The diagonal graph

R. A. Bailey and Peter J. Cameron
School of Mathematics and Statistics, University of St Andrews,
North Haugh, St Andrews, Fife, KY16 9SS, U.K.

Abstract

According to the O'Nan–Scott Theorem, a finite primitive permutation group either preserves a structure of one of three types (affine space, Cartesian lattice, or diagonal semilattice), or is almost simple. However, diagonal groups are a much larger class than those occurring in this theorem. For any positive integer m and group G (finite or infinite), there is a diagonal semilattice, a sub-semilattice of the lattice of partitions of a set Ω, whose automorphism group is the corresponding diagonal group. Moreover, there is a graph (the diagonal graph), bearing much the same relation to the diagonal semilattice and group as the Hamming graph does to the Cartesian lattice and the wreath product of symmetric groups.

Our purpose here, after a brief introduction to this semilattice and graph, is to establish some properties of this graph. The diagonal graph $\Gamma_D(G,m)$ is a Cayley graph for the group G^m, and so is vertex-transitive. We establish its clique number in general and its chromatic number in most cases, with a conjecture about the chromatic number in the remaining cases. We compute the spectrum of the adjacency matrix of the graph, using a calculation of the Möbius function of the diagonal semilattice. We also compute some other graph parameters and symmetry properties of the graph.

We believe that this family of graphs will play a significant role in algebraic graph theory.

1 Introduction

Let m be a positive integer and G a group, finite or infinite. The *diagonal group* $D(G,m)$ is the group of permutations of G^m generated by the following transformations:

- G^m, acting by right multiplication;
- G, acting diagonally by left multiplication (that is, the element x of G induces the map $(g_1, \ldots, g_m) \mapsto (x^{-1}g_1, \ldots, x^{-1}g_m)$);
- automorphisms of G, acting coordinatewise;
- the symmetric group $\mathrm{Sym}(m)$, acting by permuting the coordinates;
- the map $(g_1, g_2, \ldots, g_m) \mapsto (g_1^{-1}, g_1^{-1}g_2, \ldots, g_1^{-1}g_m)$.

It is a transitive permutation group of order $|G|^m \cdot |\operatorname{Aut}(G)| \cdot (m+1)!$ see [4, Section 1.3].

Diagonal groups play an important role in the O'Nan–Scott theorem describing finite primitive permutation groups, given in [14]. One of the types which occur consists of the *simple diagonal groups*, subgroups of $D(G, m)$ where G is a non-abelian finite simple group.

In the case that $m = 1$, the diagonal group $D(G, 1)$ is the group of permutations of G generated by left and right translation, automorphisms, and inversion. In this case there is no geometry associated with the group, although it does preserve a fusion of the *conjugacy class association scheme* of G; we do not consider this case further, but usually assume that $m \geqslant 2$ in what follows.

We now outline the contents of the paper. We give a brief introduction to the lattice of partitions of a set in Section 2; then we define the semilattice $\mathcal{D}(G, m)$ associated with the diagonal group $D(G, m)$, and the corresponding *diagonal graph* $\Gamma_D(G, m)$. We identify this graph with the Latin square graph of the Cayley table of G if $m = 2$, and with the folded cube if $G = C_2$, and give an example satisfying neither of these conditions.

Sections 4 and 5 calculate the Möbius function of the diagonal semilattice and use this to find the spectrum of the diagonal graph. Section 6 states a theorem and conjecture on the chromatic number of the diagonal graph. The final section gives some further properties of the diagonal graph: it is a Cayley graph, but not in general either edge-transitive or distance-regular; we give a formula for its diameter.

2 The partial order on partitions

In this section, we briefly remind readers about the partial order on partitions.

Let P and Q be two partitions of a given set Ω. Then P is defined to be *finer* than Q, written $P \prec Q$, if every part of P is contained in a single part of Q but $P \neq Q$. Write $P \preccurlyeq Q$ to mean that $P \prec Q$ or $P = Q$. Then $\preccurlyeq$ is a partial order.

If $|\Omega| \geqslant 2$ then there are two trivial partitions of Ω. The universal partition U has a single part; at the other extreme, the parts of the equality partition E are all singletons. Thus $E \preccurlyeq P \preccurlyeq U$ for every partition P of Ω.

The *meet* $P \wedge Q$ of P and Q is the partition whose parts are all non-empty intersections of a part of P with a part of Q. Thus $P \wedge Q \preccurlyeq P$, $P \wedge Q \preccurlyeq Q$, and, if R is any partition of Ω satisfying $R \preccurlyeq P$ and $R \preccurlyeq Q$, then $R \preccurlyeq P \wedge Q$.

The dual notion is the *join* $P \vee Q$ of P and Q. Draw a graph with vertext-set Ω, joining two distinct vertices if they lie in the same part of P or the same part of Q. Then the parts of $P \vee Q$ are the connected components of this graph. It follows that $P \preccurlyeq P \vee Q$, $Q \preccurlyeq P \vee Q$, and, if R is any partition of Ω satisfying $P \preccurlyeq R$ and $Q \preccurlyeq R$, then $P \vee Q \preccurlyeq R$.

A set of partitions which is closed under both join and meet is called a *lattice*. We have to consider sets which are closed under join but not under meet; such a set is called a *join semilattice*. See the next section for how our examples arise.

Partial orders are often represented by *Hasse diagrams*. For a collection of partitions of a set, there is one dot for each partition. If $P \prec Q$ then the dot for P is lower in the diagram than the dot for Q. If, in addition, there is no partition R in the collection with $P \prec R \prec Q$, then there is a line joining the dots for P and Q. We give two examples in the next section.

Given any partially ordered set $\mathcal{S}$, its *zeta function* is the $\mathcal{S} \times \mathcal{S}$ matrix defined by $\zeta(P,Q) = 1$ if $P \preccurlyeq Q$ and $\zeta(P,Q) = 0$ otherwise. This matrix is invertible, and it inverse is called the *Möbius function* μ for $\mathcal{S}$. See [13].

From this definition, the *Möbius inversion formula* follows:

Proposition 2.1 *Let $\mathcal{S}$ be a partially ordered set, and F and G two functions from $\mathcal{S} \times \mathcal{S}$ to $\mathbb{R}$ which take the value 0 on a pair (P,Q) unless $P \preccurlyeq Q$. If*

$$G(P,Q) = \sum_{P \preccurlyeq S \preccurlyeq Q} F(S,Q),$$

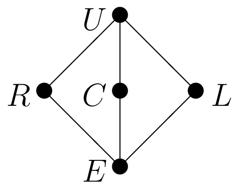

Figure 1: The Hasse diagram for a Latin square

then

$$F(P,Q) = \sum_{P \preccurlyeq S \preccurlyeq Q} \mu(P,S)G(S,Q).$$

3 Diagonal semilattice and diagonal graph

We begin by defining some (semi)lattices of partitions of a set Ω.

A *Latin square* is usually defined as a square array of size $q \times q$ with entries from an alphabet of size q. We can interpret this as a lattice of partitions of the cells of the array containing five partitions $\{E, R, C, L, U\}$, where E is the partition into singletons, U is the partition with a single part, and R, C and L are the partitions into rows, columns, and letters. We have $R \wedge C = R \wedge L = C \wedge L = E$ and $R \vee C = R \vee L = C \vee L = U$. The set $\{E, R, C, L, U\}$ of partitions determines the Latin square up to paratopism. The Hasse diagram is shown in Figure 1. Two Latin squares are *paratopic* if one can be obtained from the other by independent permutations of rows, columns and letters, followed by a permutation of the three partitions R, C, L. The map producing this change is a *paratopism.* This is the natural notion of isomorphism for Latin squares. In group-theoretic terms, a paratopism is an element of the *wreath product* $\mathrm{Sym}(q) \wr Sym(3)$.

If $\Omega = A^m$ (the set of m-tuples over an alphabet A), we define the m-dimensional *Cartesian lattice* to be the lattice consisting of the partitions Q_I for all $I \subseteq \{1, \ldots, m\}$, where Q_I corresponds to the equivalence relation in which two m-tuples are equivalent if they agree in all coordinates outside the subset I. It is isomorphic to the Boolean lattice of subsets of the set $\{1, \ldots, m\}$ by the map $I \mapsto Q_I$ for all $I \subseteq \{1, \ldots, m\}$.

Let G be a group and m a positive integer. In the first section we defined

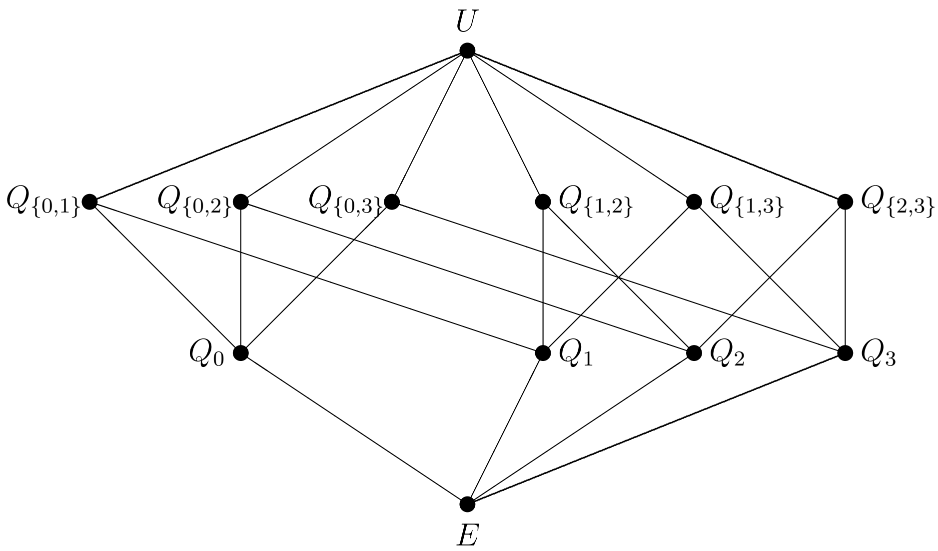

Figure 2: The Hasse diagram for a diagonal semi-lattice with dimension 3

the diagonal group $D(G, m)$ as a permutation group on the set $\Omega = G^m$. Now we construct on Ω a semilattice of partitions, and a graph, which admit the diagonal group as a group of automorphisms.

For $1 \leqslant i \leqslant m$, let Q_i be the partition of Ω defined by the equivalence relation $\equiv_i$, where

$$(g_1, \ldots, g_m) \equiv_i (h_1, \ldots, h_m) \Leftrightarrow (\forall j \neq i)(g_j = h_j);$$

this is the orbit partition of the jth coordinate subgroup of G^m. Also, let Q_0 be the orbit partition of the group G acting on Ω by left multiplication, that is, corresponding to the equivalence relation $\equiv_0$ defined by

$$(g_1, \ldots, g_m) \equiv_0 (h_1, \ldots, h_m) \Leftrightarrow (\exists x \in G)(\forall i)(h_i = xg_i).$$

The *diagonal semilattice* $\mathcal{D}(G, m)$ is the join-semilattice generated by the partitions $Q_0, Q_1, \ldots, Q_m$. Figure 2 shows the Hasse diagram of $\mathcal{D}(G, 3)$.

Note that, in a Latin square (regarded as a partition lattice) or a diagonal semilattice, if there are $m + 1$ minimal non-trivial partitions, then any m of them generate, by taking joins, a Cartesian lattice (in the Latin square case, a square grid). Also, the diagonal semilattice $\mathcal{D}(G,2)$ is isomorphic to the lattice defined by a Latin square which is the Cayley table of G.

Now we can state the main theorems of [4].

Theorem 3.1 *Let $m \geq 2$, and let Ω be a set and $Q_0, Q_1, \ldots, Q_m$ a set of partitions of Ω. Suppose that any m of these partitions are the minimal non-trivial elements of a lattice that is isomorphic to a Cartesian lattice.*

(a) If $m = 2$, then the three partitions together with the trivial partitions E and U form a Latin square, unique up to paratopism.

(b) If $m \geq 3$, then there is a group G, unique up to isomorphism, such that the $m+1$ partitions generate the diagonal semilattice $\mathcal{D}(G,m)$.

Theorem 3.2 *Let G be a group and $m \geq 2$. Then the automorphism group of the diagonal semilattice $\mathcal{D}(G,m)$ is the diagonal group $D(G,m)$ defined earlier.*

Note that, by "automorphism group of the diagonal semilattice", we mean the group of permutations of Ω preserving all the partitions of the semilattice, not the group of order-preserving permutations of the semilattice as poset.

For example, the automorphism group of the diagonal semilattice $\mathcal{D}(C_3,3)$ whose Hasse diagram is shown in Figure 2 is $C_3^3 \rtimes (C_2 \times C_4)$; this group is `PrimitiveGroup(27,8)` in the computer algebra system `GAP` [8].

Associated with a semilattice satisfying the hypotheses of Theorem 3.1 is a graph, defined as follows: the vertex set is $\Omega = G^m$; two vertices are adjacent if they are contained in a part of one of the partitions $Q_0, \ldots, Q_m$. If $m = 2$ and Q_0, Q_1, Q_2 are the rows, columns and letters of a Latin square Λ, then this graph is precisely the *Latin square graph* associated with Λ. If $Q_0, \ldots, Q_m$ are the minimal non-trivial partitions in a diagonal semilattice $\mathcal{D}(G,m)$, then the graph is the *diagonal graph*, which we denote by $\Gamma_D(G,m)$.

For later use, we note that, if $m = 1$, the diagonal semilattice has just two partitions E and U (indeed $Q_0 = Q_1 = U$), and the diagonal graph is a complete graph of order $|G|$.

Theorem 3.3 *If $m > 2$, or if $m = 2$ and $|G| > 4$, then the automorphism group of the diagonal graph $\Gamma_D(G,m)$ is the diagonal group $D(G,m)$.*

We conclude this section with further examples.

Example 1 Take $G = C_2$, the cyclic group of order 2. Then the vertex set of $\Gamma_D(C_2, m)$ is the set of all binary m-tuples, and the partitions $Q_1, \dots, Q_m$ correspond to the usual parallel classes of edges of the m-dimensional cube, while Q_0 consists of the antipodal pairs of vertices. So $\Gamma_D(m, C_2)$ is the m-cube with antipodal vertices joined. This is the *folded cube* (see [6, p. 264]).

Example 2 Let $m = 3$ and $G = C_3$. Let x be a generator of G, and put $a = (x, 1, 1)$, $b = (1, x, 1)$ and $c = (1, 1, x)$. Then $\Omega = G^3$ and the parts of Q_0, Q_1, Q_2 and Q_3 are the (right) cosets of the subgroups $\langle abc\rangle$, $\langle a\rangle$, $\langle b\rangle$ and $\langle c\rangle$ respectively. The vertices of the diagonal graph $\Gamma_D(G, 3)$ are the elements of G^3. Let g and h be two such vertices. These are joined by an edge if and only if gh^{-1} is one of a, a^2, b, b^2, c, c^2, abc and $a^2b^2c^2$. Thus $\Gamma_D(G, 3)$ is regular with valency 8.

Vertices 1 and ab are at distance two. Their common neighbours are a, b, c^2 and abc^2. Vertices 1 and a^2b are also at distance two, but their common neighbours are only a^2 and b. Therefore this diagonal graph is not distance-regular in the sense of [6].

4 The Möbius function of the diagonal semilattice

Let m be a natural number greater than 1. Let $Q_0, \dots, Q_m$ be $m+1$ partitions of a set Ω with the property that any m of them are the minimal elements of a Cartesian lattice of partitions of Ω. Let q be the (constant) size of a part of one of the Q_i. (The constancy of q is shown in [4]; here is a self-contained argument. Each partition Q_i belongs to a Cartesian decomposition, so its parts have constant size q_i; thus, for any j, $|\Omega|$ is equal to the product of the q_i for $i \neq j$. Since these numbers are all equal, q_i is independent of i.)

By Theorem 3.1, either $m = 2$ and Q_0, Q_1, Q_2 are the row, column and letter partitions of the set of cells of a Latin square (unique up to paratopism), or $m \geqslant 3$ and $Q_0, \dots, Q_m$ are the minimal partitions of the diagonal semilattice $\mathcal{D}(G, m)$ of dimension m over a group G (unique up to isomorphism), with automorphism group the diagonal group $D(G, m)$.

In the case $m = 2$, the graph with vertex set Ω, with edges joining two elements of Ω if and only if they are contained in a part of one of the three partitions, is the Latin square graph associated with the Latin square. Latin square graphs form a prolific family of *strongly regular graphs*: they give rise to more than exponentially many such graphs with the same parameters on a given (square) number of vertices. The spectrum of a Latin square graph is well known. We extend this to higher-dimensional diagonal graphs. First, we compute the *Möbius function* [13] of the diagonal semilattice. For each partition S in the semilattice, let $\rho(S)$ be its *rank*, which is the number of steps in a maximal chain from E to S, so that $\rho(U) = m$.

Theorem 4.1 *The Möbius function of $\mathcal{D}(G, m)$ is given by*

$$\mu(S,T) = \begin{cases} (-1)^{\rho(T)-\rho(S)} & \text{if } T \neq U, \\ (-1)^{\rho(U)-\rho(S)}(\rho(U) - \rho(S)) = (-1)^{m-\rho(S)}(m - \rho(S)) & \text{if } T = U, \end{cases}$$

for $S \preccurlyeq T$.

Proof Every interval $[E, T]$ with $T \neq U$ is a isomorphic to a Boolean lattice of rank equal to $\rho(T)$. So the values of $\mu(S, T)$ for $T \neq U$ are equal to those in the Boolean lattice, and are as claimed.

As shown in [4], each of the remaining intervals $[S, U]$ is a diagonal semilattice $\mathcal{D}(G, m - \rho(S))$. Therefore we can obtain $\mu(S, U)$ by replacing m by $m - \rho(S)$ in the formula for $\mu(E, U)$.

Thus it suffices to calculate $\mu(E, U)$. This we can now do as follows:

$$\begin{aligned} \mu(E,U) &= -\sum_{E \preccurlyeq S \prec U} \mu(E,S) \\ &= -\sum_{i=0}^{m-1} (-1)^i \binom{m+1}{i}, \end{aligned}$$

since there are $\binom{m+1}{i}$ elements of rank i in the semilattice when $0 \leq i \leq m-1$ (the joins of all i-subsets of $\{Q_0, \ldots, Q_m\}$).

Now the last sum is the negative of all terms of the binomial expansion of $(1-1)^{m+1}$ (which is 0) except for the terms with $i = m$ and $i = m+1$. So

$$\mu(E,U) = (-1)^m \binom{m+1}{m} + (-1)^{m+1} = (-1)^m m,$$

as required. $\square$

5 The spectrum of the diagonal graph

Put $\Omega = G^m$. For $0 \leqslant i \leqslant m$, let A_i be the adjacency matrix of the graph Γ_i on the vertex set Ω in which two vertices are joined if they lie in the same part of Q_i. This graph is the disjoint union of q^{m-1} copies of the complete graph of order q; so its spectrum is $(q-1)$ with multiplicity q^{m-1} and -1 with multiplicity $q^{m-1}(q-1)$. Since the matrices A_i commute pairwise and their sum is the adjacency matrix A of the diagonal graph $\Gamma_D(G,m)$, we see that the set of eigenvalues of A is contained in

$$\{-(m+1)+kq : 0 \leqslant k \leqslant m+1\}.$$

Computing the multiplicities is a little more difficult. We use the technique from experimental design for finding stratum dimensions in Tjur block structures: see [1, 2, 3].

Let $V = \mathbb{R}^\Omega$ be the vector space of real functions on Ω. For each element S in the diagonal semilattice, let V_S be the subspace of functions which are constant on the parts of S. If $\rho(S) = k$, then $\dim(V_S) = q^{m-k}$. For convenience we will denote V_{Q_i} by V_i.

Any vector in V_i is an eigenvector for A_i with eigenvalue $q-1$, while any vector orthogonal to V_i is an eigenvector for A_i with eigenvalue -1. Hence, if $v \in V_S$ but v is orthogonal to V_i whenever Q_i is not below S, then v is an eigenvector of A with eigenvalue $-(m+1)+\rho(S)q$.

Clearly V_U consists of constant functions and has dimension 1, associated with the eigenvalue $(m+1)(q-1)$.

For $S \neq U$, let

$$W_S = V_S \cap \left(\sum_{S \prec T} V_T\right)^\perp.$$

We calculate $n_S = \dim(W_S)$ by Möbius inversion. We have

$$V_S = \bigoplus_{S \preccurlyeq T} W_T,$$

so

$$q^{m-\rho(S)} = \sum_{S \preccurlyeq T} n_T.$$

Möbius inversion gives

$$n_S = \sum_{S \preccurlyeq T} \mu(S,T) q^{m-\rho(T)}.$$

Suppose that $m-\rho(S)=s$. Using the fact that the interval $[S,U]$ is isomorphic to the diagonal semilattice of dimension $m-\rho(S)=s$, as well as the results of Theorem 4.1, we have

$$\begin{aligned}
n_S &= \sum_{i=0}^{s-1}\binom{s+1}{i}(-1)^i q^{s-i}+(-1)^s s \\
&= q^{-1}((q-1)^{s+1}-(s+1)(-1)^s q-(-1)^{s+1}+(-1)^s sq) \\
&= q^{-1}((q-1)^{s+1}+(-1)^{s+1}(q-1)) \\
&= q^{-1}(q-1)((q-1)^s-(-1)^s).
\end{aligned}$$

Since there are $\binom{m+1}{k}$ elements of the diagonal semilattice with rank k, for $0\leqslant k\leqslant m-1$, we conclude:

Theorem 5.1 *If G is a group of order q, then the adjacency matrix of the diagonal graph $\Gamma_D(G,m)$ has eigenvalue $-(m+1)+kq$ with multiplicity*

$$\binom{m+1}{k}q^{-1}(q-1)((q-1)^{m-k}-(-1)^{m-k}),$$

for $k\in\{0,\ldots,m-1\}$, and eigenvalue $(m+1)(q-1)$ with multiplicity 1. $\square$

Remark The formula for n_S differs only in a factor of q from the chromatic polynomial of the $(s+2)$-cycle graph (which can be obtained by a similar Möbius inversion over the poset of all subsets of the edge set of the cycle graph).

Remark This formula agrees with the known formula for the cases $m=2$ (Latin square graphs, with eigenvalues $3(q-1)$, $q-3$, -3 having multiplicities 1, $3(q-1)$, $(q-1)(q-2)$), and $q=2$ (the folded cube, where the eigenvalues $-(m+1)+2k$ occur only if $m-k$ is odd, since $(q-1)^{m-k}-(-1)^{m-k}=0$ when $q=2$ and $m-k$ is even).

6 Clique number and chromatic number

Small diagonal graphs (of dimension 2 over groups of orders at most 4) are somewhat exceptional. It is easy to see that

- $\Gamma_D(C_2,2)$ is the complete graph K_4;

- $\Gamma_D(C_3, 2)$ is the complete multipartite graph $K_{3,3,3}$ with three parts of size 3;
- $\Gamma_D(V_4, 2)$ (where $V_4 = C_2 \times C_2$) is the complement of the 4×4 square lattice graph $L_2(4)$ (the line graph of the complete bipartite graph $K_{4,4}$);
- $\Gamma_D(C_4, 2)$ is the complement of the *Shrikhande graph*, the exceptional strongly regular graph having the same parameters as $L_2(4)$, discovered by Shrikhande [15].

With these exceptions, the clique number of $\Gamma_D(G, m)$ is equal to the order of G, and the cliques of maximum size are precisely the parts of the partitions $Q_0, \ldots, Q_m$ (the minimal partitions in the diagonal semilattice $\mathcal{D}(G, m)$). In fact, if $m > 2$, then every clique of size greater than 1 is of this form; that is, every edge is contained in a unique maximal clique.

An important problem which we have not been able to answer completely is to find the chromatic number of $\Gamma_D(G, m)$. Recall that the *chromatic number* $\chi(\Gamma)$ of a graph Γ is the smallest number of colours needed to colour the vertices of Γ so that adjacent vertices have different colours.

We approach this problem using the notion of graph homomorphism. Let Γ and Δ be graphs. A map $F : V(\Gamma) \to V(\Delta)$ is a *homomorphism* if it maps edges to edges. (Non-edges may map to non-edges, or to edges, or collapse to single vertices.) We note two important properties of graph homomorphisms:

- A homomorphism $\Gamma \to K_r$ (where K_r is the complete graph on r vertices) is a proper vertex-colouring of Γ with r colours (since adjacent vertices of Γ must map to distinct vertices of K_r).
- If F is a homomorphism from Γ to Δ, then $\chi(\Gamma) \leqslant \chi(\Delta)$. For, if we give to a vertex $v \in V(\Gamma)$ the colour of $F(v)$ in the colouring of Δ, we have a proper colouring of Γ.

Proposition 6.1 *For $m > 2$, the map*

$$(g_1, g_2, g_3, g_4, \ldots, g_m) \mapsto (g_1 g_2^{-1} g_3, g_4, \ldots, g_m)$$

is a homomorphism from $\Gamma_D(G, m)$ to $\Gamma_D(G, m-2)$.

Proof This is routine checking. Take an edge in $\Gamma_D(G, m)$, joining $(g_1, \ldots, g_m)$ to $(h_1, \ldots, h_m)$. There are two possibilities:

- There is some i such that $g_i \neq h_i$ and $g_j = h_j$ for $j \neq i$. If $i \leqslant 3$, then $g_1 g_2^{-1} g_3 \neq h_1 h_2^{-1} h_3$ and $g_j = h_j$ for $j > 3$; if $i > 3$ then $g_1 g_2^{-1} g_3 = h_1 h_2^{-1} h_3$ and $g_j = h_j$ for $j > 3$ and $j \neq i$. In either case, the images are adjacent in $\Gamma_D(G, m-2)$.
- There is some $x \in G$ such that $h_i = x g_i$ for $1 \leqslant i \leqslant m$. Then we have

$$h_1 h_2^{-1} h_3 = x g_1 g_2^{-1} x^{-1} x g_3 = x(g_1 g_2^{-1} g_3)$$

  and $h_i = x g_i$ for $i > 4$. □

Proposition 6.2 *The chromatic number of $\Gamma_D(G, 2)$ is at least $|G|$, with equality if and only if either G has odd order or the Sylow 2-subgroups of G are non-cyclic.*

Proof A *complete mapping* on a group G is a bijection $\phi : G \to G$ such that the map ψ given by $\psi(g) = g\phi(g)$ for $g \in G$ is also a bijection. It is well-known (see [11, 5]) that the following are equivalent:

- G has a complete mapping;
- the Cayley table of G has a transversal;
- the Cayley table of G has an orthogonal mate;
- the Latin square graph of the Cayley table of G has chromatic number equal to $|G|$.

The *Hall–Paige conjecture* [10] asserts that a group G has a complete mapping if and only if either G has odd order or the Sylow 2-subgroups of G are not non-trivial cyclic groups. The conjecture was proved in 2009 by Wilcox, Evans and Bray (see [16, 7, 5]). □

From these two results, our main theorem follows:

Theorem 6.3 *If m is odd, or if $|G|$ is odd, or if the Sylow 2-subgroups of G are non-cyclic, then $\chi(\Gamma_D(G, m) = m$. Otherwise, $\chi(\Gamma_D(G, m) \leqslant \chi(\Gamma_D(G, 2)$.*

Proof Assume that $m > 2$. If m is odd, then Proposition 6.1 shows that $\chi(\Gamma_D(G, m)) \leqslant \chi(\Gamma_D(G, 1)$; but $\Gamma_D(G, 1)$ is a complete graph of order $|G|$. Also, $\Gamma_D(G, m)$ contains a clique of size $|G|$; so its chromatic number is $|G|$.

If m is even, the result follows from Propositions 6.1 and 6.2. □

We end this section with two remarks. First, the chromatic number of $\Gamma_D(C_2, m)$ (the folded cube) for m even is known to be 4 (see [12]). Second, it is conjectured in [9] that, if G has non-trivial cyclic Sylow 2-subgroups, then the chromatic number of $\Gamma_D(G, 2)$ (the Latin square graph of the Cayley table of G) is $|G| + 2$. If so, then this would be an upper bound for $\chi(\Gamma_D(G, m))$ for even $m \geqslant 2$, and we further conjecture that this bound is attained for all even m:

Conjecture 1 Suppose that G is a grooup with non-trivial cyclic Sylow 2-subgroups, and that m is even. Then the chromatic number of $\Gamma_D(G, m)$ is $m + 2$.

7 Other properties

In the final section we give a few more properties of the diagonal graph.

7.1 Basic properties

We list here some properties established in [4].

Proposition 7.1 *Assume that $m \geqslant 2$ and $|G| \geqslant 2$, and let Γ denote the diagonal graph $\Gamma_D(G, m)$.*

(a) There are $|G|^m$ vertices, and the valency is $(m + 1)(|G| - 1)$.

(b) Except for the case $m = |G| = 2$, the clique number is $|G|$, and the clique cover number is $|G|^{m-1}$.

(c) $\Gamma_D(G_1, m_1)$ is isomorphic to $\Gamma_D(G_2, m_2)$ if and only if $m_1 = m_2$ and $G_1 \cong G_2$.

(d) The diameter of Γ is $m + 1 - \lceil (m + 1)/|G| \rceil$, which is at most m, with equality if and only if $|G| > m + 1$.

7.2 Symmetry

Proposition 7.2 *Assume that $m \geqslant 2$ and $|G| \geqslant 2$, and let Γ denote the diagonal graph $\Gamma_D(G, m)$.*

(a) Γ is a Cayley graph for the group G^m, and hence is vertex-transitive.

(b) Γ is edge-transitive if and only if G is elementary abelian.

(c) Γ is vertex-primitive if and only if

- *G is characteristically simple (that is, a direct product of simple groups), and*
- *if G is an elementary abelian p-group then $p \nmid m+1$.*

(d) If $m > 2$ or $|G| > 4$, then $\mathrm{Aut}(\Gamma)$ is transitive on the set of cliques of maximal size in Γ.

Proof (a) Recall that $\mathrm{Aut}(\Gamma)$ is the diagonal group $D(G, m)$, and also the list of generators of the diagonal group given in the first section. The generators of the first type in the list form a group isomorphic to G^m, acting regularly on the vertex set of Γ; so Γ is a Cayley graph.

We remark here that the generators of the fourth and fifth type generate a group isomorphic to $\mathrm{Sym}(m+1)$ normalising the group generated by those of the first two types, and acting as the symmetric group on the $m+1$ partitions $Q_0, \ldots, Q_m$. (The fourth type induce $\mathrm{Sym}(m)$ on $Q_1, \ldots, Q_m$, while the fifth type interchanges Q_0 and Q_1 and fixes the others.) If G is non-abelian, then the group G^m generated by elements of the first type has $m+1$ images under $\mathrm{Sym}(m+1)$; so there are $m+1$ subgroups of $\mathrm{Aut}(\Gamma)$ acting regularly, and so Γ is a Cayley graph for $m+1$ distinct, though isomorphic, groups. On the other hand, if G is abelian then elements of the second type are already contained in the group G^m generated by elements of the first type, and so the images of this subgroup under $\mathrm{Sym}(m+1)$ are all equal.

(b) The stabiliser of a vertex has structure $\mathrm{Aut}(G) \times \mathrm{Sym}(m+1)$. The symmetric group permutes the $m+1$ cliques of size $|G|$ containing the fixed vertex; each clique is bijective with G, the fixed vertex corresponding to the identity, and $\mathrm{Aut}(G)$ acts on it in the natural way. Thus Γ is edge-transitive if and only if $\mathrm{Aut}(G)$ is transitive on the non-identity elements of G, which occurs if and only if G is elementary abelian.

(c) This is proved in [4, Theorem 1.6].

(d) This follows from the above remarks: each such clique is a part of a partition Q_i; now $\mathrm{Sym}(m+1)$ permutes the partitions transitively, and G^m fixes each partition and permutes transitively the parts of each. $\square$

Recall the definition of distance-regularity from [6].

Proposition 7.3 *The graph $\Gamma_D(G, m)$ is distance-regular if and only if either $m = 2$ or $|G| = 2$.*

Proof If $m = 2$, then $\Gamma_D(G, m)$ is a Latin square graph, which is strongly regular; if $G = C_2$, then $\Gamma_D(G, m)$ is a folded cube, which is distance-transitive. In either case the graph is distance-regular.

So suppose that $m > 2$ and $|G| > 2$.

First consider the case where m is odd, say $m = 2k + 1$. We argue as in Example 2 given earlier. Take two non-identity elements $g, h \in G$. Let a and b be the elements of G^m given by $a = (g, \ldots, g, 1, \ldots, 1)$ and $b = (h, g, \ldots, g, 1, \ldots, 1)$, where in each case the number of non-identity elements is $k+1$. Each of these elements has distance $k+1$ from the identity element of G^m. In the case of b, there are $k + 1$ neighbours at distance k from the identity, obtained by changing one of the non-identity entries in h to the identity. In the case of a, there are $k + 2$ such elements, since additionally we may multiply on the left by g^{-1} to get $(1, \ldots, 1, g^{-1}, \ldots, g^{-1})$ with k non-identity elements.

Now suppose that m is even, say $m = 2k$ with $k > 1$. Again take g, h to be non-identity elements in G, and let $a = (g, \ldots, g, 1, \ldots, 1)$ and $b = (h, g, \ldots, g, 1, \ldots, 1)$, where in each case there are k non-identity elements. These vertices are at distance k from the identity; we count neighbours which are also at distance k from the identity. In the case of b, there are $k(|G| - 2)$ of these, since we may change any of the first k elements to a different non-identity element of G. In the case of a, there is one extra such vertex, namely $(1, \ldots, 1, g^{-1}, \ldots, g^{-1})$.

In both cases the graph fails to be distance-regular. $\square$

References

[1] R. A. Bailey, Factorial design and Abelian groups, *Linear Algebra and its Applications* **70** (1985), 349–368.

[2] R. A. Bailey, Orthogonal partitions in designed experiments, *Designs, Codes and Cryptography* **8** (1996), 45–77.

[3] R. A. Bailey, *Design of Comparative Experiments*, Cambridge University Press, Cambridge, 2008.

[4] R. A. Bailey, Peter J. Cameron, Cheryl E. Praeger and Csaba Schneider, The geometry of diagonal groups, arXiv `2007.10726`.

[5] J. N. Bray, Q. Cai, P. J. Cameron, P. Spiga and H. Zhang, The Hall–Paige conjecture, and synchronization for affine and diagonal groups, *J. Algebra* **545** (2020), 27–42.

[6] Andries E. Brouwer, Arjeh M. Cohen and Arnold Neumaier, *Distance-Regular Graphs*, Springer-Verlag, New York, 1989.

[7] Anthony B. Evans, The admissibility of sporadic simple groups, *J. Algebra* **321** (2009), no. 1, 105–116.

[8] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.11.1 (2021), `https://www.gap-system.org`

[9] Luis Goddyn, Kevin Halasz, and E. S. Mahmoodian, The chromatic number of finite group Cayley tables, *Electron. J. Combin.*, **26**(1) (2019), Paper 1.36, 15 pp.

[10] Marshall Hall Jr. and L. J. Paige, Complete mappings of finite groups, *Pacific J. Math.* **5** (1955), 541–549.

[11] L. J. Paige, Complete mappings of finite groups, *Pacific J. Math.* **1** (1951), 111–116.

[12] Charles Payan, On the chromatic number of cube-like graphs, *Discrete Math.* **103** (1992), 271–277.

[13] G.-C. Rota, On the foundations of combinatorial theory I: Theory of Möbius functions, *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete* **2** (1964), 340–368.

[14] L. L. Scott, Representations in characteristic p, In *The Santa Cruz Conference on Finite Groups* (Univ. California, SantaCruz, Calif., 1979), Proc. Sympos. Pure Math., vol. 37, Amer. Math. Soc., Providence, R.I., 1980, pp. 319–331.

[15] S. S. Shrikhande, The uniqueness of the L_2 association scheme, *Ann. Math. Statist.* **30** (1959), 781–798.

[16] Stewart Wilcox, Reduction of the Hall–Paige conjecture to sporadic simple groups, *J. Algebra* **321** (2009), no. 5, 1407–1428.