Synchronization 5: Graphs and monoids

Peter J. Cameron

LTCC

10-11 June 2010

From graphs to monoids and back

In this section of the notes we describe a pair of maps between graphs on the vertex set Ω and transformation monoids on Ω. These maps do not form a 'Galois correspondence' but have some nice properties relevant to the synchronization project.

Since G will always be a group, we use X to denote a graph.

From graphs to monoids

The map in this direction is simple: to a graph X on Ω we associate the transformation monoid $\mathrm{End}(X)$.

We note the following observation from the preceding chapter:

Theorem 1. *The graph X is a core if and only if $\mathrm{End}(X) = \mathrm{Aut}(X)$.*

From monoids to graphs

Let M be a transformation monoid on Ω. Define a graph $\mathrm{Gr}(M)$ on Ω by the rule that, for any two distinct vertices $v, w \in \Omega$, we put $v \sim w$ if and only if there does not exist $f \in M$ with $vf = wf$.

A transformation monoid is *synchronizing* if it contains an element whose image has cardinality 1.

Theorem 2.

- *$\mathrm{Gr}(M)$ is complete if and only if M is a permutation group (that is, contained in the symmetric group).*
- *$\mathrm{Gr}(M)$ is null if and only if M is synchronizing.*

Proof. (a) $\mathrm{Gr}(M)$ is complete if and only if no element of M ever maps two points to the same place.

(b) Let $f \in M$ be an element whose image is as small as possible. Then no two elements of the image of f can be mapped to the same place; so they are pairwise adjacent. So, if $\mathrm{Gr}(M)$ is null, then the image of f has cardinality 1. The converse is clear. □

Theorem 3. *For any transformation monoid M, the graph $\mathrm{Gr}(M)$ has core a complete graph.*

Proof. The argument in (b) above shows that the image of an element of M of minimal rank is a complete subgraph of $\mathrm{Gr}(M)$. It is hom-equivalent to $\mathrm{Gr}(M)$ (the homomorphism in the other direction is just the embedding), and it is clearly a core. □

Both ways

Theorem 4. *For any transformation monoid M,*

- *$M \leq \mathrm{End}(\mathrm{Gr}(M))$;*
- *$\mathrm{Gr}(\mathrm{End}(\mathrm{Gr}(M))) = \mathrm{Gr}(M)$.*

Proof. (a) Let f be an endomorphism of M, and let v and w be adjacent in $\mathrm{Gr}(M)$. By definition, $vf \neq wf$. Could vf and wf be non-adjacent in $\mathrm{Gr}(M)$? if so, then there is an element $h \in \mathrm{End}(M)$ with $(vf)h = wf(h)$. But this contradicts the adjacency of v and w, since $fh \in M$ by closure.

Conversely, suppose that v and w are not adjacent in $\mathrm{Gr}(M)$. Then there is an element $f \in M$ satisfying $vf = wf$. By (a), $f \in \mathrm{End}(\mathrm{Gr}(M))$, and so v and w are non-adjacent in $\mathrm{Gr}(\mathrm{End}(\mathrm{Gr}(M)))$. □

Theorem 5. *The maps $M \mapsto \mathrm{End}(\mathrm{Gr}(M))$ and $X \mapsto \mathrm{Gr}(\mathrm{End}(X))$ are idempotent.*

Proof. This follows immediately from part (b) of the preceding theorem. □

Write $\mathrm{Cl}(M) = \mathrm{End}(\mathrm{Gr}(M))$. Then $M \leq \mathrm{Cl}(M)$ and $\mathrm{Cl}(\mathrm{Cl}(M)) = \mathrm{Cl}(M)$, so Cl is an idempotent operator on transformation monoids on $\{1, \ldots, n\}$. I don't have a satisfactory description of the "closed" objects (those with $\mathrm{Cl}(M) = M$); more on this below.

Hulls

In the other direction, let $\mathrm{Hull}(X) = \mathrm{Gr}(\mathrm{End}(X))$, so that $\mathrm{Hull}(\mathrm{Hull}(X)) = \mathrm{Hull}(X)$. The hull of a graph has the following properties:

Theorem 6.

- *X is a spanning subgraph of $\mathrm{Hull}(X)$ (that is, these graphs have the same vertex set, and every edge of X is an edge of $\mathrm{Hull}(X)$).*
- *$\mathrm{End}(X) \leq \mathrm{End}(\mathrm{Hull}(X))$ and $\mathrm{Aut}(X) \leq \mathrm{Aut}(\mathrm{Hull}(X))$.*
- *$\mathrm{Core}(\mathrm{Hull}(X))$ is a complete graph on the vertex set of $\mathrm{Core}(X)$.*

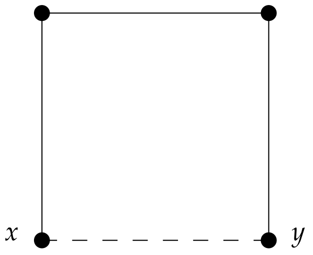
Proof. (a) If v and w are adjacent in X, then no endomorphism of X can collapse v and w, so they are adjacent in $\mathrm{Gr}(\mathrm{End}(X))$.

(b) $\mathrm{End}(\mathrm{Hull}(X)) = \mathrm{End}(\mathrm{Gr}(\mathrm{End}(X))) \geq \mathrm{End}(X)$. Now an endomorphism is an automorphism if and only if it is a permutation.

(c) The vertex set of $\mathrm{Core}(X)$ cannot be collapsed by endomorphisms, so is a complete subgraph of $\mathrm{Gr}(\mathrm{End}(X)) = \mathrm{Hull}(X)$. □

By (c), if X is a hull, then $\mathrm{Core}(X)$ is complete; but the converse is false. If X is the path of length 3, then $\mathrm{Core}(X)$ is a complete graph on two vertices, but $\mathrm{Hull}(X)$ is the 4-cycle, by our previous argument.

Example 7.



No homomorphism can identify x and y, so they are joined in the hull.

Note the increase in symmetry: $|\mathrm{Aut}(X)| = 2$ but $|\mathrm{Aut}(\mathrm{Hull}(X))| = 8$.

Closure revisited

Theorem 8. *A transformation monoid M is closed (that is, satisfies $M = \mathrm{Cl}(M)$) if and only if $M = \mathrm{End}(X)$ for some graph X which is a hull (and in particular, whose core is complete).*

Proof. Suppose that M is closed. Then $M = \mathrm{End}(X)$, where $X = \mathrm{Gr}(M)$; so $X = \mathrm{Gr}(\mathrm{End}(X)) = \mathrm{Hull}(X)$.

Conversely, if $X = \mathrm{Hull}(X)$, then $\mathrm{End}(X) = \mathrm{End}(\mathrm{Gr}(\mathrm{End}(X))) = \mathrm{Cl}(\mathrm{End}(X))$. □

A theorem

Recall that a graph is *non-trivial* if it is not complete or null.

Theorem 9. *Let M be a submonoid of T_n which is not contained in the symmetric group S_n. Then the following are equivalent:*

- *M is not synchronizing (that is, contains no constant function);*
- *$M \leq \mathrm{End}(X)$, where X is a non-trivial graph which is not a core;*
- *$M \leq \mathrm{End}(X)$, where X is a non-trivial graph whose core is complete.*

Note that the third condition on X is much stronger than the second. We will return to this!

Proof of the theorem

The implications from bottom to top are trivial. We show that the first condition implies the last.

Let M be a submonoid of T_n which is not contained in S_n and contains no constant function. Let $X = \mathrm{Gr}(M)$; recall that $v \sim w$ if and only if there is no $f \in M$ with $vf = wf$.

If $v \sim w$ and $f \in M$, then $vf \neq wf$ by definition. Moreover, if $vf \not\sim wf$ then $(vf)h = (wf)h$ for some h, contradicting the fact that $v \sim w$ (since $fh \in M$). So $M \leq \mathrm{End}(X)$.

Finally, if $f \in M$ has minimum rank, then the image of f carries a complete graph Y (since it cannot be made smaller by any element of M), and so Y is the core of X.

Synchronizing groups

The consequence of the preceding theorem for synchronizing groups is:

Theorem 10. *Let G be a permutation group on Ω. Then G is non-synchronizing if and only if there is a non-trivial graph X on Ω with $G \leq \mathrm{Aut}(X)$ such that $\mathrm{Core}(X)$ is complete (that is, $\omega(X) = \chi(X)$).*

Proof. If such an X exists, then choose f to be any endomorphism of X which is not an automorphism; then $\langle G, X \rangle \leq \mathrm{End}(X)$, so this monoid contains no constant function.

Conversely, if f is a witness that G is not synchronizing, let $M = \langle G, f \rangle$, and let $X = \mathrm{Gr}(M)$. □

An algorithm

Given a permutation group G on Ω, is it synchronizing?

- Check whether G is primitive (this can be done efficiently); if not, then G is not synchronizing.
- Construct all the non-trivial G-invariant graphs on Ω. (There are $2^r - 2$ of these, where r is the number of G-orbits on 2-subsets of Ω.)
- If any of these graphs X has $\omega(X) = \chi(X)$, then G is not synchronizing. If none has this property, then G is synchronizing.

Note that we have to solve two "hard" problems (clique number and chromatic number) for graphs with a large amount of symmetry.

Although both problems are NP-hard, in practice they can be solved for permutation groups with degrees in the hundreds without too much difficulty.

In the computer algebra system GAP, the package GRAPE will find all cliques of given size, or of maximum size, in a graph, up to the action of a specified group of automorphisms of the graph; the larger the group, the more efficient the computation.

Primitive and 2-set transitive groups

Let us note here that there is a similar, but easier, graph-theoretic test for other properties in our hierarchy.

Theorem 11. *Let G be a permutation group on Ω.*

- *G is imprimitive if and only if there is a non-trivial disconnected graph X on Ω with $G \leq \mathrm{Aut}(X)$.*
- *G is not 2-set transitive if and only if there is a non-trivial graph X on Ω with $G \leq \mathrm{Aut}(X)$.*

Proof. (a) If X exists, then its connected components are blocks of imprimitivity. Conversely, if G is imprimitive, the disjoint union of complete graphs on the blocks of imprimitivity is G-invariant.

(b) Clear. □

This test for primitivity is due to Donald Higman. There is an algorithmic version, though things are much simpler than for synchronization:

- instead of checking all $2^r - 2$ G-invariant graphs (where r is the number of orbits on 2-sets), we only need to check r graphs, those whose edges form G-orbits;
- instead of solving hard problems (clique size, chromatic number), we only need to solve the easy problem of connectedness.

There is no point in turning the second part into an algorithm for 2-set transitivity. The algorithm would begin by finding the orbits on 2-sets; but G is 2-set transitive if and only if there is just one orbit.

Separation

There is a similar test for separation, but we need to assume that the group we are testing is transitive. Recall that the *independence number* $\alpha(X)$ of a graph X is the size of the largest set of vertices containing no edges; that is, it is the clique number of the complementary graph.

Theorem 12. *Let G be a transitive permutation group on Ω. Then G is non-separating if and only if there is a non-trivial graph X on the vertex set Ω with $G \leq$ $\mathrm{Aut}(X)$, having the property that $\omega(X) \cdot \alpha(X) = |\Omega|$.*

Proof. Suppose first that there is a G-invariant graph X with $\omega(X)\alpha(X) = |\Omega|$. A clique and an independent set can meet in at most one point, since two points in the intersection would have to be both joined and not joined. So our earlier theorem shows that any clique of size $\omega(X)$ and any independent set of size $\alpha(X)$ meet in one point, and G is not separating.

Conversely, suppose that G is not separating; let sets A and B be witnesses. Let X be the graph whose edges are all images under G of pairs of points in A. Then A is a clique and (since no pair of points of B can be an image of a pair in A by g, else $|Ag \cap B| \geq 2$) B is an independent set. □

This theorem is the basis of an algorithmic test of the separation property. Given a transitive permutation graph G on Ω, let r be the number of orbits of G on 2-element subsets of Ω. The $2^r - 2$ non-trivial G-invariant graphs fall into $2^{r-1} - 1$ complementary pairs. Choose one graph X from each pair and compute its clique number $\omega(X)$ and its independence number $\alpha(X) = \omega(\overline{X})$. Check whether their product is $|\Omega|$.

- This test is easier than testing whether G is synchronizing. We have only half as many graphs to test, and we replace finding the chromatic number with the (easier) task of finding the independence number. (This is easier in the practical rather than the theoretical sense; both tasks are NP-hard.)
- For this reason, given G, it is better to test first whether G is separating. If so, then we know it is synchronizing. If not, we only have to compute the chromatic number of those G-invariant graphs X for which we already discovered that $\omega(X)\alpha(X) = |\Omega|$ and their complements.

Spreading groups

There is no such graph-theoretic test for the spreading property.

Instead, I will describe an example of the computation used to show that a certain permutation group is not spreading. The group is the classical group $G = \mathrm{PSp}(4,3)$, acting primitively on 40 points.

This group has rank 3, and so there are just two non-trivial G-invariant graphs. The first has clique size 4, the cliques being lines in a geometry called a *generalized quadrangle*: this means that two adjacent vertices lie in a unique line, and a point v not on a line L is collinear with a unique point of L.

The independence number of the graph is smaller than 10 (as we will see); so G is separating.

We will attempt to take a line L of the geometry as one of our sets.

As a first attempt, let $B = L$, and let A be the multiset which consists of a vertex v with multiplicity 3 and all of its non-neighbours each with multiplicity 1. Then it is easy to see that $A = 30$, and $|A * Bg| = 3$ for all $g \in G$ (a line either contains v or contains three non-neighbours of v).

So $(1)_3$ and (3) hold, but not (4), since 30 does not divide 40. (If we reverse the roles of A and B, we satisfy $(1)_3$, (2) and (4).)

So we sought a multiset of size 20 meeting every line in 2 points. Using the integer programming package in MAGMA, Pablo Spiga succeeded in constructing such a multiset; it has two points with multiplicity 2, and sixteen with multiplicity 1.

So the group $\mathrm{PSp}(4,3)$ is non-spreading (though it is separating).

The implication from spreading to separating thus does not reverse.

The multiset does not obviously generalise. Further computation shows that $\mathrm{PSp}(4,5)$ and $\mathrm{PSp}(4,7)$ are also non-spreading; the general case is unknown.

Cores of symmetric graphs

This theorem began as a conjecture, when Cristy Kazanidis and I were investigating cores of highly symmetric graphs. This arose before the development of the material in this lecture, and indeed helped lead to this development.

We were considering *rank-*3 *graphs*, those whose automorphism group is transitive on vertices, (ordered) edges, and (ordered) non-edges. The terminology comes from permutation group theory, where the *rank* of a permutation group G on Ω is the number of G-orbits on $\Omega \times \Omega$: in the case of a rank 3 graph, these orbits are the sets of pairs (v, w) where v and w are respectively equal, adjacent, and non-adjacent.

After considering a number of cases, we were led to the conjecture that, for any rank 3 graph X, either $\mathrm{Core}(X) = X$, or $\mathrm{Core}(X)$ is a complete graph. (Recall that the latter holds if and only if the clique number and chromatic number of X are equal.)

In fact a much stronger result is true:

Theorem 13. *Let X be a graph whose automorphism group is transitive on non-edges. Then either the core of X is complete, or X is a core.*

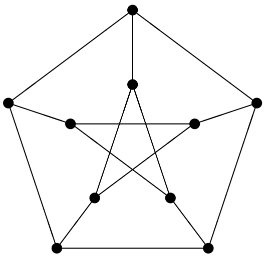
Proof. Let X' be the hull of X. Recall that X' contains X as a spanning subgraph (that is, it is X with possibly extra edges), and that $\mathrm{Aut}(X) \leq \mathrm{Aut}(X')$ (so that the extra edges form a union of $\mathrm{Aut}(X)$-orbits).

In our case, this implies that either $X' = X$ (whence X is a hull, so its core is complete), or X' is complete (whence no endomorphism of X collapses vertices, so X is a core). □

Here is another look at an example discussed earlier.

The permutation group induced by S_n on the set of 2-element subsets of $\{1, \ldots, n\}$ has rank 3 for $n \geq 4$. The two non-trivial graphs preserved by this group are

- the graph where two 2-sets are adjacent if they intersect (the *line graph* of the complete graph K_n, also called the "triangular graph");
- the graph where two 2-sets are adjacent if they are disjoint. For $n = 5$, this is the celebrated *Petersen graph*.



Let X be the line graph of K_n. Then $\omega(X) = n - 1$: the pairs containing a fixed element of $\{1, \ldots, n\}$ form a clique of maximum size. Also $\chi(X)$ is the *edge-chromatic number* (or *chromatic index*) of K_n, which is welll known to be $n - 1$ if n is even, or n if n is odd.

The complementary graph $\overline{X}$ has $\omega(\overline{X}) = \lfloor n/2 \rfloor$ (this is the maximum number of pairwise disjoint pairs); its chromatic number is $\chi(\overline{X}) = n - 2$ by special case of a theorem of Lovász. (In fact it is easy to see that it is greater than $n/2$).

So we conclude that, for $X = L(K_n)$,

- X is a core if and only if n is odd (its core is K_{n-1} if n is even);
- $\overline{X}$ is a core for all n.

Non-synchronizing ranks

This is an attempt to quantify the fact that not all primitive groups are synchronizing.

Let G be a transitive permutation group on Ω, and m an integer with $1 < m < n$. We say that m is a *non-synchronizing rank* of G if there exists a function $f : \Omega \to \Omega$ with image of cardinality m such that $\langle G, r \rangle$ is not synchronizing.

Let $NS(G)$ be the set of non-synchronizing ranks of G.

Thus, G is synchronizing if and only if $NS(G) = \emptyset$.

Conjecture 14. *An imprimitive group has very many non-synchronizing ranks, while a primitive group has very few.*

This conjecture is somewhat imprecise; I will now present some evidence for it.

Note that $NS(G)$ is the set of ranks (cardinalities of images) of endomorphisms of non-trivial G-invariant graphs.

Theorem 15. *If G is imprimitive, with l blocks of imprimitivity of size k (so that $n = |\Omega| = kl$), then*

$$\{k, 2k, \dots, n-k\} \cup \{l, l+1, \dots, n-1\} \subseteq NS(G).$$

Proof. Among the G-invariant graphs we have

- the disjoint union of l complete graphs of size k, which can be mapped onto any proper subset of its connected components;
- the complete multipartite graph with l blocks of size k, which can be mapped onto any set containing a transversal for the blocks.

□

In particular, G has at least $n/2$ non-synchronizing ranks.

Theorem 16. *If either $2 \in NS(G)$ or $n-1 \in NS(G)$, then G is imprimitive. In particular, if $2 \in NS(G)$, then G has (possibly trivial) blocks B_1 and B_2 with $B_1 \subseteq B_2$ and $|B_2| = 2|B_1|$.*

Proof. Let f have rank $n-1$ and not synchronize G. There is a graph X, necessarily regular, with $G \leq \mathrm{Aut}(X)$ and $f \in \mathrm{End}(X)$. Suppose that f maps x and y to z. Then x and y are non-adjacent; and f maps the neighbour sets of both x and y bijectively to the neighbour set of z. So x and y have the same neighbour sets. Now the relation $\equiv$ on Ω defined by $u \equiv v$ if u and v have the same neighbour sets is a non-trivial congruence; so G is imprimitive.

Let f have rank 2 and not synchronize G. There is a graph X with $G \leq \mathrm{Aut}(X)$, $f \in \mathrm{End}(X)$, and $\mathrm{Core}(X)$ complete. Clearly $\mathrm{Core}(X) = K_2$, so X is bipartite. Now let B_2 be a connected component of X and B_1 a bipartite block of this component. □

Example 17. Let G be the wreath product $S_m \operatorname{Wr} S_k$, with the power action, of degree $n = m^k$. Then $\{m, m^2, \dots, m^{k-1}\} \subseteq NS(G)$.

For let $H(k, m)$ be the k-dimensional hypercube with edges of size m: that is, the vertices are the k-tuples of elements of $\mathbb{Z}/(m)$, two vertices adjacent if they agree in all but one coordinate. For any s with $0 < s < k$, the map

$$(x_1, x_2, \dots, x_k) \mapsto (x_1, \dots, x_{s-1}, x_s + \cdots + x_k)$$

is a homomorphism from $H(k, m)$ onto $H(s, m)$.

In this example the number of non-synchronizing ranks is the logarithm of the number of vertices, while for an imprimitive group it is at least a constant fraction of this number.