Permutation groups and transformation semigroups: 2. Synchronization

Peter J. Cameron, University of St Andrews

Theoretical and Computational Algebra
July 2023

"When I use a word", Humpty Dumpty said, in rather a scornful tone, "it means just what I choose it to mean—neither more nore less."

Lewis Carroll

Synchronizing automata

This topic arose first in automata theory in the 1960s.

Synchronizing automata

This topic arose first in automata theory in the 1960s.
Our automata are extremely simple machines. They read a symbol from a string over an alphabet, change state according to a deterministic rule, and repeat the procedure.

Synchronizing automata

This topic arose first in automata theory in the 1960s.

Our automata are extremely simple machines. They read a symbol from a string over an alphabet, change state according to a deterministic rule, and repeat the procedure.

Imagine you are lost in a dungeon which has a number of rooms, joined by passages. These are identified by red and blue doors. Once you have gone through a door, you cannot return. You have a map of the dungeon, marking the room which has the exit door, but you don't know where you are. So if you can take a sequence of red and blue doors which lead to the exit room from any possible starting point, you can escape.

Synchronizing automata

This topic arose first in automata theory in the 1960s.

Our automata are extremely simple machines. They read a symbol from a string over an alphabet, change state according to a deterministic rule, and repeat the procedure.

Imagine you are lost in a dungeon which has a number of rooms, joined by passages. These are identified by red and blue doors. Once you have gone through a door, you cannot return. You have a map of the dungeon, marking the room which has the exit door, but you don't know where you are. So if you can take a sequence of red and blue doors which lead to the exit room from any possible starting point, you can escape.

So you want to decide from the map whether such a sequence exists, and if so, find one.

From dungeon to automaton

The dungeon is an automaton; the rooms are the states, and the alphabet has two letters red and blue. Assuming that the dungeon is connected, if you can find a sequence of moves which brings you to a known state, then you can use the map to navigate to the exit.

From dungeon to automaton

The dungeon is an automaton; the rooms are the states, and the alphabet has two letters red and blue. Assuming that the dungeon is connected, if you can find a sequence of moves which brings you to a known state, then you can use the map to navigate to the exit.

So we call an automaton synchronizing if there is a word in the alphabet (called a reset word) with the property that, after reading the word, the machine is in a known state. There are many applications: aligning objects on a conveyor belt in a factory; making a machine safe for repairs; communicating with a satellite which has just passed behind the moon.

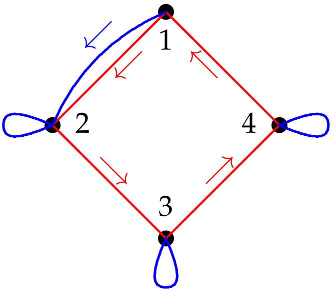
From dungeon to automaton

The dungeon is an automaton; the rooms are the states, and the alphabet has two letters red and blue. Assuming that the dungeon is connected, if you can find a sequence of moves which brings you to a known state, then you can use the map to navigate to the exit.

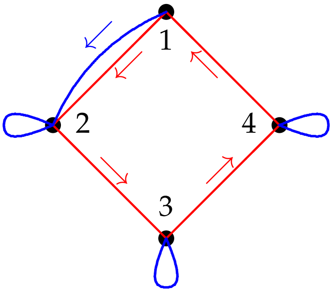
So we call an automaton synchronizing if there is a word in the alphabet (called a reset word) with the property that, after reading the word, the machine is in a known state. There are many applications: aligning objects on a conveyor belt in a factory; making a machine safe for repairs; communicating with a satellite which has just passed behind the moon.

There is a polynomial-time algorithm to decide whether an automaton is synchronizing. (It is synchronizing if and only if, given any two states, there is a word which maps them to the same place.)

An example

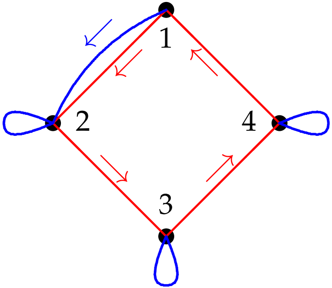


An example



	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

An example



	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 (and is in fact the shortest).

The Černý conjecture

Given a synchronizing automaton, the question arises: what is the smallest reset word? This is harder. The infamous Černý conjecture, one of the oldest open problems in automata theory, asserts that any n-state synchronizing automaton has a reset word of length at most $(n-1)^2$ (the previous example generalised). The best known upper bound is cn^3.

The Černý conjecture

Given a synchronizing automaton, the question arises: what is the smallest reset word? This is harder. The infamous Černý conjecture, one of the oldest open problems in automata theory, asserts that any n-state synchronizing automaton has a reset word of length at most $(n-1)^2$ (the previous example generalised). The best known upper bound is cn^3.

I am not going to discuss the Černý conjecture, but will move in a different direction. Note that any symbol in the alphabet of an automaton corresponds to a map from the set Ω of states to itself. Moreover, reading a word corresponds to composing the maps corresponding to the symbols. Moreover, the identity transformation is produced by the empty word. So the set of transformations an automaton can generate is a monoid (a semigroup with identity).

Rank, image and kernel

The rank of a transformation is the cardinality of its image. So the Černý conjecture can be stated in a different way: Given a transformation monoid on a set of cardinality n which contains an element of rank 1, and given a generating set for the monoid, what is the shortest word in the generators which evaluates to a transformation of rank 1? The conjecture asserts that there is such a word of length at most $(n-1)^2$.

Rank, image and kernel

The rank of a transformation is the cardinality of its image. So the Černý conjecture can be stated in a different way: Given a transformation monoid on a set of cardinality n which contains an element of rank 1, and given a generating set for the monoid, what is the shortest word in the generators which evaluates to a transformation of rank 1? The conjecture asserts that there is such a word of length at most $(n-1)^2$.

The image of a map f is defined as usual; the kernel is the partition induced by the equivalence relation $\alpha \equiv \beta$ if and only if $\alpha f = \beta f$. Note that the rank, which is the cardinality of the image, is also the cardinality (that is, the number of parts) of the kernel.

Image and kernel

A key observation I will use several times is the following.

Proposition

Let S be a transformation semigroup on Ω. Suppose that s is an element of S of minimal rank. Then, for any $t \in S$, elements of $\mathrm{Im}(s)$ lie in distinct classes of $\mathrm{Ker}(t)$.

Image and kernel

A key observation I will use several times is the following.

Proposition

Let S be a transformation semigroup on Ω. Suppose that s is an element of S of minimal rank. Then, for any $t \in S$, elements of $\mathrm{Im}(s)$ lie in distinct classes of $\mathrm{Ker}(t)$.

This is clear since, if not, then $\mathrm{rank}(st) < \mathrm{rank}(s)$. In particular, if t also has minimal rank, then $\mathrm{Im}(s)$ is a transversal for $\mathrm{Ker}(t)$.

Image and kernel

A key observation I will use several times is the following.

Proposition

Let S be a transformation semigroup on Ω. Suppose that s is an element of S of minimal rank. Then, for any $t \in S$, elements of $\mathrm{Im}(s)$ lie in distinct classes of $\mathrm{Ker}(t)$.

This is clear since, if not, then $\mathrm{rank}(st) < \mathrm{rank}(s)$. In particular, if t also has minimal rank, then $\mathrm{Im}(s)$ is a transversal for $\mathrm{Ker}(t)$. Note that a product of transformations s and t is a permutation if and only if s and t are permutations. Thus, the permutations in a transformation monoid S form a permutation group G, the group of units of S. Our general theme is the question: how does the structure of the group of units affect the structure of a transformation monoid?

Synchronization and groups

A transformation monoid is synchronizing if it contains an element of rank 1. Thus, a permutation group cannot be synchronizing (unless it is the trivial group on a set of size 1). So, following Humpty Dumpty, we extend the usage of the term with a slightly different meaning.

Synchronization and groups

A transformation monoid is synchronizing if it contains an element of rank 1. Thus, a permutation group cannot be synchronizing (unless it is the trivial group on a set of size 1). So, following Humpty Dumpty, we extend the usage of the term with a slightly different meaning.

Let G be a permutation group on Ω. We say that G synchronizes a transformation t if the monoid $\langle G, t \rangle$ is synchronizing. If G synchronizes every non-permutation of Ω, we say that G is a synchronizing permutation group.

Synchronization and groups

A transformation monoid is synchronizing if it contains an element of rank 1. Thus, a permutation group cannot be synchronizing (unless it is the trivial group on a set of size 1). So, following Humpty Dumpty, we extend the usage of the term with a slightly different meaning.

Let G be a permutation group on Ω. We say that G synchronizes a transformation t if the monoid $\langle G, t\rangle$ is synchronizing. If G synchronizes every non-permutation of Ω, we say that G is a synchronizing permutation group.

The main question in this lecture is:

Question

Which permutation groups are synchronizing?

Section-regular partitions

The first translation of the synchronizing property is due to Peter Neumann.

Section-regular partitions

The first translation of the synchronizing property is due to Peter Neumann.

Proposition

Suppose that s has minimum rank in a transformation monoid S with unit group G. Then, for every element $g \in G$, $\mathrm{Im}(s)g$ is a transversal to $\mathrm{Ker}(s)$.

Section-regular partitions

The first translation of the synchronizing property is due to Peter Neumann.

Proposition

Suppose that s has minimum rank in a transformation monoid S with unit group G. Then, for every element $g \in G$, $\mathrm{Im}(s)g$ is a transversal to $\mathrm{Ker}(s)$.

A partition P of Ω is section-regular for a permutation group G if there is a set $A \subseteq \Omega$ such that Ag is a transversal for P for all $g \in G$.

Section-regular partitions

The first translation of the synchronizing property is due to Peter Neumann.

Proposition

Suppose that s has minimum rank in a transformation monoid S with unit group G. Then, for every element $g \in G$, $\mathrm{Im}(s)g$ is a transversal to $\mathrm{Ker}(s)$.

A partition P of Ω is section-regular for a permutation group G if there is a set $A \subseteq \Omega$ such that Ag is a transversal for P for all $g \in G$.

Proposition

A permutation group is non-synchronizing if and only if it has a nontrivial section-regular partition.

Section-regular partitions

The first translation of the synchronizing property is due to Peter Neumann.

Proposition

Suppose that s has minimum rank in a transformation monoid S with unit group G. Then, for every element $g \in G$, $\mathrm{Im}(s)g$ is a transversal to $\mathrm{Ker}(s)$.

A partition P of Ω is section-regular for a permutation group G if there is a set $A \subseteq \Omega$ such that Ag is a transversal for P for all $g \in G$.

Proposition

A permutation group is non-synchronizing if and only if it has a nontrivial section-regular partition.

If P is section-regular with witness A, then the map s with kernel P and image A is not synchronized by G. The converse is proved similarly, taking s to be an element of minimal rank (greater than 1) in a monoid containing G.

Graphs and homomorphisms

Now I give a more convenient criterion for non-synchronization.

Graphs and homomorphisms

Now I give a more convenient criterion for non-synchronization.

Graphs here will be simple undirected graphs. The vertex and edge sets of a graph Γ are denoted by $V\Gamma$ and $E\Gamma$.

Graphs and homomorphisms

Now I give a more convenient criterion for non-synchronization.

Graphs here will be simple undirected graphs. The vertex and edge sets of a graph Γ are denoted by $V\Gamma$ and $E\Gamma$.

A homomorphism from Γ to Δ is a map θ from $V\Gamma$ to $V\Delta$ mapping $E\Gamma$ into $E\Delta$. (The action on nonedges is not specified: a nonedge may map to a nonedge, or to an edge, or collapse to a single vertex.) As usual a homomorphism from Γ to itself is an endomorphism of Γ.

Graphs and homomorphisms

Now I give a more convenient criterion for non-synchronization.

Graphs here will be simple undirected graphs. The vertex and edge sets of a graph Γ are denoted by $V\Gamma$ and $E\Gamma$.

A homomorphism from Γ to Δ is a map θ from $V\Gamma$ to $V\Delta$ mapping $E\Gamma$ into $E\Delta$. (The action on nonedges is not specified: a nonedge may map to a nonedge, or to an edge, or collapse to a single vertex.) As usual a homomorphism from Γ to itself is an endomorphism of Γ.

The endomorphisms of Γ form a transformation monoid on $V\Gamma$, with unit group $\mathrm{Aut}(\Gamma)$. Since homomorphisms cannot destroy edges, we see that, if Γ is not the null graph, then $\mathrm{Aut}(\Gamma)$ is non-synchronizing.

Graphs and homomorphisms

Now I give a more convenient criterion for non-synchronization.

Graphs here will be simple undirected graphs. The vertex and edge sets of a graph Γ are denoted by $V\Gamma$ and $E\Gamma$.

A homomorphism from Γ to Δ is a map θ from $V\Gamma$ to $V\Delta$ mapping $E\Gamma$ into $E\Delta$. (The action on nonedges is not specified: a nonedge may map to a nonedge, or to an edge, or collapse to a single vertex.) As usual a homomorphism from Γ to itself is an endomorphism of Γ.

The endomorphisms of Γ form a transformation monoid on $V\Gamma$, with unit group $\mathrm{Aut}(\Gamma)$. Since homomorphisms cannot destroy edges, we see that, if Γ is not the null graph, then $\mathrm{Aut}(\Gamma)$ is non-synchronizing.

We will see that there is a converse as well.

Cliques and colourings

A clique of Γ is a complete subgraph, hence is the image of a homomorphism $K_m \to \Gamma$ (where K_m is the complete graph on m vertices). The clique number of Γ, denoted by $\omega(\Gamma)$, is the size of the largest clique in Γ.

Cliques and colourings

A clique of Γ is a complete subgraph, hence is the image of a homomorphism $K_m \to \Gamma$ (where K_m is the complete graph on m vertices). The clique number of Γ, denoted by $\omega(\Gamma)$, is the size of the largest clique in Γ.

A proper colouring of Γ assigns colours to the vertices in such a way that adjacent vertices get different colours. In other words, it is a homomorphism $\Gamma \to K_l$ for some l. The minimum number of colours in a proper colouring is the chromatic number of Γ, denoted by $\chi(\Gamma)$.

Cliques and colourings

A clique of Γ is a complete subgraph, hence is the image of a homomorphism $K_m \to \Gamma$ (where K_m is the complete graph on m vertices). The clique number of Γ, denoted by $\omega(\Gamma)$, is the size of the largest clique in Γ.

A proper colouring of Γ assigns colours to the vertices in such a way that adjacent vertices get different colours. In other words, it is a homomorphism $\Gamma \to K_l$ for some l. The minimum number of colours in a proper colouring is the chromatic number of Γ, denoted by $\chi(\Gamma)$.

The vertices of a clique all get different colours; so $\chi(\Gamma) \geq \omega(\Gamma)$. Equality holds if and only if there are homomorphisms in both directions between Γ and K_m for some m. Such a graph is called weakly perfect.

A test for synchronization

Theorem

A permutation group is non-synchronizing if and only if it is contained in the automorphism group of a weakly perfect graph.

A test for synchronization

Theorem

A permutation group is non-synchronizing if and only if it is contained in the automorphism group of a weakly perfect graph.

In the language introduced in the first lecture, G is synchronizing if and only if it is $\mathcal{C}$-free, where $\mathcal{C}$ is the class of weakly perfect graphs.

A test for synchronization

Theorem

A permutation group is non-synchronizing if and only if it is contained in the automorphism group of a weakly perfect graph.

In the language introduced in the first lecture, G is synchronizing if and only if it is $\mathcal{C}$-free, where $\mathcal{C}$ is the class of weakly perfect graphs.

We have seen the reverse direction in the theorem. For the converse, suppose that $S = \langle G, t \rangle$ contains no element of rank 1. Form a graph Γ by joining α to β if and only if no element $s \in S$ satisfies $\alpha s = \beta s$. Then $S \leq \mathrm{End}(\Gamma)$. Moreover, if s has minimum rank in S, then $\mathrm{Im}(s)$ is a clique, and s is a proper colouring, of Γ.

Consequences

Theorem

- *A 2-homogeneous group is synchronizing.*

Consequences

Theorem

- *A* 2*-homogeneous group is synchronizing.*
- *A synchronizing group is primitive and basic.*

Consequences

Theorem

- *A* 2*-homogeneous group is synchronizing.*
- *A synchronizing group is primitive and basic.*

The first holds since a 2-homogeneous group preserves no non-trivial graph (it is $\mathcal{C}$-free, for the class $\mathcal{C}$ of all graphs).

Consequences

Theorem

- *A* 2*-homogeneous group is synchronizing.*
- *A synchronizing group is primitive and basic.*

The first holds since a 2-homogeneous group preserves no non-trivial graph (it is $\mathcal{C}$-free, for the class $\mathcal{C}$ of all graphs). For the second, note that a transitive imprimitive group preserves a complete multipartite graph with parts of the same size, while a primitive non-basic group preserves a Hamming graph; both are weakly perfect. (For the Hamming graph $H(m, q)$, the set of vertices $(x_1, \ldots, x_m)$ with $x_2, \ldots, x_m$ constant is a clique of size q. For a colouring, assume that the alphabet is the integers mod q, and give $(x_1, \ldots, x_m)$ the colour $x_1 + \cdots + x_m$.)

Consequences

Theorem

- *A 2-homogeneous group is synchronizing.*
- *A synchronizing group is primitive and basic.*

The first holds since a 2-homogeneous group preserves no non-trivial graph (it is $\mathcal{C}$-free, for the class $\mathcal{C}$ of all graphs).
For the second, note that a transitive imprimitive group preserves a complete multipartite graph with parts of the same size, while a primitive non-basic group preserves a Hamming graph; both are weakly perfect. (For the Hamming graph $H(m, q)$, the set of vertices $(x_1, \ldots, x_m)$ with $x_2, \ldots, x_m$ constant is a clique of size q. For a colouring, assume that the alphabet is the integers mod q, and give $(x_1, \ldots, x_m)$ the colour $x_1 + \cdots + x_m$.)
According to the O'Nan–Scott Theorem, a synchronizing group must be affine, diagonal or almost simple. We examine these in turn.

Affine and almost simple

In each of these classes, some basic groups are synchronizing and some are not. I will not discuss these in detail, but just give one example.

Affine and almost simple

In each of these classes, some basic groups are synchronizing and some are not. I will not discuss these in detail, but just give one example.

One of the best-known examples of a basic but not 2-homogeneous group is the symmetric group S_m acting on the $n = \binom{m}{2}$ 2-element subsets of $\{1, \ldots, m\}$.

Affine and almost simple

In each of these classes, some basic groups are synchronizing and some are not. I will not discuss these in detail, but just give one example.

One of the best-known examples of a basic but not 2-homogeneous group is the symmetric group S_m acting on the $n = \binom{m}{2}$ 2-element subsets of $\{1, \ldots, m\}$.

On the next slide I will show you that this group is synchronizing if and only if m is odd.

Affine and almost simple

In each of these classes, some basic groups are synchronizing and some are not. I will not discuss these in detail, but just give one example.

One of the best-known examples of a basic but not 2-homogeneous group is the symmetric group S_m acting on the $n = \binom{m}{2}$ 2-element subsets of $\{1, \ldots, m\}$.

On the next slide I will show you that this group is synchronizing if and only if m is odd.

Mohammed Aljohani, John Bamberg and I have a conjectured generalisation to S_m acting on k-sets, involving Peter Keevash's construction of t-designs.

S_m acting on 2-sets preserves the triangular graph, in which two 2-sets are joined if they have non-empty intersection.

S_m acting on 2-sets preserves the triangular graph, in which two 2-sets are joined if they have non-empty intersection. For $m \geq 5$, a maximal clique in this graph has size $m - 1$, and is the star consisting of all 2-sets containing a fixed point. On the other hand, the sets in a colour class have size at most $\lfloor m/2 \rfloor$, since they must be pairwise disjoint; so there must be at least $m(m-1)/(2\lfloor m/2 \rfloor)$ colours; this number is $m - 1$ if m is even, m if m is odd. It is easy to show that this is the chromatic number of the graph. So the graph is weakly perfect if and only if m is even.

S_m acting on 2-sets preserves the triangular graph, in which two 2-sets are joined if they have non-empty intersection.
For $m \geq 5$, a maximal clique in this graph has size $m - 1$, and is the star consisting of all 2-sets containing a fixed point. On the other hand, the sets in a colour class have size at most $\lfloor m/2 \rfloor$, since they must be pairwise disjoint; so there must be at least $m(m-1)/(2\lfloor m/2 \rfloor)$ colours; this number is $m - 1$ if m is even, m if m is odd. It is easy to show that this is the chromatic number of the graph. So the graph is weakly perfect if and only if m is even.
It is also easy to show that the complementary graph is never weakly perfect. So the claimed result holds.

Diagonal groups

I mentioned the diagonal groups $D(T, m)$ in the first lecture. They are primitive (and basic) if and only if T is non-abelian simple. Here I will discuss just $m = 1$ and $m = 2$, but explain how the result extends to all m.

Diagonal groups

I mentioned the diagonal groups $D(T, m)$ in the first lecture. They are primitive (and basic) if and only if T is non-abelian simple. Here I will discuss just $m = 1$ and $m = 2$, but explain how the result extends to all m.

The group $D(T, 1)$ is the group of permutations of T generated by left and right translations, automorphisms, and the inversion map $x \mapsto x^{-1}$.

Diagonal groups

I mentioned the diagonal groups $D(T, m)$ in the first lecture. They are primitive (and basic) if and only if T is non-abelian simple. Here I will discuss just $m = 1$ and $m = 2$, but explain how the result extends to all m.
The group $D(T, 1)$ is the group of permutations of T generated by left and right translations, automorphisms, and the inversion map $x \mapsto x^{-1}$.
This group may or may not be synchronizing. If T has an exact factorisation, then $D(T, 1)$ is non-synchronizing.

Diagonal groups

I mentioned the diagonal groups $D(T, m)$ in the first lecture. They are primitive (and basic) if and only if T is non-abelian simple. Here I will discuss just $m = 1$ and $m = 2$, but explain how the result extends to all m.

The group $D(T, 1)$ is the group of permutations of T generated by left and right translations, automorphisms, and the inversion map $x \mapsto x^{-1}$.

This group may or may not be synchronizing. If T has an exact factorisation, then $D(T, 1)$ is non-synchronizing.

Recently, John Bamberg, Michael Giudici, Jesse Lansdown and Gordon Royle showed that, for the simple groups $T = \mathrm{PSL}(2, 13)$ and $\mathrm{PSL}(2, 17)$, the diagonal group is synchronizing. These were the first synchronizing diagonal groups found.

Transversals and orthogonal mates

A transversal of a Latin square is a set of cells, one in each row, one in each column, and one containing each letter.

e	**a**	**b**	**c**
a	**e**	**c**	**b**
b	**c**	**e**	**a**
c	**b**	**a**	**e**

Transversals and orthogonal mates

A transversal of a Latin square is a set of cells, one in each row, one in each column, and one containing each letter.

e	**a**	**b**	**c**
a	**e**	**c**	**b**
b	**c**	**e**	**a**
c	**b**	**a**	**e**

In this case we can partition the cells into transversals:

e	**a**	**b**	**c**
a	**e**	**c**	**b**
b	**c**	**e**	**a**
c	**b**	**a**	**e**

Transversals and orthogonal mates

A transversal of a Latin square is a set of cells, one in each row, one in each column, and one containing each letter.

e	**a**	**b**	**c**
a	**e**	**c**	**b**
b	**c**	**e**	**a**
c	**b**	**a**	**e**

In this case we can partition the cells into transversals:

e	**a**	**b**	**c**
a	**e**	**c**	**b**
b	**c**	**e**	**a**
c	**b**	**a**	**e**

Regarding the colours as an alphabet we see a second Latin square which is orthogonal to the first square, in the sense that each combination of letter and colour occurs precisely once.

Latin square graphs and Cayley tables

From a Latin square, we get a Latin square graph whose vertices are the q^2 cells, two vertices joined if they lie in the same row or column or contain the same letter.

Latin square graphs and Cayley tables

From a Latin square, we get a Latin square graph whose vertices are the q^2 cells, two vertices joined if they lie in the same row or column or contain the same letter.
The Cayley table of a group T is a Latin square. If $|T| > 4$, then the automorphism group of the corresponding Latin square graph is the diagonal group $D(T, 2)$.

Latin square graphs and Cayley tables

From a Latin square, we get a Latin square graph whose vertices are the q^2 cells, two vertices joined if they lie in the same row or column or contain the same letter.

The Cayley table of a group T is a Latin square. If $|T| > 4$, then the automorphism group of the corresponding Latin square graph is the diagonal group $D(T, 2)$.

If a Latin square has order q, its Latin square graph is q. If it has an orthogonal mate, its entries define a proper colouring of the Latin square graph with q colours. So a Latin square graph is weakly perfect if and only if the square has an orthogonal mate.

Latin square graphs and Cayley tables

From a Latin square, we get a Latin square graph whose vertices are the q^2 cells, two vertices joined if they lie in the same row or column or contain the same letter.

The Cayley table of a group T is a Latin square. If $|T| > 4$, then the automorphism group of the corresponding Latin square graph is the diagonal group $D(T, 2)$.

If a Latin square has order q, its Latin square graph is q. If it has an orthogonal mate, its entries define a proper colouring of the Latin square graph with q colours. So a Latin square graph is weakly perfect if and only if the square has an orthogonal mate.

So to decide whether $D(T, 2)$ is synchronizing, we need to know whether the Cayley table of T has an orthogonal mate.

The Hall–Paige conjecture

In 1955, Marshall Hall and Lowell Paige conjectured that the Cayley table of T has an orthogonal mate if and only if the Sylow 2-subgroups of T are either trivial or non-cyclic. They proved that this condition is necessary.

The Hall–Paige conjecture

In 1955, Marshall Hall and Lowell Paige conjectured that the Cayley table of T has an orthogonal mate if and only if the Sylow 2-subgroups of T are either trivial or non-cyclic. They proved that this condition is necessary.
As an exercise, prove that the Cayley table of a cyclic group of even order n has no orthogonal mate. (It suffices to show it has no transversal, that is, it is impossible to choose n cells, one in each row, one in each column, and one containing each letter.

The proof of the conjecture

In 2009, Stewart Wilcox reduced the conjecture to the case of non-abelian simple groups (these all have non-cyclic Sylow subgroups), and proved it for groups of Lie type, except the Tits group (alternating groups were done by Hall and Paige). Then Tony Evans dealt with the remaining case and the sporadic groups with one exception (the Janko group J_4). The final case was done (but not published) by John Bray.

The proof of the conjecture

In 2009, Stewart Wilcox reduced the conjecture to the case of non-abelian simple groups (these all have non-cyclic Sylow subgroups), and proved it for groups of Lie type, except the Tits group (alternating groups were done by Hall and Paige). Then Tony Evans dealt with the remaining case and the sporadic groups with one exception (the Janko group J_4). The final case was done (but not published) by John Bray.

So the Hall–Paige conjecture is true.

The proof of the conjecture

In 2009, Stewart Wilcox reduced the conjecture to the case of non-abelian simple groups (these all have non-cyclic Sylow subgroups), and proved it for groups of Lie type, except the Tits group (alternating groups were done by Hall and Paige). Then Tony Evans dealt with the remaining case and the sporadic groups with one exception (the Janko group J_4). The final case was done (but not published) by John Bray.
So the Hall–Paige conjecture is true.
Using this, and the notion of graph homomorphism, Bray, Cai, Spiga, Zhang, and I showed, by induction:

Theorem

For every $m > 2$ and every non-abelian simple group T, the diagonal group $D(T, m)$ is non-synchronizing.

References

- Mohammed Aljohani, John Bamberg and Peter J. Cameron, Synchronization and separation in the Johnson scheme, *Portugaliae Mathematica* **74** (2018), 213–232.
- João Araújo, Peter J. Cameron and Benjamin Steinberg, Between primitive and 2-transitive: Synchronization and its friends, *Europ. Math. Soc. Surveys* **4** (2017), 101–184.
- John Bamberg, Michael Giudici, Jesse Lansdown and Gordon Royle, Synchronizing primitive groups of diagonal type exist, arXiv `2104.13355`.
- J. N. Bray, Q. Cai, P. J. Cameron, P. Spiga and H. Zhang, The Hall–Paige conjecture, and synchronization for affine and diagonal groups, *J. Algebra* **545** (2020), 27–42.