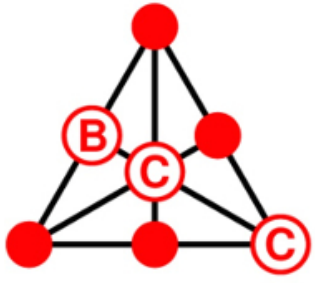
Diagonal semilattices and their graphs

Peter J. Cameron
University of St Andrews

BCC, Durham, July 2021



An analogy

If you know any projective geometry, you will know the following fact:

> Two-dimensional geometries are projective planes and exist in great profusion. But in higher dimension, the geometries are coordinatised by an algebraic object (a division ring), and there is just one geometry for each dimension and each coordinatising algebra.

I am going to tell you a very similar story, for which a similar statement holds:

- In place of "projective planes" we put "Latin squares".
- In place of "division ring" we put "group".
- The role of Desargues' Theorem is taken by the quadrangle condition, defined by Frolov in 1890.

Diagonal groups

The other motivation for this work was to provide geometries for the "diagonal groups", one of the classes in the celebrated O'Nan–Scott Theorem.

According to this theorem, a finite primitive permutation group is of one of four types: affine, Cartesian, diagonal, or almost simple.

Affine groups act on affine spaces, and Cartesian groups on Cartesian lattices (which will be defined shortly); no uniform description of geometry for the almost simple groups is possible. But what about diagonal groups?

The diagonal groups in this theorem are built from finite simple groups; but we remove both assumptions. Our groups are completely arbitrary, finite or infinite, simple or not.

This is joint work with Rosemary Bailey, Cheryl Praeger and Csaba Schneider.

Diagonal groups defined

Let m be a positive integer and T a group, finite or infinite. I define the diagonal group $D(T,m)$ to be the group of permutations of $\Omega = T^m$ generated by the following transformations. (I put the elements of Ω in square brackets to distinguish them from group elements.)

- The group T^m acting by right multiplication.
- another copy T_0 of T acting by simultaneous left multiplication of all coordinates by the inverse.
- $\mathrm{Aut}(T)$ acting in the same way on all coordinates.
- S_m acting by permuting the coordinates.
- An element τ:

$$[t_1, t_2, \ldots, t_m] \mapsto [t_1^{-1}, t_1^{-1}t_2, \ldots, t_1^{-1}t_m].$$

Don't remember the details: this is just a group built from T and m.

Partitions and the partition lattice

Our geometry will be defined in terms of partitions. So here is a brief introduction.
The set $\mathbb{P}(\Omega)$ of partitions of Ω is partially ordered by refinement: $P \preccurlyeq Q$ if every part of P is contained in a part of Q. With this order, $\mathbb{P}(\Omega)$ is a lattice: any two partitions P and Q have a unique infimum or meet $P \wedge Q$, and a unique supremum or join $P \vee Q$.

- $P \wedge Q$ is the partition of Ω whose parts are all *non-empty* intersections of a part of P and a part of Q.
- $P \vee Q$ is the partition into connected components of the graph in which two points are adjacent if they lie in the same part of *either* P or Q.

A subset of $\mathbb{P}(\Omega)$ is a lattice if it is closed under the meet and join operations of $\mathbb{P}(\Omega)$; it is a join-semilattice, closed under join but maybe not under meet.

Cartesian lattices

The Boolean lattice $\mathcal{B}_n$ is the lattice of all subsets of $\{1,\ldots,n\}$.
Let A be an alphabet, finite or infinite (with $|A| > 1$). Let $\Omega = A^n$ be the set of all words of length n over the alphabet A.
For $I \subseteq \{1,\ldots,n\}$, let Q_I be the partition of Ω corresponding to the equivalence relation $\equiv_I$, where

$$(a_1,\ldots,a_n) \equiv_I (b_1,\ldots,b_n) \Leftrightarrow (\forall j \notin I)(a_j = b_j).$$

Now the partitions Q_I for $I \subseteq \{1,\ldots,n\}$ form a sublattice of the partition lattice on Ω which is isomorphic to $\mathcal{B}_n$ by the map $I \mapsto Q_I$.
I will call this a Cartesian lattice. Note that the group of permutations of Ω mapping the lattice to itself (as set of partitions) is the wreath product $\mathrm{Sym}(A)\ Wr\ \mathrm{Sym}(\{1,\ldots,n\})$.

Latin squares, 1

You probably think of a Latin square as something like this: a square array of size $n \times n$ filled with letters from an alphabet of size n, so that each letter occurs once in each row and column.

A	B	C
B	C	A
C	A	B

Latin squares exist in great profusion. There are more than $\exp(m^2)$ Latin squares of order m; exact numbers are only known up to $m = 11$.
We are going to give a different definition. Let Ω consist of the n^2 cells of the array. We have three partitions of Ω: R, the rows; C, the columns; and L, the letters (the partition into sets of cells containing the same letter).

Latin squares, 2

A	B	C
B	C	A
C	A	B

1	2	3
4	5	6
7	8	9

- $R = \{\{1,2,3\},\{4,5,6\},\{7,8,9\}\}$;
- $C = \{\{1,4,7\},\{2,5,8\},\{3,6,9\}\}$;
- $L = \{\{1,6,8\},\{2,4,9\},\{3,5,7\}\}$.

Together with E (the partition into singletons) and U (the partition with a single part), these three partitions form a lattice. It has the very special property that, if one of R, C, L is omitted, the resulting four partitions form a Cartesian lattice on Ω.

This property characterises Latin squares.

Latin squares, 3

With the partition definition, we could define an automorphism of a Latin square to be a permutation of Ω fixing $\{R, C, L\}$ setwise. (These mappings are usually called paratopisms in the Latin squares literature.)
However, one case is interesting to us: the Cayley table of a group T is a Latin square, and its paratopism group is the diagonal group $D(T, 2)$ defined earlier. (This fact is maybe not as well known as it should be!)

Diagonal semilattices

Let us return to diagonal groups for a moment. Recall that $D(T,m)$ acts on T^m, where m copies $T_1,\dots,T_m$ of T act on the corresponding coordinate of T^m by right multiplication, while the last factor T_0 acts by simultaneous left multiplication by the inverse.

Let $Q_0,\dots,Q_m$ be the orbit partitions of $\Omega = T^m$ corresponding to these groups. Thinking of T^m as a group, these are the coset partitions of the coordinate groups $T_1,\dots,T_m$ and the diagonal subgroup of T^m (hence the name).

The join-semilattice generated by $Q_0,\dots,Q_m$ (it is not a lattice for $m \geqslant 3$) is an object which we will call a diagonal semilattice and denote by $\mathcal{D}(T,m)$.

Theorem

The automorphism group of $\mathcal{D}(T,m)$ is the diagonal group $D(T,m)$.

The main theorem

Theorem

Let $m \geqslant 2$, and let $Q_0, Q_1, \ldots, Q_m$ be partitions of Ω. Suppose that any m of these partitions are the minimal non-trivial elements in an m-dimensional Cartesian lattice on Ω.

- *If $m = 2$, then $\{Q_0, Q_1, Q_2\}$, together with E and U, form a Latin square, unique up to isotopism; every Latin square arises in this way.*
- *If $m \geqslant 3$, then there is a group T, determined up to isomorphism, such that the join-semilattice generated by $\{Q_0, \ldots, Q_m\}$ is the diagonal semilattice $\mathcal{D}(T, m)$.*

As promised, for $m = 2$ the situation is chaotic, but for $m \geqslant 3$ the algebraic structure coordinatising the semilattice (the group T) emerges naturally from the combinatorics.

A word about the proof

The proof is by induction on m. For $m = 2$, there is nothing to prove; and the general case follows by induction from the case $m = 3$. That is where the real work lies!
For $m = 3$, we have four partitions $Q_0, \ldots, Q_3$. For any i, the three partitions $Q_i \vee Q_j$ (for $j \neq i$) define a Latin square on the set of parts of Q_i. We have to show:

- All four Latin squares are isotopic.
- One of them satisfies the quadrangle condition, and so is isotopic to the Cayley table of a group, by Frolov's theorem.
- By a theorem of Albert, all the groups are isomorphic, and the partitions form a diagonal semilattice $\mathcal{D}(T, 3)$.

The diagonal graph

Let $\mathcal{D}(T, m)$ be a diagonal structure, with $m \geq 2$. Form a graph $\Gamma(T, m)$ on Ω by joining two points if they lie together in a part of one of the minimal partitions Q_i.
Note that this construction applied to the Cartesian lattice gives the famous Hamming graph.

- For $m = 2$, the diagonal graph is the strongly regular Latin square graph associated with the Latin square.
- For $|T| = 2$, it is the distance-transitive folded cube graph.

In other cases, it is not distance-regular, but is still a very nice graph whose automorphism group is the diagonal group (except in a couple of small cases).

The diagonal graph, 2

We have computed the spectrum of the diagonal graph, using Möbius inversion.
We also have some information about its chromatic number, which turns out to be related to the Hall–Paige conjecture and synchronizing automata. Note that the clique number is $|T|$ in general: the parts of the partitions Q_i are the mimimal cliques.

Proposition

If m is odd, or if $|T|$ is odd, or if the Sylow 2-subgroups of T are not cyclic, then the chromatic number of $\Gamma(T, m)$ is equal to $|T|$.

We conjecture that in the excluded case, the chromatic number is equal to $|T| + 2$. This is true if $T \cong C_2$ (the non-bipartite folded cubes have chromatic number 4) and if $m = 2$ and $T \cong C_4$ (the complement of the Shrikhande graph has chromatic number 6).

Synchronizing automata

An automaton is a very simple machine: it has a set Ω of internal states; when it reads a letter from its alphabet A, it changes state in a deterministic fashion.
It can read a word, and undergo a sequence of transitions. So the set of possible transitions is closed under composition, and contains the identity: it is a monoid. So an automaton is equivalent to a transformation monoid with a fixed generating set.
An automaton is synchronizing if there is a word (called a reset word) such that, when the automaton reads that word, it ends in a fixed state, independent of its starting state.
The Černý conjecture (still open after 60 years) asserts that, if an n-state automaton is synchronizing, then it has a reset word of length at most $(n-1)^2$.

Synchronizing permutation groups

A transformation monoid is synchronizing if it contains a transformation of rank 1 (that is, one whose image is a singleton).
Clearly a permutation group of degree greater than 1 cannot be synchronizing in this sense. So we abuse language and say that a permutation group G on Ω is synchronizing if and only if, for any non-permutation f on Ω, the monoid $\langle G, f \rangle$ is synchronizing.
It is known that a permutation group is non-synchronizing if and only if it is contained in the automorphism group of a graph with clique number equal to chromatic number.

It is known that a synchronizing permutation group must be primitive, and hence (by O'Nan–Scott) affine, wreath product, diagonal, or almost simple.
Wreath products preserve Hamming graphs, and so are non-synchronizing. For the other three types, both synchronizing and non-synchronizing groups exist.
However, we can say more in the diagonal case. If the diagonal group $D(T,m)$ is primitive, then T is simple, and so its Sylow 2-subgroups cannot be non-trivial cyclic groups (by Burnside's transfer theorem); so, if $m \geq 2$, then $D(T,m)$ is non-synchonizing. So in this case, synchronizing groups can arise only for $m = 1$.