AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **75(3)** (2019), Pages 357–364

Association schemes for diagonal groups

Peter J. Cameron

School of Mathematics and Statistics
University of St Andrews
North Haugh, St Andrews, KY16 9SS
U.K.

Sean Eberhard

Centre for Mathematical Sciences
University of Cambridge
Wilberforce Road, Cambridge, CB3 0WB
U.K.

Abstract

For any finite group G, and any positive integer n, we construct an association scheme which admits the diagonal group $D_n(G)$ as a group of automorphisms. The rank of the association scheme is the number of partitions of n into at most $|G|$ parts, so is $p(n)$ if $|G| \geq n$; its parameters depend only on n and $|G|$. For $n = 2$, the association scheme is trivial, while for $n = 3$ its relations are the Latin square graph associated with the Cayley table of G and its complement.

A transitive permutation group G is said to be *AS-free* if there is no non-trivial association scheme admitting G as a group of automorphisms. A consequence of our construction is that an AS-free group must be either 2-homogeneous or almost simple.

We construct another association scheme, finer than the above scheme if $n > 3$, from the Latin hypercube consisting of n-tuples of elements of G with product the identity.

1 Introduction

An *association scheme* consists of a finite set Ω and a collection of non-empty binary relations $R_1, \ldots, R_r$ (where r is the *rank* of the scheme) such that

(a) the relations form a partition of Ω^2;

(b) one of the relations (say R_1) is equality;

(c) all relations are symmetric;

ISSN: 2202-3518

(d) given $i, j, k \in \{1, \ldots, r\}$, there is a non-negative integer p_{ij}^k such that, for all $(a, b) \in R_k$, there are exactly p_{ij}^k points $c \in \Omega$ such that $(a, c) \in R_i$ and $(c, b) \in R_j$.

In the literature, conditions (b) and (c) are sometimes relaxed. But it is important for our application to keep these conditions. (See [1, 3] for discussion of this point.)

Representing the relations R_i by matrices A_i, the conditions in the definition can be expressed as follows:

(a) $A_1 + \cdots + A_r = J$, where J is the all-1 matrix;

(b) $A_1 = I$, the identity matrix;

(c) each matrix A_i is symmetric;

(d) for any i, j, k, we have $A_i A_j = \sum_{k=1}^{r} p_{ij}^k A_k$; so the span of $A_1, \ldots, A_r$ over $\mathbb{R}$ is an algebra (whose structure constants p_{ij}^k relative to this basis are non-negative integers).

See [2] for more on association schemes.

Let G be a group and n an integer at least 2. The *diagonal group* $D_n(G)$ is a permutation group of degree $|G|^{n-1}$, acting on the set of right cosets in G^n of the *diagonal subgroup* $\{(g, g, \ldots, g) : g \in G\}$. It is generated by the following elements:

(i) the group G^n acting by right multiplication;

(ii) the automorphism group of G, acting simultaneously on each coordinate;

(iii) the symmetric group S_n, permuting the coordinates.

(Permutations in (ii) and (iii) have well-defined actions since the diagonal subgroup is preserved by these elements.) It is well known that

- $D_n(G)$ is a faithful action of the group $(G^n)(\mathrm{Out}(G) \times S_n)$ if and only if G has trivial centre;
- $D_n(G)$ is primitive if and only if G is characteristically simple.

From now on, throughout the paper, we assume that G is finite. (Infinite diagonal groups are well-defined, but association schemes only make sense on finite sets.)

In the case where G is a finite simple group, these "simple diagonal groups" and their primitive subgroups form one of the classes in the O'Nan–Scott theorem [4, Theorem 4.1A].

The trivial association scheme has just two relations, equality and inequality; its automorphism group is the symmetric group. More generally, we regard a structure as being *trivial* if it is invariant under the symmetric group.

In [3], a permutation group G on Ω is said to be *AS-free* if it is not contained in the automorphism group of a non-trivial association scheme. This definition is similar in spirit to many classical definitions in permutation group theory. For example, a group is

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

It is shown in [3] that an AS-free group must be 2-homogeneous, or almost simple, or of diagonal type $D_n(G)$ with $n \geq 4$ and G simple. Our purpose here is to construct an association scheme invariant under the diagonal group, and hence show that the last case cannot occur.

2 The pre-association scheme

We begin by constructing a "pre-association scheme" on the set G^n (a structure satisfying conditions (a), (c) and (d) of the definition, but with (b) replaced by "R_1 is an equivalence relation on Ω"). Then factoring out the equivalence relation gives the required association scheme.

Our structure has one relation R_π for each partition π of the set $\{1, \ldots, n\}$, defined by the rule that for two n-tuples $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$,

$$a \; R_\pi \; b \text{ if and only if } (a_i b_i^{-1} = a_j b_j^{-1}) \Leftrightarrow (i \equiv_\pi j),$$

where $i \equiv_\pi j$ means that i and j belong to the same part of π. The matrices of these relations are symmetric and sum to the all-1 matrix. We prove that their span over $\mathbb{R}$ is closed under multiplication.

Let A_π be the matrix of the relation R_π, the $|G|^n \times |G|^n$ matrix whose (a, b) entry is 1 if $a \; R_\pi \; b$, 0 otherwise. Let B_π be the matrix of the relation S_π defined by

$$a \; S_\pi \; b \text{ if and only if } (i \equiv_\pi j) \Rightarrow (a_i b_i^{-1} = a_j b_j^{-1}).$$

Thus we have

$$B_\pi = \sum_{\pi \preceq \sigma} A_\sigma,$$

where $\preceq$ is the order in the lattice of partitions of $\{1, \ldots, n\}$ ordered by refinement, with finer partitions below coarser ones. Now Möbius inversion in the lattice of set partitions (see Stanley [9, Section 3.7]) shows that the A_π can be expressed as linear combinations of the B_σ. Thus the A and B matrices have the same span, and it suffices to show that the span of the B matrices is closed under multiplication. (The structure constants p_{ij}^k will then be non-negative integers since the matrices A_π are zero-one matrices with pairwise disjoint supports.)

The (a, b) entry of $B_\pi B_\sigma$ counts the number of n-tuples c such that $a\ S_\pi\ c$ and $c\ S_\sigma\ b$. This means that the ratios $a_i c_i^{-1}$ agree on parts of π, while the ratios $c_i b_i^{-1}$ agree on parts of σ. This is zero unless the ratios $a_i b_i^{-1}$ agree on parts of $\tau = \pi \wedge \sigma$. Assuming this does hold, we choose elements u_i and v_i such that u_i is constant on parts of π and v_i constant on parts of σ, and such that $u_i v_i = a_i b_i^{-1}$ for all i.

We claim that this can be done in $|G|^{|\pi\vee\sigma|}$ ways, where $|\rho|$ denotes the number of parts of ρ. For if we choose the value u_i, then the value of v_i is determined. Moreover, u_i is constant on parts of π, so v_j is determined on these parts; and v_j is constant on parts of σ, so u_j is determined on these. We see that the values are determined on a part of $\pi \vee \sigma$ by the choice, and the results follow.

Now each choice as above gives a unique c such that

$$a_i c_i^{-1} = u_i, \qquad c_i b_i^{-1} = v_i,$$

so the result is proved.

It is clear that these relations are invariant under right multiplication by all elements of G_n, since $(a_i g_i)(b_i g_i)^{-1} = a_i b_i^{-1}$. They are invariant under other transformations:

(i) left multiplication by elements of H, since

$$(xa_i)(xb_i)^{-1} = x(a_i b_i^{-1})x^{-1};$$

(ii) automorphisms of G acting coordinatewise.

3 Taking the quotient

The orbits of H acting by left multiplication as in (i) above are precisely the right cosets of H in G^n. Invariance of the relations above shows that the quotient of the structure by this equivalence relation has corresponding relations $\bar{R}_\pi$ induced on it. Now, if π is the universal relation, then R_π is precisely the relation of lying in the same right coset of H, and so $\bar{R}_\pi$ is the relation of equality. So, as well as the other relations defined above, we have recovered the one missing axiom for association schemes.

Thus, we have constructed an association scheme on $H\backslash G^n$ (the set of right cosets of H) invariant under right translation by G^n and automorphisms of G acting coordinatewise.

To reach the full diagonal group we need to adjoin the symmetric group. This clearly does not preserve the relations $\bar{R}_\pi$, but it induces "weak automorphisms" of the association scheme; that is, it permutes these relations among themselves. Taking the unions of orbits of S_n on the relations $\bar{R}_\pi$, we obtain an association scheme, whose relations are indexed by the orbits of S_n on set partitions of $\{1, \ldots, n\}$; that is, simply the partitions of the integer n, expressions of n as a sum of positive integers with the summands in non-increasing order. See [2, Theorem 8.17].

The valency of the relation R_π in the pre-association scheme is the number of ordered $|\pi|$-tuples of distinct elements of G, and so is non-zero if and only if $|G| \geq |\pi|$. In particular, all relations are non-empty if and only if $|G| \geq n$. Passing to the quotient divides the valency by $|G|$, and merging orbits under S_n multiplies by the number of set-partitions corresponding to a given partition of n. So, the rank is equal to the number of partitions of n into at most $|G|$ parts, and is equal to $p(n)$ if and only if $|G| \geq n$. (Thanks to Cheryl Praeger for this observation.)

To summarise:

Theorem 1 *There is an association scheme on $H\backslash G^n$ with rank equal to the number of partitions of n with at most $|G|$ parts, (so $p(n)$ if and only if $|G| \geq n$), which is invariant under the diagonal group $D_n(G)$.*

For example, when $n = 3$, we obtain the Latin square graph of the Cayley table of G and its complement. The valency of the complement is $(|G| - 1)(|G| - 2)$, so it is non-empty if and only if $n > 2$.

4 AS-free groups

As noted above, a permutation group is *AS-free* if it preserves no non-trivial association scheme. A transitive permutation group is *primitive* if it preserves no non-trivial equivalence relation on its domain; a primitive group is *basic* if it preserves no Cartesian structure on its domain [7]. Moreover, a permutation group is 2-*homogeneous* if it acts transitively on the set of 2-element subsets of its domain; and a group G is *almost simple* if $T \leq G \leq \mathrm{Aut}(T)$ for some non-abelian finite simple group T.

Theorem 2 *An AS-free permutation group is primitive and basic, and is either* 2-*homogeneous or almost simple.*

Proof This is a combination of a theorem in [3] and the result of this note. Specifically, if G is imprimitive, then it preserves the *group-divisible* association scheme, whose relations are "equal", "same part of the G-invariant partition", and the rest. If G is primitive but not basic, it preserves a Hamming scheme (see [2]). If G is basic, then according to the O'Nan–Scott Theorem, it is affine (that is, has an elementary abelian regular normal subgroup), or diagonal, or almost simple. If G is affine, then the matrices of the G-orbits on pairs belong to the group algebra of the regular normal subgroup, and so commute; adding each non-symmetric matrix to its transpose then gives an association scheme, whose rank is the number of G-orbits on 2-sets plus one (for the diagonal), so is trivial if and only if G is 2-homogeneous. If G is contained in $D_n(T)$ for some non-abelian simple group T, then G preserves the symmetrised conjugacy class scheme of T. And finally, if G is contained in $D_n(T)$ for

$n > 2$, then G preserves the association scheme constructed above, which is trivial only in the case $n = 2$. (We have $|T| \geq 60$, so relations corresponding to partitions with at most 60 parts are non-empty.)

Note that any 2-homogeneous group is AS-free. There exist AS-free almost simple groups which are not 2-homogeneous, but the situation is not well understood. We record here some examples taken from [3]:

- PSL(3, 3) and PSL(3, 3).2, degree 234 (numbers $(234, 1)$ and $(234, 2)$ in the GAP list);
- M_{12}, degree 1320 (number $(1320, 1)$);
- J_1, degree 1463, 1540 or 1596 (numbers $(1463, 1)$, $(1540, 1)$ and $(1596, 1)$);
- J_2, degree 1800 (number $(1800, 1)$).

5 Further remarks

5.1 Latin squares

A Latin square of order n can be regarded as an orthogonal array of strength 2 with 3 factors [5, p. 2]: this means that we can represent it with a set of n^2 triples of the form (row,column,entry) so that, in any pair of positions, each of the n^2 possible entries occurs exactly once. If G is a group, we can describe the orthogonal array coming from the Cayley table of G very simply: it is the set of triples $(x, y, z) \in G^3$ with $xyz = 1$. It is clear that this set is invariant under G^3 acting as follows:

$$(g, h, k) : (x, y, z) \mapsto (h^{-1}xk, k^{-1}yg, g^{-1}zh).$$

Moreover, the set also admits automorphisms of G acting coordinatewise, as well as permutations of the three coordinates with a small twist: $xyz = 1$ implies $yzx = 1$ and $z^{-1}y^{-1}x^{-1} = 1$, so odd permutations must be combined with inversion. So this set of triples admits $D_3(G)$ (though the action is slightly different from the one described earlier).

The corresponding Latin square, as an $n \times n$ array, is obtained by indexing rows and columns by G and writing z in the (x, y) cell if $xyz = 1$. The "traditional" Cayley table has z in position (x, y) if $z = xy$. For the record, we match up these two representations with ours.

- The usual Latin square has (x, y) entry $(xy)^{-1}$, so is obtained from the traditional description by the permutation of letters which replaces each letter by its inverse.
- Represent the cosets of H in G^3 by noting that each coset contains a unique element of the form $(x, y, 1)$; we regard this as indexing a cell (x, y) of a square array. Now the relation corresponding to the partition $2 + 1$ of 3 makes two

of the three coordinate ratios equal. So consider two coset representatives $(a_1, a_2, 1)$ and $(b_1, b_2, 1)$. If the first and third coordinate ratios are equal then $a_1 = b_1$; so this is the relation "same row". Similarly, equality of the second and third rations is the relation "same column". In the remaining case, $a_1 b_1^{-1} = a_2 b_2^{-1}$, which is equivalent to $a_2^{-1} a_1 = b_2^{-1} b_1$; so this is the relation "same letter" if we put entry $y^{-1}x$ in cell (x, y). So this Latin square is obtained from the orthogonal array form by the permutation of columns which replaces each column label by its inverse.

We now extend this to higher dimensions. A group G defines a Latin hypercube L, the set of n-tuples $(g_1, \ldots, g_n)$ of group elements whose product is the identity; these form an orthogonal array of strength $n - 1$. The set is invariant under cyclic permutations of the group elements, and reversal together with inversion: $(g_1, \ldots, g_n) \mapsto (g_n^{-1}, \ldots, g_1^{-1})$. Now we can define a map from G^n to L by the rule

$$(a_1, \ldots, a_n) \mapsto (g_1 = a_1^{-1}a_2, g_2 = a_2^{-1}a_3, \ldots, g_n = a_n^{-1}a_1).$$

This map is invariant under left multiplication by elements of H, so induces a bijection $H\backslash G^n \to L$. Now the cyclic shift on L is realised by the cyclic shift on $H\backslash G^n$, while the reversal-and-inversion of L is induced by reversal on $H\backslash G^n$. Thus the dihedral group is a group of weak automorphisms of the association scheme on $H\backslash G^n$ with relations R_π, and fusing orbits gives an association scheme. This association scheme does not admit the full diagonal group, since only elements of the dihedral group act as coordinate permutations. (In the case $n = 3$, the dihedral group is equal to the full symmetric group.)

5.2 Isomorphisms

There exist superexponentially many strongly regular graphs with certain parameters, for example Latin square graphs.

Our construction potentially gives many (though not superexponentially many) non-isomorphic association schemes of relatively large rank with the same parameters. As noted earlier, the parameters depend only on n and $|G|$, so we can choose an order for which many groups exist. It is known that the number of groups of order $q = 2^d$ is about $q^{c(\log_2 q)^2}$, with $c = \frac{2}{27}$ [6, 8]. However, we have not proved that non-isomorphic groups give non-isomorphic association schemes. We hope that work in progress by the first author with Bailey, Praeger and Schneider will resolve this in the affirmative for diagonal groups $D_n(G)$ for $n > 2$.

References

[1] P. P. Alejandro, R. A. Bailey and P. J. Cameron, Association schemes and permutation groups, *Discrete Math.* **266** (2003), 47–67.

[2] R. A. Bailey, *Association Schemes: Designed Experiments, Algebra and Combinatorics*, Cambridge University Press, Cambridge, 2004.

[3] Peter J. Cameron, Coherent configurations, association schemes, and permutation groups, pp. 55-71 in Groups, Combinatorics and Geometry (ed. A. A. Ivanov, M. W. Liebeck and J. Saxl), World Scientific, Singapore, 2003.

[4] John D. Dixon and Brian Mortimer, *Permutation Groups*, Springer, New York, 1996.

[5] A. S. Hedayat, N. J. A. Sloane and John Stufken, *Orthogonal Arrays: Theory and Applications*, Springer-Verlag, New York, 1999.

[6] Graham Higman, Enumerating p-groups, I: Inequalities, *Proc. London Math. Soc.* (3) **10** (1960), 24–30.

[7] C. E. Praeger and C. Schneider, *Permutation Groups and Cartesian Decompositions*, London Math. Soc. Lecture Notes **449**, Cambridge University Press, Cambridge, 2018.

[8] Charles C. Sims, Enumerating p-groups, *Proc. London Math. Soc.* (3) **15** (1965), 151–166.

[9] Richard Stanley, *Enumerative Combinatorics*, Volume 1, Cambridge University Press, Cambridge, 1997.

(Received 16 May 2019; revised 11 Oct 2019)