Synchronization 6: Examples

Peter J. Cameron

10-11 June 2010

Summary and direction

We have seen that

spreading ⇒ separating ⇒ synchronizing ⇒ basic

while, by the O'Nan–Scott Theorem, basic groups are affine, diagonal, or almost simple.

In this section, I will examine two families of almost simple groups, to see where they fit in this part of the hierarchy:

- the symmetric group S_n acting on k-sets;
- classical groups acting on their associated polar spaces.

We will see that

- the techniques are combinatorial and geometric rather than group-theoretic;
- we reach very hard problems very quickly.

Of course there are many more classes of groups to study!

S_n on k-sets

Let $G = S_n$, and let Ω be the set of all k-subsets of $\{1, \ldots, n\}$.

We may assume that $n \geq 2k$, since the actions of S_n on k-sets and on $(n-k)$-sets are isomorphic.

In fact we may assume that $n \geq 2k+1$, since the action of S_n on k-sets is imprimitive if $n = 2k$: the relation "equal or disjoint" is a congruence.

Now G has k orbits on the 2-element subsets of Ω, namely,

$$O_l = \{S_1, S_2 : |S_1 \cap S_2| = l\}$$

for $l = 0, 1, \ldots, k-1$. These k graphs together with the relation of equality form a combinatorial structure known as an *association scheme*, specifically the *Johnson scheme* $J(n,k)$.

All these graphs are connected (this is an exercise), so G is primitive on Ω. Since its socle is simple, it is basic.

If $k = 1$, then G is 2-transitive. We ignore this case.

The case $k = 2$

We begin by recalling the result for $k = 2$.

Theorem 1. *Let $G = S_n$ acting on the set of 2-subsets of $\{1, \ldots, n\}$, with $n \geq 5$. Then G is non-spreading. Moreover, the following are equivalent:*

- *G is separating;*
- *G is synchronizing;*
- *n is odd.*

Baranyai's Theorem

Let $\mathcal{F}$ be a set of k-subsets of $\{1, \ldots, n\}$, where k divides n. A 1-*factorization* of $\mathcal{F}$ is a partition of $\mathcal{F}$ such that each part is a partition of $\{1, \ldots, n\}$ (that is, a set of n/k pairwise disjoint subsets).

Theorem 2. *If k divides n, then there is a 1-factorization of the set of all k-subsets of $\{1,\ldots,n\}$.*

The theorem was proved by Baranyai in 1973. The proof is a beautiful application of the Max-Cut Min-Flow Theorem for networks.

As a corollary we have:

Theorem 3. *If k divides n, then S_n acting on k-sets is not synchronizing.*

For the set of all k-sets containing a fixed element (say 1) is a section of the Baranyai partition, which is thus section-regular.

The case $k = 3$

We now consider the case $k = 3$, and resolve completely the question of synchronization and separation.

Theorem 4. *Let $G = S_n$ acting on the set of 3-subsets of $\{1,\ldots,n\}$, with $n \geq 7$. Then the following are equivalent:*

- *G is synchronizing;*
- *G is separating;*
- *n is congruent to 2, 4 or 5 (mod 6), and $n \neq 8$.*

Note that synchronization and separation are equivalent for this class of groups.

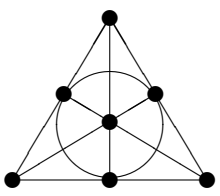
Teirlinck's theorem

A *Steiner triple system* is a collection $\mathcal{S}$ of 3-subsets of $\{1,\ldots,n\}$ with the property that every pair of points of $\{1,\ldots,n\}$ is contained in a unique member of $\mathcal{S}$.

Kirkman proved in 1847 that a Steiner triple system on n points exists if and only if n is congruent to 1 or 3 mod 6.

A *large set* of Steiner triple systems is a partition of the set of all 3-subsets of $\{1,\ldots,n\}$ into Steiner triple systems. (Counting shows that there must be $n-2$ such systems.)

For $n = 7$, there is a unique Steiner triple system, the *Fano plane*:



We cannot find more than two disjoint copies of the Fano plane. This fact goes back to Cayley. However, Teirlinck showed:

Theorem 5. *If n is congruent to 1 or 3 (mod 6) and $n > 7$, then there exists a large set of Steiner triple systems on n points.*

Now let G be S_n acting on 3-sets, for $n \geq 7$.

Baranyai's theorem shows that G is non-synchronizing if n is divisible by 3, that is, if n is congruent to 0 or 3 (mod 6).

Teirlinck's theorem shows that G is non-synchronizing if n is congruent to 1 or 3 (mod 6) and $n \neq 7$. (The set of triples through two given points is a section for all images of the large set.)

The cases $n = 7$ and $n = 8$ require special treatment.

The case $n = 7$

For each line L of the Fano plane, let $S(L)$ be the set of 3-sets equal to or disjoint from L. Then $|S(L)| = 5$.

Since no two lines of the Fano plane are disjoint, and no 3-set is disjoint from more than one line, we see that the sets $S(L)$ are pairwise disjoint. Since $5 \cdot 7 = 35 = \binom{7}{3}$, they form a partition of Ω.

Now 3-sets in the same $S(L)$ meet in 0 or 2 points. So any image of the Fano plane meets each $S(L)$ in at most (and hence exactly) one set. Thus the partition is section-regular, the Fano plane being the section.

So S_7 acting on 3-sets is not synchronizing.

The case $n = 8$

Take a Fano plane on $\{1,\ldots,7\}$. For each line L of the Fano plane, partition the eight points into $L \cup \{8\}$ and the rest, and take the set $T(L)$ of eight triples contained in a part of this partition. This gives a partition of all the $\binom{8}{3} = 56 = 7 \cdot 8$ 3-sets into seven subsets of size 8.

Once again we find that this partition is section-regular, with the Fano plane as a section.

The separating cases

We have now shown that, in the cases not stated in the theorem, G is non-synchronizing and hence non-separating. We have to show that, in the remaining cases, G is separating, and hence synchronizing.

There are $2^3 - 2$ graphs to consider. We denote them by X_I, for $\emptyset \subset I \subset \{0,1,2\}$; the vertices are the 3-sets, and two vertices are adjacent if and only if the cardinality of their intersection belongs to I.

We have to find the clique number of each of these graphs, and check whether $\omega(X_I)\omega(X_{I^*}) = \binom{n}{3}$, where $I^* = \{0,1,2\} \setminus I$.

The Erdős–Ko–Rado theorem

The following theorem finds the clique number of some of these graphs. A family $\mathcal{F}$ of k-subsets of $\{1,\ldots,n\}$ is *t-intersecting* if $|A \cap B| \geq t$ for all $A, B \in \mathcal{F}$.

Theorem 6. *For $n \geq n_0(k,t)$, the maximum size of a t-intersecting family of k-sets of $\{1,\ldots,n\}$ is $\binom{n-t}{k-t}$, with equality realised only by the family of all k-sets containing a fixed t-set.*

The correct value of $n_0(k,t)$ is known. We need only that the assertion of the theorem is true for $k = 3$, $n \geq 7$, and $t = 1$ or $t = 2$.

The cases $I = \{0\}$ and $I = \{1,2\}$

Clearly $\omega(X_{\{0\}}) = \lfloor n/3 \rfloor$.

By Erdős–Ko–Rado, $\omega(X_{\{1,2\}}) = \binom{n-1}{2}$. The product of these numbers is $\binom{n}{3}$ if and only if n is a multiple of 3; but this case is excluded.

The cases $I = \{0,1\}$ and $I = \{2\}$

By Erdős–Ko–Rado, $\omega(X_{\{2\}}) = n - 2$.

A clique in $X_{\{0,1\}}$ has the property that two points lie in at most one set in the clique; so $\omega(X_{\{0,1\}}) \leq n(n-1)/6$, with equality if and only if there is a Steiner triple system of order n, that is, n is congruent to 1 or 3 (mod 6). But these cases are excluded.

The cases $I = \{1\}$ and $I = \{0,2\}$

It is easy to show that a maximum clique in $X_{\{0,2\}}$ is obtained by dividing most of $\{1,\ldots,n\}$ into disjoint 4-sets and taking all the 3-subsets of these 4-sets. In particular, $\omega(X_{\{0,2\}}) \leq n$.

A maximum clique in $X_{\{1\}}$ is obtained by taking $\lfloor n/2 \rfloor$ triples through a fixed point but having no further point in common, provided that $n \geq 17$. For smaller values, a Fano plane may be better.

A little calculation shows that the product of these bounds is strictly smaller than $\binom{n}{3}$ except for $n = 7$ and $n = 8$; but these cases are excluded.

Spreading

Theorem 7. *The symmetric group S_n acting on k-sets is always non-spreading.*

Proof. Let d be the greatest common divisor of n and k. Let H be a cyclic group of order n permuting the elements of $\{1,\ldots,n\}$ in the natural way. Now choose a k-subset of $\{1,\ldots,n\}$ which is a union of k/d orbits of the subgroup of order d of H, and let A be the H-orbit (in Ω) containing this set; so $|A| = n/d$. Let B consist of all k-sets containing the element 1. Since A is invariant under a transitive group, $|A \cap Bg|$ is constant for $g \in G$. Also, clearly A and B are sets.

It remains only to show that $|A| = n/d$ divides $|\Omega| = \binom{n}{k}$. The stabiliser in H of any k-set has order dividing k and also dividing n, hence dividing d; so the size of any H-orbit in Ω is a multiple of n/d. The assertion follows. □

Classical groups and polar spaces

Now we turn to the other family of examples discussed here: classical (symplectic, unitary and orthogonal groups) acting on the associated polar spaces.

I will give a brief introduction to these groups and geometries; more detail is available in several places, including my notes on *Projective and Polar Spaces* and Don Taylor's book *The Geometry of the Classical Groups*.

We are only interested in finite classical groups; this makes the theory simpler in several respects.

A classical group acts on a vector space and preserves a form of some type:

- for *symplectic groups*, an alternating bilinear form;
- for *unitary groups*, a Hermitian sesquilinear form;
- for *orthogonal groups*, a quadratic form, and the symmetric bilinear form obtained from it by *polarization*.

The basic form should be *non-degenerate* or *non-singular*. The reason for separating cases is that strange things happen with quadratic forms in characteristic 2. I shall ignore this complication!

There are three parameters associated with a classical group:

- q, the order of the field over which the matrices are defined;
- r, the *Witt index*, the dimension of the largest subspace on which the form vanishes identically;
- ϵ, a parameter defined on the next slide.

We denote the dimension of the underlying vector space by n.

We divide the classical groups into six families:

- symplectic: $\mathrm{PSp}(2r,q)$, $n = 2r$
- unitary: $\mathrm{PSU}(2r,q)$, $n = 2r$, and $PSU(2r+1,q)$, $n = 2r+1$;
- orthogonal: $\mathrm{P\Omega}^+(2r,q)$, $n = 2r$; $\mathrm{P\Omega}(2r+1,q)$, $n = 2r+1$; and $\mathrm{P\Omega}^-(2r+2,1)$, $n = 2r+2$.

Note that for the unitary groups, the field order must be a square, say $q = q_0^2$, and there is a field automorphism $x \mapsto x^{q_0}$ of order 2. We use the group-theorists' notation $\mathrm{PSU}(n,q_0)$, but the field of definition is $\mathbb{F}_q$.

We need not consider orthogonal groups of odd dimension over fields of characteristic 2, since they turn out to be isomorphic to symplectic groups of one dimension less.

The values of the parameter ϵ are given in the table:

Type	ϵ
$\mathrm{PSp}(2r,q)$	0
$\mathrm{PSU}(2r,q_0)$	$-\frac{1}{2}$
$\mathrm{PSU}(2r+1,q_0)$	$\frac{1}{2}$
$\mathrm{P\Omega}^+(2r,q)$	-1
$\mathrm{P\Omega}(2r+1,q)$	0
$\mathrm{P\Omega}^-(2r+2,q)$	1

Polar spaces

The *polar space* associated with a classical group acting on a vector space V is the geometry of *totally isotropic* subspaces of V, those on which the form vanishes identically. We abbreviate this to *t.i.*

In the case of orthogonal groups, we should really use the term *totally singular* or *t.s.* instead; but we will ignore this distinction.

Subspaces of (vector space) dimension 1 or 2 are called *points* and *lines*, as usual in projective geometry. Subspaces of maximum dimension r are called *maximal subspaces*.

Numerical information

Numerical information about polar spaces can be expressed in terms of the parameters q, r, ϵ:

Theorem 8.
- *The number of points of the polar space is* $(q^r-1)(q^{r+\epsilon}+1)/(q-1)$*; each maximal subspace contains* $(q^r-1)/(q-1)$ *points.*
- *The number of points not collinear with a given point is* $q^{2r+\epsilon-1}$.
- *The number of maximal subspaces is*

$$\prod_{i=1}^{r}(1+q^{i+\epsilon}).$$

Witt's Lemma

Witt's Lemma asserts that the action of the classical group on a polar space is "homogeneous", in the sense that any linear isometry between subspaces of the vector space is induced by an element of the group.

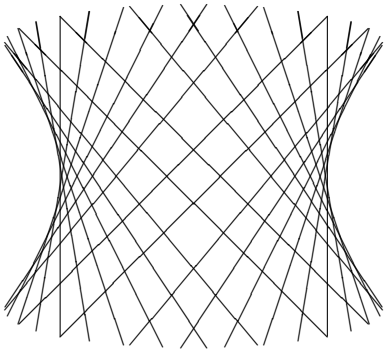
In particular, the group acts transitively on points, on collinear pairs of points, and on non-collinear pairs of points.

So the *graph* of the polar space (whose vertices are the points, two vertices joined if they are collinear) is a rank 3 graph.

In the case $r = 1$, there are no lines, so the graph of the polar space is null; Witt's lemma implies that the action of the group is 2-transitive. We will ignore this case.

An example

The polar space of type $\mathrm{P}\Omega^+(4, q)$ is the familiar *ruled quadric*:



Combinatorially this structure is just a grid, so the classical group is non-basic. We will also ignore this case.

Cliques and cocliques

We must now look at cliques and cocliques in the graph X of a polar space.

A clique is a set of 1-dimensional subspaces on which the form vanishes and which are pairwise orthogonal; so its span is also a clique. Thus the cliques of maximal size are just the maximal subspaces, of size $(q^r - 1)/(q - 1)$.

Two points are non-adjacent if and only if no maximal subspace contains both; so a coclique is a set of points meeting every maximal subspace in at most one point.

Hence a coclique contains at most $q^{r+\epsilon} + 1$ points, with equality if and only if it meets every maximal in exactly one point.

A coclique meeting this bound is called an *ovoid*.

We need one further definition: a *spread* is a family of maximal subspaces which partitions the set of points.

Theorem 9.

- *A classical group is non-separating if and only if its polar space possesses an ovoid.*
- *A classical group is non-synchronizing if and only if its polar space possesses either*
  - *an ovoid and a spread; or*
  - *a partition into ovoids.*

Ovoids, spreads and partitions

You might expect at this point to be told that the question of which polar spaces contain ovoids, spreads, or partitions into ovoids has been completely solved by finite geometers.

Unfortunately, despite a lot of effort, this is not the case.

I will summarise some of the results which have been obtained.

Ovoids

$\mathrm{PSp}(2r, q)$	Yes for $r = 2$ and q even; no in all other cases
$\mathrm{PSU}(2r, q_0)$	Yes for $r = 2$
$\mathrm{PSU}(2r + 1, q_0)$	No
$\mathrm{P}\Omega^+(2r, q)$	Yes for $r = 2, 3$; yes for $r = 4$ and q even, or q prime, or $q \equiv 3$ or 5 mod 6; no for $r \geq 4$ and $q = 2$ or $q = 3$
$\mathrm{P}\Omega(2r + 1, q)$	Yes for $r = 2$; yes for $r = 3$ and $q = 3^h$
$\mathrm{P}\Omega^-(2r + 2, q)$	No

Spreads

$\mathrm{PSp}(2r, q)$	Yes
$\mathrm{PSU}(2r, q_0)$	No
$\mathrm{PSU}(2r + 1, q_0)$	No for $r = 2$, $q_0 = 2$
$\mathrm{P}\Omega^+(2r, q)$	No if r is odd; yes if $r = 2$, or $r = 4$ with q prime or $q \equiv 3$ or 5 mod 6; yes if r and q are even
$\mathrm{P}\Omega(2r + 1, q)$	No if r is even (and q odd); yes if $r = 3$ with q prime or $q \equiv 3$ or 5 mod 6
$\mathrm{P}\Omega^-(2r + 2, q)$	Yes if $r = 2$, or if q is even

Some conclusions

We conclude that $\mathrm{PSp}(2r,q)$, $\mathrm{PSU}(2r+1,q_0)$, and $\mathrm{P\Omega}^-(2r+2,q)$ are separating for all $r \geq 2$, except for $\mathrm{PSp}(4,q)$ with q even. Cases where the group is not separating can also be read off from the first table. However, less is known about partitions into ovoids, so results about synchronization are less clear.

Example 10. The polar space of the group $\mathrm{P\Omega}(5,q)$, for q odd, possesses ovoids but no spreads. For $q = 3,5,7$, these ovoids are all *classical*; that is, they consist of the set of points lying in a non-singular 4-dimensional space of type $\mathrm{P\Omega}^-(4,q)$ (this polar space has Witt index 1, so contains no lines). Any two such spaces meet in a 3-dimensional space, so two such ovoids meet in a *conic*. In particular, there are no partitions into ovoids.

So the group $\mathrm{P\Omega}(5,q)$, for $q = 3,5,7$, is synchronizing but not separating. This is our first example of such a group.

Spreading

Theorem 11. *Let G be a classical group of Witt index at least 2, acting on the points of its polar space. Suppose that there exists a non-degenerate hyperplane which has Witt index smaller than that of the whole space. Then G is non-spreading.*

Proof. We take A to be a maximal subspace, and B to be the set of points lying in the assumed hyperplane. Then $|A \cap B^g| = (q^{r-1}-1)/(q-1)$ for all $g \in G$, and A and B are both sets with $|A|$ dividing $|\Omega|$. □

This theorem covers the classical groups $\mathrm{PSU}(2r,q_0)$, $\mathrm{P\Omega}^+(2r,q)$, and $\mathrm{P\Omega}(2r+1,q)$, but not $\mathrm{PSp}(2r,q)$, $\mathrm{PSU}(2r+1,q_0)$, or $\mathrm{P\Omega}^-(2r+2,q)$.

Conclusions

We have found examples of groups which are synchronizing but not separating.

But we have failed to find examples of groups which are spreading but not 2-set transitive.

We turn to this in the next lecture.