = n$. Note also that the existence of such S, T, P is equivalent to the group G being non-synchronizing; the parameter $m(G)$ is not defined unless G is non-synchronizing. We call $m(G)$ the *non-synchronizing parameter* of G.

We also need an additional condition. For two distinct G-non-synchronizing partitions P and P' of the same rank k, let $M(P, P') = \frac{|P \cap P'|}{k}$; and set $M(G)$ to be the maximum over all such pairs.

3 First method: the main result

We will show that every non-synchronizing group $G \leq S_n$ with $m(G) = 2$ and $M(G) \leq 1/2$ is almost synchronizing, that is, it synchronizes every non-uniform transformation. (Note that condition $M(G) \leq 1/2$ is satisfied by all examples of groups with $m(G) = 2$ known to us.)

Throughout this section let $G \leq S_n$ be such a group, and $t \in T_n$ be a map whose kernel is a non-uniform partition. Set $U = \langle G, t\rangle$, and let k_U be the smallest rank of the transformations in U, say $\mathrm{rank}(p) = k_U$, for some $p \in U$. It follows that all the maps in $\langle G, p\rangle$ either are in G or have rank k_U. Note that $k_U < \mathrm{rank}(t)$, as (by [18]), for some $g \in G$, we have $\mathrm{rank}(tgt) < \mathrm{rank}(t)$. Our goal is to show that $k_U = 1$.

Lemma 3 *With notation as above, there exists a map $q \in U$ such that $\mathrm{rank}(q) > k_U$, $\mathrm{rank}(qgq) \in \{\mathrm{rank}(q), k_U\}$ for all $g \in G$, and that there exists an $h \in G$ with $\mathrm{rank}(qhq) = k_U$.*

Proof: Let

$$M = \{a \in \langle G, t\rangle \mid \mathrm{rank}(a) > k_U \text{ and } (\exists h \in G)\ \mathrm{rank}(aha) = k_U\}.$$

As $\mathrm{rank}(t) > k_U$, there exist elements $g_1, \ldots, g_n \in G$, such that $\mathrm{rank}(tg_1t \ldots tg_{n-1}t) > k_U$ and $\mathrm{rank}(tg_1t \ldots tg_nt) = k_U$. This implies that

$$\mathrm{rank}\left((tg_1t \ldots g_{n-1}t)g_n(tg_1t \ldots tg_{n-1}t)\right) \leq \mathrm{rank}(tg_1t \ldots g_nt) = k_U$$

and in fact $\mathrm{rank}\left((tg_1t \ldots g_{n-1}t)g_n(tg_1t \ldots tg_{n-1}t)\right) = k_U$, as k_U is the smallest rank possible. Hence M is non-empty. Let $q \in M$ be of minimal rank. We claim that q satisfies the desired property.

By definition of M, $\mathrm{rank}(q) > k_U$ and there exists $h \in G$, with $\mathrm{rank}(qhq) = k_U$. Let $g \in G$. If $\mathrm{rank}(qgq) > k_U$, then $\mathrm{rank}((qgq)h(qgq)) = \mathrm{rank}(qg(qhq)gq) \leq \mathrm{rank}(qhq) = k_U$. As above, it follows that $\mathrm{rank}((qgq)h(qgq)) = k_U$. Thus $qgq \in M$ and as q has minimal rank in M, $\mathrm{rank}(qgq) = \mathrm{rank}(q)$. The result follows. ■

Fix any map q satisfying the condition of Lemma 3, and denote by $Q_q \subseteq G$ the set of group elements g such that $\mathrm{rank}(qgq) = k_U < \mathrm{rank}(q)$. (If q is clear we might write Q instead of Q_q.)

We will make repeated use of transformations of the form qgq and $qhqgq$, where $h, g \in G$. Let the partition induced by $Ker(q)$, $Ker(qgq)$ and $Ker(qhqgq)$ be denoted by K, K_g, and $K_{h,g}$, respectively, and let $X_g = Xqgq$, $X_{h,g} = Xqhqgq$. We will occasionally blur the distinction between partition and equivalence relations.

Observe that, for all $(g, h, h') \in Q \times G \times Q$, we have that $X_g h$ is a section for $K_{h'}$. Otherwise, $qgqhqh'q$ would have rank smaller than $\mathrm{rank}(qgq) = k_U$. Therefore $\{X_g \mid g \in Q\}$ is a set of G-regular sections for every partition in the set $\{K_g \mid g \in Q\}$.

The following Lemma is a direct consequence of $m(G) = 2$.

Lemma 4 *Suppose that $S \subseteq X$ is a G-section for two (necessarily non-synchronizing) partitions P and P'. If $x \neq y$ and $y \in [x]_P \cap [x]_{P'}$, then $[x]_P = [x]_{P'}$.*

Proof: As $m(G) = 2$, we get that

$$[x]_P = \overline{\Gamma}_S[x] \cap \overline{\Gamma}_S[y] = [x]_{P'}.$$

■

The next two results will show that if G is not almost synchronizing, then the transformation q will take a very specific form.

Lemma 5 *If $k_U > 1$, then for any $g \in G$, a block of K_g is either a block of K or a union of singleton blocks from K.*

Proof: We may assume that $g \in Q$, the result being trivially true otherwise. Let A_1 and A_2 be distinct blocks of K such that $A_1 \cup A_2$ is contained in a block B of K_g, say $A_1 q = \{a_1\}$ and $A_2 q = \{a_2\}$ with $a_1 \neq a_2$.

As $k_U > 1$, $\{B, X - B\}$ is a partition of X. By primitivity, there exists an $h \in G$ such that $a_1 h \in B$ and $a_2 h \notin B$. Note that for any $g' \in G$, $X_g g'$ is a section for both K_g (as noted above) and $K_{h,g}$ (otherwise, $qgqg'qhqgq$ would have rank smaller than qgq). So, by the previous lemma, we know that any two blocks of K_g and $K_{h,g}$ that have two elements in common must agree.

However, the A_1-block of K_g contains A_2 while the A_1-block of $K_{h,g}$ does not. Hence A_1 cannot contain two elements and must be a singleton. The general result follows by symmetry. ■

Lemma 6 *Let $k_U > 1$. Then the partition K consists of r sets of order 1, and s sets of order $p > 1$, such that r is a multiple of p, $r < sp$, $r \geq 1$, $s \geq 1$.*

Proof: Pick any $g \in Q_q$. In order for qgq to have smaller rank then q, only singleton classes of the kernel can form larger blocks of K_g by the previous lemma. As qgq is uniform by the theorem of [18], the non-singleton classes must have the same size, say p. Moreover, the singletons must combine in multiples of p. As q is non-uniform we also get that $s, r \geq 1$

Now pick an element $d \notin im(q)$ and an image f of a non-singleton block of K. Let $h \in G$ be such that dh is in the union of the singleton classes of K and fh in its complement. Note that $\mathrm{rank}(qhq) < \mathrm{rank}(q)$ as $dhq \notin X_h$, and hence $\mathrm{rank}(qhq) = k_U$. However this requires that h maps all images of singleton classes into non-singleton classes (of K). As h also maps f into this set, it follows that r is strictly less than sp. ■

The lemma in particular shows that for any $g \in Q$, over half of the K_g-blocks are also blocks of K, as opposed to blocks made up of singleton classes of K. We are now ready to prove our main theorem.

Theorem 7 *Let $G \leq S_n$ be a non-synchronizing group with $m(G) = 2$ and $M(G) \leq 1/2$. If $t \in T_n$ is a transformation such that $Ker(t)$ is a non-uniform partition, then $\langle G, t \rangle$ contains a constant function; that is, G is almost synchronizing.*

Proof: Assume otherwise, i.e. that in the notation from above $k_U > 1$, and let q be a transformation satisfying the conditions of Lemma 3 and Lemma 6. Let $g \in Q_q$ such that $\mathrm{rank}(qgq) = k_U$, and let $(a, b) \in K_g$ such that $(a, b) \notin K$. Let $h \in G$ satisfy $aqh \in B$, $bqh \notin B$ for some block B of K_g.

Consider the functions $qhqgq$ and qgq, both of rank k_U. Note that X_g must be a G-regular section for both $K_{h,g}$ and K_g. All non-singleton blocks of K are in K_g by Lemma 5. The same holds for $K_{h,g}$, as it needs to be unifom and contained in K.

By Lemma 6 we have that the number of these blocks is larger than $k_U/2$. Our assumption $M(G) \leq 1/2$ now shows that $K_g = K_{h,g}$. However, it is easy to check that $(a, b) \notin K_{h,g}$.

Hence $k_U = 1$ and $\langle G, t\rangle$ contains a constant function. ■

4 First method: examples

We now give two infinite classes of examples and one sporadic example of groups which satisfy the hypotheses of the main theorem, and hence which synchronize any non-uniform mapping.

A sporadic example The automorphism group of the 3×3 grid (the wreath product of S_3 with S_2) and its primitive subgroup of index 2, are examples. For there are four non-synchronizing partitions: the rows and columns of the grid, and two partitions into diagonal sets (corresponding to the even and odd permutations of $\{1, 2, 3\}$ respectively). It is easy to see that, for these groups, $m(G) = 2$, and $M(G) = 0$ (since distinct non-synchronizing partitions have no sets in common).

Examples from projective planes Let G be the group $\mathrm{P\Gamma L}(3, q) \cdot 2$ or a subgroup containing $\mathrm{PSL}(3, q) \cdot 2$, where 2 denotes the *inverse transpose automorphism*. The subgroup of index 2 acts on the projective plane over the field $\mathrm{GF}(q)$, and the outer automorphism induces a duality of the plane interchanging points and lines. Then G acts on X, the set of *flags* (incident point-line pairs) in the projective plane. There are three orbits of G on pairs of flags:

- $O_1 = \{\{(P, L), (P', L')\} : P = P' \text{ or } L = L'\}$;
- $O_2 = \{(P, L), (P', L')\} : P \in L' \text{ or } P' \in L\}$;
- O_3, the remaining pairs (consisting of "opposite" flags).

There are only two non-synchronizing partitions for G. In the first partition, two flags are in the same part if they share a point; in the second, they are in the same part if they share a line. These two partitions have no common parts, so $M(G) = 0$.

A G-regular section for either partition consists of a set of $q^2 + q + 1$ flags, no two sharing a point or a line. Such a set can be constructed as an orbit on flags of a *Singer cycle* of G, a cyclic subgroup of order $q^2 + q + 1$ permuting points and lines transitively. It must contain a pair of flags lying in O_2 and a pair lying in O_3. So the edges of $\overline{\Gamma}_S$ are the pairs in O_1. Now any two flags adjacent in this graph determine a common point or line, so the intersection of their closed neighbourhood consists of all flags using this point or line. Thus $m(G) = 2$.

Examples from symplectic groups Let G be the projective symplectic group $\mathrm{PSp}(4, q)$, where q is a power of 2, or any group obtained by adjoining field automorphisms. The group G acts on the symplectic generalized quadrangle $W(q)$ whose points are those of the 3-dimensional projective space over $\mathrm{GF}(q)$, and whose lines are the lines of projective space which are totally isotropic with respect to a symplectic polarity. The only G-invariant graphs are the *collinearity graph* of the quadrangle (two vertices joined if they are orthogonal with respect to the symplectic form) and its complement.

The only non-synchronizing partitions for G are *spreads* of lines, families of pairwise disjoint lines covering the point set; the G-section for such a partition is an *ovoid*, a set of points meeting every line in precisely one point. (The other possibility for a non-synchronizing partition would be a partition into ovoids; but a theorem of Butler [9] shows that any two ovoids intersect in an odd number of points, so no such partition exists.) A spread consists of q^2+1 lines, each of cardinality m$q+1$. If S is an ovoid, then $\bar{\Gamma}_S$ is the collinearity graph. A generalized quadrangle has the property that any point x not on a line l is collinear with a unique point of l; so $m(G)=2$.

Since the characteristic is 2, the generalized quadrangle admits a *duality* interchanging points and lines and preserving incidence. Such a duality interchanges spreads with ovoids; so the maximum size of the intersection of two spreads is equal to the maximum size of the intersection of two ovoids. This parameter was first studied by Glynn [15], who showed that two ovoids intersect in at most $q(q-1)/2$ points. (A more accessible proof is in Butler [10].) So

$$M(G) \leq \frac{q(q-1)}{2(q^2+1)} < \frac{1}{2},$$

and our main theorem shows that G is almost synchronizing.

5 Second method: graphs

The core of a graph Γ is the smallest graph Δ that is homomorphically equivalent to Γ (that is, there exist homomorphisms in both directions). The core of Γ is unique up to isomorphism and is an induced subgraph of Γ. It is well known that all the endomorphisms of a core are automorphisms.

We will denote the clique number of a graph Γ by $\omega(\Gamma)$, and its chromatic number by $\chi(\Gamma)$.

There is a natural connection between transformation monoids and graphs. To every graph X, we associate its *endomorphism monoid* $\mathrm{End(X)}$. In the other direction, given a transformation monoid M on Ω, we define a graph $\mathrm{Gr}(M)$ on Ω by the rule that $x \sim y$ in $\mathrm{Gr}(X)$ if and only if there is no element $f \in M$ satisfying $xf = yf$. The next result gives some simple properties of this construction. This is an extension of the methods in [11].

Theorem 8 *(a)* $\mathrm{Gr}(M)$ *has complete core; that is, its clique number and chromatic number are equal.*

(b) $M \leq \mathrm{End}(\mathrm{Gr}(M))$.

Proof: (a) Let f be an element of minimal rank in M. Then the induced subgraph on the image of f is complete; for if x, y are not joined, then there exists $g \in M$ with $xg = yg$, so fg has smaller rank than f. Now the map f is a colouring of $\mathrm{Gr}(M)$ (since if two vertices have the same image under f they cannot be adjacent), and the number of colours is equal to the rank of f.

(b) Take $f \in M$, and suppose that f is not an endomorphism of $\mathrm{Gr}(M)$. Now f cannot collapse an edge of $\mathrm{Gr}(M)$ to a single vertex, by definition; so it must map an edge xy to a non-edge uv. But then there is $g \in M$ with $ug = vg$; so $x(fg) = y(fg)$, a contradiction. ■

Theorem 9 *Let f be a map not synchronized by the permutation group G. Then there is a G-invariant graph X with $f \in \mathrm{End(X)}$ and $\omega(X) = \chi(X)$.*

Proof: Let $M = \langle G, f \rangle$ and $X = \mathrm{Gr}(M)$. ■

We conclude that a group G is non-synchronizing if and only if there is a G-invariant graph X, not complete or null, with $\omega(X) = \chi(X)$.

6 Second method: results of Godsil and Royle

Godsil and Royle [16] have shown that certain strongly regular graphs X are what they call *pseudo cores*: this means that every endomorphism of X is either an automorphism or a colouring. (We recall that a core is a graph for which every endomorphism is an automorphism.)

If we can show that a primitive permutation group G has the property that the only G-invariant graphs X with $\omega(X) = \chi(X)$ are pseudocores, then we have shown that G is almost synchronizing; for if f is not synchronized by G, then f is a colouring of a G-invariant graph X; so f has minimal rank in $\mathrm{End(X)}$, and is uniform.

In each case, a necessary condition is that any clique of maximum size in the graph is a line of the corresponding geometry. There is an inequality which guarantees this, which we have placed in square brackets. If this condition could be shown directly, this inequality would not be required. No condition is required for generalized quadrangles, since an edge lies in a unique maximal clique, namely a line.

Among the graphs that Godsil and Royle show to be pseudo cores are

(a) the line graphs of 2-$(v, k, 1)$ designs with $k > 2$ [and $v > k(k^2 - 2k + 2)$].

(b) the graphs on n^2 points obtained from orthogonal arrays $O(2, k, n)$, where $k > 2$ [and $n > (k - 1)^2$].

(c) The collinearity graphs of generalized quadrangles with $s, t > 1$.

We refer to their paper for definitions.

7 Second method: Examples

Theorem 10 *(a) Let G be a subgroup of $\mathrm{P\Gamma L}(n, q)$ containing $\mathrm{PSL}(n, q)$, where $n \geq 5$, acting on the lines of the projective space. Then G is almost synchronizing.*

(b) Let G be the semidirect product of the additive group of $\mathrm{GF}(p^2)$ by the subgroup of index 2 in the multiplicative group of the field, where p is prime. Then G is almost synchronizing.

(c) Let G be the symplectic group $\mathrm{PSp}(4, q)$ or be obtained from it by adjoining field automorphisms, where q is a power of 2. Then G is almost synchronizing.

Proof: (a) Here G is a rank 3 group, and so there are just two non-trivial G-invariant graphs, the concurrence graph of the lines of the projective space and its complement.

The lines form a 2-$(v, q + 1, 1)$ design, where $v = (q^n - 1)/(q - 1)$. We see that $v > k(k^2 - 2k + 2)$ if and only if $n \geq 5$. So in this case, the graph is a pseudocore. (The cliques

of maximum size consist of all lines through a point. If $n = 4$, there are further such cliques, namely all the lines in a plane, and the method fails.)

In the complementary graph, the clique number is at most $(q^n - 1)/(q^2 - 1)$, since clearly we cannot find more than this number of disjoint lines. However, a maximal coclique has size $(q^{n-1}-1)/(q-1)$ (these are cliques in the complementary graph, and consist of all lines through a point), and any two of these cocliques intersect; so the chromatic number is strictly greater than

$$\frac{(q^n - 1)(q^{n-1} - 1)/(q^2 - 1)(q - 1)}{(q^{n-1} - 1)/(q - 1)},$$

the numerator being the total number of vertices; so the clique number and chromatic number are not equal.

Note that the geometry has a *parallelism* (a partition of the lines into spreads) only if n is even; so for n odd, the groups are synchronizing. Parallelisms have been shown to exist for $n = 4$ by Beutelspacher [7] and $q = 2$ by Baker [4], and are conjectured to exist for all even n.

(b) Again the group has rank 3, and the two G-invariant graphs correspond to orthogonal arrays $(2, (p + 1)/2, p)$. The vertices in each case are points of the affine space, and the $p + 1$ directions of lines are partitioned into two subsets of $(p + 1)/2$ such that in each graph, two vertices are joined if the line joining them has direction lying in the corresponding set. In this case, the inequality given in square brackets is not satisfied; but the graphs are pseudo cores provided that we can prove otherwise that there are no cliques of size p other than lines of the affine space.

This follows from Theorem 24' of Rédei [20], according to which a set of p points in the affine plane which is not a line determines at least $(p + 3)/2$ directions. Since only $(p + 1)/2$ directions correspond to adjacency, no such set is a clique.

So both graphs are pseudo cores, and the result follows.

(c) For any classical generalized quadrangle, the automorphism group is a rank 3 group whose invariant graphs are the collinearity graph and its complement. The number of points is $(s + 1)(st + 1)$, and a line has $s + 1$ points.

The collinearity graph has clique number $s + 1$ (the cliques are lines); an independent set meet each line in at most one point, and so has size at most $st + 1$, with equality if and only it is an ovoid. So the chromatic number is $s + 1$ if and only if there is a partition into ovoids.

In the complement of the collinearity graph, as we have seen, the clique number is at most $st + 1$, with equality if and only if there is an ovoid; the chromatic number is at least $st + 1$, with equality if and only if there is a spread (a set of lines partitioning the point set).

So one of these groups is almost synchronizing if the generalized quadrangle has ovoids and spreads but no partition into ovoids.

The symplectic generalized quadrangles in even characteristic have these properties. (Note that these examples in (c) are also covered by our first method.) ■

8 Some more examples

Here is a class of examples that use the same technique as that of Godsil and Royle but are not covered by their results. The symmetric group S_m acting on 2-sets (for $m \geq 5$) is synchronizing

if and only if m is odd. It is the automorphism group of a 2-$(m, 2, 1)$ design; but this is not covered since Godsil and Royle assume that the block size is greater than 2.

Theorem 11 *The symmetric group S_m acting on 2-sets is almost synchronizing if m is even and $m \geq 6$.*

Proof: As usual the groups have rank 3, and the graphs we have to consider are the line graph of the complete graph K_m and its complement.

The line graph of K_m has clique number $m-1$ (take all the edges containing a given point) and chromatic number $m-1$ if m is even (take a 1-factorization of K_m). The complement has clique number $m/2$ and chromatic number strictly greater. (This can be seen by an argument similar to the one we used for the projective space: the maximal cliques have size $m-1$ and any two intersect. In fact a result of Lovász [17] shows that the chromatic number is $m-2$.) So we only need consider the line graph.

Suppose that f is an endomorphism of $L(K_m)$ which is not an automorphism. Let C_i denote the $(m-1)$-clique consisting of all edges through the point i. Each such clique must be mapped to another by f; we have to show that they all collapse to a single clique.

We will use the fact that the octahedron (the induced subgraph on the six 2-subsets of a 4-set) is a pseudo-core, that is, every endomorphism which is not an automorphism maps it onto a triangle. This is easy to prove directly. Below we will say "the octahedron $abcd$" to mean the octahedron formed by the six pairs from this set.

Suppose that 12 and 34 map to the same point, which we may suppose to be 12. Then C_1 maps to either C_1 or C_2; without loss of generality, C_1 is mapped to C_1.

Consider the octahedron 1234. Since 12 and 34 map to 12, and 13 and 14 both map into C_1, the whole set maps into C_1.

Next we claim that C_2 maps to C_1. For it contains three points 12, 23, 24 which all map into C_1.

Finally, every pair ij maps into C_1. For consider the octahedron $12ij$; we know that all except ij map into C_1, so ij does as well. ■

This method also applies to the alternating group A_n and the Mathieu groups M_{12} and M_{24}.

9 Complexity

The person inside the dungeon wants to find as quickly as possible if the permutations in the automaton generate an almost synchronizing group. So that person needs a fast algorithm to decide the question in terms of the given group generators.

There exist efficient polynomial-time algorithms for deciding whether a permutation group with a given set of generators is transitive, or primitive, or 2-transitive. In particular, primitivity can be checked in time $O(n^2)$ if the number of generators is not too large. We refer to [21] for a survey of these algorithms. Indeed, if we are given an unnecessarily large set of generators, it can be transformed with *polynomial delay* into a set of size at most $n-1$ (this means that a polynomial amount of computation is done after reading each generator). After this has been done, the tests for transitivity etc. are polynomial in n.

The synchronizing property lies between primitivity and 2-transitivity, and currently no efficient algorithm is known. In fact, the best known algorithm is based on the considerations in

Section 5. It consists of the following steps:

(a) construct all the non-trivial G-invariant graphs;

(b) for each such graph X, decide whether $\omega(X) = \chi(X)$.

In the first step, the number of graphs is $2^r - 2$, where r is the number of G-orbits on the set of 2-subsets. Although this is exponential, for many primitive groups the number r is relatively small. The second step, however, is NP-hard for general graphs, though the possibility that it is easier for graphs with primitive automorphism group remains open.

We do not currently have any reasonable algorithm for testing whether a group is almost synchronizing. However if, as we suspect, this property is equivalent to primitivity, there would be a polynomial-time test!

For the particular groups in our examples, recognition by standard group-theoretic algorithms is easy and can certainly be done in random polynomial time.

10 Problems

The results in this paper prompt a number of very natural problems that might attract the attention of experts in computer science, combinatorics and geometry, groups and semigroups, linear algebra and matrix theory.

We could find no group G such that $m(G) = 2$ and $M(G) > \frac{1}{2}$ and hence we do not know if the latter condition is redundant.

Problem 10.1 *Is it true that $m(G) = 2$ implies $M(G) \leq \frac{1}{2}$?*

Even if this is not true, what really matters regarding the classification of non-synchrozoning but almost synchronizing groups, is to prove a result similar to Theorem 7, but with no assumptions on $M(G)$.

Problem 10.2 *Is it possible to prove Theorem 7 without any assumption about $M(G)$?*

Since we have a general result linking almost non-synchronizing groups and parameter 2 non-synchronizing groups, the next goal is a classification of these groups.

Problem 10.3 *Classify the primitive non-synchronizing groups G such that $m(G) = 2$.*

The parameter $m(G)$ induces an hierarchy on the class of non-synchronizing groups. We hope this hierarchy helps splitting the classification of synchronizing groups and almost synchronizing groups down to more tractable subclasses.

Problem 10.4 *For each $k \geq 2$, classify the primitive almost synchronizing groups such that $m(G) = k$.*

The main conjecture in this paper is that primitive groups are almost synchronizing.

Problem 10.5 *Is it true that primitive groups are almost synchronizing?*

In this setting, and regarding algorithms, the main problem is the following.

Problem 10.6 *Find an efficient algorithm to decide if a given set of permutations generate a synchronizing group.*

Acknowledgements

We are grateful to Simeon Ball and Tim Penttila for help with the literature on ovoids and spreads in symplectic generalized quadrangles.

We are also very grateful for the two referees for their very careful reviews and helpful suggestions that led to a much improved version of the paper.

The first author was partially supported by FCT through the following projects: Strategic Project of Centro de Álgebra da Universidade de Lisboa (PEst-OE/MAT/UI1043/2011); and Project Computations in groups and semigroups (PTDC/MAT/101993/2008). The second author has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. PCOFUND-GA-2009-246542 and from the Foundation for Science and Technology of Portugal. The third author is grateful to the Center of Algebra of the University of Lisbon for supporting a visit to the Centre in which some of this research was done.

References

[1] D. S. Ananichev and M. V. Volkov, Some results on Černý type problems for transformation semigroups, Semigroups and languages, 23–42, World Sci. Publ., River Edge, NJ, 2004.

[2] J. Araújo, A group theoretical approach to synchronizing automata and the Černy problem. Unpublished manuscript, 2006.

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

[4] R. D. Baker, Partitioning the planes of $\mathrm{AG}_{2m}(2)$ into 2-designs. *Discrete Math.* **15** (1976), no. 3, 205–211.

[5] Y. Beneson, T. Paz-Elizur, R. Adar, E. Keinan, Z. Livneh, E. Shapiro, Programable and autonomous computing machine made of biomolecules. *Nature* **414** (2001), no. 1, 430–434.

[6] M. V. Berlinkov, On the probability to be synchronizable.
http://arxiv.org/pdf/1304.5774v3.pdf

[7] A. Beutelspacher, On parallelisms in finite projective spaces. *Geometriae Dedicata* **3** (1974), 35–40.

[8] MAGMA. W. Bosma, John Cannon, and Catherine Playoust, The Magma algebra system. I. The user language. *J. Symbolic Comput.*, **24** (1997), 235–265.

[9] D. Butler, On the intersection of ovoids sharing a polarity. *Geometriae Dedicata* **135** (1978), 157–165.

[10] D. Butler, The maximum size of intersection of two ovoids. *J. Combinatorial Theory* (A) **116** (2009), 242–245.

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

[12] E.W. Dijkstra, Self-stabilizing systems in spite of distributed control. *Communications of the ACM* **17** (11) (1974), 643–644.

[13] D. Eppstein, Reset sequences for monotonic automata. *SIAM J. Comput.* **19** (1990), 500–510.

[14] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.12; 2008. (http://www.gap-system.org)

[15] D. Glynn, "Finite projective planes and related combinatorial systems", PhD thesis, University of Adelaide, 1978.

[16] C. D. Godsil and G. F. Royle. Cores of geometric graphs. *Ann. Combinatorics* **15** (2011), 267–276.

[17] L. Lovász, Kneser's conjecture, chromatic number, and homotopy. *J. Combinatorial Theory* Ser. A **25** (1978), 319–324.

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

[19] J.-E. Pin, Černý's conjecture.

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

[20] L. Rédei, Lacunary Polynomials over Finite Fields. North-Holland, Amsterdam, 1973.

[21] Á. Seress, *Permutation Group Algorithms*, Cambridge Tracts in Mathematics **152**, Cambridge University Press, Cambridge, 2003.

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

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

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

[24] A.N. Trahtman, *Some new Features and Algorithms for the Study of DFA*, Open J. Discr. Math. **2** (2012), (2), 45–50.

[25] M. Volkov, Synchronizing finite automata

`http://csseminar.kadm.usu.ru/SLIDES/synchrolectures/lecture1.pdf`

João Araújo (corresponding author)
Universidade Aberta and Centro de Álgebra
Universidade de Lisboa
Av. Gama Pinto, 2, 1649-003 Lisboa
Portugal

(+351) 217904719
jaraujo@ptmat.fc.ul.pt

Wolfram Bentz
Centro de Álgebra
Universidade de Lisboa
Av. Gama Pinto, 2, 1649-003 Lisboa
Portugal
wfbentz@fc.ul.pt

Peter Cameron
Department of Mathematics
School of Mathematical Sciences at Queen Mary
University of London
P.J.Cameron@qmul.ac.uk