Designs in finite general linear groups

Kai-Uwe Schmidt

Paderborn University Germany

(joint work with Alena Ernst)

sets







Coding Theory

Design Theory

Coding Theory Separation Design Theory Approximation

Coding Theory Separation

ordinary codes constant weight codes subspace codes permutation codes

:

Design Theory Approximation

orthogonal arrays combinatorial designs subspace designs

transitive sets

Coding Theory Separation

ordinary codes constant weight codes subspace codes permutation codes :

full rank codes

Design Theory Approximation

orthogonal arrays combinatorial designs subspace designs transitive sets :

transitive linear sets

Coding Theory Separation

ordinary codes constant weight codes subspace codes permutation codes Design Theory Approximation

orthogonal arrays combinatorial designs subspace designs transitive sets :

full rank codes

transitive linear sets

Common framework: association schemes

Association scheme: A finite set X and a finite-dimensional subspace of $\mathbb{C}^{X \times X}$.

Association scheme: A finite set X and a finite-dimensional subspace of $\mathbb{C}^{X \times X}$.

Subset: $Y \subseteq X$.

Association scheme: A finite set X and a finite-dimensional subspace of $\mathbb{C}^{X \times X}$.

Subset: $Y \subseteq X$.

Basis of matrices with entries 0 or 1 $\{D_0, D_1, \dots, D_m\}$ Basis of matrices with eigenvalues 0 or 1 $\{E_0, E_1, \dots, E_m\}$

Association scheme: A finite set X and a finite-dimensional subspace of $\mathbb{C}^{X \times X}$.

Subset: $Y \subseteq X$.

Basis of matrices with entries 0 or 1 $\{D_0, D_1, \dots, D_m\}$

Inner distribution (A_i) $A_i = \frac{1}{|Y|} \mathbf{1}_Y^T D_i \mathbf{1}_Y$ Basis of matrices with eigenvalues 0 or 1 $\{E_0, E_1, \dots, E_m\}$

Dual distribution (A'_k) $A'_k = \frac{|X|}{|Y|} \mathbf{1}_Y^T E_k \mathbf{1}_Y$

Association scheme: A finite set X and a finite-dimensional subspace of $\mathbb{C}^{X \times X}$.

Subset: $Y \subseteq X$.

Basis of matrices with entries 0 or 1 $\{D_0, D_1, \dots, D_m\}$

Inner distribution (A_i) $A_i = \frac{1}{|Y|} \mathbf{1}_Y^T D_i \mathbf{1}_Y$

 $\begin{array}{c} D\text{-code} \\ A_i \neq 0 \Rightarrow i \in D \end{array}$

Basis of matrices with eigenvalues 0 or 1 $\{E_0, E_1, \dots, E_m\}$

Dual distribution (A'_k) $A'_k = \frac{|X|}{|Y|} \mathbf{1}_Y^T E_k \mathbf{1}_Y$

T-design $k \in T \Rightarrow A'_k = 0$



For
$$T = \{1, 2, \dots, t\}$$
, the *T*-designs

For $T = \{1, 2, \dots, t\}$, the *T*-designs in the

Hamming scheme are orthogonal arrays;

For $T = \{1, 2, \dots, t\}$, the *T*-designs in the

- Hamming scheme are orthogonal arrays;
- Johnson scheme are combinatorial designs;

For $T = \{1, 2, \dots, t\}$, the *T*-designs in the

- Hamming scheme are orthogonal arrays;
- Johnson scheme are combinatorial designs;
- *q*-Johnson scheme are subspace designs.

For $T = \{1, 2, \dots, t\}$, the *T*-designs in the

- Hamming scheme are orthogonal arrays;
- Johnson scheme are combinatorial designs;
- *q*-Johnson scheme are subspace designs.

For $T = \{1, 2, \dots, t\}$, the *T*-designs in the

- Hamming scheme are orthogonal arrays;
- Johnson scheme are combinatorial designs;
- *q*-Johnson scheme are subspace designs.

. . . .

This motivates the present general definition [of T-designs], the "conjecture" being that T-designs will often have interesting properties.

- Delsarte's Thesis, 1973

Let G be a finite group with

- conjugacy classes C_1, C_2, \ldots, C_m and
- (complex) irreducible characters $\chi_1, \chi_2, \ldots, \chi_m$.

Let G be a finite group with

- conjugacy classes C_1, C_2, \ldots, C_m and
- (complex) irreducible characters $\chi_1, \chi_2, \ldots, \chi_m$.

Every finite group gives an association scheme with

$$D_i(x,y) = \mathbb{1}[x^{-1}y \in C_i]$$
 $E_k(x,y) = \chi_k(1)\chi_k(x^{-1}y).$

Let G be a finite group with

- conjugacy classes C_1, C_2, \ldots, C_m and
- (complex) irreducible characters $\chi_1, \chi_2, \ldots, \chi_m$.

Every finite group gives an association scheme with

$$D_i(x,y) = \mathbb{1}[x^{-1}y \in C_i]$$
 $E_k(x,y) = \chi_k(1)\chi_k(x^{-1}y).$

The dual distribution of a subset Y of G then satisfies

$$A'_k = \chi_k(1) \sum_{x,y \in Y} \chi_k(x^{-1}y).$$

$$\sigma = (421)$$

$$\sigma = (421)$$



$$\sigma = (421)$$

$$\sigma = (421)$$



 σ -tabloid

$$\sigma = (421)$$

1 3 6 7

4 5 σ -tabloid

2

A subset Y of S_n is transitive on σ -tabloids if the number of $\pi \in Y$ such that



is independent of the two σ -tabloids.



transitive on (41)-tabloids



Designs in S_5

transitive on (32)-tabloids



transitive on (41)-tabloids



Designs in S_5

transitive on (32)-tabloids



transitive on (41)-tabloids

transitive on (41)-tabloids



Partitions and the symmetric group

For the symmetric group, the conjugacy classes and the irreducible characters are naturally indexed by partitions.

Partitions and the symmetric group

For the symmetric group, the conjugacy classes and the irreducible characters are naturally indexed by partitions.

The partitions are partially ordered by dominance \trianglelefteq .


Theorem (Martin-Sagan 2007) $Y \subseteq S_n$ is transitive on σ -tabloids if and only if $A'_{\lambda} = 0$ for all $\sigma \leq \lambda < (n)$.

Theorem (Martin-Sagan 2007) $Y \subseteq S_n$ is transitive on σ -tabloids if and only if $A'_{\lambda} = 0$ for all $\sigma \trianglelefteq \lambda \lhd (n)$.

Theorem (Livingstone-Wagner 1965)

Every subgroup of S_n that is *t*-homogeneous for some *t* satisfying $1 \le t \le n/2$ is also (t-1)-homogeneous.

Theorem (Martin-Sagan 2007) $Y \subseteq S_n$ is transitive on σ -tabloids if and only if $A'_{\lambda} = 0$ for all $\sigma \leq \lambda < (n)$.

Theorem (Livingstone-Wagner 1965) Every subgroup of S_n that is *t*-homogeneous for some *t* satisfying $1 \le t \le n/2$ is also (t-1)-homogeneous.

Corollary (Martin-Sagan 2007) If Y is transitive on σ -tabloids, then Y is also transitive on τ -tabloids for all $\sigma \leq \tau$.

Theorem (Martin-Sagan 2007) $Y \subseteq S_n$ is transitive on σ -tabloids if and only if $A'_{\lambda} = 0$ for all $\sigma \trianglelefteq \lambda \lhd (n)$.

Theorem (Livingstone-Wagner 1965) Every subgroup of S_n that is *t*-homogeneous for some *t* satisfying $1 \le t \le n/2$ is also (t-1)-homogeneous.

Corollary (Martin-Sagan 2007) If Y is transitive on σ -tabloids, then Y is also transitive on τ -tabloids for all $\sigma \leq \tau$.

This implies the Livingstone-Wagner Theorem since

$$(n-t,t) \trianglelefteq (n-t+1,t-1)$$
 for $1 \le t \le n/2$.

Let GL(n, q) be the group of invertible $n \times n$ matrices over \mathbb{F}_q .

Let GL(n,q) be the group of invertible $n \times n$ matrices over \mathbb{F}_q .

Let GL(n,q) be the group of invertible $n \times n$ matrices over \mathbb{F}_q .

$$\sigma = (241) \qquad \sigma \text{-flag}$$

$$V_1 \quad V_2 \qquad V_1 = \langle v_1, v_2 \rangle$$

$$V_3 \quad V_4 \quad v_5 \quad v_6 \qquad V_2 = \langle v_1, v_2, v_3, v_4, v_5, v_6 \rangle$$

$$V_3 = \langle v_1, v_2, v_3, v_4, v_5, v_6, v_7 \rangle$$

Let GL(n,q) be the group of invertible $n \times n$ matrices over \mathbb{F}_q .

$$\sigma = (241) \qquad \sigma \text{-flag}$$

$$V_1 \quad V_2 \qquad V_1 = \langle v_1, v_2 \rangle$$

$$V_3 \quad v_4 \quad v_5 \quad v_6 \qquad V_2 = \langle v_1, v_2, v_3, v_4, v_5, v_6 \rangle$$

$$V_3 = \langle v_1, v_2, v_3, v_4, v_5, v_6, v_7 \rangle$$

Our interest: subsets of GL(n, q) that are transitive on σ -flags.

Some facts about GL(n,q)

Reminder: The conjugacy classes of GL(n, q) correspond to the Jordan normal forms.

Some facts about GL(n,q)

Reminder: The conjugacy classes of GL(n, q) correspond to the Jordan normal forms.

The conjugacy classes and the (complex) irreducible characters of GL(n, q) are naturally indexed by mappings

 $\underline{\lambda}$: {monic irr. polynomials in $\mathbb{F}_q[X]$ } \ {X} \rightarrow Partitions

of finite support such that

$$\sum_{f} \deg(f) |\underline{\lambda}(f)| = n.$$

Notation: Composition $\sigma = (241) \longrightarrow$ partition $\tilde{\sigma} = (421)$.

Notation: Composition $\sigma = (241) \longrightarrow$ partition $\tilde{\sigma} = (421)$.

Theorem (Ernst-S. 2022) A subset $Y \subseteq GL(n, q)$ is transitive on σ -flags if and only if $A'_{\lambda} = 0$ for all $\tilde{\sigma} \leq \underline{\lambda}(X-1) < (n)$.

Notation: Composition $\sigma = (241) \longrightarrow$ partition $\tilde{\sigma} = (421)$.

Theorem (Ernst-S. 2022) A subset $Y \subseteq GL(n,q)$ is transitive on σ -flags if and only if $A'_{\lambda} = 0$ for all $\tilde{\sigma} \leq \underline{\lambda}(X-1) < (n)$.

Corollary Transitivity on σ -flags implies transitivity on τ -flags, where τ has the same parts as σ .

Notation: Composition $\sigma = (241) \longrightarrow$ partition $\tilde{\sigma} = (421)$.

Theorem (Ernst-S. 2022) A subset $Y \subseteq GL(n,q)$ is transitive on σ -flags if and only if $A'_{\lambda} = 0$ for all $\tilde{\sigma} \leq \underline{\lambda}(X-1) < (n)$.

Corollary Transitivity on σ -flags implies transitivity on τ -flags, where τ has the same parts as σ .

E.g., transitivity on t-spaces implies transitivity on (n - t)-spaces.

Notation: Composition $\sigma = (241) \longrightarrow$ partition $\tilde{\sigma} = (421)$.

Theorem (Ernst-S. 2022) A subset $Y \subseteq GL(n,q)$ is transitive on σ -flags if and only if $A'_{\lambda} = 0$ for all $\tilde{\sigma} \leq \underline{\lambda}(X-1) < (n)$.

Corollary Transitivity on σ -flags implies transitivity on τ -flags, where τ has the same parts as σ .

E.g., transitivity on t-spaces implies transitivity on (n - t)-spaces.

Corollary Transitivity on σ -flags implies transitivity on τ -flags for all τ satisfying $\tilde{\sigma} \leq \tilde{\tau}$.

Notation: Composition $\sigma = (241) \longrightarrow$ partition $\tilde{\sigma} = (421)$.

Theorem (Ernst-S. 2022) A subset $Y \subseteq GL(n,q)$ is transitive on σ -flags if and only if $A'_{\lambda} = 0$ for all $\tilde{\sigma} \leq \underline{\lambda}(X-1) < (n)$.

Corollary Transitivity on σ -flags implies transitivity on τ -flags, where τ has the same parts as σ .

E.g., transitivity on t-spaces implies transitivity on (n - t)-spaces.

Corollary Transitivity on σ -flags implies transitivity on τ -flags for all τ satisfying $\tilde{\sigma} \leq \tilde{\tau}$.

E.g., transitivity on *t*-spaces implies transitivity on (t-1)-spaces for $1 \le t \le n/2$. For subgroups this was proved by (Perin 1972).



$$\sigma = (241)$$



$$\sigma = (241)$$
 σ -flag

<i>v</i> ₁	<i>V</i> ₂		
<i>V</i> 3	<i>v</i> ₄	<i>V</i> 5	<i>v</i> ₆
<i>v</i> ₇			

$$V_{1} = \langle v_{1}, v_{2} \rangle$$
$$V_{2} = \langle v_{1}, v_{2}, v_{3}, v_{4}, v_{5}, v_{6} \rangle$$
$$V_{3} = \langle v_{1}, v_{2}, v_{3}, v_{4}, v_{5}, v_{6}, v_{7} \rangle$$

$$\sigma = (241)$$
 σ -flag



$$\begin{split} V_1 &= \langle v_1, v_2 \rangle \\ V_2 &= \langle v_1, v_2, v_3, v_4, v_5, v_6 \rangle \\ V_3 &= \langle v_1, v_2, v_3, v_4, v_5, v_6, v_7 \rangle \end{split}$$

$$\sigma = (241)$$
 σ -flag bases



$$V_{1} = \langle v_{1}, v_{2} \rangle \qquad (v_{1}, v_{2})$$
$$V_{2} = \langle v_{1}, v_{2}, v_{3}, v_{4}, v_{5}, v_{6} \rangle$$
$$V_{3} = \langle v_{1}, v_{2}, v_{3}, v_{4}, v_{5}, v_{6}, v_{7} \rangle \quad (v_{7})$$



We call this a signed σ -flag with signature $S = (* \circ *)$.



We call this a signed σ -flag with signature $S = (* \circ *)$.

The type of this flag is the double partition ((21), (4)).



We call this a signed σ -flag with signature $S = (* \circ *)$.

The type of this flag is the double partition ((21), (4)).

Two special cases:

$$(t, n - t)$$
-flag with signature (00): t-space of V.
 $(t, n - t)$ -flag with signature (*0): basis of a t-space of V.

Its type equals $((2^51^6), (31))$.

A partial order \preceq on double partitions: reverse refinement in first coordinate, dominance in second coordinate.

A partial order \leq on double partitions: reverse refinement in first coordinate, dominance in second coordinate.

Theorem (Ernst-S. 2022) A subset $Y \subseteq GL(n, q)$ is transitive on signed flags of type (σ, τ) with fixed signature if and only if $A'_{\lambda} = 0$ for all

 $(\sigma, \tau) \preceq \operatorname{type}(\underline{\lambda}) \prec (\emptyset, (n)).$

A partial order \leq on double partitions: reverse refinement in first coordinate, dominance in second coordinate.

Theorem (Ernst-S. 2022) A subset $Y \subseteq GL(n, q)$ is transitive on signed flags of type (σ, τ) with fixed signature if and only if $A'_{\lambda} = 0$ for all

$$(\sigma, \tau) \preceq \operatorname{type}(\underline{\lambda}) \prec (\emptyset, (n)).$$

This has similar consequences as the result for unsigned flags.

Transitive subgroups of GL(n, q)

A Singer cycle is sharply transitive nonzero points of \mathbb{F}_q^n and it contains a subgroup that is sharply transitive on 1-spaces.

Transitive subgroups of GL(n,q)

A Singer cycle is sharply transitive nonzero points of \mathbb{F}_q^n and it contains a subgroup that is sharply transitive on 1-spaces.

If G is a subgroup of GL(n, q) with stronger transitivity and does not contain SL(n, q), then one of the following holds:

Transitive subgroups of GL(n, q)

A Singer cycle is sharply transitive nonzero points of \mathbb{F}_q^n and it contains a subgroup that is sharply transitive on 1-spaces.

If G is a subgroup of GL(n, q) with stronger transitivity and does not contain SL(n, q), then one of the following holds:

(n,q)	group	(σ, τ)
(2,3)	$G \cong \Gamma L(1, 3^2)$	$((1^2), \emptyset)$
(2,5)	G = 96	$((1^2), \emptyset)$
(3,2)	$G\cong \GammaL(1,2^3)$	$((1^3), \emptyset)$
(4, 2)	$G \cong A_7$	$((31), \emptyset)$
(5,2)	$G\cong \GammaL(1,2^5)$	(Ø, (32))

Transitive subgroups of GL(n, q)

A Singer cycle is sharply transitive nonzero points of \mathbb{F}_q^n and it contains a subgroup that is sharply transitive on 1-spaces.

If G is a subgroup of GL(n, q) with stronger transitivity and does not contain SL(n, q), then one of the following holds:

$$(n,q)$$
group (σ,τ) $(2,3)$ $G \cong \Gamma L(1,3^2)$ $((1^2),\emptyset)$ $(2,5)$ $|G| = 96$ $((1^2),\emptyset)$ $(3,2)$ $G \cong \Gamma L(1,2^3)$ $((1^3),\emptyset)$ $(4,2)$ $G \cong A_7$ $((31),\emptyset)$ $(5,2)$ $G \cong \Gamma L(1,2^5)$ $(\emptyset,(32))$

SL(n, q) is transitive on bases of (n - 1)-spaces.

t-design in GL(V): Transitive on bases of *t*-spaces of $V = \mathbb{F}_q^n$.

t-design in GL(V): Transitive on bases of *t*-spaces of $V = \mathbb{F}_q^n$.

t-design in $J_q(n, k)$: Subset *D* of the Grassmannian $J_q(n, k)$ of *V* such that the number of elements in *D* containing a given *t*-space of *V* is independent of the choice of this *t*-space.

t-design in GL(V): Transitive on bases of *t*-spaces of $V = \mathbb{F}_q^n$. *t*-design in $J_q(n, k)$: Subset *D* of the Grassmannian $J_q(n, k)$ of *V* such that the number of elements in *D* containing a given *t*-space of *V* is independent of the choice of this *t*-space.

Theorem (Ernst-S. 2022) Write $V = U \oplus W$ with dim U = k. If there is a (1) a *t*-design *Y* in GL(*U*), (2) a *t*-design *Z* in GL(*W*), (3) a *t*-design *D* in $J_q(n, k)$,

then there is a *t*-design in GL(V) of size $|Y| \cdot |Z| \cdot |D| \cdot q^{k(n-k)}$.

t-design in GL(V): Transitive on bases of *t*-spaces of $V = \mathbb{F}_q^n$. *t*-design in $J_q(n, k)$: Subset *D* of the Grassmannian $J_q(n, k)$ of *V* such that the number of elements in *D* containing a given *t*-space of *V* is independent of the choice of this *t*-space.

Theorem (Ernst-S. 2022) Write $V = U \oplus W$ with dim U = k. If there is a (1) a *t*-design *Y* in GL(*U*), (2) a *t*-design *Z* in GL(*W*), (3) a *t*-design *D* in $J_q(n, k)$,

then there is a *t*-design in GL(V) of size $|Y| \cdot |Z| \cdot |D| \cdot q^{k(n-k)}$.

Example. Taking $Y = Z \cong GL(3, 2)$ and D a 2-design in $J_2(6, 3)$ of size 279 gives a 2-design in GL(6, 2) of size $\frac{1}{5}|GL(6, 2)|$.
An existence result

It was shown by (Fazeli-Lovett-Vardy 2014) that small t-designs in $J_q(n, k)$ exist for all t.

An existence result

It was shown by (Fazeli-Lovett-Vardy 2014) that small t-designs in $J_q(n, k)$ exist for all t.

Theorem (Ernst.-S. 2022) Let t be a positive integer and let $\epsilon > 0$. Then, for all sufficiently large n, there is a t-design in GL(n, q) whose cardinality N satisfies $N/|GL(n, q)| < \epsilon$.

An existence result

It was shown by (Fazeli-Lovett-Vardy 2014) that small t-designs in $J_q(n, k)$ exist for all t.

Theorem (Ernst.-S. 2022) Let t be a positive integer and let $\epsilon > 0$. Then, for all sufficiently large n, there is a t-design in GL(n, q) whose cardinality N satisfies $N/|GL(n, q)| < \epsilon$.

Through our algebraic characterisation this also gives similar existence results for subsets of GL(n, q) that are transitive on signed flags.

Designs in finite general linear groups

Kai-Uwe Schmidt

Paderborn University Germany

(joint work with Alena Ernst)