Synchronization and homomorphisms

Peter J. Cameron

p.j.cameron@qmul.ac.uk

July 2008

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

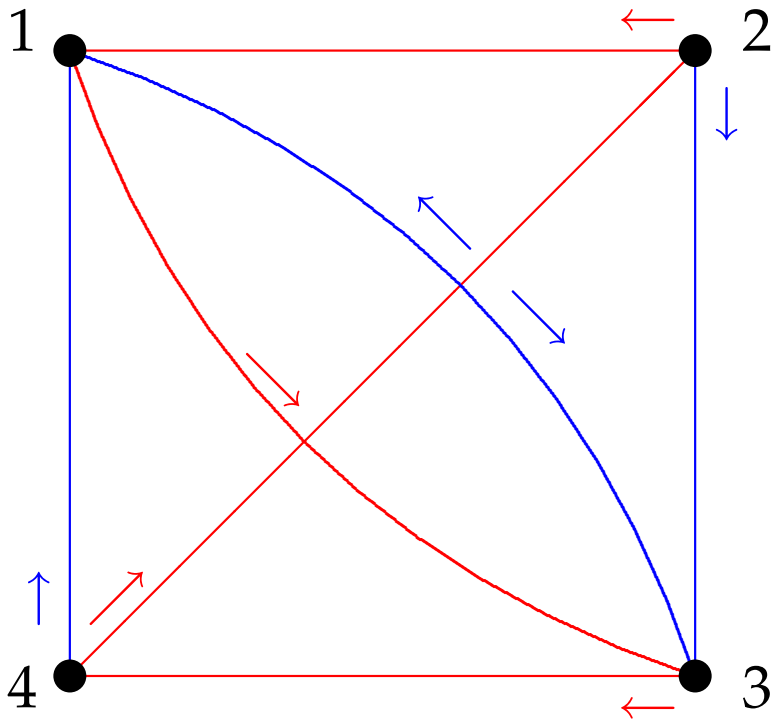
Suppose that you are given an automaton (whose structure you know) in an unknown state. You would like to put it into a known state, by applying a sequence of transitions to it. Of course this is not always possible!

Synchronization

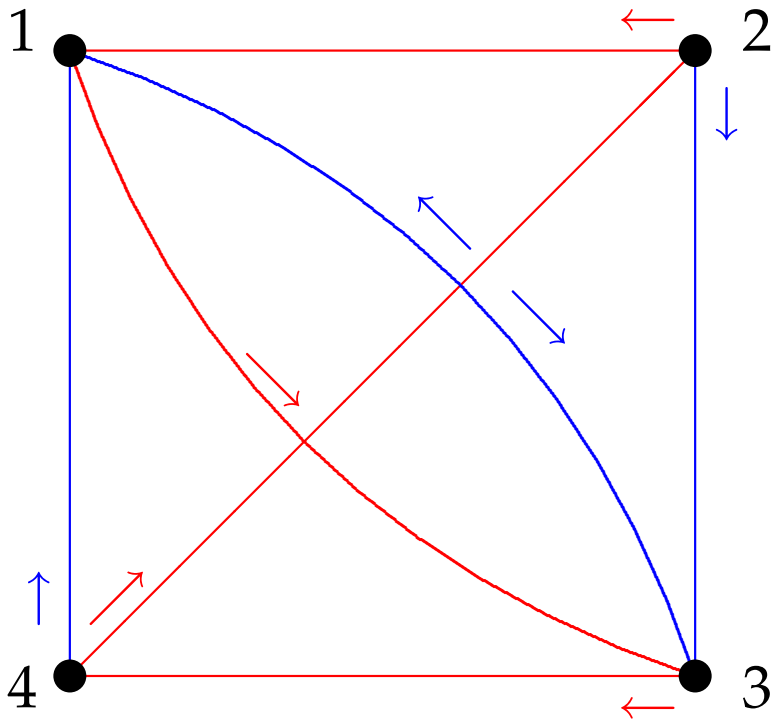
Suppose that you are given an automaton (whose structure you know) in an unknown state. You would like to put it into a known state, by applying a sequence of transitions to it. Of course this is not always possible!

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 state 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 strongly 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 strongly 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).

Which permutation groups are synchronizing?

Synchronizing groups

This condition can be reformulated in more group-theooretic 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-theooretic 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-theooretic 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.

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 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 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 separating if and only if there is a non-trivial G-invariant graph X such that $\omega(X) \cdot \alpha(X) = n$.*

An application: homomorphisms and cores

A homomorphism from a graph X to a graph Y is a map from the vertices of X to the vertices of Y which takes edges to edges (we don't care what it does to non-edges).

An application: homomorphisms and cores

A homomorphism from a graph X to a graph Y is a map from the vertices of X to the vertices of Y which takes edges to edges (we don't care what it does to non-edges).

The core of a graph X is the smallest graph Y such that there are homomorphisms in both directions between X and Y. For example, a non-null graph is bipartite if and only if its core is a single edge.

An application: homomorphisms and cores

A homomorphism from a graph X to a graph Y is a map from the vertices of X to the vertices of Y which takes edges to edges (we don't care what it does to non-edges).

The core of a graph X is the smallest graph Y such that there are homomorphisms in both directions between X and Y. For example, a non-null graph is bipartite if and only if its core is a single edge.

Finding the core of a graph is a hard computational problem!

An application: homomorphisms and cores

A homomorphism from a graph X to a graph Y is a map from the vertices of X to the vertices of Y which takes edges to edges (we don't care what it does to non-edges).

The core of a graph X is the smallest graph Y such that there are homomorphisms in both directions between X and Y. For example, a non-null graph is bipartite if and only if its core is a single edge.

Finding the core of a graph is a hard computational problem!

Proposition

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

An application: homomorphisms and cores

A homomorphism from a graph X to a graph Y is a map from the vertices of X to the vertices of Y which takes edges to edges (we don't care what it does to non-edges).

The core of a graph X is the smallest graph Y such that there are homomorphisms in both directions between X and Y. For example, a non-null graph is bipartite if and only if its core is a single edge.

Finding the core of a graph is a hard computational problem!

Proposition

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

However, deciding which possibility occurs is hard ...

The hull of a graph

The hull of a graph X is defined as follows:

- $\mathrm{hull}(X)$ has the same vertex set as X;
- $v \sim w$ in $\mathrm{hull}(X)$ if and only if there is no element $f \in \mathrm{End}(X)$ with $v^f = w^f$.

The hull of a graph

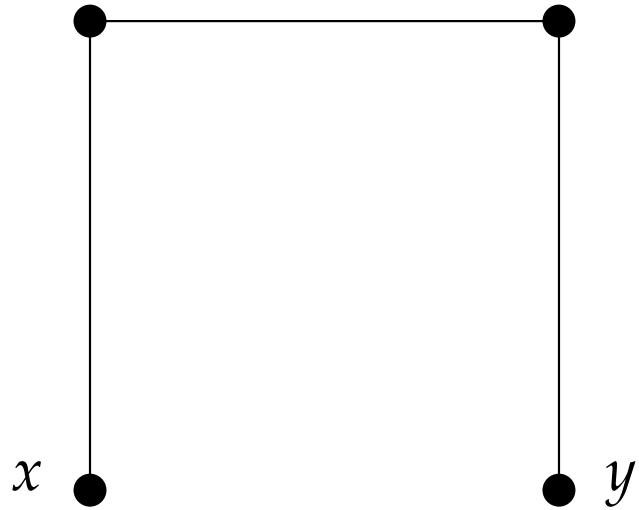
The hull of a graph X is defined as follows:

- $\mathrm{hull}(X)$ has the same vertex set as X;
- $v \sim w$ in $\mathrm{hull}(X)$ if and only if there is no element $f \in \mathrm{End}(X)$ with $v^f = w^f$.

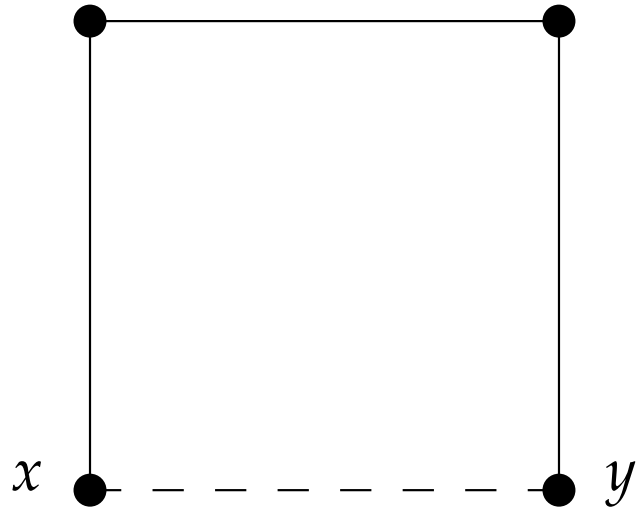
Theorem

- *X is a spanning subgraph of* $\mathrm{hull}(X)$ *(this means that they have the same vertex set, and every edge of X is an edge of* $\mathrm{hull}(X)$*);*
- $\mathrm{End}(X) \leq \mathrm{End}(\mathrm{hull}(X))$ *and* $\mathrm{Aut}(X) \leq \mathrm{Aut}(\mathrm{hull}(X))$ *(End and Aut are the endomorphism semigroup and automorphism group respectively);*
- *if* $\mathrm{core}(X)$ *has m vertices then* $\mathrm{core}(\mathrm{hull}(X))$ *is the complete graph on m vertices.*

An example

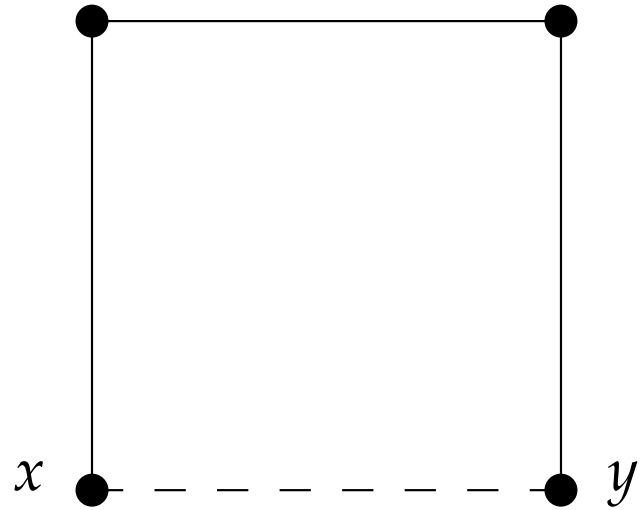


An example



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

An example



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

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

Proof of the theorem

Let X be non-edge transitive. Then hull(X) consists of X with some orbits on non-edges changed to edges. So there are only two possibilities:

Proof of the theorem

Let X be non-edge transitive. Then $\mathrm{hull}(X)$ consists of X with some orbits on non-edges changed to edges. So there are only two possibilities:

- $\mathrm{hull}(X) = X$. Then $\mathrm{core}(X) = \mathrm{core}(\mathrm{hull}(X))$ is complete;
- $\mathrm{hull}(X)$ is the complete graph on the vertex set of X. Then $\mathrm{core}(X)$ has as many vertices as X, so that $\mathrm{core}(X) = X$.

2-closure

The classes of synchronizing and separating group are upward-closed. They have some downward closure properties too.

2-closure

The classes of synchronizing and separating group are upward-closed. They have some downward closure properties too.

The 2-closure of a permutation group G on V consists of all the permutations of V which preserve every G-orbit on $V \times V$.

2-closure

The classes of synchronizing and separating group are upward-closed. They have some downward closure properties too.

The 2-closure of a permutation group G on V consists of all the permutations of V which preserve every G-orbit on $V \times V$.

Proposition

A permutation group is synchronizing (resp. separating) if and only if its 2-closure is synchronizing (resp. separating).

2-closure

The classes of synchronizing and separating group are upward-closed. They have some downward closure properties too.

The 2-closure of a permutation group G on V consists of all the permutations of V which preserve every G-orbit on $V \times V$.

Proposition

A permutation group is synchronizing (resp. separating) if and only if its 2-closure is synchronizing (resp. separating).

This is because failure of these properties is "detected" by a graph admitting the group (and hence admitting its 2-closure).

More general closure properties

This is based on an idea of Arnold and Steinberg.

More general closure properties

This is based on an idea of Arnold and Steinberg.

Let F be a field, and G a permutation group on V. The F-closure of G consists of all permutations of V which preserve all the FG-submodules of the permutation module FV.

More general closure properties

This is based on an idea of Arnold and Steinberg.

Let F be a field, and G a permutation group on V. The F-closure of G consists of all permutations of V which preserve all the FG-submodules of the permutation module FV.

It is easy to see that $\mathbb{C}$-closure is equivalent to 2-closure.

More general closure properties

This is based on an idea of Arnold and Steinberg.

Let F be a field, and G a permutation group on V. The F-closure of G consists of all permutations of V which preserve all the FG-submodules of the permutation module FV.

It is easy to see that $\mathbb{C}$-closure is equivalent to 2-closure.

Proposition

For any field F, a permutation group is synchronizing (resp. separating) if and only if its F-closure is synchronizing (resp. separating).

An example

The group $\mathrm{PSL}(2, 2^n)$ has permutation actions of degrees $2^{n-1}(2^n \pm 1)$, on the cosets of its maximal dihedral subgroups of orders $2(2^n \mp 1)$. It is 2-closed in both actions.

An example

The group $\mathrm{PSL}(2, 2^n)$ has permutation actions of degrees $2^{n-1}(2^n \pm 1)$, on the cosets of its maximal dihedral subgroups of orders $2(2^n \mp 1)$. It is 2-closed in both actions.

Suppose that $2^n - 1$ is a Mersenne prime.

An example

The group $\mathrm{PSL}(2, 2^n)$ has permutation actions of degrees $2^{n-1}(2^n \pm 1)$, on the cosets of its maximal dihedral subgroups of orders $2(2^n \mp 1)$. It is 2-closed in both actions.

Suppose that $2^n - 1$ is a Mersenne prime.

The permutation character of the action of degree $2^{n-1}(2^n - 1)$ is the sum of the trivial character and a family of algebraically conjugate characters, whose sum is $\mathbb{Q}$-irreducible. So the $\mathbb{Q}$-closure is the symmetric group, which is trivially separating; so the original group is separating, and hence synchronizing. (This was the example of Arnold and Steinberg.)

An example

The group $\mathrm{PSL}(2, 2^n)$ has permutation actions of degrees $2^{n-1}(2^n \pm 1)$, on the cosets of its maximal dihedral subgroups of orders $2(2^n \mp 1)$. It is 2-closed in both actions.

Suppose that $2^n - 1$ is a Mersenne prime.

The permutation character of the action of degree $2^{n-1}(2^n - 1)$ is the sum of the trivial character and a family of algebraically conjugate characters, whose sum is $\mathbb{Q}$-irreducible. So the $\mathbb{Q}$-closure is the symmetric group, which is trivially separating; so the original group is separating, and hence synchronizing. (This was the example of Arnold and Steinberg.)

More generally, a QI-group (one whose permutation character is the sum of the trivial character and a rational irreducible) is separating.

Another example

We take the same group $\mathrm{PSL}(2, 2^n)$, with $2^n - 1$ a Mersenne prime, and consider the other action described earlier.
The permutation character of the action of degree $2^{n-1}(2^n + 1)$ is equal to the above character plus an irreducible of degree 2^n.
So its $\mathbb{Q}$-closure is the group S_{2^n+1} acting on 2-sets.

Another example

We take the same group $\mathrm{PSL}(2, 2^n)$, with $2^n - 1$ a Mersenne prime, and consider the other action described earlier. The permutation character of the action of degree $2^{n-1}(2^n + 1)$ is equal to the above character plus an irreducible of degree 2^n. So its $\mathbb{Q}$-closure is the group S_{2^n+1} acting on 2-sets.

The only invariant graphs are the line graph of K_{2^n+1} and its complement; and if $X = L(K_{2^n+1})$, then $\omega(X) = 2^n$, but $\alpha(X) = 2^{n-1}$.

Another example

We take the same group $\mathrm{PSL}(2, 2^n)$, with $2^n - 1$ a Mersenne prime, and consider the other action described earlier. The permutation character of the action of degree $2^{n-1}(2^n + 1)$ is equal to the above character plus an irreducible of degree 2^n. So its $\mathbb{Q}$-closure is the group S_{2^n+1} acting on 2-sets.

The only invariant graphs are the line graph of K_{2^n+1} and its complement; and if $X = L(K_{2^n+1})$, then $\omega(X) = 2^n$, but $\alpha(X) = 2^{n-1}$.

So again, the original group is separating, and hence synchronizing.