Applications of the Arithmetic of Finite Fields to Finite Projective Geometries via the Action of the Singer Cycle

Akihiro Munemasa
Kyushu University
Fukuoka, Japan

Construction of combinatorial configurations in finite projective spaces

$PG(n-1, q)$ (n−1)-dim. projective space over $GF(q)$

$P\Gamma L(n, q)$ projective semilinear group

Standard method of construction

Take an orbit (or union of orbits) on subspaces under a subgroup of $P\Gamma L(n, q)$.

$PG(n-1, q) \longleftrightarrow GF(q^n)^\times / GF(q)^\times$

cyclic group of order $\frac{q^n-1}{q-1}$

(Singer cycle)

lines $\longleftrightarrow$ $\left(\begin{array}{l} \text{2-dim.} \\ GF(q)\text{-subspace of} \\ GF(q^n) \text{ minus } \{0\} \end{array} \right) / GF(q)^\times$

planes $\longleftrightarrow$ $\left(\begin{array}{l} \text{3-dim.} \\ \quad \cdots\cdots \end{array} \right)$

$(k-1)$-subspaces $\longleftrightarrow$ $\left(\begin{array}{l} k\text{-dim.} \\ \quad \cdots \end{array} \right)$

2-designs over $GF(q)$

a collection $\mathcal{B}$ of k-subspaces of $PG(n-1, q)$ such that

$\exists \lambda > 0$, $\forall$ two distinct points are contained in exactly λ members of $\mathcal{B}$.

Thomas (1987)
Suzuki (1990, 1992)
Miyakawa-Yoshiara-Munemasa (1995)

A resolution (parallelism, packing) in $PG(2n-1, q)$ is a partition of the set of lines into line-spreads.

Construction using Singer cycle

$PG(5,2)$ Sarmiento

$PG(7,2)$ Hishida-Jimbo

$PG(2n-1, q)$ has $\dfrac{q^{2n}-1}{q-1}$ points,

a line has $q+1$ points,

a line-spread has $\dfrac{q^{2n}-1}{q^2-1}$ lines.

Problem Find all line-spreads whose members are permuted cyclically by the subgroup of index $q+1$ of the Singer cycle. Does there exist such a line-spread other than **Example** ?
(open for $q \geq 3$, $n \geq 6$)

If $q=2$ then there are

$p^1_{23} = \dfrac{(2^n+(-1)^{n+1})^2}{9}$ such line-spreads.

intersection number of the association scheme

$(K, \{R_0, R_1, R_2, R_3\})$

$K = GF(2^{2n})$, $K^\times = \langle \beta \rangle$

$H = \langle \beta^3 \rangle$ $|K^\times : H| = 3$

$R_0 = \{(x,x) \mid x \in K\}$

$R_1 = \{(x,y) \mid x+y \in H\}$

$R_2 = \{(x,y) \mid x+y \in H\beta\}$

$R_3 = \{(x,y) \mid x+y \in H\beta^2\}$

van Lint - Schrijver (1981)

$F = GF(4)$ $\qquad$ $K = GF(2^{2n})$

$= \{0, 1, \alpha, \underset{\overset{\parallel}{1+\alpha}}{\alpha^2}\}$ $\qquad$ $= \{0, 1, \beta, \beta^2, \cdots\}$

additive character

$\chi : F \to \{\pm 1\}$ $\qquad$ $\tilde{\chi} = \chi \circ Tr_{K/F}$

$0 \mapsto 1$

$1 \mapsto 1$

$\alpha \mapsto -1$

$\alpha^2 \mapsto -1$

multiplicative character

$\psi : F^\times \to \mathbb{C}^\times$ $\qquad$ $\tilde{\psi} = \psi \circ N_{K/F}$

Gauss Sum

$$G(\psi, \chi) = -\sum_{a \in F^\times} \psi(a)\chi(a)$$

$$\tilde{G}(\tilde{\psi}, \tilde{\chi}) = -\sum_{a \in K^\times} \tilde{\psi}(a)\tilde{\chi}(a)$$

Hasse-Davenport Theorem

$$\tilde{G}(\tilde{\psi}, \tilde{\chi}) = G(\psi, \chi)^n$$

$$\omega = e^{2\pi i/3}$$

$$\psi : F^\times \to \mathbb{C}^\times \quad \psi(\alpha^j) = \omega^j$$

$$G(1, \chi) = -(\chi(1) + \chi(\alpha) + \chi(\alpha^2)) = 1$$

$$G(\psi, \chi) = -(\psi(1)\chi(1) + \psi(\alpha)\chi(\alpha) + \psi(\alpha^2)\chi(\alpha^2))$$

$$= -(1 - \omega - \omega^2) = -2$$

$$G(\psi^2, \chi) = -2$$

By Hasse-Davenport Theorem

$$\tilde{G}(\tilde{1}, \tilde{\chi}) = 1,$$

$$\tilde{G}(\tilde{\psi}, \tilde{\chi}) = \tilde{G}(\tilde{\psi}^2, \tilde{\chi}) = (-2)^n$$

$$\tilde{\psi}(a) = \begin{cases} 1 & a \in H \\ \omega & a \in H\beta \\ \omega^2 & a \in H\beta^2 \end{cases}$$

$$G(\Psi, \chi) = -\sum_{a \in k^\times} \Psi(a)\chi(a)$$

$$= -\Big(\underbrace{\sum_{a \in H} \tilde{\chi}(a)}_{\eta_0} + \omega \underbrace{\sum_{a \in H\beta} \tilde{\chi}(a)}_{\eta_1} + \omega^2 \underbrace{\sum_{a \in H\beta^2} \tilde{\chi}(a)}_{\eta_2} \Big)$$

$$\tilde{G}(\tilde{1}, \tilde{\chi}) = -(\eta_0 + \eta_1 + \eta_2) = 1$$

$$\tilde{G}(\tilde{\Psi}, \tilde{\chi}) = -(\eta_0 + \omega\eta_1 + \omega^2\eta_2) = (-2)^n$$

$$\tilde{G}(\tilde{\Psi}^2, \tilde{\chi}) = -(\eta_0 + \omega^2\eta_1 + \omega\eta_2) = (-2)^n$$

$$\eta_1 = \eta_2 = \frac{(-2)^n - 1}{3}$$

$$\eta_0 = -1 - 2\eta_1$$

$$\lambda_0 = \left| \left\{ (a,b) \in H\beta \times H\beta^2 \mid a+b = 1 \right\} \right|$$

$$\lambda_1 = \left| \left\{ (a,b) \in H\beta \times H\beta^2 \mid a+b = \beta \right\} \right|$$

$$\lambda_2 = \left| \left\{ (a,b) \in H\beta \times H\beta^2 \mid a+b = \beta^2 \right\} \right|$$

In group algebra $\mathbb{Z}[K]$

$$\widehat{H\beta}\ \widehat{H\beta^2} = \lambda_0 \hat{H} + \lambda_1 \widehat{H\beta} + \lambda_2 \widehat{H\beta^2}$$

$\Downarrow \tilde{\chi}$ (additive character)

$$\eta_1 \eta_2 = \lambda_0 \eta_0 + \lambda_1 \eta_1 + \lambda_2 \eta_2$$

$$\eta_2 \eta_0 = \lambda_0 \eta_1 + \lambda_1 \eta_2 + \lambda_2 \eta_0$$

$$\eta_0 \eta_1 = \lambda_0 \eta_2 + \lambda_1 \eta_0 + \lambda_2 \eta_1$$

Solve for $\lambda_0, \lambda_1, \lambda_2$,

$$\lambda_0 = \frac{(2^n + (-1)^{n+1})^2}{9}$$

$$\lambda_0 = \left| \{ (a,b) \in H\beta \times H\beta^2 \mid a+b=1 \} \right|$$

$$\Downarrow$$

$L = \{1, a, \underset{\substack{\shortparallel \\ a+1}}{b}\}$ is a line.

($\{0, 1, a, a+1\}$ is a 2-dim. GF(2)-subspace of K)

The subgroup of index 3 of the Singer cycle = multiplication by the elements of H

$\{hL \mid h \in H\}$ is a line-spread

covers

$$H \cup Ha \cup Hb$$
$$= H \cup H\beta \cup H\beta^2$$
$$= K^\times$$
$$= K^\times / GF(2)^\times = PG(2n-1, 2)$$

X : a set with v elements

$\mathcal{B}$: a collection of k-element subsets of X

$(X, \mathcal{B})$ is called a 2-(v, k, λ) design if

$\forall x, y \in X,\ x \neq y$

$\exists$ exactly λ members of $\mathcal{B}$ containing x, y.

$(X, \mathcal{B})$ is called flag-transitive if its automorphism group acts transitively on

$$\{(x, B) \in X \times \mathcal{B} \mid x \in B\}$$

If D is a $2\text{-}(2^{2n}, 4, 1)$ design not isomorphic to $AG(n,4)$, then

$$\mathrm{Aut}\, D < A\Gamma L(1, 2^{2n})$$
$$= K . K^{\times} . \mathrm{Aut}\, K$$

Buekenhout
Delandtsheer
Doyen (1990)
Kleidman
Liebeck
Saxl

mass formula

$$\sum_{D} \frac{1}{|\mathrm{Aut}\, D|} = \frac{\left(2^{n}+(-1)^{n+1}\right)^{2}}{9n \cdot 2^{2n+1}\left(2^{2n}-1\right)} - \delta$$

where

$$\delta = \begin{cases} \dfrac{1}{n \cdot 2^{2n+1}\left(2^{2n}-1\right)} & \text{if } n \not\equiv 0 \pmod{3} \\ 0 & \text{otherwise} \end{cases}$$

$\sum_{D}$ is over isomorphism classes of 2-$(2^{2n}, 4, 1)$ designs D with

$$\underbrace{K.H < \mathrm{Aut}\, D}_{\text{index } 6n} < A\Gamma L(1, 2^{2n})$$

$K.H$: acts sharply transitively on flags