Synchronization 3: Synchronizing and separating groups

Peter J. Cameron

10-11 June 2010

The story so far

We have the following properties of permutation groups:

$$\begin{aligned}&\text{transitive} \Leftarrow \text{primitive} \Leftarrow \text{basic}\\ &\qquad \Leftarrow \text{2-set transitive} \Leftarrow \text{2-transitive.}\end{aligned}$$

Note in passing that each of these properties is closed upwards: a supergroup of a permutation group with the property also has the property.

We also said that a permutation group G on Ω is *synchronizing* if, for any $f : \Omega \to \Omega$ which is not a permutation, the monoid $\langle G, f\rangle$ contains a constant function.

Where does this concept fit into the hierarchy above?

Section-regular partitions

We start with three ingredients:

- G is a permutation group on Ω;
- π is a partition of Ω;
- S is a subset of Ω.

We say that S is a *section*, or *transversal*, of π, if S contains exactly one point of every part of π.

We say that π is *section-regular* for G, with section S, if Sg is a section for π, for every $g \in G$. (Here Sg is the set $\{sg : s \in S\}$.) Equivalently, S is a section for πg, for all $g \in G$.

Synchronization and section-regularity

Theorem 1. *The permutation group G on Ω is synchronizing if and only if there is no non-trivial section-regular partition for G.*

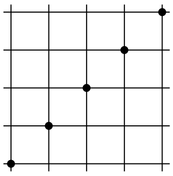
Proof. Suppose that π is a non-trivial section-regular partition. Let f map $v \in \Omega$ to the unique point s of S in the same part of π containing v. Then any map $g_1 f g_2 f \cdots g_r f$, for $g_1, \ldots, g_r \in G$, has image S; so G is not synchronizing.

Conversely, suppose that $\langle G, f\rangle$ contains no constant function, and, without loss, let f be an element of smallest possible rank in this monoid. Then one can check that, if S is the image of f, and π the partition of Ω into inverse images of elements of S, then π is section-regular with section S. □

Theorem 2. *A synchronizing group is primitive, and basic.*

Proof. If π is a non-trivial partition fixed by G, then π is section-regular for G, with any section S.

Now suppose that G is primitive but not basic, so that Ω is identified with Γ^n for some $n > 1$. Let π be the partition of Ω according to the element of Γ which occurs in the first coordinate, and let S be the diagonal $\{(x, x, \ldots, x) : x \in \Gamma\}$. Now every image of π under G is the partition according to the element of Γ in the ith coordinate, for some i; so S is a section for every such partition. □



The picture shows the structure for the non-basic group $G = S_5 \text{ Wr } S_2$. The rows and columns are partitions which are section-regular for the set of circled points; but no partition is fixed by G, since it contains elements swapping rows and columns.

Theorem 3. *A 2-set transitive group is synchronizing.*

Proof. Let G be 2-set transitive. Let π be any non-trivial partiton, and S a subset with $|S| > 1$. If $a, b \in S$ and c, d belong to the same part of π, there is an element $g \in G$ mapping $\{a, b\}$ to $\{c, d\}$; then Sg is not a section for π. □

Theorem 4. *The property of synchronization is closed upwards.*

Proof. If $G_1 \leq G_2$, then any section-regular partition for G_2 is clearly section-regular for G_1. □

An example

Let Ω be the set of all 2-element subsets of $\{1, \ldots, n\}$, and let G be the permutation group on Ω induced by the action of S_n on $\{1, \ldots, n\}$. Assume that $n \geq 4$.

Now G is primitive if and only if $n \geq 5$. For if $n = 4$, then the partition $\{\{12, 34\}, \{13, 24\}, \{14, 23\}\}$ is preserved by G, and G is imprimitive. (Some braces have been omitted for clarity.)

Suppose that $n \geq 5$, and let B be a block of imprimitivity containing 12. If B contains a pair disjoint from 12, say 34, then it contains every such pair, since the setwise stabiliser of 12 is transitive on these pairs. Then B contains 34 and 35, and as before contains every pair containing 3. We find in this manner that $B = \Omega$. A similar argument applies if B contains a pair intersecting 12, such as 13. So no non-trivial block exists, and G is primitive.

It is also easy to see that G is basic for $n \geq 5$.

Theorem 5. *The above group G is synchronizing if and only if n is odd.*

If n is even, we use the fact that the complete graph K_n can be edge-coloured with $n - 1$ colours; that is, there is a partition π of Ω into $n - 1$ sets of size $n/2$ with the property that any two pairs in the same part are disjoint. Now the set of all pairs containing 1 is a section for πg for any $g \in G$; so G is not synchronizing. (This gives us examples of groups which are basic but not synchronizing.)

Suppose that π is a section-regular partition with section S. Since S meets every part of π in a unique point, there are two possibilities:

- pairs in the same part of π intersect, while pairs in S are disjoint;
- pairs in the same part of π are disjoint, while pairs in S intersect.

The maximum number of intersecting pairs is $n - 1$, while the maximum number of disjoint pairs is $\lfloor n/2 \rfloor$. If n is odd, the product of these numbers is smaller than $n(n-1)/2 = |\Omega|$; so no section-regular partition can exist.

Neumann's separation lemma

We get further insight into synchronization from the following result which was first proved in the context of finitary permutation groups and has since found a variety of other uses.

Theorem 6. *Let G be a permutation group on a set Ω, and let A and B be finite subsets of Ω.*

- *If all G-orbits are infinite, then there exists $g \in G$ such that $Ag \cap B = \emptyset$.*
- *If G is transitive on Ω and $|\Omega| > |A| \cdot |B|$, then here exists $g \in G$ such that $Ag \cap B = \emptyset$.*

We will need the finite part of this theorem; so we give the proof.

Proof. Suppose that $|A| = k$, $|B| = l$, and $|\Omega| = n > kl$. If G is transitive on Ω, then the order of the stabiliser of a point is $|G|/n$; and, for any $a, b \in \Omega$, the set of elements $g \in G$ satisfying $ag = b$ is a right coset of the stabiliser of a (or a left coset of the stabiliser of b), so also has cardinality $|G|/n$.

Now the number of triples (a, b, g) with $a \in A$, $b \in B$ and $ag = b$ is $kl|G|/n < |G|$ (by assumption); so there is some element $g \in G$ lying in no such triple, so that $Ag \cap B = \emptyset$. □

Separating groups

Let G be a transitive permutation group on Ω, with $|\Omega| = n$. We say that G is *non-separating* if there exist subsets A, B of Ω, with $|A|, |B| > 1$ and $|A| \cdot |B| = n$, such that, for all $g \in G$, $Ag \cap B = \emptyset$; and G is *separating* otherwise (that is, if any pair A and B of subsets satisfying these conditions can be "separated" by an element of G).

So, for example, a transitive permutation group on a prime number of points is separating (vacuously, since no sets A, B can satisfy the requirements).

Theorem 7.

- *A separating group is synchronizing.*
- *A 2-set transitive group is separating.*

Proof. (a) If π is section-regular with section S, then S and a part of π cannot be separated.

(b) Use the same argument that showed that a 2-set transitive group is synchronizing, replacing S and a part of π by A and B. □

Examples

The group induced by the symmetric group S_n on 2-element subsets of $\{1, \ldots, n\}$ for odd $n \geq 5$ is separating but not 2-set transitive. The proof is virtually the same as the argument showing that this group is synchronizing.

Another example of a separating group which is not 2-set transitive is the cyclic group of prime order $p > 3$, acting regularly.

So, in our hierarchy

$$\begin{aligned} &\text{transitive} \Leftarrow \text{primitive} \Leftarrow \text{basic} \\ &\quad \Leftarrow \text{synchronizing} \Leftarrow \text{separating} \\ &\quad \Leftarrow \text{2-set transitive} \Leftarrow \text{2-transitive,} \end{aligned}$$

no arrows reverse except possibly that from separating to synchronizing.

Examples are more difficult to find; we will see some later.

A generalisation

Theorem 8. *Let G be a transitive permutation group on Ω, and let A and B be subsets of Ω, satisfying $|A| \cdot |B| = \lambda |\Omega|$ for some positive integer λ. Then the following are equivalent:*

- *for all $g \in G$, $|Ag \cap B| = \lambda$;*
- *for all $g \in G$, $|Ag \cap B| \geq \lambda$;*
- *for all $g \in G$, $|Ag \cap B| \leq \lambda$;*

The proof is an exercise.

We ssy that G is *λ-separating* if no such sets A, B with $|A|, |B| > \lambda$ exist.

It will turn out that a slightly different concept is better adapted to the study of synchronization, however.

Section-regular partitions are uniform

First we apply the above theorem. A partition π of Ω is *uniform* if all its parts have the same size.

Theorem 9. *Let G be transitive on Ω. Then any section-regular partition for G is uniform.*

Proof. Let π be section-regular with section S. If A is any part of π, we have $|Ag \cap S| = 1$. By the theorem, $|A| \cdot |S| = |\Omega|$. □

Multisets

A *multiset* of Ω is a function from Ω to the natural numbers (including zero). If A is a multiset, we call $A(i)$ the *multiplicity* of i in A. The set of elements of Ω with non-zero multiplicity is the *support* of A. We can regard a set as a special multiset in which all multiplicites are zero and one (identifying the set with its characteristic function).

The *cardinality* of A is

$$|A| = \sum_{i \in \Omega} A(i);$$

this agrees with the usual definition in the case of a set.

The *product* of two multisets A and B is the multiset $A * B$ defined by

$$(A * B)(i) = A(i)B(i).$$

This is a generalisation of the usual definition of intersection of sets; but the "intersection" of multisets is defined differently in the literature.

- The product of two sets is their intersection.
- The product of a multiset A and a set B is the "restriction of A to B", that is, points of B have the same multiplicity as in A, while points outside B have multiplicity zero.

- if we identify a multiset A with a vector v_A of non-negative integers with coordinates indexed by Ω, then we have $|A * B| = v_A \cdot v_B$ for all multisets A and B. In particular, $|A| = v_A \cdot j$, where j is the all-one vector.

The image of a multiset A under a permutation g is defined by

$$Ag(i) = A(ig^{-1}).$$

This agrees with the usual image of a set under a permutation.

Theorem 10. *Let G be a transitive permutation group on Ω, and let A and B be multisets of Ω. Then the average cardinality of the product of A and Bg is given by*

$$\frac{1}{|G|}\sum_{g\in G}|A * Bg| = \frac{|A|\cdot|B|}{|\Omega|}.$$

Proof. We count triples (a, g, b) with $a \in A$, $g \in G$, $b \in B$, and $bg = a$. (Points of A or B are counted according to their multiplicity.) There are $|A|$ choices for a and $|B|$ choices for b. Then the set of elements of G mapping b to a is a right coset of the stabiliser G_b (since G is transitive), so there are $|G|/|\Omega|$ such elements.

On the other hand, for each element $g \in G$, if $bg = a$, then this element belongs to $A * Bg$. The number of choices of a is equal to the sum of multiplicities in A, and for each one, the number of choices of b is the multiplicity of ag^{-1} in B, that is, of a in Bg. So the product counts the multiplicities correctly.

Equating the two sides gives the result. □

Spreading

Let G be a transitive permutation group on Ω, and A and B multisets of Ω. Consider the following four conditions:

$(1)_\lambda$: $|A * Bg| = \lambda$ for all $g \in G$.

(2): A is a set.

(3): B is a set.

(4): $|A|$ divides $|\Omega|$.

Note that

- $(1)_\lambda$ is symmetric in A and B.
- $(1)_\lambda$ with $\lambda = 1$ implies (2), (3) and (4). For, if $A(i) > 1$, the choosing g to map a point in the support of B to i, we would have $|A \cap Bg| > 1$; so (2) holds, and (3) is similar. Finally, if $(1)_\lambda$ holds with $\lambda = 1$ then $|A| \cdot |B| = |\Omega|$.
- If (2) and (3) hold, then we can replace product by intersection in $(1)_\lambda$.

We will call a multiset *trivial* if either it is constant or its support is a singleton.

The transitive permutation group G on Ω is *non-spreading* if there exist non-trivial multisets A and B and a positive integer λ such that $(1)_\lambda$, (3) and (4) hold, and is *spreading* otherwise.

Theorem 11. *The permutation group G on Ω is spreading if and only if, for any function $t : \Omega \to \Omega$ which is not a permutation and any non-trivial subset S of Ω, there exists $g \in G$ such that $|Sgt^{-1}| > |S|$.*

Proof. Suppose that G is non-spreading, and let the multiset A and set B be witnesses. Since $|A|$ divides $|\Omega|$, there is a function t from Ω to Ω so that $|at^{-1}|$ is proportional to the multiplicity of a in A (the constant of proportionality being $|\Omega|/|A|$). Let $S = B$. Then for any $g \in G$, we have

$$|Sgt^{-1}| = |A * Sg| \cdot |\Omega|/|A| = |S|,$$

by the definition of non-spreading.

Conversely, suppose that there is a function t and subset S for which the condition in the theorem is false. Let A be the multiset in which the multiplicity of a is equal to $|at^{-1}|$. Then we have $|A| = |\Omega|$ and it is false that $|A * Sg| > |S|$ for any $g \in G$; thus we have $|A \cap Sg| = |S|$ for all $g \in G$. We conclude that $(1)_{|S|}$, (3) and (4) hold, so that G is non-spreading. □

Spreading groups in the hierarchy

Theorem 12.
- *A spreading permutation group is separating.*
- *A 2-set-transitive group is spreading.*

Proof. (a) Witnesses to non-separation are also witnesses to non-spreading (with $\lambda = 1$).

(b) The arguments are similar to those we have seen before. □

We will see that neither implication reverses.

Spreading groups and the Černý conjecture

Theorem 13. *Let G be a spreading permutation group on Ω, and f a function from Ω to Ω which is not a permutation. Then $\langle G, f \rangle$ contains a reset word which has at most $n-1$ occurrences of f.*

In other words, the property of being spreading not only implies synchronization, but also realises the first part of our programme for bounding the length of the reset word.

Proof. Suppose that we have a set S_k with $|S_k| \geq k$, such that there is a word w in $\langle G, f \rangle$ with at most $k-1$ occurrences of k which maps S_k to a singleton.

By the preceding theorem, there exists $g \in G$ such that $S_{k+1} = S_k g f^{-1}$ satisfies $|S_{k+1}| \geq k+1$. We have $S_k = S_{k+1} f g^{-1}$, so the word $f g^{-1} w$ with at most k occurrences of f maps S_{k+1} to a singleton.

By induction on k, the result is proved. □

A non-spreading group

We have seen that S_n, acting on the set of 2-subsets of $\{1, \ldots, n\}$, is separating if n is odd and $n \geq 5$. We now show that it is not spreading.

Let A be a set of n pairs forming a cycle: $A = \{\{1,2\}, \{2,3\}, \ldots, \{n-1, n\}, \{n, 1\}\}$.

Let B be the set of $n-1$ pairs containing the fixed element 1. Then

- $|Ag \cap B| = 2$ for all $g \in G$;
- A and B are sets;
- $|A| = n$ divides $|\Omega| = n(n-1)/2$ if n is odd.