

Synchronization

Peter J. Cameron
University of St Andrews

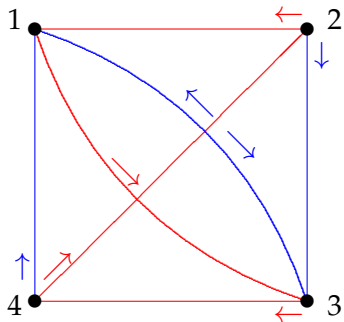


Firenze, February 2020

The dungeon

You are in a dungeon consisting of a number of rooms. Each room has two doors, coloured red and blue, which open into passages leading to another room (maybe the same one). Each room also contains a special door; in one room, the door leads to freedom, but in all the others, to death. You have a map of the dungeon, but you do not know where you are.

Can you escape? In other words, is there a sequence of colours such that, if you use the doors in this sequence from any starting point, you will end in a known place?



You can check that (Blue, Red, Blue) takes you to room 1 no matter where you start.

Automata

The diagram on the last page shows a finite-state deterministic **automaton**. This is a machine with a finite set of **states**, and a finite set of **transitions**, each transition being a map from the set of states to itself. The machine starts in an arbitrary state, and reads a word over an alphabet consisting of labels for the transitions (**Red** and **Blue** in the example); each time it reads a letter, it undergoes the corresponding transition.

A **reset word** is a word with the property that, if the automaton reads this word, it arrives at the same state, independent of its start state. An automaton which possesses a reset word is called **synchronizing**.

Not every finite automaton has a reset word. For example, if every transition is a permutation, then every word in the transitions evaluates to a permutation. How do we recognise when an automaton is synchronizing?

Automata and transformation monoids

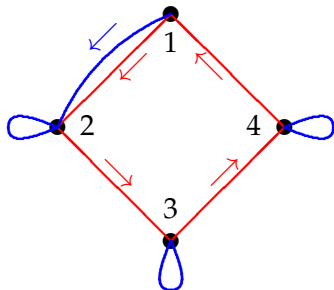
Combinatorially, an automaton is an edge-coloured digraph with one edge of each colour out of each vertex. Vertices are states, colours are transitions.

Algebraically, if $\Omega = \{1, \dots, n\}$ is the set of states, then any transition is a map from Ω to itself. Reading a word composes the corresponding maps, so the set of maps corresponding to all words is a **transformation monoid** on Ω .

So an automaton is a transformation monoid with a distinguished generating set. It is synchronizing if it contains a map with **rank** 1.

Another example

This example arises in industrial robotics.



	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.

The Černý conjecture

Much of the research on synchronization has been driven by the Černý conjecture, over 50 years old and still unsolved.

The conjecture is very simple. It states that if an n -state automaton is synchronizing, then it has a reset word of length at most $(n - 1)^2$.

The example on the last slide meets the bound when $n = 4$, and has an obvious generalisation to any n ; so, if true, the conjecture would be best possible for all n .

This conjecture comes with a health warning. Despite its apparent simplicity, it does fight back!

What follows is not a contribution to this conjecture, although these methods have allowed us to make small progress. See the paper by João Araújo, Ben Steinberg and me for more detail. Rather, the subject is of interest in its own right.

Testing synchronization

Proposition

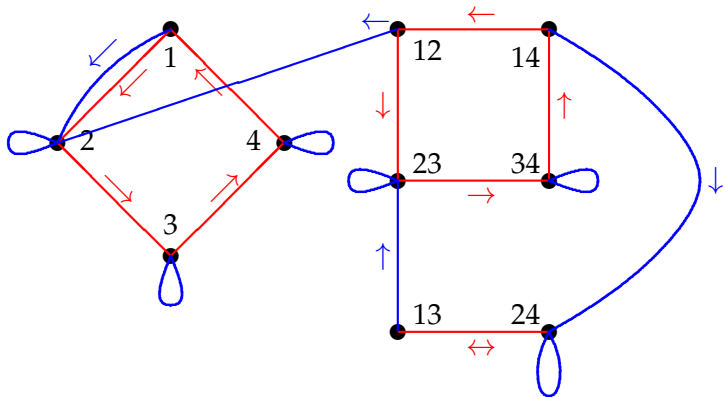
An automaton (Ω, S) is synchronizing if and only if, for any two states $a, b \in \Omega$, there is a word $w_{a,b}$ in the elements of S which maps a and b to the same place.

Proof.

“Only if” is clear, so suppose that the condition holds. Let f be an element of $\langle S \rangle$ of smallest possible rank. If the rank of S is greater than 1, then choose two points a, b in the image; then fw_{ab} has smaller rank than f . So f has rank 1, and the automaton is synchronizing. □

So we only have to consider all pairs of states.

The picture shows the previous example, extended to pairs of states.



Now it suffices to check that there is a path from any vertex on the right to some vertex on the left; this can clearly be done in polynomial time.

Graph endomorphisms

Our graphs are **simple** (no directions, loops, or multiple edges). The **clique number** $\omega(\Gamma)$ of a graph Γ is the number of vertices in its largest complete subgraph, and the **chromatic number** $\chi(\Gamma)$ is the smallest number of colours required for a vertex-colouring so that adjacent vertices get different colours. Let Γ and Δ be graphs. A **homomorphism** from Γ to Δ is a map f from the vertex set of Γ to that of Δ with the property that, for any edge $\{v, w\}$ of Γ , the image $\{vf, wf\}$ is an edge of Δ . An **endomorphism** of Γ is a homomorphism from Γ to itself.

Proposition

- ▶ *A homomorphism from K_m to Γ is an embedding of K_m into Γ ; such a homomorphism exists if and only if $\omega(\Gamma) \geq m$.*
- ▶ *A homomorphism from Γ to K_m is a proper colouring of Γ with m colours; such a homomorphism exists if and only if $\chi(\Gamma) \leq m$.*
- ▶ *There are homomorphisms in both directions between Γ and K_m if and only if $\omega(\Gamma) = \chi(\Gamma) = m$.*

The obstruction to synchronization

The endomorphisms of a graph Γ form a transformation monoid; if Γ is not a null graph, then $\text{End}(\Gamma)$ is not synchronizing, since edges cannot be collapsed.

Theorem

Let S be a transformation monoid on Ω . Then S fails to be synchronizing if and only if there exists a non-null graph Γ on the vertex set Ω for which $S \leq \text{End}(\Gamma)$. Moreover, we may assume that $\omega(\Gamma) = \chi(\Gamma)$.

Proof.

Given a transformation monoid S , we define a graph $\text{Gr}(S)$ in which x and y are joined if and only if there is no element $s \in S$ with $xs = ys$. Show that $S \leq \text{End}(\text{Gr}(S))$, that $\text{Gr}(S)$ has equal clique and chromatic number, and that S is synchronizing if and only if $\text{Gr}(S)$ is null. □

Synchronizing groups

A permutation group is never synchronizing as a monoid, since no collapses at all occur.

We abuse language by making the following definition. A permutation group G on Ω is **synchronizing** if, for any map f on Ω which is not a permutation, the monoid $\langle G, f \rangle$ generated by G and f is synchronizing.

Theorem

A permutation group G on Ω is non-synchronizing if and only if there exists a G -invariant graph Γ , not complete or null, which has clique number equal to chromatic number.

So the definition of “synchronizing” exactly matches our previous template for permutation group properties: G is synchronizing if and only if there is no non-trivial G -invariant graph with clique number equal to chromatic number.

Synchronization in the hierarchy

An imprimitive group preserves a partition, and so a disjoint union of complete graphs of the same size (which clearly has clique number equal to chromatic number).

A non-basic group preserves a Hamming graph (two n -tuples adjacent if their Hamming distance is 1); this graph has clique number equal to chromatic number, both equal to the alphabet size.

A 2-homogeneous group preserves no non-trivial graph at all. So we have:

Theorem

Let G be a permutation group of degree $n > 2$.

- ▶ *If G is synchronizing, then it is primitive and basic.*
- ▶ *If G is 2-homogeneous, then it is synchronizing.*
- ▶ *None of these implications reverses.*

The O'Nan–Scott Theorem

Recall that, by the O'Nan–Scott Theorem, a basic group is affine, diagonal or almost simple.

Affine groups have abelian normal subgroups. They have the form

$$\{x \mapsto xA + c : c \in V, A \in H\},$$

where V is a finite vector space and H an irreducible linear group on V . They may or may not be synchronizing.

Almost simple groups satisfy $T \leq G \leq \text{Aut}(T)$, where T is a non-abelian finite simple group. The action is not specified. They may or may not be synchronizing.

Diagonal groups are considered below.

Counterexamples to a theorem of Cauchy

This was the wonderful title of a paper by Peter Neumann, Charles Sims and James Wiegold in 1968.

Cauchy “proved” that a primitive permutation group whose degree is one more than a prime must be doubly transitive.

Neumann, Sims and Wiegold noted that, if T is a finite simple group, then the group induced on T by left and right multiplication,

$$\{(g, h) : x \mapsto g^{-1}xh\}$$

is primitive. One can enlarge the group by adjoining automorphisms of S (the inner automorphisms are already included as the “diagonal” subgroup $\{(g, g) : g \in T\}$) and the map $x \mapsto x^{-1}$. The result is the **2-factor diagonal group** $D(T, 2)$.

They noted that $|A_5| = 59 + 1$, $|\mathrm{PSL}(2, 7)| = 167 + 1$,
 $|A_6| = 359 + 1$, $|\mathrm{PSL}(2, 8)| = 503 + 1$, $|\mathrm{PSL}(2, 11)| = 659 + 1$,
.... (It is not known whether there are infinitely many counterexamples.)

Latin squares

A **Latin square** of order n is an $n \times n$ array with entries taken from an alphabet of size n , so that each letter in the alphabet occurs once in each row and once in each column.

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

This is not just any old Latin square: it is the **Cayley table**, or multiplication table, of the Klein group of order 4.

Latin square graphs

Given a Latin square L , we define a graph whose vertices are the n^2 cells of the square, two vertices adjacent if they lie in the same row or the same column or contain the same symbol. This is a **Latin square graph**.

If L is the Cayley table of a group T , the graph admits T^3 (acting on rows, columns and symbols), as well as automorphisms of T and the symmetric group permuting the three types of object. If T is simple, the group generated by all of these is primitive, and is a **three-factor diagonal group** $D(T, 3)$.

Latin square graphs are **strongly regular**, but almost all have only the trivial group of automorphisms.

Transversals and orthogonal mates

A *transversal* 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.

Not all Latin squares have transversals. Consider the following square:

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

Given a set of cells, one from each row and one from each column, the sum of the row indices is $0 + 1 + 2 + 3 = 2 \pmod{4}$. Similarly for the columns. Since each entry is the sum of its row and column indices, the entries sum to $2 + 2 = 0 \pmod{4}$. Thus the entries cannot be $\{0, 1, 2, 3\}$.

More generally, the Cayley table of a cyclic group of even order has no transversal.

Complete mappings

Let G be a group. A **complete mapping** of G is a bijective map $\phi : G \rightarrow G$ such that the map ψ defined by $\psi(x) = x\phi(x)$ is also a bijection.

Given a transversal in the Cayley table of G , define ϕ and ψ by the rule that $\phi(g)$ and $\psi(g)$ are the column label and entry of the transversal cell in row g . Then ϕ is a complete mapping as above.

Also, if ϕ and ψ are as above, then the array with (g, h) entry $g\psi(h)$ is a Latin square, which is an orthogonal mate for the Cayley table.

Thus the following are equivalent:

- ▶ the Cayley table of G has a transversal;
- ▶ the Cayley table of G has an orthogonal mate;
- ▶ G has a complete mapping.

The Hall–Paige conjecture

In 1955, Marshall Hall Jr and Lowell J. Paige made the following conjecture:

Conjecture

A finite group G has a complete mapping if and only if the Sylow 2-subgroups of G are trivial or non-cyclic.

They proved the necessity of their condition, and its sufficiency in a number of cases, including soluble groups and symmetric and alternating groups.

Hall was a well known group theorist and combinatorialist. Paige was much less well known: he was a student of Richard Bruck, had 6 students at UCLA, and has 18 papers (including his thesis on **neofields**) listed on MathSciNet.

Proof of the Hall–Paige conjecture

The Hall–Paige conjecture was proved in 2009 by Stuart Wilcox, Anthony Evans, and John Bray.

Wilcox showed that its truth for all groups follows from its truth for simple groups, and proved it for groups of Lie type, except for the **Tits group** ${}^2F_4(2)'$. (The first two types, cyclic and alternating, are covered by Hall and Paige.)

Evans dealt with the Tits group and 25 of the 26 sporadic groups.

Bray dealt with the final group, the **Janko group** J_4 .

The papers of Wilcox and Evans were published in the *Journal of Algebra* in 2009. But Bray's work has not been published at the time. (It has now appeared, together with the following discussion on synchronization, in the memorial issue of the *Journal of Algebra* for Charles Sims.)

Latin square graphs

Let L be a Latin square of order n , and Γ its Latin square graph. For $n > 2$, this graph has clique number n : any row, column or letter is a clique.

Also, the chromatic number is n if and only if A has an orthogonal mate:

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

Diagonal groups

We saw that 3-factor diagonal groups are automorphism groups of the Latin square graphs associated with Cayley tables of finite simple groups.

Proposition

The group $D(T, 3)$ is non-synchronizing.

Proof.

By Burnside's Transfer Theorem, a non-abelian simple group cannot have cyclic Sylow 2-subgroups. So by Hall–Paige, the Latin square graph of its Cayley table has clique number equal to chromatic number. □

With a little more effort, we have:

Theorem

The diagonal group $D(T, r)$ is non-synchronizing for $r \geq 3$.

How to test synchronization?

The synchronizing property lies between primitivity and 2-transitivity. Each of these can be tested algorithmically in polynomial time. What about synchronization?

The discussion so far gives an algorithm for deciding if G is synchronizing:

- ▶ Construct all the G -invariant graphs.
- ▶ For each, test whether its clique number and chromatic number are equal.
- ▶ If any such graph is found, then G is non-synchronizing; if not, it is synchronizing.

This appears to be a very stupid algorithm: there are potentially exponentially many graphs to check, and for each graph we have to solve an NP-hard problem

Can we do better?

Separation

The only general improvement we have uses the concept of **separation**.

Note that, for a transitive group of degree n , if A and B are subsets of the domain with $|A| \cdot |B| < n$, then there exists $g \in G$ with $Ag \cap B = \emptyset$. This is proved by a simple counting argument.

We say that the transitive group G is **separating** if for any subsets A, B with $|A| \cdot |B| = n$ and $|A|, |B| > 1$, there exists $g \in G$ with $Ag \cap B = \emptyset$. Otherwise G is **non-separating**. It turns out that a separating group is synchronizing.

Graph-theoretic form

Theorem

A transitive group G of degree n is non-separating if and only if there exists a G -invariant graph, not complete or null, such that the product of its clique number and independence number is n .

Now, if G is non-synchronizing, it preserves a graph with clique number and chromatic number k , for some k . Each colour class in the k -colouring has cardinality n/k . So G is non-separating. It is slightly easier to test separation than synchronization: we only have to find the clique number of the G -invariant graphs (the independence number of a graph is the clique number of its complement), and according to parameterized complexity theory, clique number is “easier” than chromatic number.

Synchronizing, not separating?

For some time we had no examples of groups which are synchronizing but not separating. Now we know a little more:

Theorem

For primitive groups of affine or diagonal type, synchronization and separation are equivalent.

So we are looking for almost simple groups. One infinite family and a few sporadic examples are known. The infinite family consists of the orthogonal groups $O_5(p)$, for p an odd prime, acting on the parabolic quadric in projective 4-space. In the orthogonality graph, a line is a coclique and an ovoid is a clique; but there is no partition of the quadric into either lines or ovoids.

References

J. Araújo, P. J. Cameron and B. Steinberg, Between primitive and 2-transitive: Synchronization and its friends, *Europ. Math. Soc. Surveys* **4** (2017), 101–184.

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.

