Synchronization and permutation groups

Peter J. Cameron

Queen Mary
University of London

p.j.cameron@qmul.ac.uk

4-ICC, Auckland
December 2008

This is part of an investigation involving, among others, João Araújo, Πeter Neumann, Jan Saxl, Csaba Schneider, Pablo Spiga, and Ben Steinberg. Cristy Kazanidis, Nik Ruskuc, Colva Roney-Dougal, Ian Gent and Tom Kelsey have also been involved.

This is part of an investigation involving, among others, João Araújo, Πeter Neumann, Jan Saxl, Csaba Schneider, Pablo Spiga, and Ben Steinberg. Cristy Kazanidis, Nik Ruskuc, Colva Roney-Dougal, Ian Gent and Tom Kelsey have also been involved.

There is far more material than can be presented here; I will talk about other aspects of this topic in Perth next month. See you there!

This is part of an investigation involving, among others, João Araújo, Πeter Neumann, Jan Saxl, Csaba Schneider, Pablo Spiga, and Ben Steinberg. Cristy Kazanidis, Nik Ruskuc, Colva Roney-Dougal, Ian Gent and Tom Kelsey have also been involved.

There is far more material than can be presented here; I will talk about other aspects of this topic in Perth next month. See you there!

See also Gordon Royle's talk at this meeting for a more combinatorial approach.

Automata

An automaton is a machine which can be in any of a set of internal states which cannot be directly observed.

Automata

An automaton is a machine which can be in any of a set of internal states which cannot be directly observed.

We can force the machine to make any desired sequence of transitions (each transition being a mapping from the set of states to itself).

Automata

An automaton is a machine which can be in any of a set of internal states which cannot be directly observed.

We can force the machine to make any desired sequence of transitions (each transition being a mapping from the set of states to itself).

We can represent an automaton as an edge-coloured directed graph, where the vertices are the states, and the colours are the transitions. We require that the graph should have exactly one edge of each colour *leaving* each vertex.

Synchronization

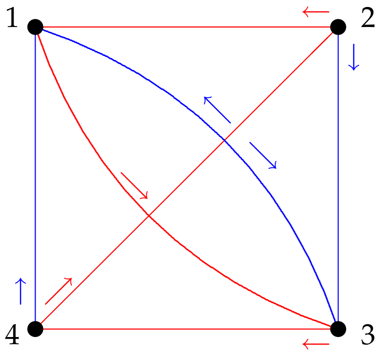
Suppose that you are given an automaton (whose structure you know) in an unknown state. You would like to put it into a known state, by applying a sequence of transitions to it. Of course this is not always possible!

Synchronization

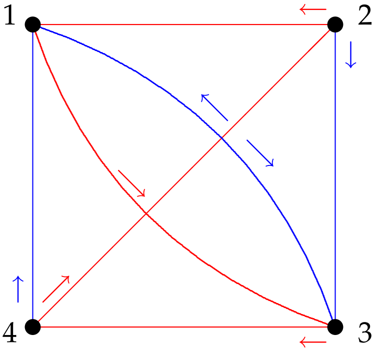
Suppose that you are given an automaton (whose structure you know) in an unknown state. You would like to put it into a known state, by applying a sequence of transitions to it. Of course this is not always possible!

A reset word is a sequence of transitions which take the automaton from any state into a known state; in other words, the composition of the corresponding transitions is a constant mapping.

An example



An example



You can check that (Blue, Red, Blue, Blue) is a reset word which takes you to room 3 no matter where you start.

Applications

- Industrial robotics: pieces arrive to be assembled by a robot. The orientation is critical. You could equip the robot with vision sensors and manipulators so that it can rotate the pieces into the correct orientation. But it is much cheaper and less error-prone to regard the possible orientations of the pieces as states of an automaton on which transitions can be performed by simple machinery, and apply a reset word before the pieces arrive at the robot.

Applications

- Industrial robotics: pieces arrive to be assembled by a robot. The orientation is critical. You could equip the robot with vision sensors and manipulators so that it can rotate the pieces into the correct orientation. But it is much cheaper and less error-prone to regard the possible orientations of the pieces as states of an automaton on which transitions can be performed by simple machinery, and apply a reset word before the pieces arrive at the robot.
- Bioinformatics: If a soup of DNA molecules is to perform some computation, we need the molecules to be all in a known state first. We can simultaneously apply a reset word to all of them, where the transitions are induced by some chemical or biological process.

The road-colouring problem

Trivially, a directed graph with constant out-degree can be edge-coloured to produce an automaton. The conditions in the next paragraph are easily seen to be necessary for the resulting automaton to have a reset word.

The road-colouring problem

Trivially, a directed graph with constant out-degree can be edge-coloured to produce an automaton. The conditions in the next paragraph are easily seen to be necessary for the resulting automaton to have a reset word.

Problem

Suppose that D is a directed graph in which all edges have out-degree d. Then the edges of D can be coloured with d colours to produce an automaton with a reset word if and only if D is connected and the greatest common divisor of the cycle lengths in D is 1.

The road-colouring problem

Trivially, a directed graph with constant out-degree can be edge-coloured to produce an automaton. The conditions in the next paragraph are easily seen to be necessary for the resulting automaton to have a reset word.

Problem

Suppose that D is a directed graph in which all edges have out-degree d. Then the edges of D can be coloured with d colours to produce an automaton with a reset word if and only if D is connected and the greatest common divisor of the cycle lengths in D is 1.

This was the road-colouring conjecture until it was proved by Avraham Trahtman last year.

The Černý conjecture

How do we decide whether a reset word exists? We can search for one by trial and error; how far do we have to go before we can conclude that there is no reset word?

The Černý conjecture

How do we decide whether a reset word exists? We can search for one by trial and error; how far do we have to go before we can conclude that there is no reset word?

Problem

Suppose that an n-vertex automaton has a reset word. Show that it has one of length at most $(n-1)^2$.

The Černý conjecture

How do we decide whether a reset word exists? We can search for one by trial and error; how far do we have to go before we can conclude that there is no reset word?

Problem

Suppose that an n-vertex automaton has a reset word. Show that it has one of length at most $(n-1)^2$.

This is the Černý conjecture, and is still open. If true, the bound would be best possible.

A group-theoretic approach

At the other extreme from a synchronizing automaton is one in which all the transitions are permutations (and generate a permutation group). One approach to the Černý conjecture is to separate out this difficulty.

A group-theoretic approach

At the other extreme from a synchronizing automaton is one in which all the transitions are permutations (and generate a permutation group). One approach to the Černý conjecture is to separate out this difficulty.

A permutation group G on a set Ω is said to be synchronizing if, whenever $f : \Omega \to \Omega$ is a mapping which is not a permutation, the semigroup generated by G and f contains a reset word (a constant mapping).

A group-theoretic approach

At the other extreme from a synchronizing automaton is one in which all the transitions are permutations (and generate a permutation group). One approach to the Černý conjecture is to separate out this difficulty.

A permutation group G on a set Ω is said to be synchronizing if, whenever $f : \Omega \to \Omega$ is a mapping which is not a permutation, the semigroup generated by G and f contains a reset word (a constant mapping).

Problem

Which permutation groups are synchronizing?

Synchronizing groups

This condition can be reformulated in more group-theoretic terms.

Synchronizing groups

This condition can be reformulated in more group-theoretic terms.

Proposition

A permutation group G on Ω is non-synchronizing if and only if there is a non-trivial partition π of Ω and a subset Δ of Ω such that, for all $g \in G$, Δg is a section (of transversal) of π.

Synchronizing groups

This condition can be reformulated in more group-theoretic terms.

Proposition

A permutation group G on Ω is non-synchronizing if and only if there is a non-trivial partition π of Ω and a subset Δ of Ω such that, for all $g \in G$, Δg is a section (of transversal) of π.

Corollary

A synchronizing group is primitive.

Synchronizing groups

This condition can be reformulated in more group-theoretic terms.

Proposition

A permutation group G on Ω is non-synchronizing if and only if there is a non-trivial partition π of Ω and a subset Δ of Ω such that, for all $g \in G$, Δg is a section (of transversal) of π.

Corollary

A synchronizing group is primitive.

For if there is a G-invariant partition π, then any section of π has the required property.

Non-synchronizing ranks

This is an attempt to measure the failure of a permutation group to be synchronizing. We define the set $M(G)$ of non-synchronizing ranks of a permutation group G to be the set of ranks of functions f on Ω for which $\langle G, f \rangle$ contains no constant function. Thus $M(G) = \emptyset$ if and only if G is synchronizing.

Non-synchronizing ranks

This is an attempt to measure the failure of a permutation group to be synchronizing. We define the set $M(G)$ of non-synchronizing ranks of a permutation group G to be the set of ranks of functions f on Ω for which $\langle G, f \rangle$ contains no constant function. Thus $M(G) = \emptyset$ if and only if G is synchronizing.

Theorem

- $n - 1 \in M(G)$ *if and only if* G *is imprimitive.*

Non-synchronizing ranks

This is an attempt to measure the failure of a permutation group to be synchronizing. We define the set $M(G)$ of non-synchronizing ranks of a permutation group G to be the set of ranks of functions f on Ω for which $\langle G, f \rangle$ contains no constant function. Thus $M(G) = \emptyset$ if and only if G is synchronizing.

Theorem

- *$n - 1 \in M(G)$ if and only if G is imprimitive.*
- *$2 \in M(G)$ if and only if G has (possibly trivial) blocks B_1 and B_2 with $B_1 \subset B_2$ and $|B_2| = 2|B_1|$.*

Non-synchronizing ranks

This is an attempt to measure the failure of a permutation group to be synchronizing. We define the set $M(G)$ of non-synchronizing ranks of a permutation group G to be the set of ranks of functions f on Ω for which $\langle G, f \rangle$ contains no constant function. Thus $M(G) = \emptyset$ if and only if G is synchronizing.

Theorem

- $n-1 \in M(G)$ *if and only if* G *is imprimitive.*
- $2 \in M(G)$ *if and only if* G *has (possibly trivial) blocks* B_1 *and* B_2 *with* $B_1 \subset B_2$ *and* $|B_2| = 2|B_1|$.
- *If* G *has a block of size* k, *then*

$$\{n/k, n/k+1, \ldots, n-1\} \cup \{k, 2k, \ldots, n-k\} \subseteq M(G).$$

Non-synchronizing ranks

This is an attempt to measure the failure of a permutation group to be synchronizing. We define the set $M(G)$ of non-synchronizing ranks of a permutation group G to be the set of ranks of functions f on Ω for which $\langle G, f \rangle$ contains no constant function. Thus $M(G) = \emptyset$ if and only if G is synchronizing.

Theorem

- $n - 1 \in M(G)$ *if and only if* G *is imprimitive.*
- $2 \in M(G)$ *if and only if* G *has (possibly trivial) blocks* B_1 *and* B_2 *with* $B_1 \subset B_2$ *and* $|B_2| = 2|B_1|$.
- *If* G *has a block of size* k, *then*

$$\{n/k, n/k + 1, \ldots, n - 1\} \cup \{k, 2k, \ldots, n - k\} \subseteq M(G).$$

By contrast, we conjecture that if G is primitive then $M(G)$ is very small.

Separating groups

Let G be transitive on Ω, with $|\Omega| = n$. Let Γ and Δ be subsets of Ω, with $|\Gamma| = k$, $|\Delta| = l$.

Separating groups

Let G be transitive on Ω, with $|\Omega| = n$. Let Γ and Δ be subsets of Ω, with $|\Gamma| = k$, $|\Delta| = l$.

Lemma

if $kl < n$, then there exists $g \in G$ with $\Gamma \cap \Delta g = \emptyset$.

Separating groups

Let G be transitive on Ω, with $|\Omega| = n$. Let Γ and Δ be subsets of Ω, with $|\Gamma| = k$, $|\Delta| = l$.

Lemma

if $kl < n$, then there exists $g \in G$ with $\Gamma \cap \Delta g = \emptyset$.

We say that G is separating if the same conclusion holds when $kl = n$.

Separating groups

Let G be transitive on Ω, with $|\Omega| = n$. Let Γ and Δ be subsets of Ω, with $|\Gamma| = k$, $|\Delta| = l$.

Lemma

if $kl < n$, then there exists $g \in G$ with $\Gamma \cap \Delta g = \emptyset$.

We say that G is separating if the same conclusion holds when $kl = n$.

Proposition

A separating group is synchronizing.

Separating groups

Let G be transitive on Ω, with $|\Omega| = n$. Let Γ and Δ be subsets of Ω, with $|\Gamma| = k$, $|\Delta| = l$.

Lemma

if $kl < n$, then there exists $g \in G$ with $\Gamma \cap \Delta g = \emptyset$.

We say that G is separating if the same conclusion holds when $kl = n$.

Proposition

A separating group is synchronizing.

For if G is non-synchronizing, and Γ is a part of a partition π for which (π, Δ) witness the non-synchronization, then by assumption $|\Gamma \cap \Delta g| = 1$ for all $g \in G$.

Separation and synchronization

Since synchronizing groups are primitive, the obvious first step is to check primitive groups of small degree (up to a few hundred) for these properties. MAGMA and GAP contain lists of these groups. But the checking is non-trivial.

Separation and synchronization

Since synchronizing groups are primitive, the obvious first step is to check primitive groups of small degree (up to a few hundred) for these properties. MAGMA and GAP contain lists of these groups. But the checking is non-trivial.

In particular, we only know a tiny handful of permutation groups which are synchronizing but not separating; it would be interesting to find out why this property is so rare.

Separation and synchronization

Since synchronizing groups are primitive, the obvious first step is to check primitive groups of small degree (up to a few hundred) for these properties. MAGMA and GAP contain lists of these groups. But the checking is non-trivial.

In particular, we only know a tiny handful of permutation groups which are synchronizing but not separating; it would be interesting to find out why this property is so rare.

Some of the examples come from finite geometry (involving properties of ovoids and spreads in polar spaces), but others appear to be "sporadic".

Graph-theoretic characterisations

These properties can be detected by undirected graphs admitting the group G. The clique number $\omega(X)$ and the independence number $\alpha(X)$ are the cardinalities of the largest complete and null induced subgraphs of X; the chromatic number $\chi(X)$ is the smallest number of colours required to colour the vertices so that adjacent vertices get different colours. Clearly $\omega(X) \leq \chi(X)$, since vertices of a complete subgraph must get different colours.

Graph-theoretic characterisations

These properties can be detected by undirected graphs admitting the group G. The clique number $\omega(X)$ and the independence number $\alpha(X)$ are the cardinalities of the largest complete and null induced subgraphs of X; the chromatic number $\chi(X)$ is the smallest number of colours required to colour the vertices so that adjacent vertices get different colours. Clearly $\omega(X) \leq \chi(X)$, since vertices of a complete subgraph must get different colours.

Proposition

Let G be a permutation group on Ω, with $|\Omega| = n$.

Graph-theoretic characterisations

These properties can be detected by undirected graphs admitting the group G. The clique number $\omega(X)$ and the independence number $\alpha(X)$ are the cardinalities of the largest complete and null induced subgraphs of X; the chromatic number $\chi(X)$ is the smallest number of colours required to colour the vertices so that adjacent vertices get different colours. Clearly $\omega(X) \leq \chi(X)$, since vertices of a complete subgraph must get different colours.

Proposition

Let G be a permutation group on Ω, with $|\Omega| = n$.

- *G is non-synchronizing if and only if there is a non-trivial G-invariant graph X for which $\omega(X) = \chi(X)$.*

Graph-theoretic characterisations

These properties can be detected by undirected graphs admitting the group G. The clique number $\omega(X)$ and the independence number $\alpha(X)$ are the cardinalities of the largest complete and null induced subgraphs of X; the chromatic number $\chi(X)$ is the smallest number of colours required to colour the vertices so that adjacent vertices get different colours. Clearly $\omega(X) \leq \chi(X)$, since vertices of a complete subgraph must get different colours.

Proposition

Let G be a permutation group on Ω, with $|\Omega| = n$.

- *G is non-synchronizing if and only if there is a non-trivial G-invariant graph X for which $\omega(X) = \chi(X)$.*
- *Let G be transitive. Then G is non-separating if and only if there is a non-trivial G-invariant graph X such that $\omega(X) \cdot \alpha(X) = n$.*

Basic groups

A power structure on Ω is a hypercube with vertex set Ω, that is, a bijection between Ω aand X^n for some set X and integer $n > 1$.

Basic groups

A power structure on Ω is a hypercube with vertex set Ω, that is, a bijection between Ω aand X^n for some set X and integer $n > 1$.

A permutation group G is non-basic if it preserves a power structure on Ω. Such a group is contained in a wreath product of smaller permutation group.

Basic groups

A power structure on Ω is a hypercube with vertex set Ω, that is, a bijection between Ω aand X^n for some set X and integer $n > 1$.
A permutation group G is non-basic if it preserves a power structure on Ω. Such a group is contained in a wreath product of smaller permutation group.

Proposition

A synchronizing group is basic.

For, if G is non-basic, then let π be the partition of X^n according to the value of the first coordinate, and Δ the diagonal set $\{(x, x, \ldots,) : x \in X\}$.

The O'Nan–Scott Theorem

Theorem

A basic group is affine, diagonal, or almost simple.

The O'Nan–Scott Theorem

Theorem

A basic group is affine, diagonal, or almost simple.

So we only have to look at these three types of groups to understand synchronizing permutation groups.

The O'Nan–Scott Theorem

Theorem

A basic group is affine, diagonal, or almost simple.

So we only have to look at these three types of groups to understand synchronizing permutation groups.

In particular, product actions of wreath products, twisted wreath products, and "compound diagonal" groups cannot be synchronizing; and an affine group in which the linear subgroup (the stabiliser of the zero vector) is imprimitive (i.e. preserves a direct sum decompositon) is not synchronizing.

The O'Nan–Scott Theorem

Theorem

A basic group is affine, diagonal, or almost simple.

So we only have to look at these three types of groups to understand synchronizing permutation groups.

In particular, product actions of wreath products, twisted wreath products, and "compound diagonal" groups cannot be synchronizing; and an affine group in which the linear subgroup (the stabiliser of the zero vector) is imprimitive (i.e. preserves a direct sum decompositon) is not synchronizing.

I will look at a couple of examples, to illustrate that hard problems arise!

The symmetric group acting on k-sets

Let G be the permutation group induced by S_n on the set Ω of k-subsets of $\{1, \ldots, n\}$, for $1 < k < n/2$.

The symmetric group acting on k-sets

Let G be the permutation group induced by S_n on the set Ω of k-subsets of $\{1, \ldots, n\}$, for $1 < k < n/2$.

Proposition

If k divides n, then G is non-synchronizing.

The symmetric group acting on k-sets

Let G be the permutation group induced by S_n on the set Ω of k-subsets of $\{1, \ldots, n\}$, for $1 < k < n/2$.

Proposition

If k divides n, then G is non-synchronizing.

We use Baranyai's Theorem: there is a partition π of Ω into subsets each of which is a partition of $\{1, \ldots, n\}$. Take Δ to consist of the k-subsets containing the element 1.

The symmetric group acting on k-sets

Proposition

For $k = 2$, the following are equivalent:

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

The symmetric group acting on k-sets

Proposition

For $k = 2$, the following are equivalent:

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

To show the non-trivial implication, suppose that n is odd. The G-invariant graphs are $L(K_n)$ and its complement. Now $L(K_n)$ has clique number $n-1$ and independence number $\lfloor n/2 \rfloor$, so G is separating if n is odd.

The symmetric group acting on k-sets

Proposition

For $k = 3$, the following are equivalent:

- *G is synchronizing;*
- *G is separating;*
- *n is not a multiple of 3, not congruent to 1 mod 6, and not equal to 8.*

The symmetric group acting on k-sets

Proposition

For $k = 3$, the following are equivalent:

- *G is synchronizing;*
- *G is separating;*
- *n is not a multiple of 3, not congruent to 1 mod 6, and not equal to 8.*

One step in the proof depends on Teirlinck's theorem that there is a large set of Steiner triple systems if n is congruent to 1 or 3 mod 6 and $n > 7$ (a partition π of Ω into Steiner triple systems). Take Δ to consist of all 3-sets containing 1 and 2.

The symmetric group acting on k-sets

Proposition

For $k = 3$, the following are equivalent:

- *G is synchronizing;*
- *G is separating;*
- *n is not a multiple of 3, not congruent to 1 mod 6, and not equal to 8.*

One step in the proof depends on Teirlinck's theorem that there is a large set of Steiner triple systems if n is congruent to 1 or 3 mod 6 and $n > 7$ (a partition π of Ω into Steiner triple systems). Take Δ to consist of all 3-sets containing 1 and 2.

For $k \geq 4$ the complete answer is not known, but synchronization and separation are not always equivalent.

A linear analogue

The linear analogue of S_n on k-sets is the linear group $\mathrm{GL}(n, q)$ acting on k-dimensional subspaces of the n-dimensional vector space, i.e. on $(k-1)$-flats of $\mathrm{PG}(n-1, q)$.

A linear analogue

The linear analogue of S_n on k-sets is the linear group $\mathrm{GL}(n, q)$ acting on k-dimensional subspaces of the n-dimensional vector space, i.e. on $(k-1)$-flats of $\mathrm{PG}(n-1, q)$.
For $k = 2$ (the action on lines of the projective space), this group is separating if and only if n is odd.

A linear analogue

The linear analogue of S_n on k-sets is the linear group $\mathrm{GL}(n, q)$ acting on k-dimensional subspaces of the n-dimensional vector space, i.e. on $(k-1)$-flats of $\mathrm{PG}(n-1, q)$.
For $k = 2$ (the action on lines of the projective space), this group is separating if and only if n is odd.
For even n, it is non-synchronizing if and only if there is a parallelism of lines in the projective space. The existence of a parallelism is known only in a few cases (when n is a power of 2, or when $n = 6$ and q is even).

Classical groups

Let G be a classical symplectic, orthogonal or unitary group, acting on the point set of the corresponding polar space (embedded in a projective space). This consists of all points which are isotropic with respect to the form. We assume that the Witt index is at least 2 (so that the poar space contains lines of the projective space).

Classical groups

Let G be a classical symplectic, orthogonal or unitary group, acting on the point set of the corresponding polar space (embedded in a projective space). This consists of all points which are isotropic with respect to the form. We assume that the Witt index is at least 2 (so that the poar space contains lines of the projective space).

A maximal flat is a projective subspace of maximal dimension contained in the polar space. A spread is a partition of the polar space into maximal flats. An ovoid is a set of points meeting every maximal flat in a unique point.

Classical groups

Proposition

Let G be a classical group and $\mathcal{G}$ its associated polar space.

- *G is non-separating if and only if $\mathcal{G}$ has an ovoid.*
- *G is non-synchronizing if and only if $\mathcal{G}$ has either an ovoid and a spread, or a partition into ovoids.*

Classical groups

Proposition

Let G be a classical group and $\mathcal{G}$ its associated polar space.

- *G is non-separating if and only if $\mathcal{G}$ has an ovoid.*
- *G is non-synchronizing if and only if $\mathcal{G}$ has either an ovoid and a spread, or a partition into ovoids.*

The existence of ovoids and spreads in polar spaces is not completely resolved despite many years of study by finite geometers; this is a very hard geometric problem!

Towards the Černý conjecture

Suppose that G is a synchronizing permutation group. What further properties do we need in order that the Černý conjecture should hold for any automaton obtained by adjoining a non-permutation to a set of generators of G?

Towards the Černý conjecture

Suppose that G is a synchronizing permutation group. What further properties do we need in order that the Černý conjecture should hold for any automaton obtained by adjoining a non-permutation to a set of generators of G?

Let f be a non-permutation. Without loss of generality, a reset word will look like

$$fg_1fg_2f\cdots fg_{r-1}f$$

for $g_1,\ldots,g_r \in G$. We need to bound r and also the expressions for $g_1,\ldots,g_r$ in terms of generators.

Towards the Černý conjecture

Suppose that G is a synchronizing permutation group. What further properties do we need in order that the Černý conjecture should hold for any automaton obtained by adjoining a non-permutation to a set of generators of G?

Let f be a non-permutation. Without loss of generality, a reset word will look like

$$fg_1fg_2f\cdots fg_{r-1}f$$

for $g_1,\ldots,g_r \in G$. We need to bound r and also the expressions for $g_1,\ldots,g_r$ in terms of generators.

Suppose that G is "large" enough that, for any set S, we can move it by an element $g_i \in G$ to a position where its inverse image under f is larger than $|S|$. Then we have $r \leq n-1$.

QI groups

Let $\mathbb{F}$ be a field of characteristic zero (or not dividing n). Then the permutation module $\mathbb{F}\Omega$ is the direct sum of a 1-dimensional submodule V_0 (the constant vectors) and an $(n-1)$-dimensional submodule V_1 (the vectors with coordinate sum zero).

QI groups

Let $\mathbb{F}$ be a field of characteristic zero (or not dividing n). Then the permutation module $\mathbb{F}\Omega$ is the direct sum of a 1-dimensional submodule V_0 (the constant vectors) and an $(n-1)$-dimensional submodule V_1 (the vectors with coordinate sum zero).

- G is 2-transitive if and only if V_1 is irreducible in the case when $\mathbb{F} = \mathbb{C}$;

QI groups

Let $\mathbb{F}$ be a field of characteristic zero (or not dividing n). Then the permutation module $\mathbb{F}\Omega$ is the direct sum of a 1-dimensional submodule V_0 (the constant vectors) and an $(n-1)$-dimensional submodule V_1 (the vectors with coordinate sum zero).

- G is 2-transitive if and only if V_1 is irreducible in the case when $\mathbb{F} = \mathbb{C}$;
- G is 2-set transitive if and only if V_1 is irreducible in the case when $\mathbb{F} = \mathbb{R}$.

QI groups

Let $\mathbb{F}$ be a field of characteristic zero (or not dividing n). Then the permutation module $\mathbb{F}\Omega$ is the direct sum of a 1-dimensional submodule V_0 (the constant vectors) and an $(n-1)$-dimensional submodule V_1 (the vectors with coordinate sum zero).

- G is 2-transitive if and only if V_1 is irreducible in the case when $\mathbb{F} = \mathbb{C}$;
- G is 2-set transitive if and only if V_1 is irreducible in the case when $\mathbb{F} = \mathbb{R}$.

We say that G is QI if V_1 is irreducible in the case when $\mathbb{F} = \mathbb{Q}$.

Spreading groups

Arnold and Steinberg showed that QI-groups have the property we noted earlier to approach the Černý conjecture. Later, Steinberg remarked that something less is required.

Spreading groups

Arnold and Steinberg showed that QI-groups have the property we noted earlier to approach the Černý conjecture. Later, Steinberg remarked that something less is required. The group G is not QI if and only if there exist functions v, w from Ω to the natural numbers, which are not constant and have support size greater than 1, such that $v \cdot wg$ is constant for $g \in G$.

Spreading groups

Arnold and Steinberg showed that QI-groups have the property we noted earlier to approach the Černý conjecture.
Later, Steinberg remarked that something less is required.
The group G is not QI if and only if there exist functions v, w from Ω to the natural numbers, which are not constant and have support size greater than 1, such that $v \cdot wg$ is constant for $g \in G$.
We say that G is non-spreading if such v and w exist with the additional properties

Spreading groups

Arnold and Steinberg showed that QI-groups have the property we noted earlier to approach the Černý conjecture. Later, Steinberg remarked that something less is required. The group G is not QI if and only if there exist functions v, w from Ω to the natural numbers, which are not constant and have support size greater than 1, such that $v \cdot wg$ is constant for $g \in G$.

We say that G is non-spreading if such v and w exist with the additional properties

- v takes only the values 0 and 1;

Spreading groups

Arnold and Steinberg showed that QI-groups have the property we noted earlier to approach the Černý conjecture. Later, Steinberg remarked that something less is required. The group G is not QI if and only if there exist functions v, w from Ω to the natural numbers, which are not constant and have support size greater than 1, such that $v \cdot wg$ is constant for $g \in G$.

We say that G is non-spreading if such v and w exist with the additional properties

- v takes only the values 0 and 1;
- the sum of the values of w divides $|\Omega|$.

Spreading groups

Arnold and Steinberg showed that QI-groups have the property we noted earlier to approach the Černý conjecture. Later, Steinberg remarked that something less is required. The group G is not QI if and only if there exist functions v, w from Ω to the natural numbers, which are not constant and have support size greater than 1, such that $v \cdot wg$ is constant for $g \in G$.
We say that G is non-spreading if such v and w exist with the additional properties

- v takes only the values 0 and 1;
- the sum of the values of w divides $|\Omega|$.

Then G is spreading otherwise.

A hierarchy of properties

A spreading group if separating. If Γ and Δ witness the non-separating property of G, their characteristic functions witness the non-spreading property.

A hierarchy of properties

A spreading group if separating. If Γ and Δ witness the non-separating property of G, their characteristic functions witness the non-spreading property.
Hence we have the following hierarchy of properties of transitive permutation groups, listing in order of increasing strength:

> *primitive, basic, synchronizing, separating, spreading, QI,* 2*-set transitive,* 2*-transitive.*

A hierarchy of properties

A spreading group if separating. If Γ and Δ witness the non-separating property of G, their characteristic functions witness the non-spreading property.

Hence we have the following hierarchy of properties of transitive permutation groups, listing in order of increasing strength:

> *primitive, basic, synchronizing, separating, spreading, QI,* 2*-set transitive,* 2*-transitive.*

We currently have no example of a group which is spreading but not QI. However, all the other inclusions are strict.

Černý again

Proposition

Let G be a spreading permutation group on Ω. Then, for any map $f : \Omega \to \Omega$ which is not a permutation, there exist elements $g_1, \ldots, g_{n-2} \in G$ such that $fg_1fg_2 \cdots fg_{n-2}f$ is a constant function.

Černý again

Proposition

Let G be a spreading permutation group on Ω. Then, for any map $f : \Omega \to \Omega$ which is not a permutation, there exist elements $g_1, \ldots, g_{n-2} \in G$ such that $fg_1fg_2 \cdots fg_{n-2}f$ is a constant function.

"Spreading" is the right conjecture to make this work.

Černý again

Proposition

Let G be a spreading permutation group on Ω. Then, for any map $f : \Omega \to \Omega$ which is not a permutation, there exist elements $g_1, \ldots, g_{n-2} \in G$ such that $fg_1fg_2 \cdots fg_{n-2}f$ is a constant function.

"Spreading" is the right conjecture to make this work.

If G is spreading and we can show that $g_1, \ldots, g_{n-2}$ have average length at most $n - 1$ in terms of a given generating set for G, then we have established an instance of the Černý conjecture.

Some open problems

- Determine the QI permutation groups.

Some open problems

- Determine the QI permutation groups.
- Is there a permutation group which is spreading but not QI? (It is known that no affine group can have this property.) In particular, which classical groups (if any) are spreading?

Some open problems

- Determine the QI permutation groups.
- Is there a permutation group which is spreading but not QI? (It is known that no affine group can have this property.) In particular, which classical groups (if any) are spreading?
- Determine the spreading permutation groups.

Some open problems

- Determine the QI permutation groups.
- Is there a permutation group which is spreading but not QI? (It is known that no affine group can have this property.) In particular, which classical groups (if any) are spreading?
- Determine the spreading permutation groups.
- Determine whether permutation groups in various families such as the symmetric group S_n acting on k-sets or uniform partitions are synchronizing or separating.

Some open problems

- Determine the QI permutation groups.
- Is there a permutation group which is spreading but not QI? (It is known that no affine group can have this property.) In particular, which classical groups (if any) are spreading?
- Determine the spreading permutation groups.
- Determine whether permutation groups in various families such as the symmetric group S_n acting on k-sets or uniform partitions are synchronizing or separating.(It is known that S_n on k-sets is always non-spreading; the same is true for S_n on uniform partitions if the Hadamard conjecture is true.)

Some open problems

- Determine the QI permutation groups.
- Is there a permutation group which is spreading but not QI? (It is known that no affine group can have this property.) In particular, which classical groups (if any) are spreading?
- Determine the spreading permutation groups.
- Determine whether permutation groups in various families such as the symmetric group S_n acting on k-sets or uniform partitions are synchronizing or separating.(It is known that S_n on k-sets is always non-spreading; the same is true for S_n on uniform partitions if the Hadamard conjecture is true.)
- Decide whether there exist parallelisms of projective spaces, and ovoids, spreads, and partitions into ovoids in classical polar spaces.