Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-021-00907-2

Diagonal groups and arcs over groups

R. A. Bailey[1] · Peter J. Cameron[1] · Michael Kinyon[2] · Cheryl E. Praeger[3]

Received: 30 October 2020 / Revised: 31 March 2021 / Accepted: 21 June 2021

Abstract

In an earlier paper by three of the present authors and Csaba Schneider, it was shown that, for $m \geq 2$, a set of $m + 1$ partitions of a set Ω, any m of which are the minimal non-trivial elements of a Cartesian lattice, either form a Latin square (if $m = 2$), or generate a join-semilattice of dimension m associated with a diagonal group over a base group G. In this paper we investigate what happens if we have $m + r$ partitions with $r \geq 2$, any m of which are minimal elements of a Cartesian lattice. If $m = 2$, this is just a set of mutually orthogonal Latin squares. We consider the case where all these squares are isotopic to Cayley tables of groups, and give an example to show the groups need not be all isomorphic. For $m > 2$, things are more restricted. Any $m + 1$ of the partitions generate a join-semilattice admitting a diagonal group over a group G. It may be that the groups are all isomorphic, though we cannot prove this. Under an extra hypothesis, we show that G must be abelian and must have three fixed-point-free automorphisms whose product is the identity. (We describe explicitly all abelian groups having such automorphisms.) Under this hypothesis, the structure gives an orthogonal array, and conversely in some cases. If the group is cyclic of prime order p, then

Dedicated to Aart Blokhuis, colleague and friend

Communicated by T. Szőnyi.

Michael Kinyon partially supported by Simons Foundation Collaboration Grant 359872 and by Fundação para a Ciência e a Tecnologia (Portuguese Foundation for Science and Technology) grant PTDC/MAT-PUR/31174/2017.
Cheryl E. Praeger supported by Australian Research Council Discovery Grant DP160102323.

✉ Peter J. Cameron
pjc20@st-andrews.ac.uk

R. A. Bailey
rab24@st-andrews.ac.uk

Michael Kinyon
mkinyon@du.edu

Cheryl E. Praeger
cheryl.praeger@uwa.edu.au

[1] School of Mathematics and Statistics, University of St Andrews, St Andrews, Fife KY16 9SS, UK

[2] Department of Mathematics, University of Denver, Denver, CO 80208, USA

[3] Department of Mathematics and Statistics, University of Western Australia, Perth, WA 6009, Australia

Published online: 04 July 2021

the structure corresponds exactly to an arc of cardinality $m + r$ in the $(m - 1)$-dimensional projective space over the field with p elements, so all known results about arcs are applicable. More generally, arcs over a finite field of order q give examples where G is the elementary abelian group of order q. These examples can be lifted to non-elementary abelian groups using p-adic techniques.

Keywords Diagonal group · Arc · Orthogonal array · Diagonal semilattice · Frobenius group

Mathematics Subject Classification 20B25 · 05B15 · 51A45 · 62K15 · 94B25

1 Introduction

The origin of this paper was a realisation that, as sets of mutually orthogonal Latin squares extend the notion of Latin squares to more objects, and arcs in finite projective spaces extend to higher dimension, there should be a way to define and study objects realising both of these extensions. Given the fundamental work of Aart Blokhuis in finite geometry, especially on arcs [4], we regard this as a fitting tribute to him.

Central to our work is the notion of *diagonal groups* and the structures they act on. Diagonal groups $D(G, m)$ are one of the families of primitive permutation groups arising in the celebrated O'Nan–Scott theorem. In this theorem, the group G is a finite simple (or characteristically simple) group. In [2], the authors considered diagonal groups with an arbitrary group G (not necessarily finite), and defined a geometric object having the diagonal group as its automorphism group. This object was called a *diagonal semilattice*. We now outline the details.

We work within the lattice $\mathcal{P}(\Omega)$ of partitions of a set Ω. A *Cartesian lattice* of dimension m over an alphabet A is defined as follows: $\Omega = A^m$, and for any subset J of $\{1, \ldots, m\}$, we define the partition Q_J of Ω in which two m-tuples $(a_1, \ldots, a_m)$ and $(b_1, \ldots, b_m)$ belong to the same part if and only if $a_j = b_j$ for all $j \notin J$. These partitions form a lattice isomorphic to the Boolean lattice on $\{1, \ldots, m\}$ (the lattice of all subsets of $\{1, \ldots, m\}$); the map $J \mapsto Q_J$ is an isomorphism from the Boolean lattice to the Cartesian lattice.

Definition 1 The *diagonal group* $D(G, m)$ can be defined as a group of permutations of the set $\Omega = G^m$ generated by the following permutations:

- right translations by elements of G^m;
- left translations by elements of the subgroup $\delta(G) = \{(g, g, \ldots, g) : g \in G\}$ of G^m;
- automorphisms of G (acting in the same way on all coordinates);
- permutations of the coordinates;
- the map
$$(g_1, g_2, \ldots, g_m) \mapsto (g_1^{-1}, g_1^{-1}g_2, \ldots, g_1^{-1}g_m).$$

For $i = 1, \ldots, m$, let G_i be the ith coordinate subgroup of G^m, the set of m-tuples $(g_1, \ldots, g_m)$ with $g_j = 1$ for $j \neq i$; and let G_{m+1} be the subgroup $\delta(G)$. Then let Q_i be the partition of G^m into right cosets of G_i, for $i = 1, \ldots, m + 1$.

The main results of [2] can be stated as follows:

Theorem 1 *The join-semilattice Λ generated by the partitions $Q_1, \ldots, Q_{m+1}$ has the properties*

– *any m of $\{Q_1, \ldots, Q_{m+1}\}$ generate a Cartesian lattice under join;*
– *the automorphism group of Λ is the diagonal group $D(G, m)$.*

We call Λ a *diagonal semilattice*, and denote it by $\mathcal{D}(G, m)$.

Theorem 2 *Let $Q_1, \ldots, Q_{m+1}$ be partitions of Ω, where $m \geq 2$. Suppose that any m of these partitions generate an m-dimensional Cartesian lattice, in which they are the minimal non-trivial elements. Then one of the following holds:*

– *$m = 2$ and there is a Latin square L, unique up to paratopism, such that Ω is the set of cells of L, and Q_1, Q_2, Q_3 are the partitions of Ω corresponding to the rows, columns and letters of L;*
– *$m \geq 3$ and there is a group G, unique up to isomorphism, such that $Q_1, \ldots, Q_{m+1}$ generate the diagonal semilattice $\mathcal{D}(G, m)$.*

A *paratopism* between two Latin squares is most easily defined here as a bijection between the set of cells of the first and that of the second which carries the three partitions (letters, rows and columns) of the first set to the three partitions of the second set in some order. If rows map to rows, columns to columns and letters to letters, the map is called an *isotopism*.

In this paper, we consider what happens when we have $m + r$ partitions satisfying the hypotheses of this theorem with larger values of r. We will show that

– If $m = 2$, then the partitions form the rows, columns, and letters in r mutually orthogonal Latin squares. The case where all the Latin squares are isotopic to Cayley tables of groups is particularly interesting, and we give an example with $r = 2$ where the four groups fall into three different isomorphism classes.
– If $m \geq 3$ and $r \geq 2$, then under an additional assumption (which we call *regularity*) the groups G obtained by applying Theorem 2 to any $(m + 1)$-tuple of partitions are all isomorphic, are abelian, and this unique abelian group admits three fixed-point-free automorphisms whose product is the identity. We describe all abelian groups having such automorphisms, and give examples based on p-adic lifting of arcs in finite projective spaces. We also describe the relation of our work to orthogonal arrays.

We introduce some notation. Let $t(m, n)$ be the greatest value of r for which such a set of partitions of a set of cardinality n^m exists. (We assume that $m \geq 2$ and $n \geq 2$.) For $m = 2$, this is the maximum number of mutually orthogonal Latin squares of order n (usually denoted by $N(n)$ in the literature). Further, when $m = 2$ we denote by $t_g(2, n)$ the maximum in the case where all the Latin squares obtained by taking the partitions three at a time are Cayley tables of groups. (We do not need to define this for $m \geq 3$, because Theorem 2 shows that, in this case, any set of $m + 1$ of the partitions defines a group.) For any given group G, we also denote by $T(m, G)$ the maximum number r for which there are $m + r$ partitions satisfying our hypothesis such that any $m + 1$ of them define a group isomorphic to G. Thus $T(m, G) \leq t(m, |G|)$.

Part of our purpose here is to consider these functions and give some upper and lower bounds. We will see that our problem involves several other parts of combinatorics and finite geometry, including mutually orthogonal Latin squares, the Hall–Paige conjecture, and arcs in finite projective spaces.

2 The case $m = 2$

Suppose that we have a collection of $r + 2$ partitions of Ω with the property that any two of them give Ω the structure of an $n \times n$ grid. Any further partition can be represented by

a set of letters corresponding to the parts of the partition, and the hypothesis implies that the letters constitute a Latin square of order n on the square array. Further, any two of the resulting Latin squares are orthogonal. So we have precisely a set of r mutually orthogonal Latin squares (MOLS) of order n.

Note that the maximum number of orthogonal Latin squares of order n satisfies $t(2, n) \leq n - 1$, with equality if n is a prime power: see [7, p. 158].

A set of r MOLS defines $\binom{r+2}{3}$ Latin squares, since any triple of the partitions gives such a square. We will say that we have a set of *mutually orthogonal group squares* (MOGS) if all of these Latin squares are isotopic to Cayley tables of groups.

We note that there is a test, the *quadrangle criterion*, to determine whether a Latin square is isotopic to a Cayley table of a group, due to Frolov [15] (see [7, Theorem 1.2.1] and the following text for discussion); and a theorem of Albert [1, Theorem 2] shows that, if so, then the group is unique up to isomorphism.

MOLS have been studied since Euler, and we have nothing to add in general. But note that the classical set of $q - 1$ MOLS of order q (for prime powers q) associated with the Desarguesian projective plane of order q does indeed form a set of MOGS, where all the groups are isomorphic to the additive group of the finite field of order q. So $t_g(2, n) \leq n - 1$, with equality if n is a prime power; and $T(2, G) = q - 1$ if q is a prime power and G is elementary abelian of order q.

More interesting to us is a remarkable example of two MOLS of order 8 where all of the Latin squares are Cayley tables of groups, but the groups are not all isomorphic:

11	22	33	44	55	66	77	88
42	34	21	13	86	78	65	57
53	61	74	82	17	25	38	46
84	73	62	51	48	37	26	15
35	47	16	28	71	83	52	64
76	85	58	67	32	41	14	23
27	18	45	36	63	54	81	72
68	56	87	75	24	12	43	31

The four groups are as follows. Here G_i denotes the group obtained by omitting the ith of the four partitions (rows, columns, first letter, second letter); so G_4 and G_3 denote the groups whose multiplication tables are given by the first and second letters in the array.

G_4: $C_2 \times C_2 \times C_2$
G_3: D_8
G_2: $C_2 \times C_4$
G_1: D_8

The proof of the Hall–Paige conjecture [16] by Wilcox, Evans and Bray [5,10,26] shows that the Cayley table of a group G has an orthogonal mate if and only if the Sylow 2-subgroups of G are trivial or non-cyclic. In particular, no group of order congruent to 2 (mod 4) satisfies this condition, so in the earlier language we have the second part of the following proposition.

Proposition 1 – *If q is a prime power and G is an elementary abelian group of order q, then $T(2, G) = q - 1$; in particular, $t_g(2, q) = q - 1$.*
– *If $n \equiv 2 \pmod 4$, then $t_g(2, n) = 1$.*

Problem 1 *For $r > 1$, is there a set of r MOGS such that all $\binom{r+2}{3}$ groups are pairwise non-isomorphic?*

Problem 2 *Given a group G, what is the largest r such that there exists a set of r MOGS for which all $\binom{r+2}{3}$ groups are isomorphic to G? That is, what is $T(2, G)$?*

Owens and Preece [20,21] investigated the number of different species of Latin squares that occur in the seven different affine planes of order 9. (A *species* is an equivalence class under paratopism.) Two of the affine planes have just one species of Latin square, which is the Cayley table of $C_3 \times C_3$ in both cases. A third affine plane has some choices of which two partitions define rows and columns for which all the Latin squares are Cayley tables of $C_3 \times C_3$. The Cayley table of C_9 never occurs. Egan and Wanless [9] repeated this investigation, and extended it to other sets of MOLS. For a set of three MOLS, there are ten ways of choosing three of the five partitions to form a single Latin square. For MOLS of order 9, Egan and Wanless found that the number of different species occuring can be any integer in $\{1, \ldots, 10\}$.

Another result bearing on this question can be found in the paper of Francetić, Herke and Wanless [14]. They define the notion of the *parity* of a Latin square, and prove (among other things) that, if $n \equiv 2 \pmod 4$, then there is no complete set of $n-1$ Latin squares of order n in which all $\binom{n+1}{3}$ Latin squares are isotopic. Thus, if we extend our notation $T(2, G)$ to quasigroups, so that $T(2, Q)$ is the maximum number of MOLS in which all definable Latin squares are paratopic to the Cayley table of the quasigroup Q, then for $|Q| \equiv 2 \pmod 4$ we have $T(2, Q) < |Q| - 1$.

3 The case $m > 2$

As noted in [2], there are several definitions of "Latin cube" in the literature; the one relevant to the proof of the Main Theorem in that paper is one of these, and not the most popular. The situation for orthogonal Latin cubes is if anything worse, see [8,18,19,23,25]. To avoid causing more confusion, we will use the name *diagonal semilattices* for the objects appearing in [2]. So the objects to be studied here are sets of *mutually orthogonal diagonal semilattices*, or MODS for short.

Thus, a set of r MODS of *dimension* m and *order* n is a collection of $m + r$ partitions $Q_1, \ldots, Q_{m+r}$ of a set Ω of cardinality n^m, with the property that any m of these partitions are the minimal non-trivial elements in an m-dimensional Cartesian lattice on Ω. According to [2], if $r = 1$ (and $m > 2$) then there is a group G of order n, unique up to group isomorphism, such that Ω can be identified with G^m, and the partitions Q_i are the coset partitions of Ω with respect to subgroups $G_1, \ldots, G_{m+1}$, where G_i acts by right multiplication on the ith coordinate of elements of G^m, fixing the entries in all other coordinates, for $i = 1, \ldots, m$, and G_{m+1} acts by left multiplication of all entries by the same group element:

$$x : (g_1, \ldots, g_m) \mapsto (x^{-1}g_1, \ldots, x^{-1}g_m).$$

(The x^{-1} is to ensure that the requirements for a (right) action are satisfied.)

Let us say that a set of r MODS is *regular* if all the partitions are right coset partitions of subgroups of order n in G^m. The main problem, which we have not been able to solve, is:

Problem 3 *Does there exist a non-regular set of MODS (with $m > 2$ and $r > 1$)?*

Proposition 2 *In a regular set of MODS, every $(m + 1)$-tuple of partitions gives rise to a diagonal semilattice over a group G which is independent of the tuple of partitions chosen. Moreover, G is an abelian group which admits three fixed-point-free automorphisms whose product is the identity.*

Proof It suffices to prove this in the case $m = 3$, $r = 2$, which we assume from now on.

Each partition Q_i is the coset partition corresponding to a subgroup G_i of G^3, where we can assume that G_1, G_2, G_3 are the coordinate subgroups, as defined above. This implies that G_1, G_2 and G_3 pairwise commute elementwise. Since the choice of these three subgroups was arbitrary, we see that G_i and G_j commute elementwise for any choice of i, j.

Any further partition must be the coset partition of a subgroup intersecting the product of fewer than m of these subgroups in the identity. Such a subgroup must be a "diagonal" of the form $\{(g, g^\alpha, g^\beta) : g \in G\}$, where α and β are automorphisms of G. Moreover we may take G_4 to be the usual diagonal subgroup, defined by the choices $\alpha = \beta = 1$.

Now consider G_5, and write it in the form

$$G_5 = \{(g, g^\alpha, g^\beta) : g \in G\}$$

for some automorphisms α and β.

Now G_5 must commute with G_4 elementwise. But the projection onto the first coordinate induces an isomorphism on both G_4 and G_5, with image G in both cases; so G is abelian.

By definition, any three of G_1, G_2, G_3, G_4 and G_5 generate their direct product G^3. Now consider $G_3G_4G_5$. Since

$$G_3G_4 = \{(g, g, h) : g, h \in G\},$$

we see that the only solution of $g^\alpha = g$ must be $g = 1$; in other words, α is a fixed-point-free automorphism. Replacing G_3 by G_2 and G_1 in turn, the same argument shows that β and $\alpha^{-1}\beta$ are also fixed-point-free automorphsms. Putting $\gamma^{-1} = \beta\alpha$, we see that α^{-1}, β and γ are fixed-point-free automorphisms whose product is the identity, as required. □

It is possible to describe the abelian groups which have such triples of automorphisms:

Proposition 3 *The following are equivalent for finite abelian groups G:*

(a) *G admits three fixed-point-free automorphisms whose product is the identity;*
(b) *if G is written as a direct product of cyclic groups of prime power orders, then factors whose order is a power of* 2 *or of* 3 *occur with multiplicity greater than* 1.

Proof If the group G has this property, then so do its Sylow subgroups; so we may assume that G is a p-group.

Suppose that $p = 2$ or $p = 3$, and that in the expression for G as a direct product of cyclic groups, some cyclic group (say C_{p^e}) occurs with multiplicity 1. Taking $K = \{g | g^{p^e} = 1\}$ and $H = K^p$, we see that $|K{:}H| = p$; if α is fixed-point-free, then α induces a fixed-point-free automorphism on K/H. But it is easy to see that cyclic groups of orders 2 and 3 do not have triples of automorphisms as required.

In the other direction, cyclic groups of p-power order with $p \geq 5$, and groups $(C_{p^e})^d$, for $p > 3$ and $d > 1$, do admit such triples. □

In particular, for any n not congruent to 2 mod 4 or to ± 3 mod 9, there is an abelian group of order n with this property. One example is the direct product of elementary abelian groups, whose exponent is square-free; the condition on n ensures that, for $p = 2$ and $p = 3$, the Sylow p-subgroup is either trivial or non-cyclic.

The examples to be described in the following sections are all regular in the sense defined in this section.

4 Orthogonal arrays

If G is an abelian group then its *dual group* G^* consists of the irreducible complex characters of G, and is isomorphic to G. These are frequently used by statisticians in factorial design. For example, if $G = C_p^4$ for some prime p, then typically G is written as $\langle a\rangle \times \langle b\rangle \times \langle c\rangle \times \langle d\rangle$ and G^* as $\langle A\rangle \times \langle B\rangle \times \langle C\rangle \times \langle D\rangle$, where A simply picks out the power of a and raises $\exp(2\pi \mathrm{i}/p)$ to that power.

The elements of G^* can be thought of as partitions of G. (Strictly speaking, the character A defines the partition of G whose parts are the inverse images of each complex number in the image of A.) If G is the direct product of m abelian groups of order n, then a set of $m + r$ such partitions of G is called an *orthogonal array of strength* m and *index* 1 if any m of them form the maximal elements in a Cartesian lattice on G.

More generally, an orthogonal array with k factors having strength m and index λ over an alphabet A of size n is a set of k-tuples of elements of A with the property that, given any m distinct coordinates $i_1, \ldots, i_m$ and any m arbitrary elements $a_1, \ldots, a_m$ of A, there are exactly λ tuples having a_j in position i_j for $j = 1, \ldots, m$. The numbers n and k are sometimes called the *number of levels* and *number of factors* respectively. Such an array is denoted by $OA(N, m + r, n, m)$, where N is the number of k-tuples; see [17].

We are only concerned with index 1. In this case, each coordinate defines a partition of the set Ω of k-tuples according to the letter in that coordinate, and this set of k partitions has the property that any m of them are the *maximal* elements in a Cartesian lattice of dimension m.

For example, if $G = C_p^4$ with $p \geq 5$ then $\{A, B, C, D, ABCD, AB^2C^3D^4\}$ is an orthogonal array of strength 4. This is an $OA(p^{4,6}, p, 4)$.

In fact, the complete set of MOLS of order 9 given by Fisher and Yates in [13] was constructed in this way, using C_3^4 as the underlying set. The rows are labelled by pairs of values of A and B, while the columns are labelled by pairs of values of C and D. The letters in the first square are identified by pairs of values of AC and BD; and so on. It is thus no surprise that all eight Latin squares are Cayley tables of $C_3 \times C_3$. What was surprising to its authors was that this set of MOLS is not isomorphic to the one given in [11]. They originally thought that it was, but Fisher apologised for the mistake in [12]. In fact, these are the first two affine planes discussed at the end of Sect. 2.

Let us return to orthogonal arrays. The concept of orthogonal array is the dual notion (in the sense of reversing the partial order of refinement of partitions) of the property stated in the first part of Theorem 1. If the orthogonal array is defined by an abelian group, then taking the dual group also reverses the order of refinement. Hence the dual of each such orthogonal array gives a set of MODS.

In the running example, the dual of the orthogonal array is the set of subgroups $\langle a\rangle$, $\langle b\rangle$, $\langle c\rangle$, $\langle d\rangle$, $\langle abcd\rangle$, $\langle ab^2c^3d^4\rangle$. These have the property that every subset of four of them generate their direct product: in other words, their coset partitions form the minimal non-trivial partitions in a join semi-lattice.

If we write this in more standard notation over the field GF(p), then we have six vectors $(1, 0, 0, 0)$, $(0, 1, 0, 0)$, $(0, 0, 1, 0)$, $(0, 0, 0, 1)$, $(1, 1, 1, 1)$ and $(1, 2, 3, 4)$ with the property that every four are linearly independent. Multiplying any of these vectors by a non-zero scalar does not affect this, so we are effectively in projective geometry, and we have six points, any four of which are in general position.

We conclude this section by showing that a regular set of MODS with $r > 1$ and $m > 2$ does indeed give rise to an orthogonal array.

Proposition 4 *Given a regular set of MODS of dimension m and order n with $m+r$ partitions, for $r \geq 2$, we can construct from it an orthogonal array of strength m and index 1 with $m+r$ factors, each with n levels.*

Proof According to Proposition 2, a regular set of $m + r$ MODS of order n and dimension n, with $m > 2$ and $r > 1$, is realised by the coset partitions of G^m by $m + r$ subgroups isomorphic to G, where G is an abelian group of order n (and has three fixed-point-free automorphisms whose product is the identity).

Now the dual group $(G^m)^*$ defines an orthogonal array of strength m and index 1 over the alphabet $A = G^*$ by the following rule. First identify each subgroup G_i with G by a fixed isomorphism ψ_i. Then take $\phi \in (G^m)^*$; map ϕ to the n-tuple $a(\phi)$, where $a(\phi)_i$ is the restriction of ϕ to G_i. For $i = 1, \ldots, m$, use the isomorphism ψ_i to identify $a(\phi)_i$ with an element of G^*.

Given any set $i_1, \ldots, i_m$ of m distinct indices, G is the direct sum of the groups $G_{i_1}, \ldots, G_{i_m}$, and so an element of G^* is uniquely defined by its restriction to these subgroups; conversely, any choice of elements of $G^*_{i_j}$ for $j = 1, \ldots, m$ defines a unique homomorphism of G. So we have an orthogonal array, as claimed. □

5 Frobenius groups

A *Frobenius group* is a finite group G with a non-trivial proper subgroup H (called the *Frobenius complement*) such that $H \cap H^g = 1$ for all $g \in G \setminus H$, where H^g is the conjugate $g^{-1}Hg$. The theorem of Frobenius shows that the identity together with elements lying in no conjugate of H form a normal subgroup N, the *Frobenius kernel*. The celebrated theorem of Thompson asserts that the Frobenius kernel is nilpotent.

Alternatively, a Frobenius group is a transitive permutation group G in which the one-point stabilisers are non-trivial but all two-point stabilisers are trivial. The one-point stabilisers are the Frobenius complements, and the Frobenius kernel is a regular normal subgroup.

We refer to Passman [22] for an account of this material.

Theorem 3 *Let G be a Frobenius group whose Frobenius kernel N is abelian, with Frobenius complement H. Then there is a set of $|H|$ MOGS of order $|N| = n$ such that each of the $\binom{|H|+2}{3}$ Latin squares is isotopic to the Cayley table of N.*

Proof Each square has rows and columns indexed by N; the squares are indexed by H. The square L_h has (x, y) entry $L_h(x, y) = xy^h$. (This is analogous to the usual finite field construction of MOLS.) Now L_h is isotopic to the Cayley table of N, since if we relabel the column previously labelled y^h as y then we recover the Cayley table of N (which indeed is L_1).

To show orthogonality, take distinct $h, k \in H$ and $a, b \in N$; we need to show that the equations $xy^h = a$ and $xy^k = b$ have a unique solution $(x, y) \in N \times N$. But these equations imply $y^{-1}kh^{-1}y = kb^{-1}ah^{-1}$, so y conjugates kh^{-1} to $kb^{-1}ah^{-1}$. But the centraliser in H of a non-identity element of N is trivial. So if y_1 and y_2 were two such elements, then $y_1y_2^{-1}$ would commute with kh^{-1}, so $y_1 = y_2$. Thus y, and hence also x, is uniquely determined. (We have proved that there cannot be more than one solution: now counting shows there is exactly one.)

Now we have to show that, of the $|H| + 2$ partitions corresponding to rows, columns, and the $|H|$ squares, if we choose any two to be new rows and columns, it is still true that all the squares are isotopic to the Cayley table of N. Recall that two squares are isotopic if there

are permutations of the rows, columns and letters which transform one to the other. So we need to show that, in each case, there are bijections ϕ, χ, ψ of N such that the entry in row u and column v of the second square is given by $\psi(\phi(u)\chi(v))$, where inside the brackets we have the group operation in N. Different squares will of course require different choices of ϕ, χ, ψ. We saw an example in the first paragraph of this proof, where ϕ and ψ are the identity and $\chi(v) = v^h$.

We begin with a couple of observations.

Note 1: For any $k \in H$, there is a symmetry which maps L_h to L_{kh} and conjugates the column labels by k; and there is a symmetry which swaps rows and columns, and replaces L_h by $L_{h^{-1}}$ with its letters conjugated by h for each $h \in H$.

For the first, $L_{kh}(x, y) = xy^{kh} = x(y^k)^h$. For the second, $(yx^{h^{-1}})^h = y^h x = xy^h$.

Note 2: For $h \in H$, $h \neq 1$, the map $\zeta_h : N \to N$ given by $\zeta_h(x) = x^{-1}x^h$ is a bijection; since N is abelian, it is an automorphism. Thus we may define $\eta_h : N \to N$ to be the inverse of ζ_h.

For suppose that $x^{-1}x^h = y^{-1}y^h$. Then $yx^{-1} = (yx^{-1})^h$. Since conjugation by h is a fixed-point-free automorphism of N, this gives $yx^{-1} = 1$, so $x = y$.

Since N is abelian,

$$\zeta_h(xy) = y^{-1}x^{-1}x^h y^h,$$
$$\zeta_h(x)\zeta_h(y) = x^{-1}x^h y^{-1}y^h,$$

and the right-hand sides are equal.

Now we have to deal with the cases where the two partitions defining the rows and columns of the square are no longer the original ones. We have seen in Note 1 that swapping rows and columns gives a symmetry. Therefore, if we use one of rows and columns, we can assume that it is rows. Note 1 also shows that if we use the partition corresponding to an element $h \in H$, we can assume that $h = 1$. So there are two cases.

Case 1: We use the row partition as rows and the partition corresponding to $h = 1$ as columns. Thus, the row and column labels are x and $xy = z$.

Consider the square corresponding to the former columns, with (x, z) entry y. Since $y = x^{-1}z$, this square is isotopic to the Cayley table of N.

Now consider the square L_h, with (x, z) entry xy^h. Now

$$xy^h = xx^{-h}z^h = (x^{-1})^{-1}(x^{-1})^h z^h = \zeta_h(x^{-1})z^h.$$

Since inversion, ζ_h, and conjugation by h are bijections, this is an isotope of the Cayley table of N. (Take $\phi(x) = \zeta_h(x^{-1})$, $\chi(z) = z^h$ and ψ the identity map.)

Case 2: We use the partition corresponding to the identity as rows, the partition corresponding to h as columns, and the partition corresponding to k as letters. Thus, if the corresponding square has (u, v) entry w, then $u = xy$, $v = xy^h$, and $w = xy^k$.

Solving the first two equations for x and y gives

$$u^{-1}v = y^{-1}y^h = \zeta_h(y), \text{ so } y = \eta_h(u^{-1}v),$$
$$v^{h^{-1}}u^{-1} = x^{h^{-1}}x^{-1} = \zeta_{h^{-1}}(x), \text{ so } x = \eta_{h^{-1}}(v^{h^{-1}}u^{-1}).$$

Thus

$$w = xy^k = \eta_{h^{-1}}(v^{h^{-1}}u^{-1})(\eta_h(u^{-1}v))^k.$$

Since G is abelian and η_h, $\eta_{h^{-1}}$, inversion and conjugation are isomorphisms, we can write this in the form $w = \phi(u)\chi(v)$, where

$$\phi(u) = \eta_{h^{-1}}(u^{-1})(\eta_h(u^{-1}))^k, \qquad \chi(v) = \eta_{h^{-1}}(v^{h^{-1}})(\eta_h(v))^k.$$

Taking these functions ϕ and χ and the identity for ψ gives the required isotopism. □

6 Higher-dimensional examples

Let q be a prime power, and let G be the additive group of the finite field GF(q) of order q. An *arc* in the projective space PG($m-1, q$) is a set of points, any m of which span the space. It is called a k-arc if its cardinality is k.

In vector space terms, it is a set of 1-dimensional subspaces of the m-dimensional vector space over GF(q), such that spanning vectors of any m of the spaces form a basis for the vector space.

Now it is clear that the coset partitions of any m of these 1-dimensional subspaces are the minimal elements of a Cartesian lattice. Thus we have:

Proposition 5 *If there exists an* $(m+r)$*-arc in* PG($m-1, q$)*, then* $T(m, G) \geq r$.

The maximum cardinality of arcs in finite projective space was first studied by Segre in the 1950s. In [24], he raised some fundamental questions which have directed research since. A milestone in their study was the paper of Blokhuis, Bruen and Thas [4]. We refer to the recent survey by Ball and Lavrouw [3] for further information.

The simplest example is the *normal rational curve*. Let $a_1, a_2, \ldots, a_q$ be the elements of GF(q). For $m \leq q+1$, consider the vectors $(1, a_i, a_i^2, \ldots, a_i^{m-1})$ for $i = 1, \ldots, q$) together with $(0, 0, \ldots, 1)$. Any m of these vectors form a basis for GF$(q)^m$. For if the last vector is not included, then the vectors are the rows of a Vandermonde matrix, whose determinant is non-zero; the argument is similar if the last vector is included.

We now present examples in other abelian groups, specifically homocyclic p-groups. Such a group G is a direct power of a cyclic group of prime power order, say $G = (C_{p^e})^d$. Arcs in projective spaces give examples with $e = 1$, as we have seen. The construction involves lifting to a p-adic number field and taking quotients; all necessary information can be found in Henri Cohen's book [6].

Let $q = p^d$. The splitting field of the polynomial $X^q - X$ over the field $\mathbb{Q}_p$ of p-adic numbers is an extension F of $\mathbb{Q}_p$ of degree d. Its integers form a local ring R, with maximal ideal M satisfying $R/M \cong \mathbb{F}_q$.

Let S be the set of roots of $X^q - X$. The non-zero elements of S form a cyclic group of order $q-1$.

For a positive integer $m \leq q+1$, the set

$$\{(1, u, u^2, \ldots, u^{m-1}) : u \in S\} \cup \{(0, 0, \ldots, 0, 1)\}$$

of vectors in F^m has the property that any m of its elements form a basis for F^m. The argument is the same as in the finite field case.

Reducing this set of vectors modulo the ideal M gives a set of $q+1$ vectors in $(\mathbb{F}_q)^m$, any m forming a basis for this space. The 1-dimensional subspaces they span form the standard representation of the normal rational curve in PG($m-1, q$).

Now fix an integer $e \geq 2$. If we reduce modulo M^e, we obtain $q+1$ elements in the group G^m, where G is the homocyclic abelian group of order q^e which is the direct sum of d cyclic groups of order p^e (so that its Frattini quotient is the additive group of the field of order q). We take the R-modules generated by these vectors; each is (additively) a subgroup isomorphic to G. Thus, we have a set of $q+1$ subgroups, any m of which generate their

direct sum, and so an example of a regular set of MODS where all the groups are isomorphic to $(C_{p^e})^d$.

References

1. Albert A.A.: Quasigroups, I. Trans. Am. Math. Soc. **54**, 507–519 (1943).
2. Bailey R.A., Cameron P. J., Praeger C. E., Schneider C.: The geometry of diagonal groups. Trans. Amer. Math. Soc., in press.
3. Ball S., Lavrouw M.: Arcs in finite projective spaces. Eur. Math. Soc. Surv. **6**, 133–172 (2020).
4. Blokhuis A., Bruen A.A., Thas J.A.: On M.D.S. codes, arcs in PG(n, q) with q even, and a solution of three fundamental problems of B. Segre. Invent. Math. **92**, 441–459 (1988).
5. Bray J.N., Cai Q., Cameron P.J., Spiga P., Zhang H.: The Hall-Paige conjecture, and synchronization for affine and diagonal groups. J. Algebra **545**, 27–42 (2020).
6. Cohen H.: Number Theory, Volume I: Tools and Diophantine Equations, Graduate Texts in Mathematics. Springer, New York (2007).
7. Dénes J., Keedwell A.D.: Latin Squares and Their Applications. Akadémai Kaidó, Budapest (1974).
8. Dougherty S.T., Szczepanski T.A.: Latin k-hypercubes. Austral. J. Comb. **40**, 145–160 (2008).
9. Egan J., Wanless I.M.: Enumeration of MOLS of small order. Math. Comput. **85**, 799–824 (2016).
10. Evans A.B.: The admissibility of sporadic simple groups. J. Algebra **321**(1), 105–116 (2009).
11. Fisher R.A.: The Design of Experiments. 2nd edition, Oliver and Boyd, Edinburgh (1937).
12. Fisher R.A.: Completely orthogonal 9×9 Latin squares. A correction. Ann. Eugen. **11**, 402–403 (1942).
13. Fisher R.A., Yates F.: Statistical Tables for Biological, Agricultural and Medical Research. Oliver & Boyd, Edinburgh (1938).
14. Francetić N., Herke S., Wanless I.M.: Parity of sets of mutually orthogonal Latin squares. J. Comb. Theory (A) **155**, 67–99 (2018).
15. Frolov M.: Recherches sur les permutations carrées, J. Math. Spéc. (3) **4**, 8–11 (1890).
16. Hall L.M. Jr., Paige J.: Complete mappings of finite groups. Pac. J. Math. **5**, 541–549 (1955).
17. Hedayat A.S., Sloane N.J.A., Stufken J.: Orthogonal Arrays: Theory and Applications. Springer Series in Statistics. Springer, New York (1999).
18. McKay B.D., Wanless I.M.: A census of small Latin hypercubes. SIAM J. Discret. Math. **22**, 719–736 (2008).
19. Mullen G.L.: Orthogonal hypercubes and related designs. J. Stat. Plann. Inference **73**, 177–188 (1998).
20. Owens P.J., Preece D.A.: Complete sets of pairwise orthogonal Latin squares of order 9. J. Comb. Math. Comb. Comput. **18**, 83–96 (1995).
21. Owens P.J., Preece D.A.: Aspects of complete sets of 9×9 pairwise orthogonal Latin squares. Discret. Math. **167/168**, 519–525 (1997).
22. Passman D.S.: Permutation Groups, Dover Publications (revised republication of the work orginally published in 1968 by the W. A. Benjamin Company), New York (2012).
23. Potapov V.N.: Constructions of pairs of orthogonal Latin cubes. J. Comb. Des. **28**, 604–613 (2020).
24. Segre B.: Curve razionali normali e k-archi negli spazi finiti. Ann. Mat. Pura Appl. (4) **39**, 357–379 (1955).
25. Trenkler M.: On orthogonal Latin p-dimensional cubes. Czechosolvak Math. J. **55**, 725–728 (2005).
26. Wilcox S.: Reduction of the Hall-Paige conjecture to sporadic simple groups. J. Algebra **321**(5), 1407–1428 (2009).