

# Synchronization, association schemes and Steiner systems

Peter J. Cameron  
University of St Andrews



British Combinatorial Conference  
Strathclyde, July 2017

(joint with Mohammed Aljohani and John Bamberg)

# Synchronization

This subject has its roots in automata theory and the infamous **Černý conjecture**. Unfortunately there is no time to describe the background. The version for permutation groups is due independently to João Araújo and Ben Steinberg.

A permutation group  $G$  on  $\Omega$  is **synchronizing** if, given any map  $a : \Omega \rightarrow \Omega$  which is not a permutation, the semigroup  $\langle G, a \rangle$  generated by  $G$  and  $a$  contains a rank 1 element (one whose image consists of a single point).

## Theorem

*The permutation group  $G$  is non-synchronizing if and only if there is a non-trivial  $G$ -invariant graph  $\Gamma$  with clique number equal to chromatic number (that is, with core a complete graph).*

## Separation

There is a closely related property, which can be phrased in terms of graphs as follows (this was not the original form). The transitive permutation group  $G$  is **non-separating** if there is a non-trivial  $G$ -invariant graph for which the product of clique number and independence number is equal to the number of vertices. (For a vertex-transitive graph, the product of clique number and independence number cannot exceed the number of vertices.)

If no such graph exists, then  $G$  is **separating**.

Note that, if a vertex-transitive graph has clique number equal to chromatic number, then all the colour classes in a minimal colouring have the same size, so the product of clique and independence numbers is equal to the number of vertices.

### Theorem

*2-homogeneous  $\Rightarrow$  separating  $\Rightarrow$  synchronizing  $\Rightarrow$  primitive. None of these implications reverses.*

## The big problem

The big problem is: *Determine the synchronizing (or separating) permutation groups.*

One important family consists of the symmetric group  $S_n$  acting on  $k$ -sets, for  $k < n/2$ .

In this case, the **orbital graphs** (the minimal non-trivial  $G$ -invariant graphs) are defined by joining two  $k$ -sets if the cardinality of their intersection is  $i$ , for some fixed  $i$  with  $0 \leq i \leq k - 1$ . These are the associate classes in the **Johnson association scheme**.

So any  $G$ -invariant graph is defined by a subset  $I$  of  $\{0, \dots, k - 1\}$ , with two  $k$ -sets joined if their intersection belongs to  $I$ . Let us call this graph  $\Gamma_I(n, k)$ .

We have to decide whether such graphs can have clique number equal to chromatic number, or product of clique number and independence number equal to  $\binom{n}{k}$ .

## Steiner systems

This problem led us to a conjecture which would be a wide extension of part of Peter Keevash's existence theorem for  $t$ -designs.

A **Steiner system**  $S(t, k, n)$  is a collection of  $k$ -subsets (called **blocks**) of a set of  $n$  points with the property that any  $t$  points lie in a unique block.

If such a system exists, then  $S_n$  acting on  $k$ -sets is not separating: the blocks of the system form a clique in the graph in which two  $k$ -sets are joined if they meet in at most  $t - 1$  points, and the  $k$ -sets containing a fixed  $t$ -set form an independent set (said to be of **Erdős–Ko–Rado type**, or **EKR type**), and the product of the sizes of these sets is  $\binom{n}{k}$ . Indeed the Erdős–Ko–Rado theorem tells us that, for  $n$  sufficiently large (in terms of  $k$ ), the maximum-size independent sets are of EKR type.

# The conjecture

## Conjecture

*There is a function  $F$  such that, if  $n > F(k)$ , then  $S_n$  acting on  $k$ -sets is non-separating if and only if a Steiner system  $S(t, k, n)$  exists for some  $t$  with  $0 < t < k$ .*

In other words, out of all the graphs  $\Gamma_I(n, k)$ , the only ones that matter for large  $n$  are those with  $I = \{0, \dots, t-1\}$  or  $I = \{t, \dots, k-1\}$ .

There are well-known **divisibility conditions** which are necessary for the existence of a Steiner system:  $\binom{k-i}{t-i}$  must divide  $\binom{n-i}{t-i}$  for  $i = 0, \dots, t-1$ . Keevash showed that, for  $n$  sufficiently large, these conditions are also sufficient.

So the conjecture can be re-phrased: for  $n > G(k)$ ,  $S_n$  on  $k$ -sets is non-separating if and only if the divisibility conditions hold for some  $t$  with  $0 < t < k$ .

## And what about synchronizing?

There is a similar conjecture. A **large set** of Steiner systems  $S(t, k, n)$  is a partition of the set of  $k$ -subsets of an  $n$ -set into Steiner systems. If a large set exists, then  $S_n$  on  $k$ -sets is not synchronizing.

### Conjecture

*There is a function  $H$  such that, for  $n > H(k)$ ,  $S_n$  acting on  $k$ -sets is non-synchronizing if and only if a large set of Steiner systems  $S(t, k, n)$  exists for some  $t$  with  $0 < t < k$ .*

Less is known about the existence of large sets, and we do not feel confident enough to conjecture an analogue of Keevash's theorem for them.

## Projective planes

Suppose that  $n = q^2 + q + 1$  and  $k = q + 1$ , where a projective plane of order  $q$  exists. This is a set of  $n$  subsets of size  $k$ , any two meeting in one point. So it is a clique in the graph where two sets are joined if they intersect in one point. As a result, a coclique in this graph has size at most

$$\binom{n}{k} / n = \binom{n-2}{k-2}.$$

A set of EKR type (consisting of all  $k$ -sets containing a given pair of points) attains this bound. For  $q = 2$ , there are others, and even a colouring of the graph with  $k$  colours, as follows: For each line of the Fano plane, take the five 3-sets consisting of that line and the four sets disjoint from it. This gives a 7-colouring of  $\Gamma_1(7,3)$ .



## Conjecture

*For  $q > 2$ , a coclique attaining the bound must be of EKR type.*

Moreover, it can be seen that the  $k$ -sets cannot be partitioned into sets of EKR type.

This is true for  $q = 3$  and for  $q = 4$ . Frankl and Füredi showed that the graph  $\Gamma_1(n, k)$  has the property that its maximum cocliques are of EKR type (and so do not contain two disjoint sets) for  $n$  sufficiently large compared to  $k$ .

However, this argument is unlikely to deal with synchronization, since Magliveras conjectured that large sets of projective planes exist for every order  $q > 2$ . (This is known for  $q = 3$  and  $q = 4$ .) So, even if  $\Gamma_{\{1\}}(q^q + q + 1, q + 1)$  does not have clique number equal to chromatic number for  $q > 2$ , its complement probably does.

## Why association schemes?

The results above are about graphs which are unions of associate classes in the **Johnson association scheme** (the points are the  $k$ -subsets of an  $n$ -set, and two  $k$ -sets are  $i$ th associates if they intersect in  $k - i$  points).

The notions of synchronizing and separating can be extended to arbitrary association schemes in an analogous way. A scheme is non-synchronizing if some union of associate classes forms a graph with clique number equal to chromatic number; and non-separating if some union of classes has product of clique number and independence number equal to the number of points. (A result of Delsarte states that this is an upper bound for this product, in any association scheme.)

So plenty of good problems here!