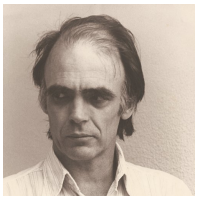
Between primitive and 2-transitive, 2: Coherent configurations and association schemes

Peter J. Cameron
(Joint work with P. P. Alejandro and R. A. Bailey)

CAUL, Lisbon, April 2012

Boris Weisfeiler and Donald Higman


Boris Weisfeiler


Donald Higman

The inventors of coherent configurations

Coherent configurations

Let Ω be a finite set. A coherent configuration on Ω is a set $\mathcal{P} = \{R_1, \ldots, R_s\}$ of binary relations on Ω (subsets of Ω^2) satisfying the following four conditions:

- $\mathcal{P}$ is a partition of Ω^2;
- there is a subset $\mathcal{P}_0$ of $\mathcal{P}$ which is a partition of the diagonal $\Delta = \{(\alpha, \alpha) : \alpha \in \Omega\}$;
- for every relation $R_i \in \mathcal{P}$, its converse $R_i^\top = \{(\beta, \alpha) : (\alpha, \beta) \in R_i\}$ is in $\mathcal{P}$; say $R_i^\top = R_{i^*}$.
- there exist integers p_{ij}^k, for $1 \le i, j, k \le s$, such that,for any $(\alpha, \beta) \in R_k$, the number of points $\gamma \in \Omega$ such that $(\alpha, \gamma) \in R_i$ and $(\gamma, \beta) \in R_j$ is equal to p_{ij}^k (and, in particular, is independent of the choice of $(\alpha, \beta) \in R_k$).

I will sometimes abbreviate "coherent configuration" to c.c.

Coherent configurations from permutation groups

Let G be a permutation group on Ω. Then Ω^2 is partitioned by the G-orbits in the induced action; these form a coherent configuration.
The first condition is clear; for the second, if $(\alpha, \beta), (\alpha', \beta') \in R_k$, then some element $g \in G$ carries the first pair to the second, so G maps the points γ with $(\alpha, \gamma) \in R_i$ and $(\gamma, \beta) \in R_j$ to the corresponding set for (α', β').
Donald Higman introduced coherent configurations to study permutation groups. His 1970 Oxford lecture notes were called *Combinatorial Considerations about Permutation Groups*.

Basis matrices

We can represent a binary relation R on Ω by its basis matrix $A(R)$, whose rows and columns are indexed by Ω, and whose (α, β) entry is 1 if $(\alpha, \beta) \in R$, 0 otherwise. If I and J are the identity and all-1 matrices, the axioms for a c.c. become:

- $\sum_{i=1}^{s} A(R_i) = J$.
- $\sum_{i=1}^{t} A(R_i) = I$, where $\{R_1, \ldots, R_t\}$ is the subset referred to in the second axiom.
- For each i, there exists i^* such that $A(R_i)^\top = A(R_{i^*})$.
- (d) For each pair i, j, we have

$$A(R_i)A(R_j) = \sum_{k=1}^{s} p_{ij}^k A(R_k).$$

The basis algebra

It follows that the span of $\{A(R_1), \ldots, A(R_s)\}$ (over the complex numbers) is an algebra, and from (c) that this algebra is semisimple (and so is isomorphic to a direct sum of matrix algebras over $\mathbb{C}$). This algebra is called the basis algebra of the configuration. We denote the basis algebra of $\mathcal{P}$ by $\mathrm{BA}(\mathcal{P})$.
Note that $\mathrm{BA}(\mathcal{P})$ consists of all the functions from Ω^2 to $\mathbb{C}$ which are constant on the parts of $\mathcal{P}$.

The intersection algebra

Moreover, if P_j is the $s \times s$ matrix with (i, k) entry p_{ij}^k, then the map $A(R_j) \mapsto P_j$ for $j = 1, \ldots, s$ extends linearly to an algebra isomorphism. Thus the matrices $P_1, \ldots, P_s$ also span an algebra, called the intersection algebra of $\mathcal{P}$.
The irreducible modules for the intersection algebra, and their multiplicities in the module $\mathbb{C}\Omega$, can in principle be calculated from the intersection numbers.
This is one of the most powerful methods for showing nonexistence of coherent configurations with given intersection numbers.

The partition lattice

The partitions of any set X are ordered by refinement: $P \leq Q$ if every part of P is a subset of a part of Q.
The top element is the partition with a single part, and the bottom element is the partition into singleton parts.
The meet of two partitions P and Q is the partition whose parts are all non-empty intersections of a part of P and a part of Q.
The join is a little harder to describe. A part of the join of P and Q consists of everything which can be reached from a single point by moving to a point in the same part of P, then to one in the same part of Q, then to one in the same part of P, and so on.

The lattice of coherent configurations

The meet of two coherent configurations (in the partition lattice) is not usually a coherent configuration. However, we have:

Theorem
The join of two coherent configurations $\mathcal{P}$ and $\mathcal{Q}$ is a coherent configuration.

For a function is constant on parts of $\mathcal{P} \vee \mathcal{Q}$ if and only if it is constant on the parts of $\mathcal{P}$ and $\mathcal{Q}$; and these functions form $\mathrm{BA}(\mathcal{P}) \cap \mathrm{BA}(\mathcal{Q})$, which is the intersection of algebras, and so an algebra.

Discrete and indiscrete

Two extreme examples of coherent configurations will be important:

- The indiscrete configuration on Ω consists of the two relations E and $\Omega^2 \setminus E$, where $E = \{(\alpha, \alpha) : \alpha \in \Omega\}$ is the diagonal (the relation of equality).
- The discrete configuration on Ω is the partition of Ω^2 into singleton sets.

Now we can define the meet of two coherent configurations to be the join of all the c.c.s lying below both: this makes sense because at least the discrete configuration lies below both.
With these operations, the coherent configurations on Ω form a lattice.

Partition refinement

More generally, given any partition P of Ω^2, there is a unique coherent configuration which is the coarsest c.c. lying below P. It is constructed from P in a canonical way, so any isomorphism or automorphism of P preserves this configuration.
In particular, a graph gives a partition of Ω^2 into diagonal, edges and non-edges. From this we get a coherent configuration.
We may also "fix" one or more vertices of the graph and again refine to a coherent configuration. This is the basis of the partition refinement algorithm used by almost all graph isomorphism or automorphism software.

Cellular algebras

This process was invented by Boris Weisfeiler, who used coherent configurations for graph isomorphism in the 1960s. He called them (or more precisely their basis algebras) cellular algebras. Unfortunately this term is now used with a different meaning ...
Actually Weisfeiler's structures were a bit more general than Higman's, since he did not require that some of the relations partition the identity.

Orders of primitive groups

In 1979 László Babai used partition refinement to give an elementary proof (i.e. one using combinatorics and probability, and no group theory) that the order of a primitive but not 2-transitive permutation group of degree n is at most $n^{4\sqrt{n}\log n}$.
Using a probabilistic argument, he showed that the coherent configuration obtained by partition refinement from that of the group with $4\sqrt{n}\log n$ fixed points is discrete.
This result is essentially best possible: if $n = m^2$, the order of the wreath product of S_m and S_2 (acting on the square grid) is about $n^{\sqrt{n}}$.
Using the Classification of Finite Simple Groups, we can now obtain more refined results: either a group is "known" or it has *much* smaller order.

Special coherent configurations

A coherent configuration $\mathcal{P}$ is

- homogeneous if the diagonal is a single relation;
- commutative if $\mathrm{BA}(\mathcal{P})$ is commutative;
- symmetric if all the relations are equal to their transposes.

These conditions become strictly stronger in the order given.

Association schemes

Symmetric c.c.s predate the general concept by many years. They were introduced in statistics by R. C. Bose and his students, and called association schemes.
The basis algebra of an association scheme is usually called the Bose–Mesner algebra of the scheme; it was introduced by Bose and Mesner in the 1950s.
To tell the story briefly: In statistics, all data consists of real numbers, and covariance matrices are real symmetric matrices. In order to extract information from the data, it is necessary to invert a large "information matrix". If this belongs to the Bose–Mesner algebra of an association scheme, this inversion can be done by working in the regular representation of the Bose–Mesner algebra, which has much smaller dimension: this was an important consideration in the days before widespread use of computers.

Terminology

In the 1970s, Delsarte showed the usefulness of association schemes in coding theory and design theory; he used the technique of linear programming to give new bounds for codes and designs.
Delsarte's methods worked more generally, for commutative c.c.s (though all his examples were symmetric); he used the term "association scheme" in this more general sense.
Subsequently, other authors have used the term to refer to homogeneous c.c.s, or even to arbitrary c.c.s. Some have even used the shorter term "scheme", which seems ill-advised due to its use in algebraic geometry.
I propose that "association scheme" should be reserved for its original usage of "symmetric c.c.", to avoid confusion.

Jordan algebras

Indeed, symmetric matrices are so important in statistics that, even when they don't commute, it is necessary to deal with them.
One strategy is to weaken the last axiom for an association scheme to the requirement that the span of the relation matrices is closed under the Jordan product $A \circ B = \frac{1}{2}(AB + BA)$.
In this case, Wedderburn's theorem on associative algebras must be replaced by the Jordan–von Neumann–Wigner theorem to decompose the algebra.
These things have not been very much studied. Here is an open problem.

Jordan schemes

We define an Jordan scheme to be a set of relations on Ω which forms a partition of Ω^2, such that the diagonal is one of the relations, each relation is symmetric, and the span of the relation matrices is closed under the Jordan product. (This can be translated into a combinatorial statement.)
If we take a homogeneous coherent configuration and symmetrize it (that is, replace each pair $R, R^\top$ of relations by $R \cup R^\top$), we obtain a Jordan scheme.

Question

Does every Jordan scheme arise in this way?

Stratifiable c.c.s

A coherent configuration is called stratifiable if its symmetrization is an association scheme.
Thus, a commutative c.c. is stratifiable, and a stratifiable c.c. is homogeneous, but examples show that neither of these implications reverses.
The name comes from statistics, where the common eigenspaces of the matrices in the Bose–Mesner algebra of an association scheme are called strata.

The semilattice of association schemes

Unlike general coherent configurations, association schemes do not form a lattice, only an upper semilattice.
The indiscrete c.c. is an association scheme, and the same proof as earlier shows that the join (as partitions) of association schemes is an association scheme.
But the discrete c.c. is not an association scheme. So the argument for producing the meet fails. (Recall that the meet of c.c.s $\mathcal{P}$ and $\mathcal{Q}$ is the join of all c.c.s below both $\mathcal{P}$ and $\mathcal{Q}$. If $\mathcal{P}$ and $\mathcal{Q}$ are association schemes, there may be no association scheme below both of them.)

AS-free and AS-friendly groups

Every permutation group is associated with a coherent configuration. But not every group acts on an association scheme.
We say that a permutation group G is AS-free if there is no G-invariant association scheme on Ω apart from the indiscrete scheme.
We say that G is AS-friendly if there is a unique minimal G-invariant association scheme on Ω.
Of course, if we replaced "AS" by "CC" in the above definitions, then every group would be CC-friendly, and the CC-free groups would be precisely the doubly transitive groups.

Implications

A permutation group G is generously transitive if every two distinct points of Ω can be interchanged by an element of G.

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

$$\begin{array}{ccccccc} 2\text{-transitive} & \Rightarrow & 2\text{-homogeneous} & \Rightarrow & \text{AS-free} & \Rightarrow & \text{primitive} \\ \Downarrow & & \Downarrow & & \Downarrow & & \Downarrow \\ \text{gen. trans.} & \Rightarrow & \text{stratifiable} & \Rightarrow & \text{AS-friendly} & \Rightarrow & \text{transitive} \end{array}$$

None of the implications reverses.

AS-free groups

Note the occurrence of AS-free groups as a class lying between "primitive" and "2-transitive". Our long detour has been simply to reach this class.

Question
Which primitive groups are AS-free?

Recall from the previous lecture the O'Nan–Scott classification:

- A primitive group is non-basic if it preserves a Cartesian structure, or power structure, on Ω;
- A primitive basic group is affine, or diagonal, or almost simple.

Non-basic groups

Recall that a Cartesian structure identifies Ω with the set of all l-tuples over an alphabet A of cardinality k.
Such a structure gives rise to an association scheme: the Hamming distance d_H between two l-tuples is the number of coordinates in which they differ; and the relations of the association scheme are given by

$$R_i = \{(v,w) : v,w \in A^l, d_H(v,w) = i\}.$$

(This is the Hamming scheme, used by Delsarte in his application of association schemes to coding theory.)
So an AS-free group is basic.

Affine groups

An affine group acts on a finite vector space V, and is generated by the translation group of V and a subgroup H of $\mathrm{GL}(V)$.
Recall that G is primitive if and only if H is irreducible, and G is basic if and only if H is primitive (as a linear group!)
Since the translations form an abelian regular normal subgroup N of G, all the basis matrices of the c.c. associated with G belong to the group algebra of N, and thus commute. So G is stratifiable.
So an AS-free group is not affine, unless it is 2-homogeneous.

Diagonal groups

Since I didn't describe diagonal groups very precisely, I will be brief.
A diagonal group with two direct factors in its socle preserves the conjugacy class scheme of a simple group T, where the relations correspond to the inverse pairs of conjugacy classes. Thus the basis algebra lies in the centre of the group algebra of T, and so is commutative, and G is stratifiable, and not AS-free.
A diagonal group with three socle factors preserves the Latin square association scheme associated with the Cayley table of a simple group T, and so cannot be AS-free.

Question

Does there exist an AS-free diagonal group with at least four socle factors?

In fact I would expect that most such groups would be AS-free; but the smallest has degree 216000, so computation is difficult!

Almost simple groups

There are a few almost simple AS-free groups. Some of these were implicitly found by some of Weisfeiler's successors in the USSR (Faradžev, Klin and Muzichuk).
The smallest example is the group $\mathrm{PSL}(3,3)$, acting on the right cosets of $\mathrm{PO}(3,3)$ (a subgroup isomorphic to S_4), with degree 234; this is the smallest AS-free group which is not 2-homogeneous. Other examples of AS-free groups are M_{12}, degree 1320; J_1, degree 1463, 1540 or 1596; and J_2, degree 1800.
The situation is not well understood!