

U

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

$\text{PG}(n-1, q)$

$(n-1)$ -dim.
projective space
over $\text{GF}(q)$

$\text{PGL}(n, q)$

projective semilinear
group

Standard method of construction

Take an orbit (or union of
orbits) on subspaces under a
subgroup of $\text{PGL}(n, q)$.

3

$$\text{PG}(n-1, q) \longleftrightarrow \frac{\text{GF}(q^n)^\times}{\text{GF}(q)^\times}$$

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

(Singer cycle)

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

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

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

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)

6

A resolution (parallelism, packing)

in $\text{PG}(2n+1, 2)$ is a partition of
the set of lines into line-spreads.

Construction using Singer cycle

$\text{PG}(5, 2)$

Sarmiento

$\text{PG}(7, 2)$

Hishida-Jimbo

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

a line has $q+1$ points,

a line-spread has $\frac{q^{2n}-1}{q^2-1}$ 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 $g=2$ then there are

$$P_{23}^1 = \frac{(2^n + (-1)^{n+1})^2}{9} \text{ such line-spreads.}$$

↑ intersection number of the association scheme

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

$$K = GF(2^{2n}), \quad K^* = \langle B \rangle$$

$$H = \langle B^3 \rangle \quad |K^*:H| = 3$$

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

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

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

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

van Lint - Schrijver (1981)

$$F = GF(4)$$

$$= \{0, 1, \alpha, \alpha^2\}$$

α
1ta

$$K = GF(2^{2n})$$

$$= \{0, 1, \beta, \beta^2, \dots\}$$

[9]

additive character

$$\chi : F \rightarrow \{\pm 1\}$$

$$0 \mapsto 1$$

$$1 \mapsto 1$$

$$\alpha \mapsto -1$$

$$\alpha^2 \mapsto -1$$

$$\tilde{\chi} = \chi \circ \text{Tr}_{K/F}$$

multiplicative character

$$\psi : F^\times \rightarrow \mathbb{C}^\times$$

$$\tilde{\psi} = \psi \circ N_{K/F}$$

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

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

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

L9

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

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

$$\begin{aligned} G(\psi, \chi) &= -(\psi(1)\chi(1) + \psi(\alpha)\chi(\alpha) + \psi(\alpha^2)\chi(\alpha^2)) \\ &= -(1 - \omega - \omega^2) = -2 \end{aligned}$$

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

By Hasse-Davenport Theorem

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

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

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

110

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

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

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

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

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

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

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

III

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

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

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

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

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

↓ $\tilde{\chi}$ (additive character)

$$\gamma_1 \gamma_2 = \lambda_0 \gamma_0 + \lambda_1 \gamma_1 + \lambda_2 \gamma_2$$

$$\gamma_2 \gamma_0 = \lambda_0 \gamma_1 + \lambda_1 \gamma_2 + \lambda_2 \gamma_0$$

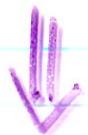
$$\gamma_0 \gamma_1 = \lambda_0 \gamma_2 + \lambda_1 \gamma_0 + \lambda_2 \gamma_1$$

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

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

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

12



$L = \{1, a, b\}$ is a line.
 $\stackrel{\text{def}}{=} a+1$

($\{0, 1, a, a+1\}$ 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

$$HUH\alpha \cup H\beta$$

$$= H \cup H\beta \cup H\beta^2$$

$$= K^\times$$

$$= K^\times /_{GF(2)^\times} = PG(2n-1, 2)$$

15

X : a set with v elements

B : a collection of k -element subsets of X

(X, B) is called a $2-(v, k, \lambda)$ design if

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

\exists exactly λ members of B containing x, y .

(X, B) is called flag-transitive

if its automorphism group acts transitively on

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

If D is a $2-(2^{2^n}, 4, 1)$ design

not isomorphic to $AG(n, 4)$, then

$$\begin{aligned} \text{Aut } D &< \text{AGL}(1, 2^{2^n}) \\ &= K \cdot K^* \cdot \text{Aut } K \end{aligned}$$

Buekenhout

De Landtsheer

Doyen

(1990)

Kleidman

Liebeck

Saxl

mass formula

U8

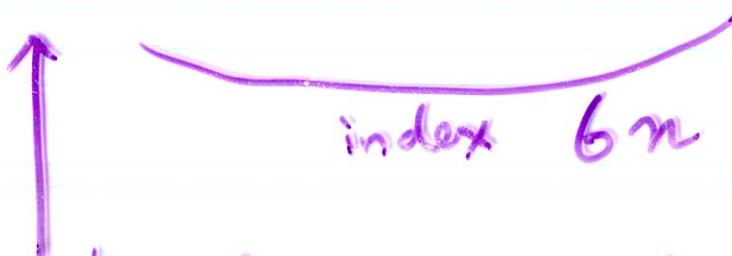
$$\sum_D \frac{1}{|\text{Aut } D|} = \frac{(2^m + (-1)^{m+1})^2}{9m \cdot 2^{2m+1} (2^{2m}-1)} - \delta$$

where

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

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

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



acts sharply transitively on flags