Association schemes, graph homomorphisms, and synchronization

Peter J. Cameron
University of St Andrews

Symmetry vs Regularity, Pilsen, July 2018

Outline

After a reminder of what association schemes and coherent configurations are, I will discuss three topics:

- Donald Higman's lectures in Oxford in 1970;
- association schemes and permutation groups;
- association schemes and transformation semigroups.

Coherent configurations

I hope everybody has seen some form of the definition before. I will give the matrix form.

A coherent configuration is a set $\mathbf{A}$ of $\Omega \times \Omega$ zero-one matrices (where Ω is a finite set) such that

- the sum of the matrices in $\mathbf{A}$ is the all-one matrix J;
- there is a subset of $\mathbf{A}$ whose sum is the identity matrix I;
- $\mathbf{A}$ is closed under transposition;
- the linear span of $\mathbf{A}$ (over a field of characteristic zero) is closed under multiplication.

The group case

The most important examples arise in the case when there is a permutation group G on the set Ω, and the matrices in $\mathbf{A}$ are the characteristic functions of the orbits of G on $\Omega \times \Omega$.
Donald Higman called this the group case; now we tend to refer to such a configuration as Schurian.
In this case, the algebra spanned by the matrices in $\mathbf{A}$ is the centraliser algebra of the group G (all matrices which commute with the permutation matrices in G).

Specialisations

The diagonal matrices in $\mathbf{A}$ define a partition of Ω whose parts are the fibres of the configuration; we say $\mathbf{A}$ is homogeneous if there is a single fibre. In the Schurian case, the fibres are the orbits of the group G in Ω.

We say that the configuration is

- commutative if the matrices in $\mathbf{A}$ commute;
- symmetric if the matrices in $\mathbf{A}$ are symmetric.

The symmetrisation of $\mathbf{A}$ is the set $\mathbf{A}^{\mathrm{sym}}$ of zero-one matrices obtained from A by replacing each pair $\{A, A^\top\}$ of distinct matrices by $A + A^\top$. We say that $\mathbf{A}$ is stratifiable if $\mathbf{A}^{\mathrm{sym}}$ is a coherent configuration.

We have the implications

$$\text{symmetric} \Rightarrow \text{commutative} \Rightarrow \text{stratifiable} \Rightarrow \text{homogeneous.}$$

History: Bose, Weisfeiler

The notions just described arose in different areas for different applications.

The first was in statistics, from R. C. Bose and his school: the paper by Bose and Nair (1939) was probably the earliest appearance. Bose used the term association scheme for a symmetric coherent configuration. (There are various reasons why statisticians prefer symmetric matrices: for example, covariance matrices are symmetric.) Bose and Mesner in 1959 introduced the algebra generated by the matrices, which now bears their names.

In the 1960s, as we celebrate here, Weisfeiler and Leman defined cellular algebras, an object slightly more general than coherent configurations, in connection with the graph isomorphism problem.

History: Higman, Delsarte

At the same time or slightly later, Donald Higman defined coherent configurations for studying permutation groups, and in particular for decomposing permutation characters (or monomial characters) into irreducibles. His first papers on this were in 1964 and 1967, and he presented a fully developed theory in 1970, as I shall tell.

Delsarte's thesis in 1973 used association schemes as a framework for both error-correcting codes and t-designs, and introduced new methods into the study of these areas (including linear programming). Delsarte's theory applies to commutative coherent configurations, but his important examples are symmetric (the Hamming schemes for codes and the Johnson schemes for designs).

Interlude

Bose and Nair considered incomplete-block designs where the number of blocks containing two points depends only on the associate class containing the pair, for some association scheme on the point set.

The notion of non-commutative or inhomogeneous coherent configuration suggests considering points and blocks together, or flags (incident point-block pairs), as carriers of the structure.

The idea was in the air at the time. Goethals and Seidel proved that, if a balanced incomplete-block design (or 2-design) has two intersection sizes for pairs of blocks, then each defines a strongly regular graph on the block set.

Around 1970, Higman used his theory to give a new proof of the Feit–Higman theorem on generalised polygons. (This name refers to Graham Higman, who was the leading algebraist in Oxford at that time.) While the original proof used the association scheme on points, the new proof used the non-commutative coherent configuration on flags.

History: Bannai and Ito, Terwilliger

The influential book by Bannai and Ito took up Delsarte's viewpoint, and put emphasis on the classes of P-polynomial and Q-polynomial schemes, and to classification problems.
Terwilliger enlarged the Bose–Mesner algebra to a non-commutative algebra, incorporating the duality between P and Q that had first appeared in Delsarte's work.
Time does not permit to trace subsequent developments…

Donald Higman in Oxford

I arrived in Oxford as a DPhil student (Oxford for PhD) in 1968. Donald Higman had a sabbatical in Oxford in 1970–1971. In the first semester he gave a course of lectures entitled "Combinatorial considerations about permutation groups". This developed the theory of coherent configurations, covering fibres, fusion, the *t*-vertex condition, the algebraic structure of the algebra generated by the configuration, and so on.

As was commonly done, two students (Susannah Howard and I) were given the job of taking notes from the lectures. We discussed the notes with the lecturer and made corrections, and the resulting notes were published in the Mathematical Institute series of mimeographed lecture notes.

So I was in quite near the beginning of this line of development.

Terminology

We have to give up the term “cellular algebra”, since this was given a completely different meaning by Graham and Lehrer, which has now become standard. What about “association scheme”?

There are conflicting ways to describe mathematical objects: we can use an adjective to restrict the structures considered (as “nilpotent group”) or to extend it (as “delta-matroid”). Thus most delta-matroids are not matroids.

As noted, Bose’s association schemes were symmetric c.c.s; Delsarte extended the term to commutative c.c.s. Bannai and Ito further extended this to homogeneous c.c.s, while Evdokimov and Ponomarenko use the term for arbitrary c.c.s. I will restrict the term to Bose’s original usage; you will see why.

Some classes of permutation groups

As we saw, a transitive permutation group defines a homogeneous c.c. If the group is 2-transitive, then the c.c. is "trivial": $\mathbf{A} = \{I, J - I\}$. So c.c.s are most useful for studying groups which are transitive (or have few orbits) but are not 2-transitive. In the rest of this lecture I will consider some such classes, first from association schemes and then from transformation semigroups and automata.

I will say that a structure on Ω is trivial if it is invariant under all permutations of Ω. Thus, a permutation group G is

- transitive if there is no non-trivial G-invariant subset of Ω;
- primitive if there is no non-trivial G-invariant partition of Ω;
- 2-homogeneous if there is no non-trivial G-invariant undirected graph on Ω;
- 2-transitive if there is no non-trivial G-invariant directed graph on Ω.

Classes related to association schemes

We call a transitive permutation group AS-free if there is no non-trivial G-invariant association scheme.

Since a transitive imprimitive group preserves a "group-divisible" scheme, and a primitive non-basic group (in the O'Nan–Scott classification) preserves a Hamming scheme, we see that AS-free groups are primitive and basic, and 2-homogeneous groups are AS-free.

Further, we say that G is AS-friendly if there is a unique minimal G-invariant association scheme.

If we replaced "AS" by "CC" in these definitions, then every group would be CC-friendly, and the CC-free groups would be the 2-transitive groups.

Finally, G is stratifiable if the c.c. it defines is stratifiable, and generously transitive if it is symmetric.

Relations

Theorem

The following implications hold between properties of a permutation group G:

$$\begin{tikzcd}
\text{2-}\textit{transitive} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \text{2-}\textit{homogeneous} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \textit{AS-free} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \textit{primitive} \arrow[d, Rightarrow] \\
\textit{gen. trans.} \arrow[r, Rightarrow] & \textit{stratifiable} \arrow[r, Rightarrow] & \textit{AS-friendly} \arrow[r, Rightarrow] & \textit{transitive}
\end{tikzcd}$$

None of these implications reverses, and no further implications hold. □

The negative implications are verified by computer; much of this uses the results obtained by Faradžev, Klin and Muzychuk using `CoCo`.

A problem

An AS-free group is basic in the O'Nan–Scott classification, and so is affine, diagonal or almost simple.

An affine group is stratifiable, and so is AS-free if and only if it is 2-homogeneous.

The existence of diagonal AS-free groups is unknown; any example must have at least four factors in its socle. (For two factors, it preserves the conjugacy class scheme, while for three factors, it preserves the Latin square scheme of the Cayley table, of a simple factor.)

There are almost simple (not 2-transitive) examples, including $\mathrm{PSL}(3,3)$ and $\mathrm{PSL}(3,3):2$ (degree 234), M_{12} (degree 1320), J_1 (degree 1463, 1540 or 1596), and J_2 (degree 1800).

Problem

Understand AS-free groups!

Some non-AS-friendly groups

Let G be the symmetric group S_n (for $n \geq 5$), acting on the set Ω of ordered pairs of distinct elements from the set $\{1, \ldots, n\}$: we write the pair (i, j) as ij for brevity. The coherent configuration consists of the following relations (where i, j, k, l are disjoint): $R_1 = \{(ij, ij)\}$; $R_2 = \{(ij, ji)\}$, $R_3 = \{(ij, ik)\}$, $R_4 = \{(ij, kj)\}$, $R_5 = \{(ij, ki)\}$, $R_6 = \{(ij, jk)\}$, and $R_7 = \{(ij, kl)\}$. We have $R_5^\top = R_6$; all other relations are symmetric. The symmetrised partition is not an association scheme, but there are three incomparable minimal association schemes as follows:

- the *pair* scheme: $\{R_1, R_2, R_3 \cup R_4, R_5 \cup R_6, R_7\}$;
- two “divisible” schemes $\{R_1, R_3, R_2 \cup R_4 \cup R_5 \cup R_6 \cup R_7\}$ and $\{R_1, R_4, R_2 \cup R_3 \cup R_5 \cup R_6 \cup R_7\}$.

Primitive examples

The examples on the last slide are imprimitive, but there are primitive examples too.
The smallest primitive group which is not AS-friendly is $\mathrm{PSL}(2,11)$, with degree 55. The smallest primitive groups which are AS-friendly but not stratifiable are $\mathrm{PSL}(2,13)$, in two actions with degrees 78 and 91.

Problem

Understand AS-friendly groups!

Note that the class of AS-friendly groups is closed upwards, and is also closed under taking wreath products or primitive components. The same holds for the classes of stratifiable or generously transitive groups.

Synchronization

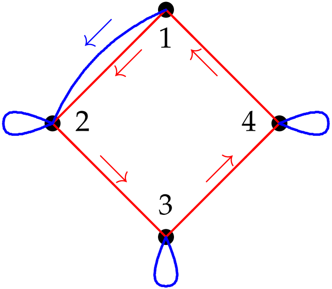
Another topic which produces classes of groups between primitive and 2-transitive comes from automata theory.

A (deterministic, finite-state) automaton is a machine which can be in one of a set Ω of internal states, and successively reads symbols from an input alphabet. When it reads a symbol, it changes state depending on the previous state and the symbol read.

An automaton can be represented by a graph with coloured directed arcs, where the vertices correspond to states and the edge colour to symbols. We require that there is a unique arc of each colour leaving each vertex. When it reads a symbol from a vertex, it moves along the edge of the corresponding colour.

An automaton is synchronizing if there is a word w in the input symbols with the property that, if the machine reads w, its final state will be determined, independent of its initial state. The word w is called a reset word.

An example



Now it can be verified that BRRRBRRRB is a reset word (and indeed that it is the shortest possible reset word for this automaton).

The Černý conjecture

A fifty-year-old conjecture, still unsolved, is the Černý conjecture:

Conjecture

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

The preceding example meets the bound for $n = 4$, and is easily generalised to give an example meeting the bound for any n.

But a typical synchronizing automaton has a much shorter reset word.

What I describe does not directly address the conjecture, but there are some connections.

Algebraic interpretation

Each symbol corresponds to a transition, a map from the set Ω of states to itself. Since we can compose transitions (by reading the symbols in turn), the set of transitions forms a transformation monoid (a semigroup with identity), with a prescribed set of generators corresponding to the symbols in the alphabet.

Conversely, a transformation monoid with a prescribed generating set corresponds to an automaton.

An automaton is synchronizing if and only if the monoid contains an element of rank 1 (that is, whose image has cardinality 1).

Graph homomorphisms

A homomorphism of an undirected graph Γ is a map on the vertex set of Γ which maps edges to edges. (What happens to non-edges is not specified). An endomorphism is a homomorphism from Γ to itself.

As an exercise, I invite you to show that if K_k is the complete graph on k vertices, then there exist homomorphisms in both directions between Γ and K_k if and only if the clique number and chromatic number of Γ are both equal to k.

The set of endomorphisms of Γ forms a monoid under composition, called the endomorphism monoid of Γ and denoted $\mathrm{End}(\Gamma)$.

Synchronizing monoids

Graphs play an unexpected role in synchronization theory:

Theorem

A transformation monoid M on Ω is non-synchronizing if and only if there is a non-null graph Γ on Ω such that $M \leq \mathrm{End}(\Gamma)$.

One way round is clear: if Γ has at least one edge, then no endomorphism can collapse it to a single point. The other direction is not hard but requires a construction.

Synchronizing groups

A permutation group G on Ω cannot be synchronizing as a monoid (if $|\Omega| > 1$. So, by abuse of language, we say that G is synchronizing if, for all non-permutations f on Ω, the monoid $\langle G, f \rangle$ is synchronizing.
Using the theorem on the preceding slide we get the following result:

Theorem

A permutation group G on Ω is non-synchronizing if and only if there is a nontrivial G-invariant graph Γ with clique number equal to chromatic number.

The G-invariant graphs are the unions of relations in $\mathbf{A}^{\text{sym}}$, where $\mathbf{A}$ is the coherent configuration obtained from G. So finally synchronization is a property of coherent configurations.

Which groups are synchronizing?

Using the above theorem it is easy to see that synchronizing groups are transitive, and primitive, and basic, and that a 2-homogeneous group is synchronizing.
None of these implications reverses.
For example, if $n \geq 5$, then the (primitive rank 3) permutation group induced by S_n on the 2-subsets of $\{1, \ldots, n\}$ is primitive but not 2-homogeneous, and is synchronizing if and only if n is odd.

Separating groups

This concept is closely related to synchronization but applies only to transitive groups (and has no obvious connection with automata).

A transitive permutation group G on Ω is separating if, whenever $A, B \subseteq \Omega$ satisfy $|A|, |B| > 1$ and $|A| \cdot |B| = |\Omega|$, there exists $g \in G$ with $Ag \cap B = \emptyset$.

Arguing as before we see that G is non-separating if and only if there is a non-trivial G-invariant graph Γ whose clique number ω and independence number α satisfy $\omega\alpha = |\Omega|$.

Separating implies synchronizing, but not conversely (though examples are not so easy to find). For the groups S_n on 2-sets, the two properties are equivalent.

The Johnson schemes

One fascinating class of groups consists of symmetric groups S_n acting on the set of k-subsets of $\{1, \ldots, n\}$, for $n > 2k$. These groups are primitive.
The corresponding coherent configuration is the Johnson association scheme, whose points are the k-subsets of $\{1, \ldots, n\}$, and the ith relation consists of pairs of subsets intersecting in $k - i$ points.
So the general question whether S_n on k-sets is synchronizing or separating is a question about graphs which are unions of basic relations in the Johnson scheme $J(n, k)$.

Keevash's Theorem

A *Steiner system* $S(t,k,n)$ is a collection B of k-subsets of $\{1,\ldots,n\}$ such that any t-set is contained in a unique member of B.
It is easy to see that a necessary condition for the existence of a Steiner system is that

$$\binom{k-i}{t-i} \text{ divides } \binom{n-i}{k-i}$$

for $i = 0,\ldots,t-1$.
Recently Peter Keevash showed that this condition is asymptotically sufficient: that is, if it is satisfied and n is sufficiently large in terms of k and t, then a Steiner system exists.

A conjecture

A Steiner system is an independent set in the graph where k-sets are adjacent if they intersect in t or more points. The set of all k-sets containing a fixed t-set is a clique in this graph of size $\binom{n-t}{k-t}$ (said to be of Erdős–Ko–Rado type). So, if a Steiner system exists, then S_n on k-sets is not separating.

Conjecture

There is a function F such that, for $n \geq F(k)$, the group S_n on k-sets is non-separating if and only if a Steiner system $S(t,k,n)$ exists for some $t \leq k-1$.

By Keevash's theorem this would imply that, for sufficiently large n, this group is non-separating if and only if the divisibility conditions hold for some t.

Synchronization

A related (but less well supported) conjecture asserts that, for sufficiently large n, the group S_n on k-sets is non-synchronizing if and only if a large set of Steiner systems (that is, a partition of the set of all k-sets into Steiner systems) exists.

Problem

Is there a Keevash-type theorem for large sets of Steiner systems?