# Synchronization 7: Representation theory

Peter J. Cameron

LTCC

10-11 June 2010

**2-closure**

We have seen that synchronization and related properties are closed upwards (i.e. preserved on passing to overgroups). They also have a limited form of downward closure, as we will now see.

Let $G$ be a permutation group on $\Omega$.

- The 2-*closure* of $G$ is the set of all permutations of $\Omega$ which preserve the $G$-orbits on $\Omega^2$ (the set of ordered pairs of elements of $\Omega$). The group $G$ is 2-*closed* if it is equal to its 2-closure.
- The *strong* 2-*closure* of $G$ is the set of all permutations of $\Omega$ which preserve the $G$-orbits on the set of 2-element subsets of $\Omega$. The group $G$ is *strongly* 2-*closed* if it is equal to its strong 2-closure.

Note that

- the 2-closure of $G$ is contained (possibly strictly) in its strong 2-closure;
- the 2-closure of $G$ is the symmetric group if and only if $G$ is 2-transitive;
- the strong 2-closure of $G$ is the symmetric group if and only if $G$ is 2-set transitive.

**Theorem 1.** *Let $P$ denote one of the conditions "primitive", "synchronizing", "separating", "2-set transitive". Then the following are equivalent:*

*(a) $G$ satisfies $P$;*

*(b) the 2-closure of $G$ satisfies $P$;*

*(c) the strong 2-closure of $G$ satisfies $P$.*

*Proof.* In view of our earlier remarks, (a) implies (b) implies (c); so it suffices to show that (c) implies (a). But each property can be defined in terms of $G$-invariant graphs, and $G$ and its strong 2-closure clearly preserve the same graphs. $\square$

**Representation theory**

We now turn to an algebraic approach to these and related closure properties. Let $\mathbb{F}$ be a field. We only consider the case $\mathbb{F} = \mathbb{C}$, $\mathbb{R}$ or $\mathbb{Q}$. Certainly there is an interesting theory waiting to be worked out in the case where $\mathbb{F}$ is, say, a finite field, a $p$-adic field, or even a ring!

Let $G$ be a permutation group on $\Omega$. The *permutation module* is the $\mathbb{F}G$-module $\mathbb{F}\Omega$ which has the elements of $\Omega$ as a basis, where $G$ acts by permuting the basis vectors.

Now the $\mathbb{F}$-*closure* of $G$ consists of all permutations which preserve all $\mathbb{F}G$-submodules pf $\mathbb{F}\Omega$; and $G$ is $\mathbb{F}$-*closed* if it is equal to its $\mathbb{F}$-closure.

Consider the case where $G$ is the symmetric group $\mathrm{Sym}(\Omega)$. The permutation module has just two non-trivial submodules:

- the 1-dimensional module $\underline{\Omega}$ spanned by the sum of the elements of $\Omega$;
- the $n-1$-dimensional *augmentation submodule* consisting of the vectors with coordinate sum zero.

For, if $W$ is a submodule containing a vector $x$ with $x_v \neq x_w$, and $g$ is the transposition $(v, w)$, then $W$ contains $x - xg = \lambda(v - w)$. By 2-transitivity, $W$ contains all differences between basis vectors; but these span the augmentation module.

**Theorem 2.** *The $\mathbb{C}$-closure of a permutation group $G$ is equal to its 2-closure.*

The proof requires a little character theory; a brief sketch follows.

### Character theory

Any representation of a group by matrices over the complex numbers is determined up to isomorphism by its *character*, the function $\phi$ which maps each group element to the trace of the matrix representing it. A character is a *class function* (constant on conjugacy classes).

Any representation can be decomposed uniquely (up to isomorphism) into *irreducible* representations. An *irreducible character* is the character of an irreducible representation.

The characters form an orthonormal basis for the space of complex class functions, under the inner product

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \phi(g) \overline{\psi(g)}.$$

The *trivial character* $1_G$ is the function mapping every group element to 1.

### The permutation character

Let $G$ be a permutation group on $\Omega$, where $|\Omega| = n$. Then we have an action of $G$ on $\mathbb{C}\Omega$ by permutation matrices. Its character is the *permutation character* $\pi$, where $\pi(g)$ is the number of fixed points of $g$.

The *Orbit-Counting Lemma* states that

$$\frac{1}{|G|} \sum_{g \in G} \pi(g) = \text{\# orbits of } G.$$

The sum on the left is just $\langle 1_G, \pi$; so the multiplicity of the trivial character in $\pi$ is equal to the number of orbits of $G$.

Applying the preceding result to the action of $G$ on $\Omega \times \Omega$ (whose permutation character is $\pi^2$), we see that

$$\langle \pi, \pi \rangle = \langle \pi^2, 1_G \rangle = \text{\# orbits of } G \text{ on } \Omega^2.$$

This number is called the *rank* of $G$.

The rank is equal to the sum of squares of the multiplicities of the irreducible characters in $\pi$ (since if $\pi = \sum a_i \phi_i$, with $\phi_i$ irreducible, then orthonormality gives

$$\langle \pi, \pi \rangle = \sum a_i^2.$$

In particular, $G$ is 2-transitive if and only if $\pi = 1_G + \phi$ for some irreducible character $\phi$. (The character $\phi$ is afforded by the action of $G$ on the augmentation submodule of the permutation module: so $G$ is 2-transitive if and only if the augmentation submodule is irreducible.)

### 2-closure = $\mathbb{C}$-closure

Let $\bar{G}$ be the 2-closure of $G$. Then $\bar{G}$ has the same sum of squares of multiplicities of irreducibles as $G$, which implies that the decomposition of the permutation character is the same for $\bar{G}$ as for $G$. Hence $\bar{G}$ is contained in the $\mathbb{C}$-closure of $G$.

Conversely, let $\hat{G}$ be the $\mathbb{C}$-closure of $G$. Then $\hat{G}$ preserves the isotypic components of the permutation module (one of these consists of the sum of all copies of a particular isomorphism type of irreducible module). The lattice of submodules of the sum of $r$ isomorphic irreducible modules is isomorphic to the $(r-1)$-dimensional complex projective space; all these submodules are preserved by $\hat{G}$. So the isomorphic $G$-modules remain isomorphic as $\hat{G}$-modules. Thus the multiplicities are the same for $\hat{G}$ as for $G$, and so the ranks of these groups are equal. Since $G \leq \hat{G}$, it follows that $\hat{G}$ preserves the $G$-orbits, and so is contained in the 2-closure $\bar{G}$.

Hence $\hat{G} = \bar{G}$.

### A problem

Is it true that the $\mathbb{R}$-closure of a permutation group coincides with its strong 2-closure?

This is not known in general, but it is true for groups whose permutation character is multiplicity-free.

### $\mathbb{F}$I groups

We say that the permutation group $G$ on $\Omega$ is $\mathbb{F}I$ if its $\mathbb{F}$-closure is the symmetric group; that is, if the only $G$-submodules of $\mathbb{F}\Omega$ are $\underline{\Omega}$ and the augmentation module.

**Theorem 3.** *Let $G$ be a permutation group on $\Omega$.*

- *$G$ is $\mathbb{C}I$ if and only if it is 2-transitive.*
- *$G$ is $\mathbb{R}I$ if and only if it is 2-set transitive.*

This naturally suggests looking at $\mathbb{Q}$I groups, to which we now turn.

**Theorem 4.** *Let $G$ be a transitive permutation group on $\Omega$, and $\mathbb{F}$ a field of characteristic zero. Then $G$ is primitive (resp. synchronizing, separating, spreading, or $\mathbb{Q}I$) if and only if its $\mathbb{F}$-closure is.*

Three of these results are immediate from the next lemma.

**Theorem 5.** *Let $G$ be a transitive permutation group on $\Omega$, and $\mathbb{F}$ a field of characteristic zero. Let $A$ and $B$ be multisets such that $|A * Bg| = \lambda$ for all $g \in G$. Then $|A * Bg| = \lambda$ for all $g$ in the $\mathbb{F}$-closure of $G$.*

Let $v_1$ and $v_2$ be the characteristic functions of $A$ and $B$ respectively. Setting $w_i = v_i - (v_i \cdot j)j/n$ for $i = 1, 2$, where $j$ is the all-1 vector, we find that $j$, $w_1$ and $w_2g$ are pairwise orthogonal for any $g \in G$. So the $G$-submodules generated by $j$, $w_1$ and $w_2$ are pairwise orthogonal. These modules are invariant under the $\mathbb{F}$-closure $\hat{G}$; reversing the argument gives the result.

This immediately proves the earlier theorem for separating, spreading and $\mathbb{Q}$I groups.

Suppose that $G$ is imprimitive, and let $\pi$ be a $G$-invariant partition. Then the characteristic functions of the parts of $\pi$ form an orthogonal basis for a submodule of $\mathbb{F}\Omega$, which is fixed by $\hat{G}$. The partition can be recovered from the submodule, since it is the coarsest partition on the parts of which the elements of the submodule are constant. So $\hat{G}$ is imprimitive.

Finally, suppose that $G$ is not synchronizing, and let the partition $\pi$ and section $S$ witness this. Let $v$ be the characteristic function of $S$, and $w = v - (v.j)j/n$. Then $wg$ is orthogonal to the characteristic functions of the parts of $\pi$ for all $g \in G$, so every vector in the submodule generated by $w$ is orthogonal to these vectors. Since this submodule is fixed by $\hat{G}$, every $\hat{G}$-image of $S$ is a section for $\pi$, and $\hat{G}$ is non-synchronizing.

### The hierarchy revisited

If $G$ is $\mathbb{Q}$I, then its $\mathbb{Q}$-closure is the symmetric group, which is spreading; so $G$ is spreading.

So our hierarchy finally looks like this:

$$\begin{aligned}&\text{transitive} \Leftarrow \text{primitive} \Leftarrow \text{basic}\\ &\quad\Leftarrow \text{synchronizing} \Leftarrow \text{separating} \Leftarrow \text{spreading}\\ &\quad\Leftarrow \mathbb{Q}\text{I} \Leftarrow \text{2-set transitive} \Leftarrow \text{2-transitive.}\end{aligned}$$

We will see that there are groups which are $\mathbb{Q}$I but not 2-set transitive; indeed, these groups have recently been classified. But no examples are currently known of groups which are spreading but not $\mathbb{Q}$I.

### Affine groups

Recall that an *affine group* is a permutation group $G$ on the $d$-dimensional vector space over $\mathbb{F}_p$ (where $p$ is prime) generated by the translation group $T$ and an irreducible linear group $H$. Thus $G$ is the semidirect product of $T$ by $H$; and $H$ is the stabiliser of the zero vector.

**Theorem 6.** *Let $G$ be an affine permutation group on $V$, with $H = G_0$ as above. Then the following are equivalent:*

- *$G$ is spreading;*
- *$G$ is $\mathbb{Q}I$;*
- *$H$ is transitive on the set of 1-dimensional subspaces of $V$;*
- *the group generated by $G$ and the scalars in $\mathrm{GF}(p)$ is 2-transitive.*

The affine groups described in the Theorem can be completely classified, using the classification of affine 2-transitive groups.

*Proof.* It is clear that (c) and (d) are equivalent. Let us suppose that they do not hold. Then $H$ is not transitive on 1-dimensional spaces of $V$, and hence not transitive on $(d-1)$-dimensional subspaces either (by Brauer's lemma). Choose hyperplanes $A$ and $B$ in different orbits of $H$. Then no image of $B$ under $G$ is parallel to $A$, so $|A \cap Bg| = p^{d-2}$ for all $g \in G$. Thus $G$ is not spreading. So (a) implies (c) and (d). It is clear that (b) implies (a); so it remains to prove that (c) and (d) imply that $G$ is $\mathbb{Q}$I.

The scalars in $\mathbb{F}_p$ act on $V$, and hence on the characters of $V$; and their action is precisely that of the Galois group of the field of $p$th roots of unity. Now assuming that (d) holds, this group permutes the non-principal irreducibles in the permutation character transitively, and so $G$ is $\mathbb{Q}$I, as required. □

## 3/2-transitive groups

A permutation group $G$ on $\Omega$ is said to be 3/2-*transitive* if it is transitive, and the stabiliser of a point $v$ has all its orbits except $\{v\}$ of the same size. (If there is just one such orbit then $G$ is 2-transitive.)

*Example* 7. Let $q$ be a power of 2. The group $\mathrm{PSL}(2,q)$ has dihedral subgroups of order $2(q+1)$; it acts transitively on the set of cosets of such a subgroup, and the stabiliser has $q/2-1$ orbits each of size $q+1$ on the remaining points.

*Example* 8. There is a "sporadic" example: the symmetric group $S_7$ acting on 2-subsets of $\{1,\ldots,7\}$. This works because $2 \cdot 5 = \binom{5}{2}$.

Using the Classification of Finite Simple Groups, John Bamberg, Michael Giudici, Martin Liebeck, Cheryl Praeger and Jan Saxl have determined all the 3/2-transitive groups. Any such group is affine, or one of the two examples described above.

Although the class of 3/2-transitive groups is not closed upwards, this classification gives us the $\mathbb{Q}$I-groups:

**Theorem 9.** *Any $\mathbb{Q}$I group is 3/2-transitive.*

The reason is that the permutation character is the sum of the trivial character and a family of algebraically conjugate characters; an old result of Frame now applies.

## The $\mathbb{Q}$I groups

The group $S_7$ acting on 2-sets is not $\mathbb{Q}$I.

Careful analysis of the character values of $\mathrm{PSL}(2,q)$ show that the 3/2-transitive action of this group described earlier is $\mathbb{Q}$I if and only if $q-1$ is a Mersenne prime.

So there are probably infinitely many examples of this form, though nobody knows for sure.

Any other $\mathbb{Q}$I group is affine.

## $\mathbb{Q}$I versus spreading

We don't know any examples of groups which are spreading but not $\mathbb{Q}$I. Moreover, there are very few $\mathbb{Q}$I groups, and there are plenty of places to look for spreading groups.

We saw above that

- $G$ is not $\mathbb{Q}$I if and only if there are non-trivial multisets $A$ and $B$ satisfying $(1)_\lambda$,

whereas, by definition,

- $G$ is not spreading if and only if there are non-trivial multisets $A$ and $B$ satisfying $(1)_\lambda$, (3) and (4).

Condition (3) says that $B$ is a set. In combinatorial problems of this kind, there is usually a big difference between asking for a multiset with a certain property and asking for a set. For this reason and others, I suspect that such groups will exist.