Singer difference sets and difference system of sets

Akihiro Munemasa

Graduate School of Information Sciences

Tohoku University

(joint work with Vladimir D. Tonchev)

November 18, 2004

Projective Geometry

- $PG(n,q) = n$-dim. projective space over $GF(q)$
  $(GF(q)^{n+1} - \{0\})/\sim$

Projective Geometry

- $PG(n, q) = n$-dim. projective space over $GF(q)$
  $(GF(q)^{n+1} - \{0\})/\sim$
- "point" = projective point
  1-dim. vector subspace

Projective Geometry

- $PG(n,q) = n$-dim. projective space over $GF(q)$
  $(GF(q)^{n+1} - \{0\})/\sim$
- "point" = projective point
  1-dim. vector subspace
- "line" = projective line
  2-dim. vector subspace

Projective Geometry

- $PG(n,q) = n$-dim. projective space over $GF(q)$
  $(GF(q)^{n+1} - \{0\})/\sim$
- "point" = projective point
  1-dim. vector subspace
- "line" = projective line
  2-dim. vector subspace
- "spread" = a set of lines which partition the points of $PG(n,q)$

Projective Geometry

- $PG(n,q) = n$-dim. projective space over $GF(q)$
  $(GF(q)^{n+1} - \{0\})/\sim$
- "point" = projective point
  1-dim. vector subspace
- "line" = projective line
  2-dim. vector subspace
- "spread" = a set of lines which partition the points of $PG(n,q)$
- "packing" = "resolution" = " parallelism" = a set of spreads which partition the set of lines

Projective Geometry

- $PG(n,q) = n$-dim. projective space over $GF(q)$
  $(GF(q)^{n+1} - \{0\})/\sim$
- "point" = projective point
  1-dim. vector subspace
- "line" = projective line
  2-dim. vector subspace
- "spread" = a set of lines which partition the points of $PG(n,q)$
- "packing" = "resolution" = " parallelism" = a set of spreads which partition the set of lines
- $\exists$ packing in $PG(n,q) \implies n$: odd ($\Longleftarrow$: open)

$PG(n,q)$, n: even

- "packing" = "resolution" = " parallelism" = a set of spreads which partition the set of points
- $\exists$ packing in $PG(n,q) \implies n$: odd

$PG(n, q)$, n: even

- "packing" = "resolution" = " parallelism" = a set of spreads which partition the set of points
- $\exists$ packing in $PG(n, q) \implies n$: odd

Question 1. Does there exist a partition of the set of lines of $PG(2n, q)$ into spreads of hyperplanes?

$PG(n,q)$, n: even

- "packing" = "resolution" = " parallelism" = a set of spreads which partition the set of points
- $\exists$ packing in $PG(n,q) \implies n$: odd

Question 1. Does there exist a partition of the set of lines of $PG(2n,q)$ into spreads of hyperplanes?
When the answer to Question 1 is affirmative, we say that $PG(2n,q)$ is $(2n-1)$-partitionable.

$PG(n,q)$, n: even

- "packing" = "resolution" = " parallelism" = a set of spreads which partition the set of points
- $\exists$ packing in $PG(n,q) \implies n$: odd

Question 1. Does there exist a partition of the set of lines of $PG(2n,q)$ into spreads of hyperplanes?
When the answer to Question 1 is affirmative, we say that $PG(2n,q)$ is $(2n-1)$-partitionable.

$$\#(\text{lines}) = \frac{(q^{n+1}-1)(q^n-1)}{(q^2-1)(q-1)} = \frac{(q^{n+1}-1)}{(q-1)} \cdot \frac{(q^n-1)}{(q^2-1)}$$

$$= \#(\text{hyperplanes}) \times \# \begin{pmatrix} \text{lines in a spread} \\ \text{of a hyperplane} \end{pmatrix}$$

Fuji-hara, Jimbo and Vanstone (1986)

Question 2. Does there exist a spread S_H for each hyperplane H of $PG(2n, q)$, such that

$$\text{lines of } PG(2n,q) = \bigcup_{H} S_H \text{ (disjoint)},$$

where H runs through all hyperplanes of $PG(2n, q)$?

Fuji-hara, Jimbo and Vanstone (1986)

Question 2. Does there exist a spread S_H for each hyperplane H of $PG(2n, q)$, such that

$$\text{lines of } PG(2n, q) = \bigcup_H S_H \text{ (disjoint)},$$

where H runs through all hyperplanes of $PG(2n, q)$?
Yes for $(2n, q) = (4, 2), (4, 3), (6, q)$, etc.

Fuji-hara, Jimbo and Vanstone (1986)

Question 2. Does there exist a spread S_H for each hyperplane H of $PG(2n, q)$, such that

$$\text{lines of } PG(2n, q) = \bigcup_H S_H \text{ (disjoint)},$$

where H runs through all hyperplanes of $PG(2n, q)$?
Yes for $(2n, q) = (4, 2), (4, 3), (6, q)$, etc.

The answer was unknown for $(4, 4), (4, 5), (4, 7)$, etc.

Singer Cycle

$$\sigma = \text{Singer cycle of } PG(2n, q)$$

$$= \text{cyclic automorphism of order } \frac{q^{2n+1}-1}{q-1}$$

Singer Cycle

$$\sigma = \text{Singer cycle of } PG(2n, q)$$

$$= \text{cyclic automorphism of order } \frac{q^{2n+1}-1}{q-1}$$

$$\langle\sigma\rangle \text{ has } \begin{cases} \text{only one orbit on points} \\ \text{only one orbit on hyperplanes} \end{cases}$$

Singer Cycle

$$\sigma = \text{Singer cycle of } PG(2n,q)$$
$$= \text{cyclic automorphism of order } \frac{q^{2n+1}-1}{q-1}$$

$$\langle\sigma\rangle \text{ has } \begin{cases} \text{only one orbit on points} \\ \text{only one orbit on hyperplanes} \end{cases}$$

In $PG(2n,q)$,

$$H = L_1 \cup L_2 \cup \cdots \cup L_s : \text{ spread of } H$$
$$H^\sigma = L_1^\sigma \cup L_2^\sigma \cup \cdots \cup L_s^\sigma : \text{ spread of } H^\sigma$$
$$\vdots$$

Orbits of Singer Cycle

In $PG(2n, q)$,

$$H = L_1 \cup L_2 \cup \cdots \cup L_s : \text{ spread of } H$$
$$H^\sigma = L_1^\sigma \cup L_2^\sigma \cup \cdots \cup L_s^\sigma : \text{ spread of } H^\sigma$$
$$\vdots$$

if distinct $\langle \sigma \rangle$-orbits $\implies$ $(2n-1)$-partitionable

Orbits of Singer Cycle

In $PG(2n, q)$,

$$H = L_1 \cup L_2 \cup \cdots \cup L_s : \text{ spread of } H$$
$$H^\sigma = L_1^\sigma \cup L_2^\sigma \cup \cdots \cup L_s^\sigma : \text{ spread of } H^\sigma$$
$$\vdots$$

if distinct $\langle\sigma\rangle$-orbits $\Longrightarrow$ $(2n-1)$-partitionable

Question 3. Does there exist a spread S of a hyperplane H in $PG(2n, q)$ such that the members of S belong to distinct $\langle\sigma\rangle$-orbits?

Orbits of Singer Cycle

In $PG(2n, q)$,

$$H = L_1 \cup L_2 \cup \cdots \cup L_s : \text{ spread of } H$$

$$H^\sigma = L_1^\sigma \cup L_2^\sigma \cup \cdots \cup L_s^\sigma : \text{ spread of } H^\sigma$$

$$\vdots$$

if distinct $\langle\sigma\rangle$-orbits $\implies$ $(2n-1)$-partitionable

Question 3. Does there exist a spread S of a hyperplane H in $PG(2n, q)$ such that the members of S belong to distinct $\langle\sigma\rangle$-orbits?

Such a spread produces a difference system of sets.

Difference System of Sets

Suppose that there is a spread S of a hyperplane H of $PG(2n, q)$ such that the members of S belong to different $\langle\sigma\rangle$-orbits.

Difference System of Sets

Suppose that there is a spread S of a hyperplane H of $PG(2n, q)$ such that the members of S belong to different $\langle\sigma\rangle$-orbits.
Then S becomes a difference system of sets, defined as follows.

Difference System of Sets

Suppose that there is a spread S of a hyperplane H of $PG(2n, q)$ such that the members of S belong to different $\langle\sigma\rangle$-orbits.
Then S becomes a difference system of sets, defined as follows.
Definition. Let G be a finite group of order v, let λ, m be positive integers.

Difference System of Sets

Suppose that there is a spread S of a hyperplane H of $PG(2n, q)$ such that the members of S belong to different $\langle\sigma\rangle$-orbits.
Then S becomes a difference system of sets, defined as follows.
Definition. Let G be a finite group of order v, let λ, m be positive integers. A family of m-subsets $\{B_1, B_2, \ldots, B_k\}$ of G is called a $(v, k, \lambda; m)$ *difference system of sets* if the multiset

$$\{gh^{-1} \mid g \in B_i,\ h \in B_j,\ 1 \leq i, j \leq k,\ i \neq j\}$$

coincides with $\lambda(G - \{1\})$.

Partitionability and DSS

Indeed, identify $\langle\sigma\rangle$ with $PG(2n, q)$. Then

Partitionability and DSS

Indeed, identify $\langle \sigma \rangle$ with $PG(2n, q)$. Then $\{gh^{-1} \mid g \in L_i,\ h \in L_j,\ 1 \leq i, j \leq k,\ i \neq j\}$

Partitionability and DSS

Indeed, identify $\langle \sigma \rangle$ with $PG(2n, q)$. Then

$$\{gh^{-1} \mid g \in L_i,\ h \in L_j,\ 1 \le i, j \le k,\ i \ne j\}$$

$$= \{gh^{-1} \mid g \in L_i,\ h \in L_j,\ 1 \le i, j \le k,\ g \ne h\}$$

$$- \{gh^{-1} \mid g \in L_i,\ h \in L_i,\ 1 \le i \le k,\ g \ne h\}$$

Partitionability and DSS

Indeed, identify $\langle\sigma\rangle$ with $PG(2n,q)$. Then
$\{gh^{-1} \mid g \in L_i,\ h \in L_j,\ 1 \leq i,j \leq k,\ i \neq j\}$
$= \{gh^{-1} \mid g \in L_i,\ h \in L_j,\ 1 \leq i,j \leq k,\ g \neq h\}$
$- \{gh^{-1} \mid g \in L_i,\ h \in L_i,\ 1 \leq i \leq k,\ g \neq h\}$
$= \{gh^{-1} \mid g \in H,\ h \in H,\ g \neq h\}$ difference set
$- \bigcup_{i=1}^{k} \{gh^{-1} \mid g \in L_i,\ h \in L_i,\ g \neq h\}$ difference family

Partitionability and DSS

Indeed, identify $\langle\sigma\rangle$ with $PG(2n, q)$. Then

$\{gh^{-1} \mid g \in L_i,\ h \in L_j,\ 1 \le i, j \le k,\ i \ne j\}$

$= \{gh^{-1} \mid g \in L_i,\ h \in L_j,\ 1 \le i, j \le k,\ g \ne h\}$

$- \{gh^{-1} \mid g \in L_i,\ h \in L_i,\ 1 \le i \le k,\ g \ne h\}$

$= \{gh^{-1} \mid g \in H,\ h \in H,\ g \ne h\}$ difference set

$- \bigcup_{i=1}^{k} \{gh^{-1} \mid g \in L_i,\ h \in L_i,\ g \ne h\}$ difference family

$= \frac{q^{n-1}-1}{q-1}(G - \{1\}) - (G - \{1\})$.

Partitionability and DSS

Indeed, identify $\langle\sigma\rangle$ with $PG(2n,q)$. Then
$\{gh^{-1} \mid g \in L_i,\ h \in L_j,\ 1 \le i,j \le k,\ i \ne j\}$
$= \{gh^{-1} \mid g \in L_i,\ h \in L_j,\ 1 \le i,j \le k,\ g \ne h\}$
$- \{gh^{-1} \mid g \in L_i,\ h \in L_i,\ 1 \le i \le k,\ g \ne h\}$
$= \{gh^{-1} \mid g \in H,\ h \in H,\ g \ne h\}$ difference set
$- \bigcup_{i=1}^{k} \{gh^{-1} \mid g \in L_i,\ h \in L_i,\ g \ne h\}$ difference family
$= \frac{q^{n-1}-1}{q-1}(G - \{1\}) - (G - \{1\})$.
Thus

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

$PG(4,4)$

Let H be a hyperplane in $PG(4,4)$. Define a graph Γ as follows.

- vertices = lines of H

$PG(4,4)$

Let H be a hyperplane in $PG(4,4)$. Define a graph Γ as follows.

- vertices = lines of H
- edges = pairs $\{L, L'\}$ of skew lines such that $L' \notin L^{\langle\sigma\rangle}$.

$PG(4,4)$

Let H be a hyperplane in $PG(4,4)$. Define a graph Γ as follows.

- vertices = lines of H
- edges = pairs $\{L, L'\}$ of skew lines such that $L' \notin L^{\langle\sigma\rangle}$.

Every clique of size $q^2+1=17$ in Γ gives a spread such that its members belong to distinct $\langle\sigma\rangle$-orbits.

$PG(4,4)$

Let H be a hyperplane in $PG(4,4)$. Define a graph Γ as follows.

- vertices = lines of H
- edges = pairs $\{L, L'\}$ of skew lines such that $L' \notin L^{\langle\sigma\rangle}$.

Every clique of size $q^2 + 1 = 17$ in Γ gives a spread such that its members belong to distinct $\langle\sigma\rangle$-orbits.
Γ has

$$357 \text{ vertices}, \quad 42,976 \text{ edges},$$

and using MAGMA, we see that Γ has no clique of size 17.

$PG(4, q)$ **with** $q \equiv 2$ **or** $3 \pmod 5$

When $q > 4$, the exhaustive search like the case of $PG(4, 4)$ does not work.

$PG(4, q)$ with $q \equiv 2$ or $3 \pmod 5$

When $q > 4$, the exhaustive search like the case of $PG(4, 4)$ does not work. So we try to perform a more restrictive search, by assuming more symmetry (Frobenius automorphism).

$PG(4, q)$ with $q \equiv 2$ or $3 \pmod 5$

When $q > 4$, the exhaustive search like the case of $PG(4, 4)$ does not work. So we try to perform a more restrictive search, by assuming more symmetry (Frobenius automorphism).

- $GF(q^5) \leftrightarrow GF(q)^5 \rightarrow PG(4, q)$

$PG(4, q)$ **with** $q \equiv 2$ **or** $3 \pmod 5$

When $q > 4$, the exhaustive search like the case of $PG(4, 4)$ does not work. So we try to perform a more restrictive search, by assuming more symmetry (Frobenius automorphism).

- $GF(q^5) \leftrightarrow GF(q)^5 \rightarrow PG(4, q)$
- $\langle f \rangle = \mathrm{Aut}GF(q^5)$.

$PG(4, q)$ with $q \equiv 2$ or $3 \pmod 5$

When $q > 4$, the exhaustive search like the case of $PG(4, 4)$ does not work. So we try to perform a more restrictive search, by assuming more symmetry (Frobenius automorphism).

- $GF(q^5) \leftrightarrow GF(q)^5 \rightarrow PG(4, q)$
- $\langle f \rangle = \mathrm{Aut} GF(q^5)$.

Regard f as an automorphism of $PG(4, q)$.

$PG(4, q)$ **with** $q \equiv 2$ **or** $3 \pmod 5$

When $q > 4$, the exhaustive search like the case of $PG(4, 4)$ does not work. So we try to perform a more restrictive search, by assuming more symmetry (Frobenius automorphism).

- $GF(q^5) \leftrightarrow GF(q)^5 \rightarrow PG(4, q)$
- $\langle f \rangle = \mathrm{Aut}GF(q^5)$.

Regard f as an automorphism of $PG(4, q)$.

- f fixes a unique hyperplane H, but none of the lines of H.

$PG(4,q)$ **with** $q \equiv 2$ **or** $3 \pmod 5$

When $q > 4$, the exhaustive search like the case of $PG(4,4)$ does not work. So we try to perform a more restrictive search, by assuming more symmetry (Frobenius automorphism).

- $GF(q^5) \leftrightarrow GF(q)^5 \rightarrow PG(4,q)$
- $\langle f \rangle = \mathrm{Aut}GF(q^5)$.

Regard f as an automorphism of $PG(4,q)$.

- f fixes a unique hyperplane H, but none of the lines of H.

Look for an f-invariant spread

$$S = \{L_1, L_1^f, L_1^{f^2}, L_1^{f^3}, L_1^{f^4}, \dots L^{f^4}_{\frac{q^2+1}{5}}\}$$

of H, such that its members belong to distinct $\langle \sigma \rangle$-orbits.

$PG(4,8)$

In graph theoretic terms again, define a graph $\overline{\Gamma}$ as follows.

- vertices $= \{L^{\langle f \rangle} \mid L : \text{ line of } H\}$: sets of skew lines

$PG(4,8)$

In graph theoretic terms again, define a graph $\overline{\Gamma}$ as follows.

- vertices = $\{L^{\langle f \rangle} \mid L: \text{ line of } H\}$: sets of skew lines
- edges = pairs $\{L^{\langle f \rangle}, M^{\langle f \rangle}\}$ such that $L^{f^i} \cap M^{f^j} = \emptyset$ and $L^{f^i} \notin M^{{f^j}^{\langle \sigma \rangle}}$.

$PG(4, 8)$

In graph theoretic terms again, define a graph $\overline{\Gamma}$ as follows.

- vertices = $\{L^{\langle f \rangle} \mid L: \text{ line of } H\}$: sets of skew lines
- edges = pairs $\{L^{\langle f \rangle}, M^{\langle f \rangle}\}$ such that $L^{f^i} \cap M^{f^j} = \emptyset$ and $L^{f^i} \notin M^{{f^j}^{\langle \sigma \rangle}}$.

Every clique of size $(q^2 + 1)/5 = 13$ in $\overline{\Gamma}$ gives an f-invariant spread such that its members belong to distinct $\langle \sigma \rangle$-orbits.

$PG(4, 8)$

$\overline{\Gamma}$ has

$$715 \text{ vertices}, \quad 107,694 \text{ edges},$$

$PG(4, 8)$

$\overline{\Gamma}$ has

$$715 \text{ vertices}, \quad 107,694 \text{ edges},$$

and using MAGMA, we see that $\overline{\Gamma}$ has a clique of size 13.

$PG(4,8)$

$\overline{\Gamma}$ has

$$715 \text{ vertices}, \quad 107,694 \text{ edges},$$

and using MAGMA, we see that $\overline{\Gamma}$ has a clique of size 13.

Theorem. $PG(4,8)$ is 3-partitionable.

$PG(4, 8)$

$\overline{\Gamma}$ has

$$715 \text{ vertices}, \quad 107,694 \text{ edges},$$

and using MAGMA, we see that $\overline{\Gamma}$ has a clique of size 13.

Theorem. $PG(4, 8)$ is 3-partitionable.

Somewhat more complicated analysis shows that $PG(4, q)$ is 3-partitionable for $q = 5, 9$.

$PG(4,8)$

$\overline{\Gamma}$ has

$$715 \text{ vertices}, \quad 107,694 \text{ edges},$$

and using MAGMA, we see that $\overline{\Gamma}$ has a clique of size 13.

Theorem. $PG(4,8)$ is 3-partitionable.

Somewhat more complicated analysis shows that $PG(4,q)$ is 3-partitionable for $q = 5, 9$.

They give

$$(v,k,\lambda) = (\frac{q^5-1}{q-1}, q^2+1, q^2+q; q+1)$$

difference system of sets for $q = 5, 8, 9$.

Spreads of Planes in $PG(5,q) \subset PG(6,q)$

As before let σ denote a Singer cycle in $PG(6,q)$.

Spreads of Planes in $PG(5,q) \subset PG(6,q)$

Question 4. Does there exist a spread Π of planes of a hyperplane H in $PG(6,q)$ such that

Spreads of Planes in $PG(5, q) \subset PG(6, q)$

Question 4. Does there exist a spread Π of planes of a hyperplane H in $PG(6, q)$ such that

- the members of Π belong to distinct $\langle\sigma\rangle$-orbits,

Spreads of Planes in $PG(5,q) \subset PG(6,q)$

Question 4. Does there exist a spread Π of planes of a hyperplane H in $PG(6,q)$ such that

- the members of Π belong to distinct $\langle\sigma\rangle$-orbits,
- Π forms a difference family.

Spreads of Planes in $PG(5, q) \subset PG(6, q)$

Question 4. Does there exist a spread Π of planes of a hyperplane H in $PG(6, q)$ such that

- the members of Π belong to distinct $\langle \sigma \rangle$-orbits,
- Π forms a difference family.

If $\Pi = \{P_1, P_2, \ldots, P_{q^3+q}\}$ is such a spread of planes, then Π forms a

$$\left(\frac{q^7-1}{q-1}, q^3+1, \frac{q^5-q^2}{q-1}; \frac{q^3-1}{q-1}\right)$$

difference system of sets.

Spreads of Planes in $PG(5,q) \subset PG(6,q)$

Question 4. Does there exist a spread Π of planes of a hyperplane H in $PG(6,q)$ such that

- the members of Π belong to distinct $\langle\sigma\rangle$-orbits,
- Π forms a difference family.

If $\Pi = \{P_1, P_2, \ldots, P_{q^3+q}\}$ is such a spread of planes, then Π forms a

$$\left(\frac{q^7-1}{q-1}, q^3+1, \frac{q^5-q^2}{q-1}; \frac{q^3-1}{q-1}\right)$$

difference system of sets.

A difference family whose members belong to distinct $\langle\sigma\rangle$-orbits was constructed for $q=2$ by Miyakawa–Munemasa–Yoshiara (1995).