Synchronization

Peter J. Cameron

AEB60, Eindhoven

4 March 2011

HAPPY BIRTHDAY, ANDRIES!

Synchronization

This subject began in the theory of finite deterministic automata.

Synchronization

This subject began in the theory of finite deterministic automata.
The story (only a small part of which I will tell here) takes us through permutation groups and graph homomorphisms to some of the toughest problems in finite geometry and combinatorics.

Synchronization

This subject began in the theory of finite deterministic automata.

The story (only a small part of which I will tell here) takes us through permutation groups and graph homomorphisms to some of the toughest problems in finite geometry and combinatorics.

I will begin with a small detour, to my favourite proof of Cayley's Theorem on trees …

Finite automata

A finite automaton is a device with a set Ω of states and a set T of transitions, each transition a function on the set of states.

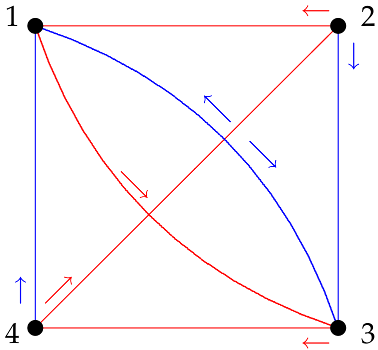
Finite automata

A finite automaton is a device with a set Ω of states and a set T of transitions, each transition a function on the set of states. Think of it as a black box with coloured buttons on front; pressing a button induces a transition on the (internal) states.

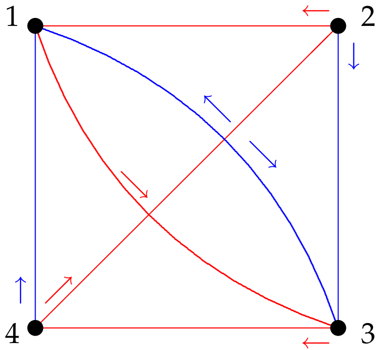
Finite automata

A finite automaton is a device with a set Ω of states and a set T of transitions, each transition a function on the set of states. Think of it as a black box with coloured buttons on front; pressing a button induces a transition on the (internal) states. An automaton is synchronizing if there is a sequence of transitions which takes it into the same state no matter which state it was in at the start. Such a sequence of transitions is called a reset word.

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.

Do random automata synchronize?

After I gave a talk on this at a conference in Kochi, Kerala, last summer, Brendan McKay asked:

> *Given n and r, what is the probability that a random automaton with n states and r transitions is synchronizing?*

Do random automata synchronize?

After I gave a talk on this at a conference in Kochi, Kerala, last summer, Brendan McKay asked:

> *Given n and r, what is the probability that a random automaton with n states and r transitions is synchronizing?*

The question is somewhat reminiscent of Dixon's Theorem, that two random permutations generate the symmetric or alternating group with high probability.

Do random automata synchronize?

After I gave a talk on this at a conference in Kochi, Kerala, last summer, Brendan McKay asked:

> *Given n and r, what is the probability that a random automaton with n states and r transitions is synchronizing?*

The question is somewhat reminiscent of Dixon's Theorem, that two random permutations generate the symmetric or alternating group with high probability.
I can't answer it in general. But in the case $r = 1$ there is a simple argument, based (a little unexpectedly) on Joyal's proof of Cayley's formula n^{n-2} for the number of trees on a set of n vertices.

Joyal's proof

Joyal defines a vertebrate to be a tree with two distinguished vertices, the head and the tail. The backbone is the path from the head to the tail.

Joyal's proof

Joyal defines a vertebrate to be a tree with two distinguished vertices, the head and the tail. The backbone is the path from the head to the tail.

Cayley's Theorem is equivalent to the statement that the number of vertebrates on n points is n^n, or (put another way) that it is equal to the number of endofunctions on n points (functions from the set of n points to itself).

Joyal's proof

Joyal defines a vertebrate to be a tree with two distinguished vertices, the head and the tail. The backbone is the path from the head to the tail.

Cayley's Theorem is equivalent to the statement that the number of vertebrates on n points is n^n, or (put another way) that it is equal to the number of endofunctions on n points (functions from the set of n points to itself).

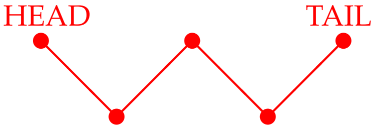
To prove this we look at vertebrates and endofunctions.

Joyal's proof

A vertebrate

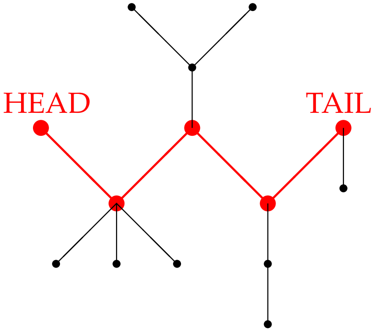
Joyal's proof

A vertebrate



Joyal's proof

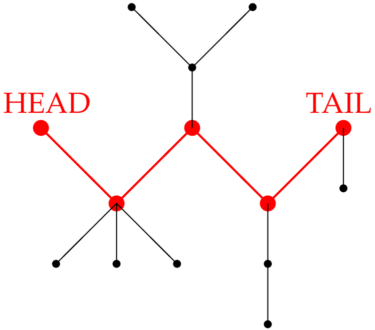
A vertebrate



Joyal's proof

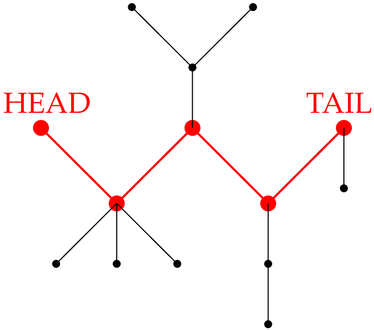
A vertebrate

An endofunction

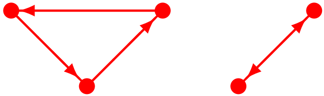


Joyal's proof

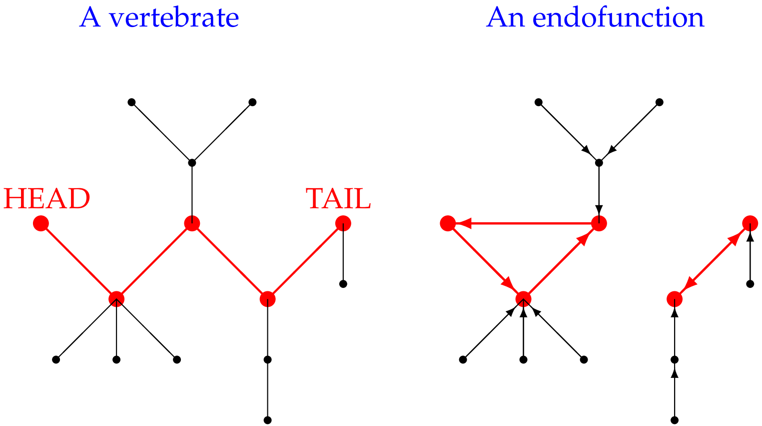
A vertebrate



An endofunction



Joyal's proof



Joyal's proof

To construct a vertebrate:

Joyal's proof

To construct a vertebrate:

- Choose a subset to be the backbone.

Joyal's proof

To construct a vertebrate:

- Choose a subset to be the backbone.
- Put a total order on it (head to tail).

Joyal's proof

To construct a vertebrate:

- Choose a subset to be the backbone.
- Put a total order on it (head to tail).
- Attach trees.

Joyal's proof

To construct a vertebrate:

- Choose a subset to be the backbone.
- Put a total order on it (head to tail).
- Attach trees.

To construct an endofunction:

Joyal's proof

To construct a vertebrate:

- Choose a subset to be the backbone.
- Put a total order on it (head to tail).
- Attach trees.

To construct an endofunction:

- Choose a set to be the periodic points.

Joyal's proof

To construct a vertebrate:

- Choose a subset to be the backbone.
- Put a total order on it (head to tail).
- Attach trees.

To construct an endofunction:

- Choose a set to be the periodic points.
- Put a permutation on it.

Joyal's proof

To construct a vertebrate:

- Choose a subset to be the backbone.
- Put a total order on it (head to tail).
- Attach trees.

To construct an endofunction:

- Choose a set to be the periodic points.
- Put a permutation on it.
- Attach trees (feeding in).

Joyal's proof

To construct a vertebrate:

- Choose a subset to be the backbone.
- Put a total order on it (head to tail).
- Attach trees.

To construct an endofunction:

- Choose a set to be the periodic points.
- Put a permutation on it.
- Attach trees (feeding in).

The number of total orders of k points is equal to the number of permutations of k points, viz. $k!$.

Joyal's proof

To construct a vertebrate:

- Choose a subset to be the backbone.
- Put a total order on it (head to tail).
- Attach trees.

To construct an endofunction:

- Choose a set to be the periodic points.
- Put a permutation on it.
- Attach trees (feeding in).

The number of total orders of k points is equal to the number of permutations of k points, viz. $k!$.
Hence the number of vertebrates on n points is equal to the number of endofunctions on n points, viz. n^n.

Random automaton with one transition

Joyal's proof shows that the number of vertebrates with k points in the backbone is equal to the number of endofunctions with k periodic points.

Random automaton with one transition

Joyal's proof shows that the number of vertebrates with k points in the backbone is equal to the number of endofunctions with k periodic points.

Theorem

The probability that a random automaton with n states and one transition synchronizes is $1/n$.

Random automaton with one transition

Joyal's proof shows that the number of vertebrates with k points in the backbone is equal to the number of endofunctions with k periodic points.

Theorem

The probability that a random automaton with n states and one transition synchronizes is $1/n$.

Proof.

The automaton synchronizes if and only if the endofunction has a unique periodic point.

Random automaton with one transition

Joyal's proof shows that the number of vertebrates with k points in the backbone is equal to the number of endofunctions with k periodic points.

Theorem

The probability that a random automaton with n states and one transition synchronizes is $1/n$.

Proof.

The automaton synchronizes if and only if the endofunction has a unique periodic point.
The vertebrate has backbone of size 1 if and only if the head is equal to the tail; this event has probability $1/n$. $\square$

Random automaton with one transition

Joyal's proof shows that the number of vertebrates with k points in the backbone is equal to the number of endofunctions with k periodic points.

Theorem

The probability that a random automaton with n states and one transition synchronizes is $1/n$.

Proof.

The automaton synchronizes if and only if the endofunction has a unique periodic point.
The vertebrate has backbone of size 1 if and only if the head is equal to the tail; this event has probability $1/n$. $\square$

I guess that automata with more than one transition have a much higher probability of synchronizing.

Černý's conjecture

One of the oldest problems in automata theory is Černý's conjecture:

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

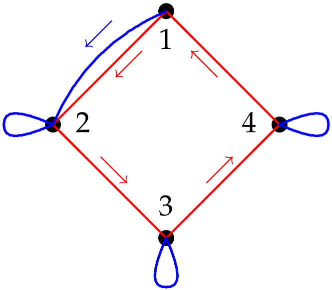
Černý's conjecture

One of the oldest problems in automata theory is Černý's conjecture:

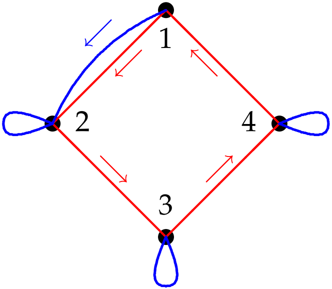
> *If an n-state automaton is synchronizing, then it has a reset word with length at most* $(n-1)^2$.

If true, this example would be best possible, as an example on the next slide shows.

Černý's conjecture is best possible

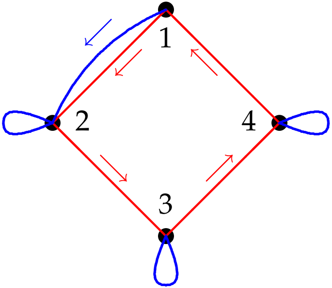


Černý's conjecture is best possible



	B	R	R	R	B	R	R	R	B
1	2	3	4	1	2	3	4	1	2
2	2	3	4	1	2	3	4	1	2
3	3	4	1	2	2	3	4	1	2
4	4	1	2	3	3	4	1	2	2

Černý's conjecture is best possible



	B	R	R	R	B	R	R	R	B
1	2	3	4	1	2	3	4	1	2
2	2	3	4	1	2	3	4	1	2
3	3	4	1	2	2	3	4	1	2
4	4	1	2	3	3	4	1	2	2

So BRRRBRRRB is a reset word. There is no shorter reset word.

Transformation monoids

Let $\Omega = \{1, \ldots, n\}$.
The full transformation monoid T_n is the set of all functions from Ω to itself. Equipped with the operation of composition, it is a monoid: that is, the operation is associative, and there is an identity element (the identity function on Ω).

Transformation monoids

Let $\Omega = \{1, \ldots, n\}$.
The full transformation monoid T_n is the set of all functions from Ω to itself. Equipped with the operation of composition, it is a monoid: that is, the operation is associative, and there is an identity element (the identity function on Ω).
Algebraically, an automaton is a submonoid of T_n, with a distinguished set of generators. (The "distinguished generators" are the transitions of the automaton. Since we are allowed to compose these arbitrarily, the allowable transitions are all words in the distinguished generators.)

Transformation monoids

Let $\Omega = \{1, \ldots, n\}$.
The full transformation monoid T_n is the set of all functions from Ω to itself. Equipped with the operation of composition, it is a monoid: that is, the operation is associative, and there is an identity element (the identity function on Ω).
Algebraically, an automaton is a submonoid of T_n, with a distinguished set of generators. (The "distinguished generators" are the transitions of the automaton. Since we are allowed to compose these arbitrarily, the allowable transitions are all words in the distinguished generators.)
An automaton is synchronizing if and only if (as transformation monoid) it contains a constant function.

An approach via permutation groups

Ben Steinberg and João Araújo suggested an approach to the Černý conjecture, based on permutation groups, which motivates this course. It has not led to a proof of the conjecture, but many interesting probems and conjectures have come up.

An approach via permutation groups

Ben Steinberg and João Araújo suggested an approach to the Černý conjecture, based on permutation groups, which motivates this course. It has not led to a proof of the conjecture, but many interesting probems and conjectures have come up.

Recall the algebraic view of an automaton, a monoid of transformations of a set Ω with a prescribed set of generators. It is synchronizing if it contains a constant function. Now:

An approach via permutation groups

Ben Steinberg and João Araújo suggested an approach to the Černý conjecture, based on permutation groups, which motivates this course. It has not led to a proof of the conjecture, but many interesting probems and conjectures have come up.

Recall the algebraic view of an automaton, a monoid of transformations of a set Ω with a prescribed set of generators. It is synchronizing if it contains a constant function. Now:

- If all the generators are permutations, then the whole monoid consists of permutations; that is, it is a subgroup of the symmetric group S_n of all permutations of $\Omega = \{1, \ldots, n\}$.

An approach via permutation groups

Ben Steinberg and João Araújo suggested an approach to the Černý conjecture, based on permutation groups, which motivates this course. It has not led to a proof of the conjecture, but many interesting probems and conjectures have come up.

Recall the algebraic view of an automaton, a monoid of transformations of a set Ω with a prescribed set of generators. It is synchronizing if it contains a constant function. Now:

- If all the generators are permutations, then the whole monoid consists of permutations; that is, it is a subgroup of the symmetric group S_n of all permutations of $\Omega = \{1, \ldots, n\}$.
- In this sense, permutations are the worst transitions for synchronization!

An approach via permutation groups

Ben Steinberg and João Araújo suggested an approach to the Černý conjecture, based on permutation groups, which motivates this course. It has not led to a proof of the conjecture, but many interesting probems and conjectures have come up.

Recall the algebraic view of an automaton, a monoid of transformations of a set Ω with a prescribed set of generators. It is synchronizing if it contains a constant function. Now:

- If all the generators are permutations, then the whole monoid consists of permutations; that is, it is a subgroup of the symmetric group S_n of all permutations of $\Omega = \{1, \ldots, n\}$.
- In this sense, permutations are the worst transitions for synchronization!
- Moreover, every permutation in the monoid actually lies in the subgroup generated by those transitions which are permutations.

The philosophy is: analyse the group generated by the permutations first!

The philosophy is: analyse the group generated by the permutations first!

Let G be a permutation group on Ω, that is, a subgroup of S_n. With an abuse of terminology, we say that G is synchronizing if the following is true:

> *If f is any function from Ω to itself which is not a permutation, then the monoid $\langle G, f \rangle$ generated by G and f is synchronizing (that is, contains a constant function).*

The philosophy is: analyse the group generated by the permutations first!

Let G be a permutation group on Ω, that is, a subgroup of S_n. With an abuse of terminology, we say that G is synchronizing if the following is true:

> *If f is any function from Ω to itself which is not a permutation, then the monoid $\langle G, f\rangle$ generated by G and f is synchronizing (that is, contains a constant function).*

Now the attack on the Černý conjecture goes like this: assume we are in the fortunate position that the transitions which are permutations generate a synchronizing group. Then, given any non-permutation f, there is a reset word in $\langle G, f\rangle$; we need to bound

- the number of occurrences of f in a reset word; and
- the number of generators of G occurring between successive occurrences.

Which groups are synchronizing?

Let G be a permutation group on Ω; π a partition of Ω; and S a subset of Ω.

Then S is a section, or transversal, of π, if S contains exactly one point of every part of π.

Which groups are synchronizing?

Let G be a permutation group on Ω; π a partition of Ω; and S a subset of Ω.
Then S is a section, or transversal, of π, if S contains exactly one point of every part of π.

We say that π is section-regular for G, with section S, if Sg is a section for π, for every $g \in G$. (Here Sg is the set $\{sg : s \in S\}$.)
Equivalently, S is a section for πg, for all $g \in G$.

Theorem
The permutation group G on Ω is synchronizing if and only if there is no non-trivial section-regular partition for G.

Proof.

Suppose that π is a non-trivial section-regular partition. Let f map $v \in \Omega$ to the unique point s of S in the same part of π containing v. Then any map $g_1 f g_2 f \cdots g_r f$, for $g_1, \ldots, g_r \in G$, has image S; so G is not synchronizing.

Proof.

Suppose that π is a non-trivial section-regular partition. Let f map $v \in \Omega$ to the unique point s of S in the same part of π containing v. Then any map $g_1fg_2f \cdots g_rf$, for $g_1, \ldots, g_r \in G$, has image S; so G is not synchronizing.

Conversely, suppose that $\langle G, f \rangle$ contains no constant function, and, without loss, let f be an element of smallest possible rank in this monoid. If S is the image of f, and π the partition of Ω into inverse images of elements of S, then π is section-regular with section S. $\square$

Proof.

Suppose that π is a non-trivial section-regular partition. Let f map $v \in \Omega$ to the unique point s of S in the same part of π containing v. Then any map $g_1 f g_2 f \cdots g_r f$, for $g_1, \ldots, g_r \in G$, has image S; so G is not synchronizing.

Conversely, suppose that $\langle G, f \rangle$ contains no constant function, and, without loss, let f be an element of smallest possible rank in this monoid. If S is the image of f, and π the partition of Ω into inverse images of elements of S, then π is section-regular with section S. □

Theorem

A synchronizing group is primitive.

Proof.

Suppose that π is a non-trivial section-regular partition. Let f map $v \in \Omega$ to the unique point s of S in the same part of π containing v. Then any map $g_1 f g_2 f \cdots g_r f$, for $g_1, \ldots, g_r \in G$, has image S; so G is not synchronizing.

Conversely, suppose that $\langle G, f \rangle$ contains no constant function, and, without loss, let f be an element of smallest possible rank in this monoid. If S is the image of f, and π the partition of Ω into inverse images of elements of S, then π is section-regular with section S. □

Theorem

A synchronizing group is primitive.

Proof.

If π is a non-trivial partition fixed by G, then π is section-regular for G, with any section S. □

Graph homomorphisms

A homomorphism from a graph X to a graph Y is thus a map f from the vertex set of X to the vertex set of Y such that, if $\{v, w\}$ is an edge of X, then $\{f(v), f(w)\}$ is an edge of Y. Note that, if $\{v, w\}$ is not an edge, then we do not specify what its image is; it may be a non-edge, or an edge, or even a single vertex. Write $X \to Y$ if a homomorphism exists.

Graph homomorphisms

A homomorphism from a graph X to a graph Y is thus a map f from the vertex set of X to the vertex set of Y such that, if $\{v, w\}$ is an edge of X, then $\{f(v), f(w)\}$ is an edge of Y. Note that, if $\{v, w\}$ is not an edge, then we do not specify what its image is; it may be a non-edge, or an edge, or even a single vertex. Write $X \to Y$ if a homomorphism exists.

An endomorphism of a graph X is a homomorphism from X to X. An automorphism is a bijective endomorphism which also maps non-edges to non-edges; that is, whose inverse is also an endomorphism.

Cores

The *core* of X is the smallest graph Y for which $X \longrightarrow Y$ and $Y \longrightarrow X$.

Cores

The *core* of X is the smallest graph Y for which $X \longrightarrow Y$ and $Y \longrightarrow X$.
It is easy to show that

Cores

The *core* of X is the smallest graph Y for which $X \longrightarrow Y$ and $Y \longrightarrow X$.

It is easy to show that

- the core of X is unique up to isomorphism;

Cores

The *core* of X is the smallest graph Y for which $X \to Y$ and $Y \to X$.

It is easy to show that

- the core of X is unique up to isomorphism;
- the core of X is an induced subgraph of X, and there is a retraction from X to its core;

Cores

The *core* of X is the smallest graph Y for which $X \to Y$ and $Y \to X$.

It is easy to show that

- the core of X is unique up to isomorphism;
- the core of X is an induced subgraph of X, and there is a retraction from X to its core;
- the core of a vertex-transitive graph is vertex-transitive;

Cores

The *core* of X is the smallest graph Y for which $X \to Y$ and $Y \to X$.
It is easy to show that

- the core of X is unique up to isomorphism;
- the core of X is an induced subgraph of X, and there is a retraction from X to its core;
- the core of a vertex-transitive graph is vertex-transitive;
- the core of X is complete if and only if $\omega(X) = \chi(X)$, where $\omega(X)$ and $\chi(X)$ are the clique number and chromatic number of X.

Synchronization and homomorphisms

Theorem

A permutation group G on Ω is non-synchronizing if and only if there exists a non-trivial G-invariant graph X on Ω with complete core (that is, with equal clique number and chromatic number).

Synchronization and homomorphisms

Theorem

A permutation group G on Ω is non-synchronizing if and only if there exists a non-trivial G-invariant graph X on Ω with complete core (that is, with equal clique number and chromatic number).

Even though this is not a polynomial-time test for the synchronizing property, it is a practical test, which has been applied computationally to permutation groups with degrees over 1000.

Example: classical groups

Let G be a classical group (a symplectic, orthogonal, or unitary group) of Witt index greater than 1, acting on the points of the associated polar space.

Example: classical groups

Let G be a classical group (a symplectic, orthogonal, or unitary group) of Witt index greater than 1, acting on the points of the associated polar space.
Since G has rank 3, there are only two non-trivial G-invariant graphs to consider.

Example: classical groups

Let G be a classical group (a symplectic, orthogonal, or unitary group) of Witt index greater than 1, acting on the points of the associated polar space.
Since G has rank 3, there are only two non-trivial G-invariant graphs to consider.
Now the synchronizing property depends on geometrical properties of the polar space, which are not completely understood despite a lot of research.

Theorem

The classical group G is non-synchronizing if and only if its associated polar space possesses either an ovoid and a spread, or a partition into ovoids.

Theorem

The classical group G is non-synchronizing if and only if its associated polar space possesses either an ovoid and a spread, or a partition into ovoids.

For, in the orthogonality graph, a maximal clique is a maximal totally isotropic subspace; a colouring with the right number of colours would be a partition into ovoids. In the complementary graph, the analogous clique and colouring would be a spread and an ovoid.

The hull of a graph

This construction is in some sense “dual” to that of a core.

The hull of a graph

This construction is in some sense "dual" to that of a core. Given a graph X, the hull of X has the same vertices as X; two vertices v and w are joined in the hull if and only if there is no endomorphism f of X such that $v^f = w^f$.

The hull of a graph

This construction is in some sense "dual" to that of a core.
Given a graph X, the hull of X has the same vertices as X; two vertices v and w are joined in the hull if and only if there is no endomorphism f of X such that $v^f = w^f$.
It has the properties:

- X is a spanning subgraph of its hull;

The hull of a graph

This construction is in some sense "dual" to that of a core.
Given a graph X, the hull of X has the same vertices as X; two vertices v and w are joined in the hull if and only if there is no endomorphism f of X such that $v^f = w^f$.
It has the properties:

- X is a spanning subgraph of its hull;
- every endomorphism of X is an endomorphism of its hull (so in particular, the automorphism group of X is contained in that of its hull);

The hull of a graph

This construction is in some sense "dual" to that of a core.
Given a graph X, the hull of X has the same vertices as X; two vertices v and w are joined in the hull if and only if there is no endomorphism f of X such that $v^f = w^f$.
It has the properties:

- X is a spanning subgraph of its hull;
- every endomorphism of X is an endomorphism of its hull (so in particular, the automorphism group of X is contained in that of its hull);
- the core of the hull of X is a complete graph on the vertex set of the core of X.

A theorem on cores

The core of a vertex-transitive graph is vertex-transitive. In fact, any reasonable transitivity property of a graph is shared by its core (e.g. edge-transitivity).

A theorem on cores

The core of a vertex-transitive graph is vertex-transitive. In fact, any reasonable transitivity property of a graph is shared by its core (e.g. edge-transitivity).
In one case, something much stronger is true:

Theorem

If X is non-edge-transitive, then either X is a core, or the core of X is complete.

A theorem on cores

The core of a vertex-transitive graph is vertex-transitive. In fact, any reasonable transitivity property of a graph is shared by its core (e.g. edge-transitivity).
In one case, something much stronger is true:

Theorem

If X is non-edge-transitive, then either X is a core, or the core of X is complete.

Proof.

The hull of X contains all the edges of X; any extra edges form a union of orbits of $\mathrm{Aut}(X)$. Hence either X is a hull, or its hull is complete.

A theorem on cores

The core of a vertex-transitive graph is vertex-transitive. In fact, any reasonable transitivity property of a graph is shared by its core (e.g. edge-transitivity).
In one case, something much stronger is true:

Theorem

If X is non-edge-transitive, then either X is a core, or the core of X is complete.

Proof.

The hull of X contains all the edges of X; any extra edges form a union of orbits of $\mathrm{Aut}(X)$. Hence either X is a hull, or its hull is complete.
If X is a hull then its core is complete; if the hull of X is complete, then the core of X has all the vertices of X, so that X is a core. $\square$

Further directions

There are many other families of primitive groups. Very often, testing the synchronizing property takes us into quite deep combinatorial or geometric problems.

Further directions

There are many other families of primitive groups. Very often, testing the synchronizing property takes us into quite deep combinatorial or geometric problems.
For example, the symmetric group S_n acting on 3-sets is primitive for $n \geq 7$; it is synchronizing if and only if $n \equiv 2, 4, 5 \pmod 6$ and $n \neq 8$. The proof uses theorems of Erdős–Ko–Rado, Baranyai and Teirlinck.

Further directions

There are many other families of primitive groups. Very often, testing the synchronizing property takes us into quite deep combinatorial or geometric problems.
For example, the symmetric group S_n acting on 3-sets is primitive for $n \geq 7$; it is synchronizing if and only if $n \equiv 2, 4, 5 \pmod{6}$ and $n \neq 8$. The proof uses theorems of Erdős–Ko–Rado, Baranyai and Teirlinck.
Some very interesting questions arise in the infinite case.

Further directions

There are many other families of primitive groups. Very often, testing the synchronizing property takes us into quite deep combinatorial or geometric problems.
For example, the symmetric group S_n acting on 3-sets is primitive for $n \geq 7$; it is synchronizing if and only if $n \equiv 2, 4, 5 \pmod{6}$ and $n \neq 8$. The proof uses theorems of Erdős–Ko–Rado, Baranyai and Teirlinck.
Some very interesting questions arise in the infinite case.
For further details, a set of lecture notes is available on my Web page:

`http://www.maths.qmul.ac.uk/~pjc/LTCC-2010-intensive3/`