Idempotent generation and road closures

Peter J. Cameron

Groups and Combinatorics seminar
Perth
23 September 2016

There have been rather a lot of road closures around St Andrews recently:

From: Daniel Glynn <Daniel.Glynn@vitalenergi.co.uk>
Subject: Road Closure
Date: 22 September 2016 13:13:54 BST

All,

Due to circumstances out of our control we have had to close the main road between Purdie building and the Sports Centre/ Physics & Astronomy, vehicles parked in the higher car park will be able to exit, however no further access in will be granted, we envisage the road will be back open by end of business Monday 26th September

We apologise for any inconvenience caused

Kind Regards

Dan Glynn
Project Manager
DDI: +44 (0) 7557110736

Permutation groups and transformation semigroups

This is part of a big project, joint with João Araújo and others, to use our knowledge of finite permutation groups to get information about transformation semigroups.
Given a transformation monoid M on a set Ω, the units of M form a permutation group G, and a generating set for M must contain a generating set for G (you can't generate permutations using non-permutations!)
So, at least to get things started, it is natural to consider the case $M = \langle G, a \rangle$, where G is a permutation group and a a non-permutation. A typical question is:

Question

Which permutation groups G guarantee that $M = \langle G, a \rangle$ has some specified nice property, for all or some choices of non-permutation a?

Semigroup properties

Some of the semigroup properties which have been considered include

- synchronization (S is synchronizing if it contains a transformation of rank 1);
- regularity (S is regular if for all $a \in S$ there exists $b \in S$ such that $aba = a$);
- idempotent generation (see below).

Here the rank of a map on Ω is the cardinality of its image. Work on synchronization is partly motivated by the famous Černý conjecture, which states that if a semigroup $S = \langle A \rangle$ on n points is synchronizing, then there is a transformation of rank 1 which is a word of length at most $(n-1)^2$ in A. I will not discuss further this very seductive conjecture ...

Idempotent generation

An idempotent is a map e satisfying $e^2 = e$.

Question

For which transitive permutation groups G is it true that, for all maps a of rank k, the semigroup $\langle G, a\rangle \setminus G$ is idempotent-generated?

(The case $k = 1$ is trivial since any rank 1 map is idempotent.)
We have conjectured a complete answer to this question, and proved part of it.

Idempotents

Start with an easier question. For which transitive groups G is it true that, for all maps a of rank k, $\langle G, a\rangle \setminus G$ contains a rank k idempotent (an element e with $e^2 = e$)?

The kernel of a is the partition of $\{1, \ldots, n\}$ into inverse images of points in the image of a.

An idempotent has the property that its image is a section (or transversal) to its kernel partition. Conversely, if the image of a is a section to its kernel, then some power of a is an idempotent.

So, if a has rank k, then there is an idempotent of rank k in $\langle G, a\rangle$ if and only if there is an element $g \in G$ mapping the image of a to a section for the kernel.

So a necessary and sufficient condition is that G has the k-universal transversal property: given any k-set S and k-partition P, there is an element of G mapping S to a section for P.

2-ut and primitivity

For $k > 2$, the k-ut property is very restrictive. But for $k = 2$, it is equivalent to something very familiar to permutation group theorists!

A group G has the 2-ut property if and only if every orbit of G on 2-sets contains a section of every 2-partition. This is equivalent to saying that every orbital graph for G (graph with edge set SG, the G-orbit of S) is connected.

An old theorem of Donald Higman says that this is equivalent to primitivity of the group G, the property that G preserves no non-trivial partitions of $\{1, \ldots, n\}$.

From now on, I will consider just the case $k = 2$.

The Houghton graph

Idempotent generation requires a stronger condition.
Given a group G, and a k-subset S and k-partition P of its domain, the Houghton graph $H(G, k, P, S)$ is the bipartite graph with vertex set $PG \cup SG$, with an edge from S' to P' whenever S' is a section of P'.
Let P and S be the kernel and image of a. If there is a product of idempotents in $\langle a, G\rangle \setminus G$ having kernel P' and image S', then the image of each idempotent is a section for the kernel of the next, so there is a path from P' to S' in $H(G, k, P, S)$.
So connectedness of the Houghton graph is a necessary condition for idempotent generation.

Theorem

$\langle G, a\rangle \setminus G$ is idempotent-generated for every rank 2 map a if and only if every 2-Houghton graph for G is connected.

We will say that G has the 2-Hc property if this condition holds. As this theorem suggests, 2-Hc is a strengthening of primitivity.

A reformulation

The condition in the theorem is still time-consuming to check, since there are exponentially many 2-partitions of $\{1, \ldots, n\}$. By focussing on the 2-sets instead, we can find a much more efficient test:

Theorem

A primitive permutation group G on $\{1, \ldots, n\}$ has the 2-Hc property if and only if, for every G-orbit O on 2-subsets of $\{1, \ldots, n\}$, and every maximal block of imprimitivity B for the action of G on O, the graph with edge set $O \setminus B$ is connected.

This is better since there are only a quadratic number of 2-sets.

Proof

Suppose that the graph with edge set $O \setminus B$ is disconnected, where O is an orbit on 2-sets and B a maximal block for the action of G on O. Let P be the partition into a connected component and its complement, and S a 2-set in B. If S is a section for Pg, then Sg^{-1} is a section for P, and so $Sg^{-1} \in B$ (since the edges in $O \setminus B$ fail to be sections). Thus all the 2-sets in a component of the Houghton graph lie within B, and this graph cannot be connected.

Conversely, suppose that the Houghton graph $H(G, 2, P, S)$ is disconnected. The edges within connected components are blocks of imprimitivity for G acting on $O = SG$; let B be one of these, with $S \in B$. Then the pairs in $O \setminus B$ cannot be sections for any partition in the block containing S, since they are not connected to S in the Houghton graph. So the graph with edge set $O \setminus B$ is disconnected, with the parts of P as unions of connected components. If $O \setminus B$ is disconnected, so is $O \setminus B'$, where B' is any maximal block containing B.

Using the test

Of course, there are only polynomially many orbital graphs to check. For each one, there are hopefully not too many maximal blocks of imprimitivity. And testing connectedness is fast!
So you could just go to the computer, start up GAP, and begin testing examples ...
But can we find the maximal blocks efficiently?

How many blocks?

Is there a polynomial upper bound for the number of maximal blocks of imprimitivity in a transitive group?
A special case is Wall's conjecture, asserting that the number of maximal subgroups of a finite group is not greater than the order of the group. (This is the case where the transitive group is regular.) Wall's conjecture was disproved by participants at an AIM workshop, written up by Guralnick, Hodge, Parshall and Scott; but they expect there to be an upper bound $n^{1+\epsilon}$, where maybe $\epsilon = 10^{-5}$. But this still leaves some questions:

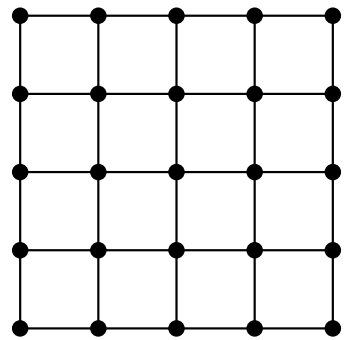
- What about the general case?
- Even if the number is not too large, can we find them all in polynomial time?

How to find them?

Checking whether a transitive group is primitive can be done in polynomial time; and a minimal block of imprimitivity can be found in polynomial time. (For each pair of points, check connectivity of the orbital graph in which that pair is an edge.)
What about maximal blocks?
We can find one block, by recursively finding a minimal block and computing the group induced on the set of its translates (moving up in the lattice of blocks containing a point). But we need to check all maximal blocks.
Of course we have more information: our group is a primitive group acting on the edges of some orbital graph ...

An example

Consider the automorphism group of a $m \times m$ grid: two points are joined if they lie in the same row or column. The automorphism group is the wreath product $S_m \wr S_2$ in its product action on m^2 points.



The edges fall into two blocks of imprimitivity under the automorphism group: horizontal and vertical.
If workmen come and dig up all the vertical roads, then it is impossible to get from one row to another. So this primitive group fails to have the 2-Hc property.

First generalisation: non-basic groups

Here is part of my take on the O'Nan–Scott theorem.
A primitive permutation group is non-basic if it preserves a Cartesian power structure on the set of points, i.e. if it is embeddable in the wreath product $S_m \wr S_k$ with the product action.
A primitive group is basic otherwise.
Just as in the previous example, it is easy to show that a non-basic primitive group fails to have the 2-Hc property.
The O'Nan–Scott theorem gives us good information about the basic primitive groups: they must be affine, diagonal, or almost simple.

Second generalisation

Another way of looking at the example leads to the following.

Proposition

Let G be a primitive permutation group. Suppose that G has an imprimitive subgroup of index 2. Then G does not have the 2-Hc property.

Suppose that G has an imprimitive subgroup N of index 2. Let $\mathcal{P}$ be a system of imprimitivity for N. Since G does not preserve $\mathcal{P}$, it interchanges it with another system $\mathcal{B}$. A non-empty intersection of a block in $\mathcal{P}$ with a block in $\mathcal{B}$ is a block for G, and so has cardinality 1. Thus we can consider the incidence structure $(\mathcal{P}, \mathcal{B})$, whose elements are called "points" and "blocks", a point and block being "incident" if they have non-empty intersection.

Thus G is a group of automorphisms and dualities of the incidence structure, and the given action is on the set of flags (incident point-block pairs) of the structure.

Now take a pair of flags sharing a point, and form the orbital graph in which this is an edge. The automorphisms form a subgroup of index 2, and the edges fall into two blocks depending on whether the shared element is a point or a block. If we remove edges of one type, we cannot move between flags with different elements of the other type.
There are two kinds of adjacency:

and

If all connections of the second type are removed, then we cannot move from a flag to another flag with a different point!

Examples for the last result include groups of projective spaces (on point-hyperplane flags or on point-hyerplane antiflags, or on i-space/$(n-1-i)$-space flags), symplectic generalised quadrangles in characteristic 2, G_2 generalised hexagons in characteristic 3, and some sporadic examples such as $\mathrm{PGL}(2,11)$ with degree 55 or 66, and HS : 2 with degree 22176 coming from symmetric 2-designs with 2-transitive groups. The examples of degree up to 120 are

- $L_3(2) : 2$, degrees 21 and 28 (flags and antiflags in Fano plane);
- $S_6 : 2$ and subgroups, degree 45;
- $L_3(3) : 2$, degrees 52 and 117;
- $L_2(11) : 2$, degrees 55 and 66;
- $\mathrm{Aut}(L_3(4))$ and subgroups, degree 105;
- $S_8 = L_4(2) : 2$, degrees 105 and 120;
- S_7, degree 120.

More examples

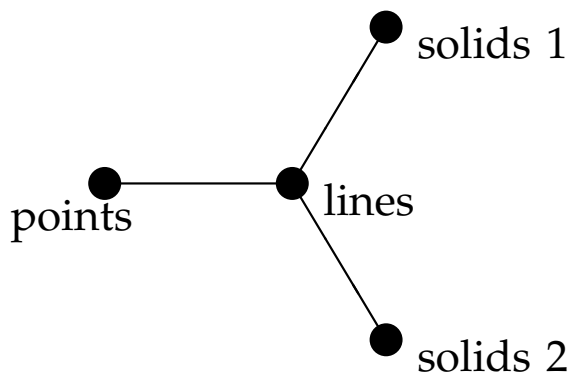
Not all examples have such a nice geometric structure.
Let p be a prime congruent to $\pm 1 \pmod 5$ and to $\pm 3 \pmod 8$.
Then $\mathrm{PGL}(2,p)$ contains a conjugacy class of subgroups isomorphic to A_5, which splits into two classes in $\mathrm{PSL}(2,p)$. An A_4 subgroup of one of these A_5's is normalised by S_4 in $\mathrm{PGL}(2,p)$; elements of S_4 not in A_4 conjugate the A_5 to one in the other $\mathrm{PSL}(2,p)$ class.
Thus $\mathrm{PGL}(2,p)$, on the cosets of S_4, is a primitive group of degree $p(p^2-1)/24$, which has an imprimitive subgroup of index 2; the corresponding incidence structure has five points in a block.
There are also a couple of sporadic actions of $M_{12} : 2$.
I do not see the prospect of determining all these groups ...

From duality to triality

There are further examples in which duality is replaced by the remarkable phenomenon of triality, associated with split quadratic forms in 8 variables.

The geometry of a split quadric in 8 vector space dimensions consists of the totally singular points, lines and solids (projective 3-spaces) on the quadric. The solids fall into two families: two solids belong to the same family if and only if their intersection has even codimension.

The principle of triality asserts that if the labels "point", "solid of class 1" and "solid of class 2" are permuted arbitrarily, the lines being preserved, then the truth of all geometric properties remains unaltered.



Thus, $\mathrm{P}\Omega(8,q) : S_3$ acts on flags consisting of a point and a pair of maximal singular subspaces of opposite types in the associated quadric, and these examples also fail the 2-Hc property.
The smallest example arising in this way, with $q = 2$, has degree 14175.

Triality was discovered by Eduard Study and developed by Élie Cartan. It is connected with other remarkable things such as the octonions, spinors, and the Leech lattice.

A conjecture

Conjecture

Let G be a basic primitive permutation group. Suppose that G does not have an imprimitive normal subgroup of index 2, and is not one of the triality examples just mentioned. Then G has the 2-Hc property. Hence, for any rank 2 map a, the semigroup $\langle G, a\rangle \setminus G$ is idempotent-generated.

This conjecture has been checked computationally for all degrees up to 130 and many larger degrees. No counterexamples have been found.

Some cases

We can settle various cases of the conjecture: it is true if

- n is prime;
- n is the square of a prime;
- G is 2-homogeneous;
- G is S_m or A_m acting on k-sets.

As noted, a group with 2-Hc must be basic, and hence is affine, diagonal or almost simple. It would be nice to resolve at least the first two cases.
I will give proofs of two of the above assertions:
2-homogeneous groups, and groups of prime-squared degree.

2-homogeneous groups

Let G be 2-homogeneous: that is, G has a single orbit O containing all 2-sets. There is a single orbital graph, which is the complete graph.
If B is a block, then $O \setminus B$ is the union of the other blocks; so, if $O \setminus B$ is disconnected, then B is disconnected.
But the complete graph cannot be the union of two disconnected graphs.
So any 2-homogeneous group is 2-Hc.

Groups of degree p^2

A theorem of Wielandt asserts that a primitive group of degree p^2 (for p prime) is affine, or contained in $S_p \wr S_2$, or is 2-transitive. In the second case, 2-Hc fails, while in the third, it holds. So it is the affine case which has to be considered. The argument is slightly fiddly but not difficult. Such groups, if not contained in $S_p \wr S_2$, do have the 2-Hc property.

Conclusion

In the last two weeks, Cheryl Praeger and I have looked at one further class of primitive groups, those of type HS, though we don't have a definitive result yet.
Any help in proving our conjecture, or in establishing exactly which primitive groups fail the 2-Hc property, would be most welcome!

. . . for your attention!