Road colouring and road closures: synchronization and idempotent generation

Peter J. Cameron

Groups & their Applications
Bristol
1 June 2016

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.

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!)

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?

Idempotent generation

Here is a special case. The rank of a map is the size of its image; and an itempotent 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 2, the semigroup $\langle G, a\rangle \setminus G$ is idempotent-generated?

Idempotent generation

Here is a special case. The rank of a map is the size of its image; and an itempotent 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 2, the semigroup $\langle G, a \rangle \setminus G$ is idempotent-generated?

(The rank 1 case is trivial since any rank 1 map is idempotent.)

Idempotent generation

Here is a special case. The rank of a map is the size of its image; and an itempotent 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 2, the semigroup $\langle G, a\rangle \setminus G$ is idempotent-generated?

(The rank 1 case 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 $e^2 = e$)?

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.

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.

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.

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!

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.

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 $\{1, \ldots, n\}$.

The Houghton graph

Idempotent generation requires a stronger condition.

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'.

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 $H(G, k, P, S)$.

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.

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.

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 $\{1, \ldots, n\}$.

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.

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.

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!

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.

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 …

How many blocks?

Is there a polynomial upper bound for the number of maximal blocks of imprimitivity in a transitive group?

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:

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?

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 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?

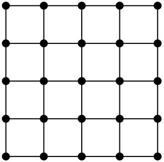
Of course we have more information: our group is a primitive group acting on the edges of some orbital graph …

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.

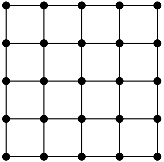
An example

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.



An example

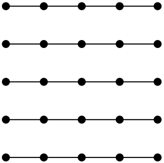
Consider the automorphism group of a $m \times m$ grid: two points are joined if they lie in the same row or column. The automorphism group is the wreath product $S_m \wr S_2$ in its product action on m^2 points.



The edges fall into two blocks of imprimitivity under the automorphism group: horizontal and vertical.

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.

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.

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.

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.

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.

Second generalisation

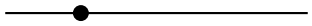
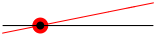
Another way of looking at the example leads to the following.

Proposition

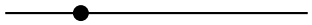
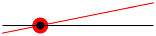
Let G be a primitive permutation group. Suppose that G has an imprimitive subgroup of index 2*. Then G does not have the* 2*-Hc property.*

Groups of this type are groups of automorphisms and anti-automorphisms of self-dual incidence structures, acting on the set of flags (incident point-block pairs) of the structure. We join two flags if they share a point or a block. 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.

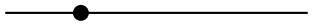
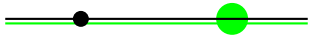
So there are two kinds of adjacency:

 is joined to 

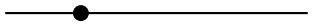
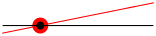
So there are two kinds of adjacency:

 is joined to 

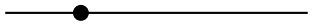
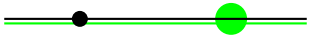
and

 is joined to 

So there are two kinds of adjacency:

 is joined to 

and

 is joined to 

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 $\mathrm{HS} : 2$ with degree 22176 coming from symmetric 2-designs with 2-transitive groups.

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.

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.

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.

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 $M_{12} : 2$.

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.

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.

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.

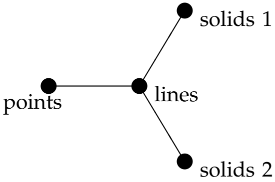
The principle of triality asserts that if the labels “point”, “solid of class 1” and “solid of class 2” are permuted arbitrarily, the lines being preserved, then the truth of all geometric properties remains unaltered.

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.

Thus, $P\Omega(8, q) : S_3$ 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.

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.

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;

Some cases

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

- n is prime;
- n is the square of a prime;

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;

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.

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.

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.

For example, a theorem of Wielandt asserts that a 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.

Synchronization

I will be brief. If you want to know more, there is a long preprint on the arXiv: 1511.03184

Synchronization

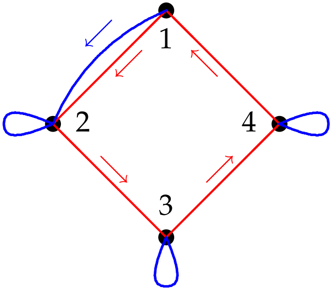
I will be brief. If you want to know more, there is a long preprint on the arXiv: 1511.03184

You are in a dungeon consisting of interconnecting caves. Each cave has two one-way exists, coloured red and blue; there is a third exit, which in one cave leads to freedom, and in the others to death. You have a map but don't know where you are.

Synchronization

I will be brief. If you want to know more, there is a long preprint on the arXiv: 1511.03184

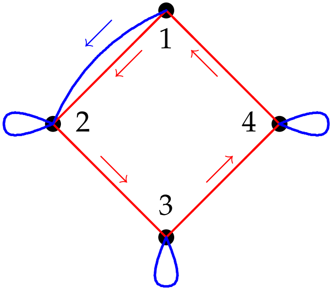
You are in a dungeon consisting of interconnecting caves. Each cave has two one-way exists, coloured red and blue; there is a third exit, which in one cave leads to freedom, and in the others to death. You have a map but don't know where you are.



Synchronization

I will be brief. If you want to know more, there is a long preprint on the arXiv: 1511.03184

You are in a dungeon consisting of interconnecting caves. Each cave has two one-way exists, coloured red and blue; there is a third exit, which in one cave leads to freedom, and in the others to death. You have a map but don't know where you are.



You can check that the sequence BRRRBRRRB will bring you to room 2 from any starting point.

Automata

A (finite-state, deterministic) automaton is a black box with a finite number of internal states. If a symbol from an alphabet is input, it undergoes a state transition. (Imagine that there are red and blue buttons on the box.)

Automata

A (finite-state, deterministic) automaton is a black box with a finite number of internal states. If a symbol from an alphabet is input, it undergoes a state transition. (Imagine that there are red and blue buttons on the box.)

Our automata are very simple: they don't have "accept states", and so they don't recognise languages; you can start in any state.

Automata

A (finite-state, deterministic) automaton is a black box with a finite number of internal states. If a symbol from an alphabet is input, it undergoes a state transition. (Imagine that there are red and blue buttons on the box.)

Our automata are very simple: they don't have "accept states", and so they don't recognise languages; you can start in any state.

An automaton can be represented combinatorially by a directed graph (whose vertices are the states) with edges labelled by symbols of the alphabet, so that there is exactly one edge with each label *leaving* each vertex, as in the preceding example.

Automata

A (finite-state, deterministic) automaton is a black box with a finite number of internal states. If a symbol from an alphabet is input, it undergoes a state transition. (Imagine that there are red and blue buttons on the box.)

Our automata are very simple: they don't have "accept states", and so they don't recognise languages; you can start in any state.

An automaton can be represented combinatorially by a directed graph (whose vertices are the states) with edges labelled by symbols of the alphabet, so that there is exactly one edge with each label *leaving* each vertex, as in the preceding example.

Algebraically, a transition is a transformation on the set of states; since we may compose transitions, an automaton is a transformation monoid on the set of states, with a prescribed set of generators.

Synchronization

An automaton is said to be synchronizing if there is a sequence of inputs which brings it to a known state, regardless of its starting point. Such a sequence is called a reset word.

Synchronization

An automaton is said to be synchronizing if there is a sequence of inputs which brings it to a known state, regardless of its starting point. Such a sequence is called a reset word.

The example on the preceding slide had a reset word of length 9 (but none of shorter length).

Synchronization

An automaton is said to be synchronizing if there is a sequence of inputs which brings it to a known state, regardless of its starting point. Such a sequence is called a reset word.

The example on the preceding slide had a reset word of length 9 (but none of shorter length).

Problem (The Černý conjecture)

If an n-state automaton is synchronizing, then it has a reset word of length at most $(n-1)^2$.

Synchronization

An automaton is said to be synchronizing if there is a sequence of inputs which brings it to a known state, regardless of its starting point. Such a sequence is called a reset word.

The example on the preceding slide had a reset word of length 9 (but none of shorter length).

Problem (The Černý conjecture)

If an n-state automaton is synchronizing, then it has a reset word of length at most $(n-1)^2$.

Our example and the obvious generalisation shows that, if true, this bound is best possible. But the conjecture is still open after half a century!

Synchronization

An automaton is said to be synchronizing if there is a sequence of inputs which brings it to a known state, regardless of its starting point. Such a sequence is called a reset word.
The example on the preceding slide had a reset word of length 9 (but none of shorter length).

Problem (The Černý conjecture)

If an n-state automaton is synchronizing, then it has a reset word of length at most $(n-1)^2$.

Our example and the obvious generalisation shows that, if true, this bound is best possible. But the conjecture is still open after half a century!
We can test whether an automaton is synchronizing in polynomial time, but finding the shortest reset word is NP-hard.

Road-colouring

A related conjecture, the road-colouring conjecture, was posed by Adler and Weiss in 1970, and solved by Trahtman in 2009.

Road-colouring

A related conjecture, the road-colouring conjecture, was posed by Adler and Weiss in 1970, and solved by Trahtman in 2009. Given a directed graph, is it possible to colour the edges in such a way that the result is an automaton which can be synchronized at any vertex?

Road-colouring

A related conjecture, the road-colouring conjecture, was posed by Adler and Weiss in 1970, and solved by Trahtman in 2009. Given a directed graph, is it possible to colour the edges in such a way that the result is an automaton which can be synchronized at any vertex?
There are some necessary conditions:

Road-colouring

A related conjecture, the road-colouring conjecture, was posed by Adler and Weiss in 1970, and solved by Trahtman in 2009. Given a directed graph, is it possible to colour the edges in such a way that the result is an automaton which can be synchronized at any vertex?

There are some necessary conditions:

- the digraph is strongly connected;

Road-colouring

A related conjecture, the road-colouring conjecture, was posed by Adler and Weiss in 1970, and solved by Trahtman in 2009. Given a directed graph, is it possible to colour the edges in such a way that the result is an automaton which can be synchronized at any vertex?
There are some necessary conditions:

- the digraph is strongly connected;
- the out-degrees of all vertices are the same;

Road-colouring

A related conjecture, the road-colouring conjecture, was posed by Adler and Weiss in 1970, and solved by Trahtman in 2009. Given a directed graph, is it possible to colour the edges in such a way that the result is an automaton which can be synchronized at any vertex?

There are some necessary conditions:

- the digraph is strongly connected;
- the out-degrees of all vertices are the same;
- the greatest common divisor of the cycle lengths is 1.

Road-colouring

A related conjecture, the road-colouring conjecture, was posed by Adler and Weiss in 1970, and solved by Trahtman in 2009. Given a directed graph, is it possible to colour the edges in such a way that the result is an automaton which can be synchronized at any vertex?

There are some necessary conditions:

- the digraph is strongly connected;
- the out-degrees of all vertices are the same;
- the greatest common divisor of the cycle lengths is 1.

The road-colouring conjecture (now theorem!) asserts that these necessary conditions are sufficient.

Synchronizing groups

With a few exceptions, all known examples meeting the Černý bound have monoids of the form $M = \langle G, a \rangle$, where G is a group of permutations, and a a transformation which is not a permutation. I will consider only this type in future.

Synchronizing groups

With a few exceptions, all known examples meeting the Černý bound have monoids of the form $M = \langle G, a \rangle$, where G is a group of permutations, and a a transformation which is not a permutation. I will consider only this type in future.

Abusing notation, we call a permutation group G synchronizing if the monoid generated by G and a is synchronizing for all non-permutations a (on the set Ω of states).

Synchronizing groups

With a few exceptions, all known examples meeting the Černý bound have monoids of the form $M = \langle G, a \rangle$, where G is a group of permutations, and a a transformation which is not a permutation. I will consider only this type in future.
Abusing notation, we call a permutation group G synchronizing if the monoid generated by G and a is synchronizing for all non-permutations a (on the set Ω of states).
Our question now is:

Question

Which permutation groups are synchronizing?

This turns out to include many problems of great interest from extremal combinatorics and finite geometry.

Synchronizing groups, 2

Proposition

A synchronizing group is primitive and basic.

For example, if G is not basic, choose a system of imprimitivity, and choose representatives for its blocks: let a map any point to its representative. Then $\langle G, a \rangle$ is not synchronizing.

Synchronizing groups, 2

Proposition

A synchronizing group is primitive and basic.

For example, if G is not basic, choose a system of imprimitivity, and choose representatives for its blocks: let a map any point to its representative. Then $\langle G, a \rangle$ is not synchronizing.

If G is not synchronizing, then a map of smallest rank not synchronized by G is uniform (all its kernel classes have the same size). We say that a group is almost synchronizing if it synchronizes any non-uniform map.

Synchronizing groups, 2

Proposition

A synchronizing group is primitive and basic.

For example, if G is not basic, choose a system of imprimitivity, and choose representatives for its blocks: let a map any point to its representative. Then $\langle G, a \rangle$ is not synchronizing.

If G is not synchronizing, then a map of smallest rank not synchronized by G is uniform (all its kernel classes have the same size). We say that a group is almost synchronizing if it synchronizes any non-uniform map.

It was conjectured for a time that every primitive group is almost synchronizing. But …

Primitive but not almost synchronizing

We found two nice counterexamples to the conjecture. These are the automorphism groups of the Tutte–Coxeter graph on 30 vertices and the Biggs–Smith graph on 102 vertices, acting on the edges of the graph.

Primitive but not almost synchronizing

We found two nice counterexamples to the conjecture. These are the automorphism groups of the Tutte–Coxeter graph on 30 vertices and the Biggs–Smith graph on 102 vertices, acting on the edges of the graph.

Said another way, the line graphs of these two interesting graphs have primitive automorphism groups and admit non-uniform endomorphisms.

Primitive but not almost synchronizing

We found two nice counterexamples to the conjecture. These are the automorphism groups of the Tutte–Coxeter graph on 30 vertices and the Biggs–Smith graph on 102 vertices, acting on the edges of the graph.

Said another way, the line graphs of these two interesting graphs have primitive automorphism groups and admit non-uniform endomorphisms.

In each case, the line graph has the property that a closed vertex neighbourhood is a butterfly (two triangles with a common vertex), and the whole graph has an endomorphism onto the butterfly.

Primitive but not almost synchronizing

We found two nice counterexamples to the conjecture. These are the automorphism groups of the Tutte–Coxeter graph on 30 vertices and the Biggs–Smith graph on 102 vertices, acting on the edges of the graph.

Said another way, the line graphs of these two interesting graphs have primitive automorphism groups and admit non-uniform endomorphisms.

In each case, the line graph has the property that a closed vertex neighbourhood is a butterfly (two triangles with a common vertex), and the whole graph has an endomorphism onto the butterfly.

Subsequently, more counterexamples were found, but these line graphs have rich and interesting endomorphisms and would surely repay further investigation!