

# TRANSITIVITY IN FINITE GENERAL LINEAR GROUPS

ALENA ERNST AND KAI-UWE SCHMIDT

ABSTRACT. It is known that the notion of a transitive subgroup of a permutation group  $G$  extends naturally to subsets of  $G$ . We consider subsets of the general linear group  $\mathrm{GL}(n, q)$  acting transitively on flag-like structures, which are common generalisations of  $t$ -dimensional subspaces of  $\mathbb{F}_q^n$  and bases of  $t$ -dimensional subspaces of  $\mathbb{F}_q^n$ . We give structural characterisations of transitive subsets of  $\mathrm{GL}(n, q)$  using the character theory of  $\mathrm{GL}(n, q)$  and interpret such subsets as designs in the conjugacy class association scheme of  $\mathrm{GL}(n, q)$ . In particular we generalise a theorem of Perin on subgroups of  $\mathrm{GL}(n, q)$  acting transitively on  $t$ -dimensional subspaces. We survey transitive subgroups of  $\mathrm{GL}(n, q)$ , showing that there is no subgroup of  $\mathrm{GL}(n, q)$  with  $1 < t < n$  acting transitively on  $t$ -dimensional subspaces unless it contains  $\mathrm{SL}(n, q)$  or is one of two exceptional groups. On the other hand, for all fixed  $t$ , we show that there exist nontrivial subsets of  $\mathrm{GL}(n, q)$  that are transitive on linearly independent  $t$ -tuples of  $\mathbb{F}_q^n$ , which also shows the existence of nontrivial subsets of  $\mathrm{GL}(n, q)$  that are transitive on more general flag-like structures. We establish connections with orthogonal polynomials, namely the Al-Salam-Carlitz polynomials, and generalise a result by Rudvalis and Shinoda on the distribution of the number of fixed points of the elements in  $\mathrm{GL}(n, q)$ . Many of our results can be interpreted as  $q$ -analogs of corresponding results for the symmetric group.

## 1. INTRODUCTION

A subgroup  $G$  of the symmetric group  $\mathrm{Sym}(n)$  is *t-homogeneous* if  $G$  is transitive on the subsets of  $\{1, 2, \dots, n\}$  with  $t$  elements. Livingstone and Wagner [24] proved the following result.

**Theorem 1.1** ([24]). *Let  $G$  be a subgroup of  $\mathrm{Sym}(n)$  that is  $t$ -homogeneous for some  $t$  satisfying  $1 \leq t \leq n/2$ . Then  $G$  is also  $(t - 1)$ -homogeneous.*

This theorem was generalised by Martin and Sagan [26] in various ways. Their first generalisation replaces subgroups of  $\mathrm{Sym}(n)$  by subsets of  $\mathrm{Sym}(n)$ . Let  $G$  be a group acting on a set  $\Omega$ . We say that a subset  $Y$  of  $G$  is *transitive* on  $\Omega$  if there is a constant  $r$  such that the following holds. For all  $a, b \in \Omega$ , there are exactly  $r$  elements  $g \in Y$  such that  $ga = b$ . If  $Y$  is a subgroup of  $G$ , then this notion coincides with that of

---

*Date:* 22 December 2022.

*2010 Mathematics Subject Classification.* 05B99, 05E30, 20C33.

Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – Project number 459964179.

a transitive group action of  $Y$  on  $\Omega$ . The second generalisation of [26] replaces subsets of  $\Omega$  by set partitions of  $\Omega$ . An (integer) *partition* of a natural number  $n$  is a sequence  $\lambda = (\lambda_1, \lambda_2, \dots)$  of nonnegative integers that sum up to  $n$  and satisfy  $\lambda_1 \geq \lambda_2 \geq \dots$ ; these numbers are called the *parts* of  $\lambda$ . For two partitions  $\lambda = (\lambda_1, \lambda_2, \dots)$  and  $\mu = (\mu_1, \mu_2, \dots)$  of  $n$ , we say that  $\lambda$  *dominates*  $\mu$  and write  $\mu \trianglelefteq \lambda$  if

$$(1) \quad \sum_{i=1}^k \mu_i \leq \sum_{i=1}^k \lambda_i \quad \text{for each } k \geq 1.$$

Finally, for a partition  $\lambda = (\lambda_1, \lambda_2, \dots)$  of  $n$ , a  $\lambda$ -*partition* is an ordered partition of the set  $\{1, 2, \dots, n\}$  into subsets of cardinality  $\lambda_1, \lambda_2, \dots$ . The following is one of the main results in [26].

**Theorem 1.2** ([26]). *Let  $Y$  be a subset of  $\text{Sym}(n)$  that is transitive on  $\sigma$ -partitions. Then  $G$  is also transitive on  $\tau$ -partitions for all  $\tau$  satisfying  $\sigma \trianglelefteq \tau$ .*

In fact, [26] systematically studies subsets of  $\text{Sym}(n)$  that are transitive on  $\sigma$ -partitions using the character theory of  $\text{Sym}(n)$ . In many aspects, this paper studies  $q$ -analogous problems, namely we replace  $\text{Sym}(n)$  by the general linear group  $\text{GL}(n, q)$ , consisting of the invertible  $n \times n$  matrices with entries in  $\mathbb{F}_q$ . Our starting point is the following  $q$ -analog of Theorem 1.1, proved by Perin [27] (who attributed it to an unpublished result by McLaughlin). Henceforth a  $t$ -*space* is a  $t$ -dimensional subspace of  $\mathbb{F}_q^n$ .

**Theorem 1.3** ([27]). *Let  $G$  be a subgroup of  $\text{GL}(n, q)$  that is transitive on  $t$ -spaces for some  $t$  satisfying  $1 \leq t \leq n/2$ . Then  $G$  is also transitive on  $(t-1)$ -spaces.*

An (integer) *composition* of a nonnegative number  $n$  is much like a partition of  $n$ , except that the sequence entries are not necessarily nonincreasing. For a composition  $\lambda = (\lambda_1, \lambda_2, \dots)$  of  $n$ , a  $\lambda$ -*flag* is a sequence of subspaces  $(V_1, V_2, \dots)$  of  $\mathbb{F}_q^n$  such that

$$\{0\} = V_0 \leq V_1 \leq V_2 \leq \dots$$

and  $\dim(V_i/V_{i-1}) = \lambda_i$  for each  $i \geq 1$ . The following is an example of the results we obtain.

**Theorem 1.4.** *Let  $Y$  be a subset of  $\text{GL}(n, q)$  that is transitive on  $\sigma$ -flags. Then  $Y$  is also transitive on  $\tau$ -flags for all compositions  $\tau$  satisfying  $\tilde{\sigma} \trianglelefteq \tilde{\tau}$ , where  $\tilde{\sigma}$  and  $\tilde{\tau}$  are the respective partitions obtained from  $\sigma$  and  $\tau$  by rearranging the parts.*

In fact we consider subsets of  $\text{GL}(n, q)$  that are transitive on more general objects, namely on pairs  $(F, B)$ , where  $F$  is a  $\sigma$ -flag and  $B$  is a tuple whose entries are ordered bases of some of the nonzero quotient spaces  $V_i/V_{i-1}$ . Such objects are called  $(\sigma, \mathcal{I})$ -*flags*, where  $\mathcal{I}$  indexes the quotient spaces whose bases occur in  $B$ . We study  $(\sigma, \mathcal{I})$ -flags using the character theory of  $\text{GL}(n, q)$  and the theory of association schemes (see [2], for example).

We organise this paper in the following way. In Section 2 we recall some relevant background on the character theory of  $\mathrm{GL}(n, q)$  and the conjugacy class association scheme of  $\mathrm{GL}(n, q)$ . In Section 3 we give structural results for transitive subsets of  $\mathrm{GL}(n, q)$ . In particular we show that such subsets can be characterised as designs in the corresponding association scheme, leading directly to results like Theorem 1.4. In Section 4 we survey the examples coming from subgroups. In Section 5 we study so-called *cliques* in  $\mathrm{GL}(n, q)$ , which are subsets of  $\mathrm{GL}(n, q)$  such that, for all distinct elements  $x, y$  in the subset,  $x^{-1}y$  fixes no  $(\sigma, \mathcal{I})$ -flag. Among other things, this will allow us to establish the nonexistence of sharply transitive subsets of  $\mathrm{GL}(n, q)$  in certain cases. In Section 6 we show the existence of small subsets of  $\mathrm{GL}(n, q)$  that are transitive on  $(\sigma, \mathcal{I})$ -flags, as long as the largest part of  $\sigma$  is large compared to the sum of all other parts of  $\sigma$ . We find this interesting since subgroups of  $\mathrm{GL}(n, q)$  that are transitive on  $(\sigma, \mathcal{I})$ -flags are extremely rare. In Section 7 we discuss connections between transitive subsets of  $\mathrm{GL}(n, q)$  and cliques in  $\mathrm{GL}(n, q)$  on one hand and certain orthogonal polynomials, namely the Al-Salam-Carlitz polynomials, on the other hand.

## 2. THE FINITE GENERAL LINEAR GROUPS

We shall give a brief account of the conjugacy classes and the (complex) irreducible characters of the general linear group  $\mathrm{GL}(n, q)$ . We mostly follow [25, Ch. IV].

### 2.1. PARTITIONS

An (integer) *partition* is a sequence  $\lambda = (\lambda_1, \lambda_2, \dots)$  of nonnegative integers that sum up to a finite number and satisfy  $\lambda_1 \geq \lambda_2 \geq \dots$ . The *size* of  $(\lambda_1, \lambda_2, \dots)$  is defined to be  $|\lambda| = \lambda_1 + \lambda_2 + \dots$  and its *length*  $\ell(\lambda)$  is the largest  $i$  such that  $\lambda_i > 0$ . We often write  $(\lambda_1, \lambda_2, \dots, \lambda_{\ell(\lambda)})$  instead of  $(\lambda_1, \lambda_2, \dots)$ . If  $|\lambda| = n$ , then we also say that  $\lambda$  is a partition of  $n$ . Let  $\mathrm{Par}$  be the set of integer partitions. We denote the unique partition of 0 by  $\emptyset$ .

The *Young diagram* of a partition  $(\lambda_1, \lambda_2, \dots, \lambda_k)$  of  $n$  is an array of  $n$  boxes with left-justified rows and top-justified columns, where row  $i$  contains  $\lambda_i$  boxes. To each partition  $\lambda$  belongs a *conjugate partition*  $\lambda'$  whose parts are the number of boxes in the columns of the Young diagram of  $\lambda$ .

We recall three partial orders on integer partitions, namely containment, refinement, and dominance order. Let  $\lambda, \mu \in \mathrm{Par}$  be two partitions. We say that  $\lambda$  *contains*  $\mu$  and write  $\mu \subseteq \lambda$  if the Young diagram of  $\mu$  is contained in the Young diagram of  $\lambda$ . We say that  $\mu$  *refines*  $\lambda$  if  $|\mu| \leq |\lambda|$  and the parts of  $\lambda$  can be partitioned to produce the parts of  $(\mu_1, \dots, \mu_{\ell(\mu)}, 1^{|\lambda| - |\mu|})$ . For example (321) refines (7422). We say that  $\lambda$  *dominates*  $\mu$  and write  $\mu \trianglelefteq \lambda$  if (1) holds. As usual we write  $\mu \triangleleft \lambda$  if  $\mu \trianglelefteq \lambda$  and  $\mu \neq \lambda$ . Typically these partial orders are only defined for partitions of the same size, but it is natural to extend these to the set of all partitions.

## 2.2. CONJUGACY CLASSES

We shall now describe the conjugacy classes of  $\mathrm{GL}(n, q)$  (see [25, Ch. IV, § 3], for example). Let  $\Phi$  be the set of monic irreducible polynomials in  $\mathbb{F}_q[X]$  distinct from  $X$ . We shall often write 1 instead of  $X - 1$  when the meaning is clear from the context. We also write  $|f|$  for the degree of  $f \in \Phi$ .

Let  $\Lambda$  be the set of mappings  $\underline{\lambda}: \Phi \rightarrow \mathrm{Par}$  of finite support (with  $\emptyset$  being the zero element in  $\mathrm{Par}$ ). We often use the short-hand notation  $f \mapsto \lambda$  for the element  $\underline{\lambda} \in \Lambda$  that is supported only on  $f$  and satisfies  $\underline{\lambda}(f) = \lambda$ . We define the *size* of an element  $\underline{\lambda} \in \Lambda$  to be

$$\|\underline{\lambda}\| = \sum_{f \in \Phi} |\underline{\lambda}(f)| \cdot |f|$$

and put  $\Lambda_n = \{\underline{\lambda} \in \Lambda : \|\underline{\lambda}\| = n\}$ .

The *companion matrix* of  $f \in \Phi$  with  $f = X^d + f_{d-1}X^{d-1} + \cdots + f_1X + f_0$  is

$$C(f) = \begin{bmatrix} & & & -f_0 \\ 1 & & & -f_1 \\ & 1 & & -f_2 \\ & & \ddots & \vdots \\ & & & 1 & -f_{d-1} \end{bmatrix} \in \mathbb{F}_q^{d \times d}.$$

(where blanks are filled with zeros). For  $f \in \Phi$  of degree  $d$  and a positive integer  $k$ , we write

$$C(f, k) = \begin{bmatrix} C(f) & I & & & \\ & C(f) & I & & \\ & & \ddots & \ddots & \\ & & & \ddots & I \\ & & & & C(f) \end{bmatrix} \in \mathbb{F}_q^{kd \times kd},$$

and for  $f \in \Phi$  and  $\mu \in \mathrm{Par}$ , we define  $C(f, \mu)$  to be the block diagonal matrix of order  $|\mu| \cdot |f|$  with blocks  $C(f, \mu_1), C(f, \mu_2), \dots$ . Finally, with every  $\underline{\mu} \in \Lambda_n$  we associate the block diagonal matrix  $R_{\underline{\mu}}$  of order  $n$  whose blocks are  $C(f, \underline{\mu}(f))$ , where  $f$  ranges through the support of  $\underline{\mu}$ . Then every element  $g$  of  $\mathrm{GL}(n, q)$  is conjugate to exactly one matrix  $R_{\underline{\mu}}$  for  $\underline{\mu} \in \Lambda_n$ , which is called the *Jordan canonical form* of  $g$ . Hence  $\Lambda_n$  indexes the conjugacy classes of  $\mathrm{GL}(n, q)$ ; we denote by  $C_{\underline{\mu}}$  the conjugacy class containing  $R_{\underline{\mu}}$ . Note that  $C_{X-1 \mapsto (1^n)}$  is the conjugacy class containing the identity.

## 2.3. PARABOLIC INDUCTION

A *composition* is much like a partition, except that the parts do not need to be nonincreasing. Let  $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$  be a composition of  $n$ . Let  $P_\lambda$  be the parabolic subgroup of  $\mathrm{GL}(n, q)$  consisting of block upper-triangular matrices with block sizes

$\lambda_1, \lambda_2, \dots, \lambda_k$ , namely

$$P_\lambda = \left\{ \begin{bmatrix} A_1 & * & \cdots & * \\ & A_2 & \cdots & * \\ & & \ddots & \vdots \\ & & & A_k \end{bmatrix} : A_i \in \mathrm{GL}(\lambda_i, q) \right\}.$$

Let  $\pi_i : P_\lambda \rightarrow \mathrm{GL}(\lambda_i, q)$  be the mapping that projects to the  $i$ -th block on the diagonal, so that

$$(2) \quad \pi_i : \begin{bmatrix} A_1 & * & \cdots & * \\ & A_2 & \cdots & * \\ & & \ddots & \vdots \\ & & & A_k \end{bmatrix} \mapsto A_i.$$

Let  $\phi_i$  be a class function of  $\mathrm{GL}(\lambda_i, q)$ . Then

$$\prod_{i=1}^k (\phi_i \circ \pi_i)$$

is a class function of  $P_\lambda$ . We define the product  $\phi_1 \cdot \phi_2 \cdots \phi_k$  to be the induction of this class function to  $\mathrm{GL}(n, q)$ , that is

$$\phi_1 \cdot \phi_2 \cdots \phi_k = \mathrm{Ind}_{P_\lambda}^{\mathrm{GL}(n, q)} \left( \prod_{i=1}^k (\phi_i \circ \pi_i) \right).$$

#### 2.4. THE IRREDUCIBLE CHARACTERS

The complete set of (complex) irreducible characters has been obtained by Green [14]. Good treatments of this topic are also contained in [25, Ch. IV] and [17]. The irreducible characters of  $\mathrm{GL}(n, q)$  are naturally indexed by  $\Lambda_n$  and, for  $\underline{\lambda} \in \Lambda_n$ , we denote by  $\chi^{\underline{\lambda}}$  the corresponding irreducible character. For  $f \in \Phi$  and a partition  $\lambda$ , the characters  $\chi^{f \rightarrow \lambda}$  are typically called the *primary* irreducible characters of  $\mathrm{GL}(n, q)$ . It is well known (see [17, § 8], for example) that the irreducible characters of  $\mathrm{GL}(n, q)$  satisfy

$$\chi^{\underline{\lambda}} = \prod_{f \in \Phi} \chi^{f \rightarrow \underline{\lambda}(f)}.$$

We use the indexing of [17], so that  $\chi^{f \rightarrow (n)}$  is a cuspidal character of  $\mathrm{GL}(n, q)$  and in particular  $\chi^{X-1 \rightarrow (n)}$  is the trivial character. In contrast,  $\lambda$  is replaced by the conjugate partition  $\lambda'$  in [25, Ch. IV]. We often denote the degree of  $\chi^{\underline{\lambda}}$  by  $f_{\underline{\lambda}}$ .

It follows from [25, Ch. IV] that, for each  $f \in \Phi$ , the algebra with multiplication  $\cdot$  generated by  $\{\chi^{f \rightarrow \lambda} : \lambda \in \mathrm{Par}\}$  is isomorphic to the algebra of symmetric functions with  $\chi^{f \rightarrow \lambda}$  being sent to the Schur function  $s_\lambda$ . In particular the decomposition

of the product  $\chi^{f \rightarrow \lambda} \cdot \chi^{f \rightarrow \nu}$  into irreducible characters is given by the Littlewood-Richardson rule [25, Ch. I]. Let  $\lambda, \mu, \nu \in \text{Par}$  and let  $c_{\lambda\nu}^{\mu}$  be the number of semistandard skew-tableaux  $T$  of shape  $\mu/\lambda$  and content  $\nu$  such that the sequence, obtained by concatenating its reversed rows, is a lattice permutation. Note that we have  $c_{\lambda\nu}^{\mu} = 0$  unless  $|\mu| = |\lambda| + |\nu|$  and  $\lambda, \nu \subseteq \mu$ . The Littlewood-Richardson rule then states that

$$\chi^{f \rightarrow \lambda} \cdot \chi^{f \rightarrow \nu} = \sum_{\mu \in \text{Par}} c_{\lambda\nu}^{\mu} \chi^{f \rightarrow \mu}$$

for all  $f \in \Phi$ . Now, for  $\underline{\lambda}, \underline{\mu}, \underline{\nu} \in \Lambda$ , define

$$c_{\underline{\lambda}\underline{\nu}}^{\underline{\mu}} = \prod_{f \in \Phi} c_{\underline{\lambda}(f)\underline{\nu}(f)}^{\underline{\mu}(f)}$$

and note that  $c_{\underline{\lambda}\underline{\nu}}^{\underline{\mu}} = 0$  unless  $\|\underline{\mu}\| = \|\underline{\lambda}\| + \|\underline{\nu}\|$  and  $\underline{\lambda}, \underline{\nu} \subseteq \underline{\mu}$ , where  $\underline{\lambda} \subseteq \underline{\mu}$  means  $\underline{\lambda}(f) \subseteq \underline{\mu}(f)$  for all  $f \in \Phi$ . The following lemma is then immediate.

**Lemma 2.1.** *For all  $\underline{\lambda}, \underline{\nu} \in \Lambda$  we have*

$$\chi^{\underline{\lambda}} \cdot \chi^{\underline{\nu}} = \sum_{\underline{\mu} \in \Lambda} c_{\underline{\lambda}\underline{\nu}}^{\underline{\mu}} \chi^{\underline{\mu}}.$$

We shall also need the following straightforward result.

**Remark 2.2.** Let  $\underline{\lambda}, \underline{\mu} \in \Lambda$  such that  $\underline{\lambda}(f) \subseteq \underline{\mu}(f)$  for all  $f \in \Phi$ . Then there exists  $\underline{\nu} \in \Lambda$  such that  $c_{\underline{\lambda}\underline{\nu}}^{\underline{\mu}} > 0$ .

The primary irreducible characters must also obey Young's rule [25, Ch. I]. For partitions  $\lambda$  and  $\mu$  of the same size, the *Kostka number*  $K_{\lambda\mu}$  is the number of semistandard Young tableaux of shape  $\lambda$  and content  $\mu$ .

**Lemma 2.3.** *For each  $f \in \Phi$  and each partition  $\mu = (\mu_1, \mu_2, \dots)$ , we have*

$$\prod_{i \geq 1} \chi^{f \rightarrow (\mu_i)} = \sum_{\lambda \supseteq \mu} K_{\lambda\mu} \chi^{f \rightarrow \lambda},$$

where  $\lambda$  ranges over the partitions of  $|\mu|$ .

## 2.5. THE CONJUGACY CLASS ASSOCIATION SCHEME

We shall study the combinatorics in  $\text{GL}(n, q)$  from the viewpoint of an association scheme. We refer to [2] for background on association schemes. Every finite group gives rise to an association scheme (see [2, Section 2.7] for details), called the *conjugacy class association scheme* of the group, but the theory of association schemes is much more general than that. We shall recall relevant background about the conjugacy class association scheme of  $\text{GL}(n, q)$ .

Henceforth we use the following notation. For a field  $K$  and finite sets  $X$  and  $Y$ , we denote by  $K(X, Y)$  the set of  $|X| \times |Y|$  matrices  $A$  with entries in  $K$ , where rows and columns are indexed by  $X$  and  $Y$ , respectively. For  $x \in X$  and  $y \in Y$ , the  $(x, y)$ -entry

of  $A$  is written as  $A(x, y)$ . If  $|Y| = 1$ , then we omit  $Y$ , so  $K(X)$  is the set of column vectors  $a$  indexed by  $X$  and, for  $x \in X$ , the  $x$ -entry of  $a$  is written as  $a(x)$ .

For  $\underline{\mu} \in \Lambda_n$ , let  $D_{\underline{\mu}} \in \mathbb{C}(\text{GL}(n, q), \text{GL}(n, q))$  be given by

$$(3) \quad D_{\underline{\mu}}(x, y) = \begin{cases} 1 & \text{for } x^{-1}y \in C_{\underline{\mu}} \\ 0 & \text{otherwise.} \end{cases}$$

Let  $\mathbb{A}$  be the vector space generated by  $\{D_{\underline{\mu}} : \underline{\mu} \in \Lambda_n\}$  over the complex numbers. Then  $\mathbb{A}$  is a commutative matrix algebra, which contains the identity and is closed under conjugate transposition. The collection of zero-one matrices  $D_{\underline{\mu}}$  therefore defines an association scheme, called the *conjugacy class association scheme* of  $\text{GL}(n, q)$ . The algebra  $\mathbb{A}$  is called the *Bose-Mesner algebra* of this association scheme.

Since  $\mathbb{A}$  is commutative, it can be simultaneously diagonalised and therefore there exists a basis  $\{E_{\underline{\lambda}} : \underline{\lambda} \in \Lambda_n\}$  of  $\mathbb{A}$  consisting of Hermitian matrices with the minimal idempotent property

$$(4) \quad E_{\underline{\kappa}}E_{\underline{\lambda}} = \delta_{\underline{\kappa}\underline{\lambda}}E_{\underline{\lambda}}.$$

These matrices are given by [2, Theorem II.7.2]

$$E_{\underline{\lambda}} = \frac{f_{\underline{\lambda}}}{|\text{GL}(n, q)|} \sum_{\underline{\mu} \in \Lambda_n} \chi_{\underline{\mu}}^{\underline{\lambda}} D_{\underline{\mu}},$$

where  $\chi_{\underline{\mu}}^{\underline{\lambda}}$  is the irreducible character  $\chi^{\underline{\lambda}}$  evaluated on the conjugacy class  $C_{\underline{\mu}}$  and  $f_{\underline{\lambda}}$  is the degree of this character. By (3) the entries of  $E_{\underline{\lambda}}$  are given by

$$(5) \quad E_{\underline{\lambda}}(x, y) = \frac{f_{\underline{\lambda}}}{|\text{GL}(n, q)|} \chi^{\underline{\lambda}}(x^{-1}y).$$

Note that  $E_{X^{-1} \mapsto (n)}$  is the all-ones matrix and that  $\sum_{\underline{\lambda} \in \Lambda_n} E_{\underline{\lambda}}$  is the identity matrix, which can be seen using standard properties of characters. Since the matrices  $E_{\underline{\lambda}}$  are idempotent, their eigenvalues are 0 or 1, and so their ranks sum up to  $|\text{GL}(n, q)|$ . Let  $V_{\underline{\lambda}}$  be the column space of  $E_{\underline{\lambda}}$ . It follows from (4) that these vector spaces are pairwise orthogonal and that

$$(6) \quad \mathbb{C}(\text{GL}(n, q)) = \bigoplus_{\underline{\lambda} \in \Lambda_n} V_{\underline{\lambda}}.$$

Now let  $Y$  be a subset of  $\text{GL}(n, q)$ . The *inner distribution* of  $Y$  is the tuple  $(a_{\underline{\mu}})_{\underline{\mu} \in \Lambda_n}$ , where

$$(7) \quad a_{\underline{\mu}} = \frac{1}{|Y|} \sum_{x, y \in Y} D_{\underline{\mu}}(x, y),$$

and the *dual distribution* of  $Y$  is the tuple  $(a'_{\underline{\lambda}})_{\underline{\lambda} \in \Lambda_n}$ , where

$$(8) \quad a'_{\underline{\lambda}} = \frac{|\text{GL}(n, q)|}{|Y|} \sum_{x, y \in Y} E_{\underline{\lambda}}(x, y).$$

Explicitly using (5) we have

$$(9) \quad a'_\lambda = \frac{f_\lambda}{|Y|} \sum_{x,y \in Y} \chi^\lambda(x^{-1}y).$$

The entries in the inner distribution are clearly nonnegative numbers. The same holds for the entries in the dual distribution. To see this, let  $\mathbb{1}_Y \in \mathbb{C}(\mathrm{GL}(n, q))$  be the characteristic vector of  $Y$ , so that  $\mathbb{1}_Y(x) = 1$  if  $x \in Y$  and  $\mathbb{1}_Y(x) = 0$  otherwise. Since  $E_\lambda$  is Hermitian and idempotent, we find from (8) that

$$\frac{|Y|}{|\mathrm{GL}(n, q)|} a'_\lambda = \mathbb{1}_Y^\top E_\lambda \mathbb{1}_Y = \mathbb{1}_Y^* E_\lambda^* E_\lambda \mathbb{1}_Y = \|E_\lambda \mathbb{1}_Y\|^2.$$

This shows that the entries in the dual distribution are real and nonnegative. Moreover the extreme case  $a'_\lambda = 0$  occurs if and only if  $\mathbb{1}_Y$  is orthogonal to  $V_\lambda$ .

The power of association schemes in combinatorics stems from the observation that interesting combinatorial structures can often be characterised as subsets of association schemes for which certain entries in the inner or dual distribution are equal to zero. Delsarte [7] calls these objects *cliques* and *designs*, respectively. We shall see that interesting subsets of  $\mathrm{GL}(n, q)$  indeed are cliques or designs in the conjugacy class association scheme of  $\mathrm{GL}(n, q)$ .

### 3. NOTIONS OF TRANSITIVITY

We consider pairs  $(\rho, \mathcal{I})$ , where  $\rho$  is a composition of  $n$  and  $\mathcal{I}$  is a subset of  $\{1, 2, \dots, \ell(\rho)\}$  and, if  $q = 2$ , we insist that  $\rho_i > 1$  for each  $i \notin \mathcal{I}$ . We denote the collection of such pairs by  $\Sigma_{n, q}$ .

For a composition  $\rho$  of  $n$ , a  $\rho$ -flag is a tuple of subspaces  $(V_1, V_2, \dots, V_{\ell(\rho)})$  of  $\mathbb{F}_q^n$  such that

$$\{0\} = V_0 \leq V_1 \leq V_2 \leq \dots \leq V_{\ell(\rho)} = \mathbb{F}_q^n$$

and  $\dim(V_i/V_{i-1}) = \rho_i$  for each  $i \in \{1, 2, \dots, \ell(\rho)\}$ . Let  $\alpha = (\rho, \mathcal{I})$  be an element of  $\Sigma_{n, q}$  with  $\mathcal{I} = \{i_1, i_2, \dots, i_k\}$ . We define an  $\alpha$ -flag to be a pair  $(F, B)$ , where  $F = (V_1, V_2, \dots, V_{\ell(\rho)})$  is a  $\rho$ -flag and  $B = (B_1, B_2, \dots, B_k)$  is a tuple of ordered bases of  $V_{i_1}/V_{i_1-1}, V_{i_2}/V_{i_2-1}, \dots, V_{i_k}/V_{i_k-1}$  with  $V_0 = \{0\}$ . For example, a  $((t, n-t), \emptyset)$ -flag is essentially a  $t$ -dimensional subspace of  $\mathbb{F}_q^n$  and a  $((t, n-t), \{1\})$ -flag is essentially a  $t$ -tuple of linearly independent elements of  $\mathbb{F}_q^n$ .

Let  $\Omega$  be a set on which  $\mathrm{GL}(n, q)$  acts. We say that a subset  $Y$  of  $\mathrm{GL}(n, q)$  is *transitive* on  $\Omega$  if there is a constant  $r$  such that the following holds. For all  $a, b \in \Omega$ , there are exactly  $r$  elements  $g \in Y$  such that  $ga = b$ . If  $r = 1$ , then we also call  $Y$  *sharply* transitive on  $\Omega$ . If  $Y$  is a subgroup of  $\mathrm{GL}(n, q)$ , then this notion coincides with that of a transitive group action of  $Y$  on  $\Omega$ .

We are interested in subsets of  $\mathrm{GL}(n, q)$  that are transitive on  $\alpha$ -flags for  $\alpha \in \Sigma_{n, q}$ . The following example gives a simple construction of subsets of  $\mathrm{GL}(n, q)$  that are sharply transitive on  $((1, n-1), \mathcal{I})$ -flags for  $\mathcal{I} = \{1\}$  and  $\mathcal{I} = \emptyset$ .



**Example 3.1.** Let  $C \in \text{GL}(n, q)$  be the companion matrix of an irreducible polynomial in  $\mathbb{F}_q[X]$  of degree  $n$ . Then  $\mathbb{F}_q[C]$  is a representation of  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$  and so the multiplicative group  $\mathbb{F}_q[C]^*$  of  $\mathbb{F}_q[C]$  is sharply transitive on  $\mathbb{F}_q^n \setminus \{0\}$ . Hence  $\mathbb{F}_q[C]^*$  is sharply transitive on  $((1, n-1), \{1\})$ -flags. Of course  $\mathbb{F}_q[C]^*$  is a cyclic subgroup of  $\text{GL}(n, q)$ , known as a *Singer cycle*. Moreover  $\mathbb{F}_q[C]^*$  contains a cyclic subgroup of order  $(q^n - 1)/(q - 1)$  that is sharply transitive on the one-dimensional subspaces of  $\mathbb{F}_q^n$ . Hence this subgroup is sharply transitive on  $((1, n-1), \emptyset)$ -flags.

More generally, a subset of  $\text{GL}(n, q)$  that is sharply transitive on  $\mathbb{F}_q^n \setminus \{0\}$  is equivalent to each of the following objects: a spread set in  $\mathbb{F}_q^{n \times n}$ , a finite quasifield of order  $q^n$ , and a finite translation plane of order  $q^n$  (see [9, § 5.1], for example).

In what follows we give a structural interpretation of subsets of  $\text{GL}(n, q)$  that are transitive on  $\alpha$ -flags (for  $\alpha \in \Sigma_{n,q}$ ). To do so, we require a few definitions.

With each  $(\rho, \mathcal{I}) \in \Sigma_{n,q}$  we associate a pair of partitions  $(\sigma, \tau)$ , called the *type* of  $(\rho, \mathcal{I})$ , where  $\sigma$  is the partition whose parts are those  $\rho_i$  with  $i \in \mathcal{I}$  and  $\tau$  is the partition whose parts are those  $\rho_i$  with  $i \notin \mathcal{I}$ . For example  $((25123), \{2, 3, 5\})$  has type  $((531), (22))$ . We denote the type of  $\alpha \in \Sigma_{n,q}$  by  $\text{type}(\alpha)$  and the set of possible such types by  $\Theta_{n,q}$ . Hence  $\Theta_{n,q}$  contains all pairs of partitions  $(\sigma, \tau)$  such that  $|\sigma| + |\tau| = n$  and all parts of  $\tau$  are strictly larger than 1 for  $q = 2$ .

We also define the *type* of  $\underline{\lambda} \in \Lambda_n$  as a pair of partitions  $(\kappa, \lambda)$ , where  $\lambda = \underline{\lambda}(1)$  and  $\kappa$  has  $|\underline{\lambda}(f)|$  parts of size  $|f|$  as  $f$  ranges through  $\Phi \setminus \{X - 1\}$ . For example, when  $q = 3$ , the type of  $\underline{\lambda} \in \Lambda_n$  given by

$$X - 1 \mapsto (31), \quad X + 1 \mapsto (31), \quad X^2 + 1 \mapsto (2), \quad X^2 + X - 1 \mapsto (21)$$

equals  $((2^5 1^4), (31))$ . We denote the type of  $\underline{\lambda} \in \Lambda_n$  by  $\text{type}(\underline{\lambda})$ . Note that, if  $(\kappa, \lambda)$  is the type of  $\underline{\lambda} \in \Lambda_n$ , then  $|\kappa| + |\lambda| = n$ . Note that the unique irreducible character  $\chi^{\underline{\lambda}}$  of  $\text{GL}(n, q)$  with  $\text{type}(\underline{\lambda}) = (\emptyset, (n))$  is the trivial character.

We define a partial order on pairs of partitions by

$$(\nu, \mu) \leq (\kappa, \lambda) \iff \kappa \text{ refines } \nu \text{ and } \mu \leq \lambda$$

and write  $(\nu, \mu) < (\kappa, \lambda)$  if  $(\nu, \mu) \leq (\kappa, \lambda)$  and  $(\nu, \mu) \neq (\kappa, \lambda)$ . The following result gives a characterisation of subsets of  $\text{GL}(n, q)$  that are transitive on  $\alpha$ -flags as a design in the corresponding conjugacy class association scheme in the sense of Delsarte [7].

**Theorem 3.2.** *Let  $Y$  be a subset of  $\text{GL}(n, q)$  with dual distribution  $(a'_{\underline{\lambda}})$  and let  $\alpha \in \Sigma_{n,q}$ . Then  $Y$  is transitive on  $\alpha$ -flags if and only if*

$$a'_{\underline{\lambda}} = 0 \quad \text{for all } \underline{\lambda} \in \Lambda_n \text{ satisfying } \text{type}(\alpha) \leq \text{type}(\underline{\lambda}) < (\emptyset, (n)).$$

Before we prove Theorem 3.2, we discuss some of its consequences. The first one is that transitivity on  $\alpha$ -flags depends only on the type of  $\alpha$ .

**Corollary 3.3.** *Let  $\alpha, \beta \in \Sigma_{n,q}$  be of the same type and let  $Y$  be a subset of  $\text{GL}(n, q)$ . Then  $Y$  is transitive on  $\alpha$ -flags if and only if  $Y$  is transitive on  $\beta$ -flags.*

Corollary 3.3 motivates the following definition.

**Definition 3.4.** For  $(\sigma, \tau) \in \Theta_{n,q}$ , we define a subset  $Y$  of  $\mathrm{GL}(n, q)$  to be  $(\sigma, \tau)$ -transitive if  $Y$  is transitive on the set of  $\alpha$ -flags for some  $\alpha \in \Sigma_{n,q}$  of type  $(\sigma, \tau)$ .

Note that Example 3.1 gives  $(\sigma, \tau)$ -transitive sets for  $(\sigma, \tau)$  equal to  $((1), (n-1))$  and  $(\emptyset, (n-1, 1))$ . We may now restate Theorem 3.2 as follows.

**Corollary 3.5.** *Let  $Y$  be a subset of  $\mathrm{GL}(n, q)$  with dual distribution  $(a'_\lambda)$  and let  $(\sigma, \tau) \in \Theta_{n,q}$ . Then  $Y$  is  $(\sigma, \tau)$ -transitive if and only if*

$$a'_\lambda = 0 \quad \text{for all } \lambda \in \Lambda_n \text{ satisfying } (\sigma, \tau) \leq \text{type}(\lambda) < (\emptyset, (n)).$$

A  $(\emptyset, \tau)$ -transitive set is just a subset of  $\mathrm{GL}(n, q)$  that is transitive on  $\tau$ -flags (where  $\tau$  is a partition of  $n$ ). In this case Corollary 3.5 specialises to the following result, which is a perfect  $q$ -analog of [26, Theorem 4].

**Corollary 3.6.** *Let  $Y$  be a subset of  $\mathrm{GL}(n, q)$  with dual distribution  $(a'_\lambda)$  and let  $\tau$  be a partition of  $n$ . Then  $Y$  is  $(\emptyset, \tau)$ -transitive if and only if*

$$a'_\lambda = 0 \quad \text{for all } \lambda \in \Lambda_n \text{ satisfying } \tau \trianglelefteq \lambda(1) \triangleleft (n).$$

Another immediate consequence of Theorem 3.2 is the following, of which Theorem 1.4 arises as a special case.

**Corollary 3.7.** *Let  $Y$  be a subset of  $\mathrm{GL}(n, q)$  and suppose that  $Y$  is  $(\sigma, \tau)$ -transitive for some  $(\sigma, \tau) \in \Theta_{n,q}$ . Then  $Y$  is also  $(\hat{\sigma}, \hat{\tau})$ -transitive for all  $(\hat{\sigma}, \hat{\tau}) \in \Theta_{n,q}$  satisfying  $(\sigma, \tau) \leq (\hat{\sigma}, \hat{\tau})$ .*

In the remainder of this section we shall give a proof of Theorem 3.2. A key step will be the following decomposition of the permutation character of  $\alpha$ -flags.

**Proposition 3.8.** *Let  $\alpha \in \Sigma_{n,q}$ , let  $\xi$  be the permutation character of  $\alpha$ -flags, and let*

$$\xi = \sum_{\lambda \in \Lambda_n} m_\lambda \chi^\lambda$$

*be the decomposition of  $\xi$  into irreducible characters. Then we have*

$$m_\lambda \neq 0 \quad \Leftrightarrow \quad \text{type}(\alpha) \leq \text{type}(\lambda).$$

*Proof.* Write  $\alpha = (\rho, \mathcal{I})$ , where  $\rho = (\rho_1, \rho_2, \dots, \rho_k)$ . We define a subgroup  $H$  of  $\mathrm{GL}(n, q)$  by

$$H = \left\{ \left[ \begin{array}{cccc} A_1 & * & \cdots & * \\ & A_2 & \cdots & * \\ & & \ddots & \vdots \\ & & & A_k \end{array} \right] : A_i \in \mathrm{GL}(\rho_i, q), A_i = I_{\rho_i} \text{ if } i \in \mathcal{I} \right\}.$$

Then  $H$  is the stabiliser of an  $\alpha$ -flag and we have

$$\xi = \mathrm{Ind}_H^{\mathrm{GL}(n,q)}(1_H),$$

where  $1_H$  is the trivial character of  $H$ . We first induce  $1_H$  to the parabolic subgroup  $P_\rho$ . For  $1 \leq i \leq k$ , let  $\pi_i : P_\rho \rightarrow \mathrm{GL}(\rho_i, q)$  be the projections given in (2). Hence

$$1_H = \prod_{i=1}^k (1_i \circ \pi_i),$$

where  $1_i$  is the trivial character on the trivial subgroup of  $\mathrm{GL}(\rho_i, q)$  for  $i \in \mathcal{I}$  and  $1_i$  is the trivial character of  $\mathrm{GL}(\rho_i, q)$  for  $i \in \mathcal{J}$ , where  $\mathcal{J}$  is the complement of  $\mathcal{I}$  in  $\{1, 2, \dots, k\}$ . We have

$$P_\rho/H \cong \prod_{i \in \mathcal{I}} \mathrm{GL}(\rho_i, q),$$

as a direct product. By Frobenius reciprocity, for each  $i \in \mathcal{I}$ , the induction of  $1_i$  to  $\mathrm{GL}(\rho_i, q)$  equals

$$\sum_{\kappa \in \Lambda_{\rho_i}} f_\kappa \chi^\kappa$$

(recall that  $f_\kappa$  is the degree of  $\chi^\kappa$ ). Hence we obtain

$$\mathrm{Ind}_H^{P_\rho}(1_H) = \left( \prod_{i \in \mathcal{J}} (1_i \circ \pi_i) \right) \left( \prod_{i \in \mathcal{I}} \sum_{\kappa \in \Lambda_{\rho_i}} f_\kappa (\chi^\kappa \circ \pi_i) \right).$$

By the transitivity of induction,  $\xi$  is obtained by inducing  $\mathrm{Ind}_H^{P_\rho}(1_H)$  to  $\mathrm{GL}(n, q)$ . To determine the irreducible constituents of  $\xi$ , it is now enough to determine the irreducible constituents of the induced characters

$$(10) \quad \phi_1 \cdot \phi_2 \cdots \phi_k,$$

where  $\phi_i$  is an irreducible character of  $\mathrm{GL}(\rho_i, q)$  for  $i \in \mathcal{I}$  and  $\phi_i$  is the trivial character of  $\mathrm{GL}(\rho_i, q)$  for  $i \in \mathcal{J}$ . Since the product of characters is commutative, we may now assume without loss of generality that  $\mathcal{I} = \{1, 2, \dots, r\}$ , where  $r = |\mathcal{I}|$ . We put  $\sigma = (\rho_1, \dots, \rho_r)$  and  $\tau = (\rho_{r+1}, \dots, \rho_k)$  (so that  $(\sigma, \tau)$  is the type of  $(\rho, \mathcal{I})$ ). Now consider the parabolic subgroup  $P = P_{(\rho_1, \dots, \rho_r, |\tau|)}$ . We have

$$P/P_\rho \cong \mathrm{GL}(|\tau|, q)/P_\tau$$

and hence by Lemma 2.3 the character (10) induces on  $P$  to

$$\sum_{\nu \supseteq \tau} K_{\nu\tau} \chi^{X^{-1} \rightarrow \nu} \cdot \phi_1 \cdots \phi_r.$$

To determine the irreducible constituents of  $\xi$ , it is now enough to determine the irreducible constituents of the induced characters

$$(11) \quad \phi_0 \cdot \phi_1 \cdots \phi_r,$$

where  $\phi_0$  is a unipotent irreducible character of  $\mathrm{GL}(|\tau|, q)$  corresponding to a partition  $\nu$  with  $\nu \supseteq \tau$  and  $\phi_i$  is an irreducible character of  $\mathrm{GL}(\rho_i, q)$  for  $1 \leq i \leq r$ .

To prove the forward direction of the lemma, assume that  $\chi^\lambda$  is a constituent of some induced character of the form (11). Let  $(\kappa, \lambda)$  be the type of  $\underline{\lambda}$  and let  $(\kappa^{(i)}, \lambda^{(i)})$

be the type of the element of  $\Lambda_{\rho_i}$  indexing  $\phi_i$ . Then Lemma 2.1 implies that the parts of  $\kappa$  are exactly the parts of  $\kappa^{(1)}, \kappa^{(2)}, \dots, \kappa^{(r)}$ . Since  $\phi_i$  is a character of  $\mathrm{GL}(\rho_i, q)$ , we find that  $\kappa^{(i)}$  refines  $(\rho_i)$  and hence  $\kappa$  refines  $\sigma$ . By assumption there is some partition  $\nu$  with  $|\nu| = |\tau|$  such that  $\nu \supseteq \tau$ , which by Lemma 2.1 satisfies  $\nu \subseteq \lambda$ . Hence we have  $\lambda \supseteq \tau$ , which proves the forward direction of the lemma.

To prove the reverse direction, let  $\underline{\lambda} \in \Lambda_n$  be such that its type  $(\kappa, \lambda)$  satisfies  $(\sigma, \tau) \leq (\kappa, \lambda)$ . Then  $\kappa$  is a refinement of  $\sigma$  and  $\tau \trianglelefteq \lambda$ . It is readily verified that there exists a partition  $\nu$  with  $|\nu| = |\tau|$  such that  $\nu \supseteq \tau$  and  $\nu \subseteq \lambda$ . Let  $\underline{\lambda}_0 \in \Lambda_{|\tau|}$  be given by  $X - 1 \mapsto \nu$ . Since  $\kappa$  is a refinement of  $\sigma$ , there is a chain of partition-valued functions

$$\underline{\lambda}_0 \subseteq \underline{\lambda}_1 \subseteq \dots \subseteq \underline{\lambda}_r = \underline{\lambda}$$

with the property  $\|\underline{\lambda}_i\| - \|\underline{\lambda}_{i-1}\| = \rho_i$  for all  $i \in \{1, 2, \dots, r\}$ . By Remark 2.2, we can choose  $\underline{\delta}_i \in \Lambda_{\rho_i}$  such that

$$c_{\underline{\lambda}_{i-1}, \underline{\delta}_i}^{\underline{\lambda}_i} > 0 \quad \text{for each } i \in \{1, 2, \dots, r\}.$$

Now we take  $\phi_0 = \chi^{\underline{\lambda}_0}$  and  $\phi_i = \chi^{\underline{\delta}_i}$  for each  $i \in \{1, 2, \dots, r\}$ . Then

$$\phi_0 \cdot \phi_1 \cdots \phi_r$$

has  $\chi^{\underline{\lambda}_i}$  as an irreducible constituent for each  $i \in \{1, 2, \dots, r\}$ . Hence  $\chi^{\underline{\lambda}}$  is an irreducible constituent of  $\phi_0 \cdot \phi_1 \cdots \phi_r$ , which completes the proof.  $\square$

Now, for  $\alpha \in \Sigma_{n,q}$ , let  $\mathcal{F}_\alpha$  be the set of  $\alpha$ -flags and define  $M_\alpha \in \mathbb{C}(\mathrm{GL}(n, q), \mathcal{F}_\alpha \times \mathcal{F}_\alpha)$  to be the incidence matrix of elements of  $\mathrm{GL}(n, q)$  versus left cosets of stabilisers of  $\alpha$ -flags by

$$M_\alpha(g, (u, v)) = \begin{cases} 1 & \text{for } gu = v \\ 0 & \text{otherwise.} \end{cases}$$

Recall the definition of the vector spaces  $V_\lambda$  from Section 2.5 and, for  $(\sigma, \tau) \in \Theta_{n,q}$ , define

$$(12) \quad U_{(\sigma, \tau)} = \sum_{\substack{\lambda \in \Lambda_n \\ (\sigma, \tau) \leq \text{type}(\lambda)}} V_\lambda.$$

Note that in view of (6) this sum is direct.

**Corollary 3.9.** *The column space of  $M_\alpha$  equals  $U_{\text{type}(\alpha)}$ .*

*Proof.* Let  $\xi$  be the permutation character of the set of  $\alpha$ -flags and define  $C_\alpha \in \mathbb{C}(\mathrm{GL}(n, q), \mathrm{GL}(n, q))$  by  $C_\alpha(x, y) = \xi(x^{-1}y)$ . Denoting by  $\mathbb{1}_{xu=v}$  the indicator of the

event that  $x \in \text{GL}(n, q)$  maps  $u$  to  $v$ , we have

$$\begin{aligned}
(M_\alpha M_\alpha^\top)(x, y) &= \sum_{u, v} M_\alpha(x, (u, v)) M_\alpha(y, (u, v)) \\
&= \sum_{u, v} \mathbb{1}_{xu=v} \mathbb{1}_{yu=v} \\
&= \sum_u \mathbb{1}_{xu=yu} \\
&= \sum_u \mathbb{1}_{x^{-1}yu=u} \\
&= \xi(x^{-1}y) = C_\alpha(x, y).
\end{aligned}$$

Hence we have  $C_\alpha = M_\alpha M_\alpha^\top$  and so the column space of  $C_\alpha$  equals the column space of  $M_\alpha$ .

From Proposition 3.8 and (5) we obtain

$$(13) \quad C_\alpha = |\text{GL}(n, q)| \sum_{\substack{\lambda \in \Lambda_n \\ \text{type}(\alpha) \leq \text{type}(\lambda)}} (m_\lambda / f_\lambda) E_\lambda.$$

Hence the column space of  $C_\alpha$  is contained in  $U_{\text{type}(\alpha)}$ . Conversely, let  $v$  be a column of  $E_{\underline{\kappa}}$  for some  $\underline{\kappa} \in \Lambda_n$  satisfying  $\text{type}(\underline{\kappa}) \geq \text{type}(\alpha)$ . From (4) we have  $E_{\underline{\lambda}}v = v$  for  $\underline{\kappa} = \underline{\lambda}$  and  $E_{\underline{\lambda}}v = 0$  for  $\underline{\kappa} \neq \underline{\lambda}$ . Hence from (13) we find that

$$C_\alpha v = |\text{GL}(n, q)| (m_{\underline{\kappa}} / f_{\underline{\kappa}}) v,$$

and, since  $m_{\underline{\kappa}} \neq 0$ , we conclude that  $v$  is in the column space of  $C_\alpha$ , as required.  $\square$

We now complete the proof of Theorem 3.2.

*Proof of Theorem 3.2.* Note that  $Y$  is transitive on  $\alpha$ -flags if and only if

$$\frac{1}{|Y|} M_\alpha^\top \mathbb{1}_Y = \frac{1}{|\text{GL}(n, q)|} M_\alpha^\top \mathbb{1}_{\text{GL}(n, q)},$$

hence if and only if

$$\mathbb{1}_Y - \frac{|Y|}{|\text{GL}(n, q)|} \mathbb{1}_{\text{GL}(n, q)}$$

is orthogonal to the column space of  $M_\alpha$ . In view of the orthogonal decomposition of this space given in Corollary 3.9 and the fact that  $V_{X^{-1} \rightarrow (n)}$  is spanned by  $\mathbb{1}_{\text{GL}(n, q)}$ , we conclude that  $Y$  is transitive on  $\alpha$ -flags if and only if  $\mathbb{1}_Y$  is orthogonal to  $V_{\underline{\lambda}}$  for each  $\underline{\lambda} \in \Lambda_n$  satisfying  $\text{type}(\alpha) \leq \text{type}(\underline{\lambda}) < (\emptyset, (n))$ . This is equivalent to the statement of the theorem.  $\square$

## 4. TRANSITIVE SUBGROUPS

In this section we classify subgroups  $G$  of  $\mathrm{GL}(n, q)$  that are  $(\sigma, \tau)$ -transitive. These results are essentially known. If  $G$  is  $((1), (n-1))$ -transitive or  $(\emptyset, (n-1, 1))$ -transitive or  $((1^2), \emptyset)$  if  $q = 2$ , then  $G$  is transitive on 1-spaces of  $\mathbb{F}_q^n$ . Such subgroups have been classified by Hering [15], see also [13, Table 3.1] for a nice summary. However, as we always have examples of sharply  $(\sigma, \tau)$ -transitive subgroups in these cases (see Example 3.1), we shall henceforth assume that  $(\sigma, \tau)$  is different from  $((1), (n-1))$  and  $(\emptyset, (n-1, 1))$  and also different from  $((1^2), \emptyset)$  if  $q = 2$ .

First consider the case  $n \geq 4$ . By Corollary 3.7,  $G$  is also  $(\emptyset, (n-2, 2))$ -transitive, namely transitive on 2-spaces of  $\mathbb{F}_q^n$ . Kantor [18] proved that  $G$  is either doubly transitive on 1-spaces of  $\mathbb{F}_q^n$  or  $G \cong \Gamma\mathrm{L}(1, 2^5)$  as a subgroup of  $\mathrm{GL}(5, 2)$ , which acts sharply transitive on 2-spaces of  $\mathbb{F}_2^5$ . Cameron and Kantor [5] proved that, if  $G$  is doubly transitive on 1-spaces of  $\mathbb{F}_q^n$ , then  $G$  either contains  $\mathrm{SL}(n, q)$ , in which case  $G$  is  $((n-1), (1))$ -transitive, or  $G \cong A_7$  as a subgroup of  $\mathrm{GL}(4, 2)$ . In fact it is computationally readily verified that the latter example is sharply  $((31), \emptyset)$ -transitive.

Next consider the case  $n = 3$ . Then by Corollary 3.7,  $G$  is also  $(\emptyset, (1^3))$ -transitive when  $q > 2$  or  $((1^3), \emptyset)$ -transitive when  $q = 2$ . That is,  $G$  is transitive on  $(1^3)$ -flags in  $\mathbb{F}_q^3$ , typically just called *flags* in the literature. Kantor [19] proved that  $G$  either contains  $\mathrm{SL}(n, q)$  or  $G$  acts sharply transitive on flags in  $\mathbb{F}_q^3$ . Higman and McLaughlin [16] showed that in the latter case the only possibility is  $G \cong \Gamma\mathrm{L}(1, 2^3)$  as a subgroup of  $\mathrm{GL}(3, 2)$ .

Now consider the case  $n = 2$ . Then we are left with the case that  $G$  is  $((1^2), \emptyset)$ -transitive and  $q > 2$ . The number of  $((1^2), \emptyset)$ -flags is  $(q^2 - 1)(q - 1)$  and the order of  $G$  must be a multiple of this number. Since  $|\mathrm{GL}(2, q)| = (q^2 - 1)(q - 1)q$ , the index of  $G$  in  $\mathrm{GL}(2, q)$  must therefore be a divisor of  $q$ . Noting that  $G$  is transitive on the 1-spaces of  $\mathbb{F}_q^2$ , an inspection of [13, Thm. 3.1] reveals that the only possible cases are  $G \cong \Gamma\mathrm{L}(1, 3^2)$  inside  $\mathrm{GL}(2, 3)$  or  $q$  is one of the numbers 5, 7, 9, 11, 19, 23, 29, 59 and a computer verification reveals that only  $\mathrm{GL}(2, 3)$  and  $\mathrm{GL}(2, 5)$  contain subgroups  $G$  in question. In the former case we have  $G \cong \Gamma\mathrm{L}(1, 3^2)$  and in the latter case  $G$  is unique up to conjugation. In both cases  $G$  is sharply  $((1^2), \emptyset)$ -transitive.

We summarise these results in the following theorem.

**Theorem 4.1.** *Suppose that  $G$  is a  $(\sigma, \tau)$ -transitive nontrivial proper subgroup of  $\mathrm{GL}(n, q)$  and  $(\sigma, \tau)$  is different from  $((1), (n-1))$  and  $(\emptyset, (n-1, 1))$  and also different from  $((1^2), \emptyset)$  if  $q = 2$ . Then one of the following holds:*

- (1)  $q > 2$  and  $G \geq \mathrm{SL}(n, q)$  and  $G$  is  $((n-1), (1))$ -transitive.
- (2)  $(n, q) = (2, 3)$  and  $G \cong \Gamma\mathrm{L}(1, 3^2)$  is sharply  $((1^2), \emptyset)$ -transitive.
- (3)  $(n, q) = (2, 5)$  and  $G$  has order 96 and is sharply  $((1^2), \emptyset)$ -transitive.
- (4)  $(n, q) = (3, 2)$  and  $G \cong \Gamma\mathrm{L}(1, 2^3)$  and  $G$  is sharply  $((1^3), \emptyset)$ -transitive.
- (5)  $(n, q) = (4, 2)$  and  $G \cong A_7$  is sharply  $((31), \emptyset)$ -transitive.
- (6)  $(n, q) = (5, 2)$  and  $G \cong \Gamma\mathrm{L}(1, 2^5)$  is sharply  $(\emptyset, (32))$ -transitive.

It should be noted that there exist groups acting transitively on flags in  $\mathbb{F}_8^3$ , namely  $\Gamma\text{L}(1, 2^9)$  and a subgroup of index 7 [16]. These groups however are not subgroups of  $\text{GL}(3, 8)$ , but rather are subgroups of  $\Gamma\text{L}(3, 8)$ .

## 5. TRANSITIVE SETS AND CLIQUES

In this section we consider so-called cliques in  $\text{GL}(n, q)$  and discuss their relationship to transitivity in  $\text{GL}(n, q)$ .

**Definition 5.1.** Let  $(\sigma, \tau) \in \Theta_{n, q}$ . We define a subset  $Y$  of  $\text{GL}(n, q)$  to be a  $(\sigma, \tau)$ -clique if, for all distinct  $x, y \in Y$ , there is no  $\alpha$ -flag with  $\text{type}(\alpha) = (\sigma, \tau)$  fixed by  $x^{-1}y$ .

For  $\underline{\mu} \in \Lambda$  we define  $\underline{\mu}' \in \Lambda$  to be the mapping  $\underline{\mu}' : \Phi \rightarrow \text{Par}$  given by  $\underline{\mu}'(f) = \underline{\mu}(f)'$ . Note that, if  $\text{type}(\underline{\mu}) = (\nu, \mu)$ , then we have  $\text{type}(\underline{\mu}') = (\nu, \mu')$ .

The following result should be compared with Corollary 3.5, showing that the concept of a  $(\sigma, \tau)$ -clique is dual to the concept of  $(\sigma, \tau)$ -transitivity.

**Theorem 5.2.** *Let  $Y$  be a subset of  $\text{GL}(n, q)$  with inner distribution  $(a_{\underline{\mu}})$  and let  $(\sigma, \tau) \in \Theta_{n, q}$ . Then  $Y$  is a  $(\sigma, \tau)$ -clique if and only if*

$$a_{\underline{\mu}} = 0 \quad \text{for all } \underline{\mu} \in \Lambda_n \text{ satisfying } (\tau, \sigma) \leq \text{type}(\underline{\mu}') < (\emptyset, (n)).$$

*Proof.* Fix  $\underline{\mu} \in \Lambda_n$ . Note that, for  $\alpha \in \Sigma_{n, q}$ , either all elements in  $C_{\underline{\mu}}$  fix an  $\alpha$ -flag or none of the elements in  $C_{\underline{\mu}}$ . We show the elements in  $C_{\underline{\mu}}$  fix an  $\alpha$ -flag with  $\text{type}(\alpha) = (\sigma, \tau)$  if and only if  $(\tau, \bar{\sigma}) \leq (\nu, \mu)$ , where  $(\nu, \mu)$  is the type of  $\underline{\mu}'$ .

First assume that  $(\tau, \sigma) \leq (\nu, \mu)$ , namely  $\sigma \trianglelefteq \mu$  and  $\nu$  refines  $\tau$ . Since  $\sigma \trianglelefteq \mu$ , rearranging rows and columns of the Jordan canonical form of  $C_{\underline{\mu}}$  shows that  $C_{\underline{\mu}}$  contains a block upper-triangular matrix whose diagonal blocks are  $I_{\sigma_1}, I_{\sigma_2}, \dots$  followed by  $|\mu| - |\sigma|$  blocks of order 1 followed by blocks of order  $\nu_1, \nu_2, \dots$ . Since  $\nu$  refines  $\tau$ , this matrix fixes an  $\alpha$ -flag with  $\text{type}(\alpha) = (\sigma, \tau)$ .

Now let  $g \in C_{\underline{\mu}}$  be in Jordan canonical form and assume that  $g$  fixes an  $\alpha$ -flag with  $\text{type}(\alpha) = (\sigma, \tau)$ . By [23, Proposition 4.4] the companion matrix of an irreducible polynomial in  $\mathbb{F}_q[X]$  of degree  $d$  does not fix a proper subspace of  $\mathbb{F}_q^d$ . Hence  $\nu$  must refine  $\tau$ . Also note that  $g$  has  $\mu_i$  Jordan blocks with eigenvalue 1 of order at least  $i$  and each such Jordan block of order  $i$  fixes a  $\beta$ -flag with  $\text{type}(\beta) = ((1^i), \emptyset)$ . Hence  $g$  must have at least

$$\sigma_i - \sum_{j=1}^{i-1} (\mu_j - \sigma_j)$$

Jordan blocks with eigenvalue 1 of order at least  $i$ . The latter statement is equivalent to  $\sigma \trianglelefteq \mu$ .  $\square$

In what follows we establish relationships between  $(\sigma, \tau)$ -cliques and  $(\sigma, \tau)$ -transitive sets in  $\text{GL}(n, q)$ .

**Theorem 5.3.** *Let  $(\sigma, \tau) \in \Theta_{n,q}$ , let  $H$  be the stabiliser of an  $\alpha$ -flag with  $\text{type}(\alpha) = (\sigma, \tau)$ , and let  $Y$  be a subset of  $\text{GL}(n, q)$ .*

- (1) *If  $Y$  is a  $(\sigma, \tau)$ -clique, then  $|Y| \leq |\text{GL}(n, q)|/|H|$  with equality if and only if  $Y$  is  $(\sigma, \tau)$ -transitive.*  
(2) *If  $Y$  is  $(\sigma, \tau)$ -transitive, then  $|Y| \geq |\text{GL}(n, q)|/|H|$  with equality if and only if  $Y$  is a  $(\sigma, \tau)$ -clique.*

*In both cases, equality implies that  $Y$  is sharply  $(\sigma, \tau)$ -transitive.*

*Proof.* Since, for each  $(x, y) \in H \times Y$ , there is a unique  $g \in \text{GL}(n, q)$  such that  $gx = y$ , we have

$$(14) \quad \sum_{g \in \text{GL}(n, q)} |Y \cap gH| = |Y| \cdot |H|.$$

The quotient of any two distinct elements in  $Y \cap gH$  fixes an  $\alpha$ -flag of type  $(\sigma, \tau)$ . Hence, if  $Y$  is a  $(\sigma, \tau)$ -clique, then each summand on the left hand side of (14) is at most 1, which gives the bound in (1). If  $H$  is the stabiliser of the  $\alpha$ -flag  $F$ , then  $gH$  contains precisely all elements of  $\text{GL}(n, q)$  mapping  $F$  to  $gF$ . Hence, if  $Y$  is  $(\sigma, \tau)$ -transitive, then each summand on the left hand side of (14) must be at least 1, which gives the bound in (2). In both cases, equality occurs if and only if  $|Y \cap gH'| = 1$  for each  $g \in G$  and the stabiliser  $H'$  of each  $\alpha$ -flag of type  $(\sigma, \tau)$ . By the same reasoning as above, this establishes the characterisations of equality.  $\square$

Note that, if  $H$  is the stabiliser of an  $\alpha$ -flag with  $\text{type}(\alpha) = (\sigma, \tau)$ , then an elementary counting argument gives

$$\frac{|\text{GL}(n, q)|}{|H|} = \frac{[n]_q!}{\left(\prod_{i \geq 1} [\sigma_i]_q!\right) \left(\prod_{i \geq 1} [\tau_i]_q!\right)} \prod_{i \geq 1} \prod_{j=1}^{\sigma_i-1} (q^{\sigma_i} - q^j),$$

where, for a nonnegative integer  $m$ , the  $q$ -factorial of  $m$  is given by

$$[m]_q! = [m]_q [m-1]_q \cdots [1]_q \quad \text{with} \quad [k]_q = \frac{q^k - 1}{q - 1}.$$

In view of Theorems 5.2 and 5.3 one can rule out the existence of sharply  $(\sigma, \tau)$ -transitive subsets of  $\text{GL}(n, q)$  by linear programming, a standard method in the theory of association schemes. The key observation is that the entries in the dual distribution of a subset of an association scheme are real and nonnegative (see Section 2.5). The so-called linear-programming (LP) bound for  $(\sigma, \tau)$ -cliques is the maximum of

$$\sum_{\underline{\mu} \in \Lambda_n} a_{\underline{\mu}}$$



subject to the constraints

$$a_{\underline{\mu}} \geq 0 \quad \text{for all } \underline{\mu} \in \Lambda_n,$$

$$\sum_{\underline{\mu} \in \Lambda_n} \text{Im}(\chi_{\underline{\mu}}^{\underline{\lambda}}) a_{\underline{\mu}} = 0 \quad \text{and} \quad \sum_{\underline{\mu} \in \Lambda_n} \text{Re}(\chi_{\underline{\mu}}^{\underline{\lambda}}) a_{\underline{\mu}} \geq 0 \quad \text{for all } \underline{\lambda} \in \Lambda_n,$$

$$a_{\underline{\mu}} = 0 \quad \text{for all } \underline{\mu} \in \Lambda_n \text{ satisfying } (\tau, \sigma) \leq \text{type}(\underline{\mu}') < (\emptyset, (n)).$$

Here the second constraint comes from the fact that the entries in the dual distribution of a subset of  $\text{GL}(n, q)$  are real and nonnegative. We have determined the LP bound for  $(\sigma, \tau)$ -cliques in  $\text{GL}(n, 2)$  for  $n \in \{2, 3, 4, 5\}$ . The LP bound coincides with the bound of Theorem 5.3 (i) except for those pairs  $(\sigma, \tau)$  shown in Table 1. Consequently no sharply  $(\sigma, \tau)$ -transitive subsets of  $\text{GL}(n, q)$  can exist in these cases.

TABLE 1. Bounds for cliques in  $\text{GL}(4, 2)$  and  $\text{GL}(5, 2)$ .

$(\sigma, \tau)$	Bound of Thm. 5.3	LP bound
$((21^2), \emptyset)$	630	420
$((1^2), (2))$	105	84
$((2), (2))$	210	168
$((32), \emptyset)$	156 240	139 500
$((31^2), \emptyset)$	78 120	53 010
$((221), \emptyset)$	39 060	24 180
$((21^3), \emptyset)$	19 530	11 718
$((3), (2))$	26 040	19 530
$((21), (2))$	6 510	3 550
$((1^3), (2))$	3 255	2 604
$((1), (22))$	1 085	805

## 6. EXISTENCE RESULTS

In this section we show that, for a partition  $\sigma$ , nonnegative integers  $\tau_2 \geq \tau_3 \geq \dots$ , and sufficiently large  $n$ , there exist  $(\sigma, \tau)$ -transitive sets in  $\text{GL}(n, q)$  that are arbitrarily small compared to  $\text{GL}(n, q)$ , where  $\tau_1 = n - |\sigma| - \tau_2 - \tau_3 - \dots$ . In view of Corollary 3.7, it suffices to consider  $((t), (n-t))$ -transitive sets in  $\text{GL}(n, q)$ . For brevity, we shall call such a set a *t-design* in  $\text{GL}(n, q)$ . These objects will be studied in more detail in Section 7.

We give a recursive construction of *t*-designs in  $\text{GL}(n, q)$  using *t*-designs in the Grassmannian  $J_q(n, k)$ , namely the collection of all  $k$ -spaces of  $\mathbb{F}_q^n$ . A *t-design* in  $J_q(n, k)$  is a subset  $D$  of  $J_q(n, k)$  such that the number of elements in  $D$  containing a

given  $t$ -space of  $\mathbb{F}_q^n$  is independent of the particular choice of this  $t$ -space. Our construction can be understood as a  $q$ -analog of the construction given in [26, Section 6] for the symmetric group  $\text{Sym}(n)$ .

Let  $V = \mathbb{F}_q^n$  and, for a  $k$ -space  $U$  of  $V$ , let  $\text{GL}(U)$  be the general linear group of  $U$ , which is of course isomorphic to  $\text{GL}(k, q)$ . Fix a  $k$ -space  $U$  of  $V$  and an  $(n - k)$ -space  $W$  of  $V$  such that

$$V = U \oplus W.$$

For our recursive construction, we need three ingredients: a  $t$ -design  $Y$  in  $\text{GL}(U)$ , a  $t$ -design  $Z$  in  $\text{GL}(W)$ , and a  $t$ -design  $D$  in  $J_q(n, k)$ . For each  $B \in D$ , there are  $q^{k(n-k)}$  complementary spaces, namely  $(n - k)$ -spaces  $C$  with  $V = B \oplus C$ . We denote the collection of such spaces by  $C_B$ . For each  $B \in D$ , we fix an isomorphism  $g_B : U \rightarrow B$  and, for each  $B \in D$  and each  $C \in C_B$ , we fix an isomorphism  $h_{B,C} : W \rightarrow C$ .

Note that, given a pair  $(B, C)$  with  $B \in D$  and  $C \in C_B$ , then every pair of isomorphisms  $(y, z)$  on  $B$  and  $C$  can be uniquely extended to an isomorphism on  $V$  by linearity. We denote this extension by  $(y, z)$ . Hence, if  $v \in V$ , then there are unique  $b \in B$  and  $c \in C$  with  $v = b + c$  and we have

$$(y, z)(v) = y(b) + z(c).$$

The following lemma contains a recursive construction of  $t$ -designs in  $\text{GL}(n, q)$ .

**Lemma 6.1.** *Let  $Y$  be a  $t$ -design in  $\text{GL}(U)$ , let  $Z$  be a  $t$ -design in  $\text{GL}(W)$ , and let  $D$  be a  $t$ -design in  $J_q(n, k)$ . Then the set*

$$(15) \quad \{(g_B \circ y, h_{B,C} \circ z) : y \in Y, z \in Z, B \in D, C \in C_B\}$$

*is a  $t$ -design in  $\text{GL}(V)$ .*

Note that, taking  $Y = \text{GL}(U)$ ,  $Z = \text{GL}(W)$ , and  $D = J_q(n, k)$ , the set constructed in Lemma 6.1 equals  $\text{GL}(V)$ .

**Example 6.2.** By [4] there exists a 2-design in  $J_2(6, 3)$  of cardinality 279. Taking  $Y$  and  $Z$  to be isomorphic to  $\text{GL}(3, 2)$  in Lemma 6.1, we obtain a 2-design in  $\text{GL}(6, 2)$  of cardinality  $\frac{1}{5}|\text{GL}(6, 2)|$ .

To prove Lemma 6.1, we shall need the following well known result about designs in  $J_q(n, k)$ , in which

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{[n]_q!}{[k]_q! [n-k]_q!}$$

is the  $q$ -binomial coefficient counting the number of  $k$ -spaces of  $\mathbb{F}_q^n$ .

**Lemma 6.3** ([29, Lemma 2.1], [20, Fact 1.5]). *Let  $D$  be a  $t$ -design in  $J_q(n, k)$  and let  $i, j$  be nonnegative integers satisfying  $i + j \leq t$ . Let  $I$  be an  $i$ -space of  $V$  and let  $J$  be a  $j$ -space of  $V$  such that  $I \cap J = \{0\}$ . Then the number*

$$m_{i,j} = |\{B \in D : I \leq B \wedge B \cap J = \{0\}\}|$$

is independent of the particular choice of  $I$  and  $J$  and given by

$$m_{i,j} = |D| q^{j(k-i)} \frac{\begin{bmatrix} n-i-j \\ k-i \end{bmatrix}_q \begin{bmatrix} k \\ t \end{bmatrix}_q}{\begin{bmatrix} n-t \\ k-t \end{bmatrix}_q \begin{bmatrix} n \\ t \end{bmatrix}_q}.$$

We are now ready to prove Lemma 6.1.

*Proof of Lemma 6.1.* Choose  $t$ -tuples  $(v_1, v_2, \dots, v_t)$  and  $(v'_1, v'_2, \dots, v'_t)$  of linearly independent vectors of  $V$ . Suppose that exactly  $i$  of the vectors  $v_1, v_2, \dots, v_t$  are in  $U$ . After reordering we can assume that these are  $v_1, v_2, \dots, v_i$ . Then the remaining  $j = t - i$  vectors  $v_{i+1}, v_{i+2}, \dots, v_t$  are outside  $U$ , namely they belong to complementary spaces of  $U$ .

The number of elements  $B \in D$  containing  $v'_1, v'_2, \dots, v'_i$ , but none of the vectors  $v'_{i+1}, v'_{i+2}, \dots, v'_t$ , equals the constant  $m_{i,j}$  given in Lemma 6.3 and, for each such  $B$ , there are  $q^{k(n-k-j)}$  complementary spaces  $C \in C_B$  containing the remaining  $j$  vectors. Fix a pair  $(C, B)$  with these properties. Write  $v_\ell = u_\ell + w_\ell$  with  $u_\ell \in U$  and  $w_\ell \in W$  for all  $\ell$  and note that our assumption implies that  $v_\ell = u_\ell$  for all  $\ell \leq i$ . There is a constant  $r_i$  such that there are exactly  $r_i$  elements  $y \in Y$  taking  $v_\ell$  to  $g_B^{-1}(v'_\ell)$  for all  $\ell \leq i$ . For each such  $y \in Y$ , there is a constant  $s_j$  such that there are exactly  $s_j$  elements  $z \in Z$  taking  $w_\ell$  to

$$h_{B,C}^{-1}(v'_\ell - g_B(y(u_\ell)))$$

for all  $\ell > i$ .

Hence the total number of automorphisms in (15) taking the tuple  $(v_1, v_2, \dots, v_t)$  to the tuple  $(v'_1, v'_2, \dots, v'_t)$  equals

$$m_{i,j} r_i s_j q^{k(n-k-j)}.$$

We have to show that this number is independent of  $i$ . Lemma 6.3 implies that

$$(q^k - q^i) m_{i,j} = (q^n - q^{k+j-1}) m_{i+1,j-1}$$

and it is readily verified that

$$r_i = (q^k - q^i) r_{i+1}$$

for  $i \leq t - 1$  and

$$s_j = (q^{n-k} - q^j) s_{j+1}$$

for  $j \leq t - 1$ . By combining these identities we find that

$$m_{i+1,j-1} r_{i+1} s_{j-1} q^{k(n-k-j+1)} = m_{i,j} r_i s_j q^{k(n-k-j)},$$

which completes the proof.  $\square$

The following existence result for  $t$ -designs in  $J_q(n, k)$  was obtained by Fazeli, Lovett, and Vardy [10], using the probabilistic approach of Kuperberg, Lovett, and Peled [22].

**Lemma 6.4.** *If  $k > 12(t + 1)$  and  $n \geq ckt$  for some universal constant  $c$ , then there exists a  $t$ -design in  $J_q(n, k)$  of cardinality at most  $q^{12(t+1)n}$ .*

We now use the recursive construction in Lemma 6.1 together with Lemma 6.4 to obtain the following existence result for  $t$ -designs in  $\text{GL}(n, q)$ .

**Theorem 6.5.** *Let  $t$  be a positive integer and let  $\epsilon > 0$ . Then, for all sufficiently large  $n$ , there exists a  $t$ -design  $Y$  in  $\text{GL}(n, q)$  satisfying  $|Y|/|\text{GL}(n, q)| < \epsilon$ .*

*Proof.* Fix  $k > 12(t + 1)$ . We apply Lemma 6.1 with  $Y = \text{GL}(U)$  and  $Z = \text{GL}(W)$ . Then from Lemma 6.4 we obtain the existence of a  $t$ -design in  $\text{GL}(n, q)$  of cardinality at most

$$N = |\text{GL}(k, q)| \cdot |\text{GL}(n - k, q)| q^{k(n-k)} q^{12(t+1)n},$$

provided that  $n \geq ckt$  for the constant  $c$  of Lemma 6.4. Note that we have

$$\frac{N}{|\text{GL}(n, q)|} = \frac{q^{12(t+1)n}}{\begin{bmatrix} n \\ k \end{bmatrix}_q} < \frac{q^{12(t+1)n}}{q^{k(n-k)}}.$$

Since  $k > 12(t + 1)$ , this number tends to zero as  $n$  tends to infinity.  $\square$

By combining Theorem 6.5 and Corollary 3.7 we obtain an existence result for general  $(\sigma, \tau)$ -transitive sets in  $\text{GL}(n, q)$ .

**Corollary 6.6.** *Let  $(\sigma, \tilde{\tau}) \in \Theta_{t,q}$  and let  $\epsilon > 0$ . Then for all sufficiently large  $n$ , there exists a  $(\sigma, \tau)$ -transitive set  $Y$  in  $\text{GL}(n, q)$  satisfying  $|Y|/|\text{GL}(n, q)| < \epsilon$ , where  $\tau = (n - |\sigma| - |\tilde{\tau}|, \tilde{\tau}_1, \tilde{\tau}_2, \dots)$ .*

## 7. DESIGNS, CODES, AND ORTHOGONAL POLYNOMIALS

Certain association schemes, namely  $P$ - and  $Q$ -polynomial association schemes, are closely related to orthogonal polynomials in the sense that their character tables arise as evaluations of such polynomials (see [2] or [7], for example). The conjugacy class association scheme of  $\text{GL}(n, q)$  does not have these properties. Nevertheless there is still a relationship to certain orthogonal polynomials, namely the Al-Salam-Carlitz polynomials.

We shall first recall and establish some basic properties of these polynomials and then apply these results to subsets of  $\text{GL}(n, q)$ .

### 7.1. AL-SALAM-CARLITZ POLYNOMIALS

The Al-Salam-Carlitz polynomials are given by

$$U_k^{(a)}(x) = \sum_{j=0}^k (-1)^{k-j} q^{\binom{k-j}{2}} \begin{bmatrix} k \\ j \end{bmatrix}_q \prod_{i=0}^{j-1} (x - aq^i).$$

They were introduced in [1] and some properties can be found in [6] and [21]. We are only interested in the case  $a = 1$  and write  $U_k(x)$  for  $U_k^{(1)}(x)$ . These polynomials satisfy the recurrence relation

$$U_{k+1}(x) = (x - 2q^k)U_k(x) + q^{k-1}(1 - q^k)U_{k-1}(x) \quad \text{for } k \geq 0$$

with the initial condition  $U_{-1}(x) = 0$  and  $U_0(x) = 1$ . The first polynomials are

$$U_1(x) = x - 2$$

$$U_2(x) = x^2 - 2(q+1)x + 3q + 1$$

$$U_3(x) = x^3 - 2(q^2 + q + 1)x^2 + (3q^3 + 4q^2 + 4q + 1)x - 2q(2q^2 + q + 1).$$

An equivalent definition of the Al-Salam-Carlitz polynomials is

$$(16) \quad \sum_{k=0}^j \begin{bmatrix} j \\ k \end{bmatrix}_q U_k(x) = \prod_{i=0}^{j-1} (x - q^i) \quad \text{for } j = 0, 1, \dots$$

This follows from the inversion formula

$$(17) \quad \sum_{k=j}^{\ell} (-1)^{k-j} q^{\binom{k-j}{2}} \begin{bmatrix} k \\ j \end{bmatrix}_q \begin{bmatrix} \ell \\ k \end{bmatrix}_q = \delta_{j\ell},$$

which in turn can be obtained from the  $q$ -binomial theorem.

The Al-Salam-Carlitz polynomials are  $q$ -analogs of the Charlier polynomials and are orthogonal with respect to a  $q$ -analog of a Poisson distribution, whose  $k$ -th moment is

$$(18) \quad \sum_{i=0}^k \begin{bmatrix} k \\ i \end{bmatrix}_q,$$

the number of subspaces of a  $k$ -dimensional vector space over  $\mathbb{F}_q$ . Let  $\theta$  denote the class function of  $\text{GL}(n, q)$  given by

$$\theta(g) = q^{n - \text{rk}(g-I)}$$

for each  $g \in \text{GL}(n, q)$ , where  $I$  is the identity of  $\text{GL}(n, q)$ . Let  $w_i$  be the number of elements  $g \in \text{GL}(n, q)$  satisfying  $\theta(g) = q^i$ . Explicit expressions for  $w_i$  were obtained by Rudvalis and Shinoda in an unpublished work [28] and by Fulman [11], which shows that

$$(19) \quad w_i = \frac{|\text{GL}(n, q)|}{|\text{GL}(i, q)|} \sum_{k=0}^{n-i} \frac{(-1)^k q^{\binom{k}{2}}}{q^{ki} |\text{GL}(k, q)|}.$$

We shall later see that this expression also follows from our results (see Remark 7.7).

The class function  $\theta$  defines a discrete random variable on  $\text{GL}(n, q)$  and it was shown in [12] that its  $k$ -th moment equals (18), provided that  $k \leq n$ . Hence the

Al-Salam-Carlitz polynomials also satisfy the orthogonality relation

$$(20) \quad \sum_{i=0}^n w_i U_k(q^i) U_\ell(q^i) = 0 \quad \text{for } k \neq \ell \text{ and } k + \ell \leq n.$$

(It follows from Theorem 7.1 that, for  $k = \ell$  and  $2k \leq n$ , the evaluation of the left-hand side is  $|\mathrm{GL}(k, q)| \cdot |\mathrm{GL}(n, q)|$ .)

With every polynomial  $f(x) = f_n x^n + \cdots + f_1 x + f_0$  in  $\mathbb{R}[x]$  we associate the class function  $f(\theta) = f_n \theta^n + \cdots + f_1 \theta + f_0$ . This induces an algebra homomorphism from  $\mathbb{R}[x]$  to the set of class functions of  $\mathrm{GL}(n, q)$ . Let  $\xi_j$  be the permutation character on ordered  $j$ -tuples of linearly independent elements of  $\mathbb{F}_q^n$ . By convention  $\xi_0$  is the trivial character of  $\mathrm{GL}(n, q)$ . Note that

$$\xi_j = \prod_{i=0}^{j-1} (\theta - q^i).$$

Hence we have

$$(21) \quad U_k(\theta) = \sum_{j=0}^k (-1)^{k-j} q^{\binom{k-j}{2}} \begin{bmatrix} k \\ j \end{bmatrix}_q \xi_j \quad \text{for } k = 0, 1, \dots, n$$

and by (16)

$$(22) \quad \xi_j = \sum_{k=0}^j \begin{bmatrix} j \\ k \end{bmatrix}_q U_k(\theta) \quad \text{for } j = 0, 1, \dots, n.$$

For  $0 \leq k \leq n/2$ , we now decompose  $U_k(\theta)$  into irreducible characters of  $\mathrm{GL}(n, q)$ .

**Theorem 7.1.** *For  $0 \leq k \leq n/2$ , the decomposition of  $U_k(\theta)$  into irreducible characters is*

$$(23) \quad U_k(\theta) = \sum_{\underline{\nu} \in \Lambda_k} f_{\underline{\nu}} \chi^{r(\underline{\nu})},$$

where  $r(\underline{\nu})$  is the element  $\underline{\lambda} \in \Lambda_n$  that agrees with  $\underline{\nu}$  except on 1, where it is  $\underline{\lambda}(1) = (n - k, \underline{\nu}(1)_1, \underline{\nu}(1)_2, \dots)$ , namely  $\underline{\lambda}(1)$  is obtained from  $\underline{\nu}(1)$  by inserting a row with  $n - k$  boxes in the Young diagram of  $\underline{\nu}(1)$ . In particular  $U_k(\theta)$  is a character.

*Proof.* Since  $U_0(\theta)$  is just the trivial character, (23) holds for  $k = 0$ . Let  $m$  be an integer satisfying  $1 \leq m \leq n/2$  and suppose that (23) holds for all  $k$  satisfying  $0 \leq k \leq m - 1$ . We show that (23) then also holds for  $k = m$ .

Recall that the standard scalar product on class functions  $\phi$  and  $\psi$  of  $\mathrm{GL}(n, q)$  is given by

$$\langle \phi, \psi \rangle = \frac{1}{|\mathrm{GL}(n, q)|} \sum_{g \in \mathrm{GL}(n, q)} \phi(g) \overline{\psi(g)}.$$

It follows from the orthogonality relation (20) that

$$\langle U_k(\theta), U_\ell(\theta) \rangle = 0 \quad \text{for } 0 \leq k < \ell \leq n/2.$$

From (22) we have  $\langle \xi_m, U_k(\theta) \rangle = \langle U_k(\theta), U_k(\theta) \rangle$  for all  $k$  satisfying  $1 \leq k \leq n/2$ . Since  $U_k(\theta)$  is a character for all  $k$  satisfying  $0 \leq k \leq m-1$ , we find from (22) that  $U_m(\theta)$  decomposes into those irreducible characters that occur in the decomposition of  $\xi_m$ , but not in the decomposition of  $U_0(\theta), U_1(\theta), \dots, U_{m-1}(\theta)$ , hence not in the decomposition of  $\xi_{m-1}$ .

As in the proof of Proposition 3.8 we have

$$\xi_m = \sum_{\underline{\nu} \in \Lambda_m} f_{\underline{\nu}} (\chi^{\underline{\nu}} \cdot 1_{\text{GL}(n-m, q)}),$$

where  $1_{\text{GL}(n-m, q)}$  is the trivial character of  $\text{GL}(n-m, q)$ . Note that the Littlewood-Richardson coefficient  $c_{\nu, (n-m)}^{\mu}$  is either 0 or 1 and it equals 1 precisely when the Young diagram of  $\mu$  is obtained from that of  $\nu$  by adding  $n-m$  cells no two of which are in the same column (this special case is also known as Pieri's rule). Hence by Lemma 2.1 the character  $\chi^{\underline{\nu}} \cdot 1_{\text{GL}(n-m, q)}$  decomposes into those irreducible characters  $\chi^{\underline{\lambda}}$  for which  $\underline{\lambda}$  agrees with  $\underline{\nu}$  except on 1 and  $\underline{\lambda}(1)$  is obtained from  $\underline{\nu}(1)$  by adding  $n-m$  boxes to the Young diagram of  $\underline{\nu}(1)$  no two of which in the same column. Hence the irreducible characters occurring in the decomposition of  $\xi_m$  but not in the decomposition of  $\xi_{m-1}$  are precisely  $\chi^{r(\underline{\nu})}$  with multiplicity  $f_{\underline{\nu}}$ , where  $\underline{\nu} \in \Lambda_m$ .  $\square$

By combining Theorem 7.1 and (22), we obtain the decomposition into irreducible characters of  $\xi_j$  for  $0 \leq j \leq n/2$ . This result strengthens Proposition 3.8 for  $(\sigma, \tau) = ((t), (n-t))$  and  $t \leq n/2$ .

**Corollary 7.2.** *For  $0 \leq j \leq n/2$  the decomposition of  $\xi_j$  into irreducible characters is*

$$\xi_j = \sum_{k=0}^j \begin{bmatrix} j \\ k \end{bmatrix}_q \sum_{\underline{\nu} \in \Lambda_k} f_{\underline{\nu}} \chi^{r(\underline{\nu})},$$

where  $r(\underline{\nu})$  is as in Theorem 7.1.

## 7.2. DESIGNS AND CODES

Henceforth we call a  $((t), (n-t))$ -transitive subset of  $\text{GL}(n, q)$  a  $t$ -design. Thus a  $t$ -design in  $\text{GL}(n, q)$  is transitive on the set of  $t$ -tuples of linearly independent elements of  $\mathbb{F}_q^n$ . We also call an  $((n-d+1), (d-1))$ -clique a  $d$ -code. Hence, for all distinct elements  $x, y$  of a  $d$ -code, there is no  $(n-d+1)$ -tuple of linearly independent elements of  $\mathbb{F}_q^n$  fixed by  $x^{-1}y$ . This implies that  $\text{rk}(x-y) \geq d$  for all distinct  $x, y$  in a  $d$ -code.

Theorems 3.2 and 5.2 specialise in these cases as follows.

**Corollary 7.3.** *Let  $Y$  be a subset of  $\text{GL}(n, q)$  with inner distribution  $(a_{\underline{\mu}})$  and dual distribution  $(a'_{\underline{\lambda}})$ . Then  $Y$  is a  $t$ -design if and only if*

$$a'_{\underline{\lambda}} = 0 \quad \text{for each } \underline{\lambda} \in \Lambda_n \text{ satisfying } n-t \leq \underline{\lambda}(1)_1 < n$$

and a  $d$ -code if and only if

$$a_{\underline{\mu}} = 0 \quad \text{for each } \underline{\mu} \in \Lambda_n \text{ satisfying } n-d+1 \leq \underline{\mu}(1)'_1 < n$$

Note that the mapping  $(x, y) \mapsto \text{rk}(x - y)$  is a metric on  $\text{GL}(n, q)$ . Accordingly, for a subset  $Y$  of  $\text{GL}(n, q)$ , we define the *distance distribution* to be the tuple  $(A_i)_{0 \leq i \leq n}$ , where

$$A_i = \frac{1}{|Y|} |\{(x, y) \in Y \times Y : \text{rk}(x - y) = i\}|$$

and the *dual distance distribution* to be the tuple  $(A'_k)_{0 \leq k \leq n}$ , where

$$A'_k = \sum_{i=0}^n U_k(q^{n-i}) A_i.$$

Note that

$$(24) \quad A'_k = \frac{1}{|Y|} \sum_{x, y \in Y} U_k(q^{n-\text{rk}(x-y)}).$$

We now characterise  $t$ -designs in terms of zeros in its dual distance distribution.

**Proposition 7.4.** *Let  $Y$  be a subset of  $\text{GL}(n, q)$  with dual distance distribution  $(A'_k)$  and let  $t$  be an integer satisfying  $1 \leq t \leq n$ . If  $Y$  is a  $t$ -design, then  $A'_k = 0$  for all  $k$  satisfying  $1 \leq k \leq t$ . Moreover the converse also holds if  $t \leq n/2$ . That is, if  $t \leq n/2$  and  $A'_k = 0$  for all  $k$  satisfying  $1 \leq k \leq t$ , then  $Y$  is a  $t$ -design.*

*Proof.* First suppose that  $Y$  is a  $t$ -design. From (24) and (21) we have

$$(25) \quad A'_k = \frac{1}{|Y|} \sum_{j=0}^k (-1)^{k-j} q^{\binom{k-j}{2}} \begin{bmatrix} k \\ j \end{bmatrix}_q \sum_{x, y \in Y} \xi_j(x^{-1}y).$$

By Proposition 3.8, the permutation character  $\xi_j$  decomposes into those irreducible characters  $\chi^\lambda$  for which  $((j), (n-j)) \leq \text{type}(\lambda)$  or equivalently  $\lambda(1)_1 \geq n-j$ . Moreover, since  $\xi_j$  is a permutation character, it contains the trivial character with multiplicity 1. From Corollary 7.3 we then find that the inner sum in (25) equals  $|Y|^2$  for all  $j$  satisfying  $0 \leq j \leq t$ . Hence we have, for all  $k$  satisfying  $0 \leq k \leq t$ ,

$$A'_k = |Y| \sum_{j=0}^k (-1)^{k-j} q^{\binom{k-j}{2}} \begin{bmatrix} k \\ j \end{bmatrix}_q = |Y| \delta_{k,0},$$

using (17) together with elementary manipulations.

Now, for each  $k$  satisfying  $0 \leq k \leq n/2$ , we find from (24), Theorem 7.1, and (9) that

$$\begin{aligned} A'_k &= \frac{1}{|Y|} \sum_{\underline{\nu} \in \Lambda_k} f_{\underline{\nu}} \sum_{x, y \in Y} \chi^{r(\underline{\nu})}(x^{-1}y) \\ &= \sum_{\underline{\nu} \in \Lambda_k} \frac{f_{\underline{\nu}}}{f_{r(\underline{\nu})}} a'_{r(\underline{\nu})}, \end{aligned}$$

where  $r(\underline{\nu})$  is as in Theorem 7.1. Suppose that  $t$  satisfies  $1 \leq t \leq n/2$  and that  $A'_k = 0$  for all  $k$  satisfying  $1 \leq k \leq t$ . Since  $f_{\underline{\nu}}/f_{r(\underline{\nu})}$  is positive, we find that  $a'_{r(\underline{\nu})} = 0$  for all



$\underline{\nu} \in \Lambda_k$  and hence  $a'_{\underline{\lambda}} = 0$  for all  $\underline{\lambda} \in \Lambda_n$  satisfying  $n - t \leq \underline{\lambda}(1)_1 < n$ . Corollary 7.3 then implies that  $Y$  is a  $t$ -design.  $\square$

Theorem 5.3 specialises as follows.

**Corollary 7.5.** *Let  $Y$  be a subset of  $\text{GL}(n, q)$  and let  $d$  and  $t$  be the largest integers such that  $Y$  is a  $d$ -code and a  $t$ -design. Then*

$$\prod_{i=0}^{t-1} (q^n - q^i) \leq |Y| \leq \prod_{i=0}^{n-d} (q^n - q^i).$$

Moreover, if equality holds in one of the bounds, then equality also holds in the other and this case happens if and only if  $d = n - t + 1$ .

The upper bound in Corollary 7.5 is a  $q$ -analog of a corresponding well known bound  $n(n-1)\cdots d$  for permutation codes [3]. The bounds in Corollary 7.5 can be achieved. A Singer cycle in  $\text{GL}(n, q)$  gives an  $n$ -code in  $\text{GL}(n, q)$  of size  $q^n - 1$  (see Example 3.1) and  $A_7$  inside  $\text{GL}(4, 2)$  is a 2-code of size 2520 (see Section 4).

It turns out that the distance distribution of a subset  $Y$  of  $\text{GL}(n, q)$  is uniquely determined by its parameters, provided that  $Y$  is a  $t$ -design and a  $d$ -code, where  $d \geq n - t$ . The following result generalises (19).

**Theorem 7.6.** *Suppose that  $Y$  is a  $t$ -design and an  $(n - t)$ -code in  $\text{GL}(n, q)$ . Then the distance distribution  $(A_i)$  of  $Y$  satisfies*

$$A_{n-i} = \sum_{j=i}^t (-1)^{j-i} q^{\binom{j-i}{2}} \begin{bmatrix} j \\ i \end{bmatrix}_q \begin{bmatrix} n \\ j \end{bmatrix}_q \left( \frac{|Y|}{\prod_{k=0}^{j-1} (q^n - q^k)} - 1 \right)$$

for each  $i \in \{0, 1, \dots, n-1\}$ .

*Proof.* We have

$$A'_k = \sum_{i=0}^n U_k(q^i) A_{n-i}.$$

Multiply both sides by  $\begin{bmatrix} j \\ k \end{bmatrix}_q$ , sum over  $k$ , and use (16) to find that

$$\sum_{k=0}^j \begin{bmatrix} j \\ k \end{bmatrix}_q A'_k = \sum_{i=0}^n A_{n-i} \prod_{k=0}^{j-1} (q^i - q^k).$$

Since  $Y$  is an  $(n - t)$ -code, we have  $A_1 = \cdots = A_{n-t-1} = 0$  and, since  $Y$  is a  $t$ -design, we find by Proposition 7.4 that  $A'_1 = \cdots = A'_t = 0$ . Moreover we have  $A_0 = 1$  and  $A'_0 = |Y|$  and therefore

$$|Y| - \prod_{k=0}^{j-1} (q^n - q^k) = \sum_{i=0}^t A_{n-i} \prod_{k=0}^{j-1} (q^i - q^k)$$

for each  $j \in \{1, 2, \dots, t\}$ . The identity

$$\prod_{k=0}^{j-1} (q^i - q^k) = \begin{bmatrix} i \\ j \end{bmatrix}_q (q^j - 1) \cdots (q^j - q^{j-1})$$

gives

$$\begin{aligned} \sum_{i=0}^t A_{n-i} \begin{bmatrix} i \\ j \end{bmatrix}_q &= \frac{|Y| - \prod_{k=0}^{j-1} (q^n - q^k)}{\prod_{k=0}^{j-1} (q^j - q^k)} \\ &= \begin{bmatrix} n \\ j \end{bmatrix}_q \left( \frac{|Y|}{\prod_{k=0}^{j-1} (q^n - q^k)} - 1 \right) \end{aligned}$$

for each  $j \in \{1, 2, \dots, t\}$ . Now the inversion formula (17) gives the desired result.  $\square$

**Remark 7.7.** Consider  $Y = \text{GL}(n, q)$  with inner distribution  $(A_i)$ , so that  $A_{n-i} = w_i$  for all  $i$ . Since  $Y$  is a 1-code and an  $n$ -design, Theorem 7.6 gives

$$A_{n-i} = \sum_{j=i}^{n-1} (-1)^{j-i} q^{\binom{j-i}{2}} \begin{bmatrix} j \\ i \end{bmatrix}_q \begin{bmatrix} n \\ j \end{bmatrix}_q \left( \prod_{k=j}^{n-1} (q^n - q^k) - 1 \right).$$

Now a lengthy, but straightforward, calculation reveals that  $A_{n-i} = w_i$ , given in (19). Note that the proof of Theorem 7.6 uses only the (easy) forward direction of Proposition 7.4 and not the decomposition in Theorem 7.1. Hence our proof of Theorem 7.6 and therefore of (19) is self-contained.

Note that the upper bound in Corollary 7.5 is at most

$$q^{n(n-d+1)}.$$

We close this section by showing that there exist  $d$ -codes almost as large as this upper bound. Our construction uses so-called *linear maximum rank distance codes* with minimum distance  $d$ , which are  $\mathbb{F}_q$ -subspaces  $Z$  of  $\mathbb{F}_q^{n \times n}$  of dimension  $n(n-d+1)$ , such that  $\text{rk}(x - y) \geq d$  for all distinct  $x, y \in Z$ . Such objects exist for all integers  $d$  satisfying  $1 \leq d \leq n$  [8, Theorem 6.3].

**Proposition 7.8.** *For each  $d$  satisfying  $1 \leq d \leq n$ , there exists a  $d$ -code in  $\text{GL}(n, q)$  of size at least*

$$\left( 1 - \frac{1}{q-1} \right) q^{n(n-d+1)}.$$

*For  $q = 2$  there exists a  $d$ -code in  $\text{GL}(n, q)$  of size at least  $q^{n(n-d)}$ .*

*Proof.* Consider a linear maximum rank distance code  $Z$  in  $\mathbb{F}_q^{n \times n}$  with minimum distance  $d$ . We show that  $Z \cap \text{GL}(n, q)$  has the required properties. It is well known [8, Theorem 5.6] that the number of matrices in  $Z$  of rank  $i$  depends only on the parameters  $q, n$ , and  $d$ . In particular the number of invertible matrices in  $Z$  equals

$$N = \sum_{j=0}^{n-d} (-1)^j C_j,$$

where

$$C_j = q^{\binom{j}{2}} \begin{bmatrix} n \\ j \end{bmatrix}_q (q^{n(n-d+1-j)} - 1).$$

It is readily verified that  $C_j/C_{j+1} \geq q^j$  for each  $j \in \{0, 1, \dots, n-d-1\}$  and therefore  $C_0, C_1, \dots, C_{n-d}$  is nonincreasing. Hence we have

$$\begin{aligned} N \geq C_0 - C_1 &= (q^{n(n-d+1)} - 1) - \frac{q^n - 1}{q - 1} (q^{n(n-d)} - 1) \\ &\geq \frac{q - 2}{q - 1} q^{n(n-d+1)} + \frac{q^{n(n-d)} - 1}{q - 1}, \end{aligned}$$

as required □

#### REFERENCES

- [1] W. A. Al-Salam and L. Carlitz, *Some orthogonal  $q$ -polynomials*, Math. Nachr. **30** (1965), 47–61.
- [2] E. Bannai and T. Ito, *Algebraic combinatorics. I: Association schemes*, The Benjamin/Cummings Publishing Co., Inc., Menlo Park, CA, 1984.
- [3] I. F. Blake, G. Cohen, and M. Deza, *Coding with permutations*, Inform. Control **43** (1979), no. 1, 1–19.
- [4] M. Braun, A. Kerber, and R. Laue, *Systematic construction of  $q$ -analogs of  $t$ - $(v, k, \lambda)$  designs*, Des. Codes Cryptogr. **34** (2005), 55–70.
- [5] P. J. Cameron and W. M. Kantor, *2-transitive and antiflag transitive collineation groups of finite projective spaces*, J. Algebra **60** (1979), no. 2, 384–422.
- [6] T. S. Chihara, *An introduction to orthogonal polynomials*, Mathematics and its Applications, Vol. 13, Gordon and Breach Science Publishers, New York-London-Paris, 1978.
- [7] Ph. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. **10** (1973).
- [8] ———, *Bilinear forms over a finite field, with applications to coding theory*, J. Combin. Theory Ser. A **25** (1978), no. 3, 226–241.
- [9] P. Dembowski, *Finite geometries*, Springer-Verlag, Berlin-New York, 1968.
- [10] A. Fazeli, S. Lovett, and A. Vardy, *Nontrivial  $t$ -designs over finite fields exist for all  $t$* , J. Combin. Theory Ser. A **127** (2014), 149–160.
- [11] J. Fulman, *A probabilistic approach toward conjugacy classes in the finite general linear and unitary groups*, J. Algebra **212** (1999), no. 2, 557–590.
- [12] J. Fulman and D. Stanton, *On the distribution of the number of fixed vectors for the finite classical groups*, Ann. Comb. **20** (2016), no. 4, 755–773.
- [13] M. Giudici, S. P. Glasby, and Ch. E. Praeger, *Subgroups of classical groups that are transitive on subspaces*, 2020, arXiv:2012.07213v1 [math.GR].
- [14] J. A. Green, *The characters of the finite general linear groups*, Trans. Amer. Math. Soc. **80** (1955), 402–447.
- [15] Ch. Hering, *Transitive linear groups and linear groups which contain irreducible groups of prime order*, Geometriae Dedicata **2** (1974), 425–460.
- [16] D. G. Higman and J. E. McLaughlin, *Geometric ABA-groups*, Illinois J. Math. **5** (1961), 382–397.
- [17] G. James, *The irreducible representations of the finite general linear groups*, Proc. London Math. Soc. (3) **52** (1986), no. 2, 236–268.

- [18] W. M. Kantor, *Line-transitive collineation groups of finite projective spaces*, Israel J. Math. **14** (1973), 229–235.
- [19] ———, *Primitive permutation groups of odd degree, and an application to finite projective planes*, J. Algebra **106** (1987), no. 1, 15–45.
- [20] M. Kiermaier and M. O. Pavčević, *Intersection numbers for subspace designs*, J. Combin. Des. **23** (2015), 463–480.
- [21] D. Kim, *On combinatorics of Al-Salam Carlitz polynomials*, European J. Combin. **18** (1997), no. 3, 295–302.
- [22] G. Kuperberg, S. Lovett, and R. Peled, *Probabilistic existence of regular combinatorial structures*, Geom. Funct. Anal. **27** (2017), no. 4, 919–972.
- [23] J. B. Lewis, V. Reiner, and D. Stanton, *Reflection factorizations of Singer cycles*, J. Algebraic Combin. **40** (2014), no. 3, 663–691.
- [24] D. Livingstone and A. Wagner, *Transitivity of finite permutation groups on unordered sets*, Math. Z. **90** (1965), 393–403.
- [25] I. G. Macdonald, *Symmetric functions and Hall polynomials*, second ed., Oxford Classic Texts in the Physical Sciences, The Clarendon Press, Oxford University Press, New York, 2015.
- [26] W. J. Martin and B. E. Sagan, *A new notion of transitivity for groups and sets of permutations*, J. London Math. Soc. (2) **73** (2006), no. 1, 1–13.
- [27] D. Perin, *On collineation groups of finite projective spaces*, Math. Z. **126** (1972), 135–142.
- [28] A. Rudvalis and K. Shinoda, *An enumeration in finite classical groups*, Tech. report, U-Mass Amherst, Department of Mathematics, 1988.
- [29] H. Suzuki, *On the inequalities of  $t$ -designs over a finite field*, European J. Combin. **11** (1990), 601–607.

DEPARTMENT OF MATHEMATICS, PADERBORN UNIVERSITY, WARBURGER STR. 100, 33098 PADERBORN, GERMANY.

*Email address:* `alena.ernst@math.upb.de`

*Email address:* `kus@math.upb.de`