Hemisystems on the Hermitian surface

Gábor Korchmáros

Università degli Studi della Basilicata, Italy

joint work with Gábor P. Nagy and Pietro Speziali

Finite Geometries, Fifth Irsee Conference

September 10-16 2017, Irsee

Hermitian surface and hemisystems

Hermitian surface and hemisystems

$\mathcal{U}_3$:=set of all isotropic points of a unitary polarity of $PG(3, q^2)$.

Hermitian surface and hemisystems

$\mathcal{U}_3$:=set of all isotropic points of a unitary polarity of $PG(3, q^2)$.

Remark

$\mathcal{U}_3$:=set of all isotropic points of a unitary polarity of $PG(3, q^2)$.

Remark

Equivalent definitions for $\mathcal{U}_3$:

$\mathcal{U}_3$:=set of all isotropic points of a unitary polarity of $PG(3, q^2)$.

Remark

Equivalent definitions for $\mathcal{U}_3$:
$\{P = (a_1, a_2, a_3, a_4) \in PG(3, q^2) | a_3^q a_0 + a_3 a_0^q + a_1^{q+1} + a_2^{q+1} = 0\}$

Hermitian surface and hemisystems

$\mathcal{U}_3$:=set of all isotropic points of a unitary polarity of $PG(3, q^2)$.

Remark

Equivalent definitions for $\mathcal{U}_3$*:*
$\{P = (a_1, a_2, a_3, a_4) \in PG(3, q^2) | a_3^q a_0 + a_3 a_0^q + a_1^{q+1} + a_2^{q+1} = 0\}$
Set of all points of $PG(3, q^2)$ *on the Hermitian surface with equation* $X_0 X_3^q + X_0^q X_3 + X_1^{q+1} + X_2^{q+1} = 0$.

Hermitian surface and hemisystems

$\mathcal{U}_3$:=set of all isotropic points of a unitary polarity of $PG(3, q^2)$.

Remark

Equivalent definitions for $\mathcal{U}_3$:
$\{P = (a_1, a_2, a_3, a_4) \in PG(3, q^2) | a_3^q a_0 + a_3 a_0^q + a_1^{q+1} + a_2^{q+1} = 0\}$
Set of all points of $PG(3, q^2)$ on the Hermitian surface with equation $X_0 X_3^q + X_0^q X_3 + X_1^{q+1} + X_2^{q+1} = 0$.

- number of points in $\mathcal{U}_3 = (q^3 + 1)(q^2 + 1)$

Hermitian surface and hemisystems

$\mathcal{U}_3$:=set of all isotropic points of a unitary polarity of $PG(3,q^2)$.

Remark

Equivalent definitions for $\mathcal{U}_3$:
$\{P=(a_1,a_2,a_3,a_4)\in PG(3,q^2) | a_3^q a_0 + a_3 a_0^q + a_1^{q+1} + a_2^{q+1} = 0\}$
Set of all points of $PG(3,q^2)$ on the Hermitian surface with equation $X_0X_3^q + X_0^qX_3 + X_1^{q+1} + X_2^{q+1} = 0$.

- number of points in $\mathcal{U}_3$= $(q^3+1)(q^2+1)$
- number of generators of $\mathcal{U}_3$ =$(q^3+1)(q+1)$

Hermitian surface and hemisystems

$\mathcal{U}_3$:=set of all isotropic points of a unitary polarity of $PG(3, q^2)$.

Remark

Equivalent definitions for $\mathcal{U}_3$:
$\{P = (a_1, a_2, a_3, a_4) \in PG(3, q^2) | a_3^q a_0 + a_3 a_0^q + a_1^{q+1} + a_2^{q+1} = 0\}$
Set of all points of $PG(3, q^2)$ on the Hermitian surface with equation $X_0 X_3^q + X_0^q X_3 + X_1^{q+1} + X_2^{q+1} = 0$.

- number of points in $\mathcal{U}_3$= $(q^3 + 1)(q^2 + 1)$
- number of generators of $\mathcal{U}_3$ =$(q^3 + 1)(q + 1)$
- number of generators on a point $= q + 1$

Hermitian surface and hemisystems

$\mathcal{U}_3$:=set of all isotropic points of a unitary polarity of $PG(3,q^2)$.

Remark

Equivalent definitions for $\mathcal{U}_3$:
$\{P=(a_1,a_2,a_3,a_4)\in PG(3,q^2)|a_3^q a_0 + a_3 a_0^q + a_1^{q+1} + a_2^{q+1} = 0\}$
Set of all points of $PG(3,q^2)$ on the Hermitian surface with equation $X_0 X_3^q + X_0^q X_3 + X_1^{q+1} + X_2^{q+1} = 0$.

- number of points in $\mathcal{U}_3 = (q^3+1)(q^2+1)$
- number of generators of $\mathcal{U}_3 = (q^3+1)(q+1)$
- number of generators on a point $= q+1$
- hemisystem:=set of generators containing exactly $\frac{1}{2}(q+1)$ generators on every point of $\mathcal{U}_3$.

Known examples

Hemisystems of $\mathcal{U}_3$ are rare objects

Known examples

Hemisystems of $\mathcal{U}_3$ are rare objects

Segre (1965) for $q = 3$

Known examples

Hemisystems of $\mathcal{U}_3$ are rare objects

Segre (1965) for $q = 3$
Cossidente-Penttila (2005) for every (odd) q

Known examples

Hemisystems of $\mathcal{U}_3$ are rare objects

Segre (1965) for $q = 3$
Cossidente-Penttila (2005) for every (odd) q
Bamberg-Giudici-Royle, Cossidente-Pavese for small $q \leq 23$'s

Known examples

Hemisystems of $\mathcal{U}_3$ are rare objects

Segre (1965) for $q = 3$
Cossidente-Penttila (2005) for every (odd) q
Bamberg-Giudici-Royle, Cossidente-Pavese for small $q \leq 23$'s
Bamberg–Lee–Momihara–Xiang (2016), for all q with $q \equiv 3 \pmod 4$

Hemisystems of $\mathcal{U}_3$ are rare objects

Segre (1965) for $q = 3$
Cossidente-Penttila (2005) for every (odd) q
Bamberg-Giudici-Royle, Cossidente-Pavese for small $q \leq 23$'s
Bamberg–Lee–Momihara–Xiang (2016), for all q with $q \equiv 3 \pmod 4$

Our contribution:

Known examples

Hemisystems of $\mathcal{U}_3$ are rare objects

Segre (1965) for $q = 3$
Cossidente-Penttila (2005) for every (odd) q
Bamberg-Giudici-Royle, Cossidente-Pavese for small $q \leq 23$'s
Bamberg–Lee–Momihara–Xiang (2016), for all q with $q \equiv 3 \pmod 4$

Our contribution:
G.K.-Nagy-Speziali (2017) for all $q = p$ with $p = 1 + 16n^2$ (infinite family if Landau's conjecture is true)

Maximal curves

Maximal curves

Maximal curve:= curve $\mathcal{X}$ whose number of points $N_{q^2}(\mathcal{X})$ attains the Hasse-Weil upper bound;

Maximal curves

Maximal curve:= curve $\mathcal{X}$ whose number of points $N_{q^2}(\mathcal{X})$ attains the Hasse-Weil upper bound;
$N_{q^2}(\mathcal{X}) = q^2 + 1 + 2\mathfrak{g}(\mathcal{X})q$ where $\mathfrak{g}(\mathcal{X})$:=genus of $\mathcal{X}$.

Maximal curves

Maximal curve:= curve $\mathcal{X}$ whose number of points $N_{q^2}(\mathcal{X})$ attains the Hasse-Weil upper bound;
$N_{q^2}(\mathcal{X}) = q^2 + 1 + 2\mathfrak{g}(\mathcal{X})q$ where $\mathfrak{g}(\mathcal{X})$:=genus of $\mathcal{X}$.

Corollary to the Natural Embedding Theorem (G.K.-F. Torres, 2000) Every curve of degree $q+1$ lying on the Hermitian surface $\mathcal{U}_3$ is a maximal curve.

Maximal curves

Maximal curve:= curve $\mathcal{X}$ whose number of points $N_{q^2}(\mathcal{X})$ attains the Hasse-Weil upper bound;
$N_{q^2}(\mathcal{X}) = q^2 + 1 + 2\mathfrak{g}(\mathcal{X})q$ where $\mathfrak{g}(\mathcal{X})$:=genus of $\mathcal{X}$.

Corollary to the Natural Embedding Theorem (G.K.-F. Torres, 2000) Every curve of degree $q+1$ lying on the Hermitian surface $\mathcal{U}_3$ is a maximal curve.
Example 1

Maximal curves

Maximal curve:= curve $\mathcal{X}$ whose number of points $N_{q^2}(\mathcal{X})$ attains the Hasse-Weil upper bound;
$N_{q^2}(\mathcal{X}) = q^2 + 1 + 2\mathfrak{g}(\mathcal{X})q$ where $\mathfrak{g}(\mathcal{X})$:=genus of $\mathcal{X}$.

Corollary to the Natural Embedding Theorem (G.K.-F. Torres, 2000) Every curve of degree $q+1$ lying on the Hermitian surface $\mathcal{U}_3$ is a maximal curve.

Example 1

Rational curve

Maximal curves

Maximal curve:= curve $\mathcal{X}$ whose number of points $N_{q^2}(\mathcal{X})$ attains the Hasse-Weil upper bound;
$N_{q^2}(\mathcal{X}) = q^2 + 1 + 2\mathfrak{g}(\mathcal{X})q$ where $\mathfrak{g}(\mathcal{X})$:=genus of $\mathcal{X}$.

Corollary to the Natural Embedding Theorem (G.K.-F. Torres, 2000) Every curve of degree $q+1$ lying on the Hermitian surface $\mathcal{U}_3$ is a maximal curve.
Example 1
Rational curve
Example 2

Maximal curves

Maximal curve:= curve $\mathcal{X}$ whose number of points $N_{q^2}(\mathcal{X})$ attains the Hasse-Weil upper bound;
$N_{q^2}(\mathcal{X}) = q^2 + 1 + 2\mathfrak{g}(\mathcal{X})q$ where $\mathfrak{g}(\mathcal{X})$:=genus of $\mathcal{X}$.

Corollary to the Natural Embedding Theorem (G.K.-F. Torres, 2000) Every curve of degree $q+1$ lying on the Hermitian surface $\mathcal{U}_3$ is a maximal curve.

Example 1

Rational curve

Example 2

Hermitian curve (non-tangent plane section of $\mathcal{U}_3$)

Maximal curves

Maximal curve:= curve $\mathcal{X}$ whose number of points $N_{q^2}(\mathcal{X})$ attains the Hasse-Weil upper bound;
$N_{q^2}(\mathcal{X}) = q^2 + 1 + 2\mathfrak{g}(\mathcal{X})q$ where $\mathfrak{g}(\mathcal{X})$:=genus of $\mathcal{X}$.

Corollary to the Natural Embedding Theorem (G.K.-F. Torres, 2000) Every curve of degree $q+1$ lying on the Hermitian surface $\mathcal{U}_3$ is a maximal curve.

Example 1

Rational curve

Example 2

Hermitian curve (non-tangent plane section of $\mathcal{U}_3$)

Example 3 (Fuhrmann-Torres curve)

Maximal curves

Maximal curve:= curve $\mathcal{X}$ whose number of points $N_{q^2}(\mathcal{X})$ attains the Hasse-Weil upper bound;
$N_{q^2}(\mathcal{X}) = q^2 + 1 + 2\mathfrak{g}(\mathcal{X})q$ where $\mathfrak{g}(\mathcal{X})$:=genus of $\mathcal{X}$.

Corollary to the Natural Embedding Theorem (G.K.-F. Torres, 2000) Every curve of degree $q+1$ lying on the Hermitian surface $\mathcal{U}_3$ is a maximal curve.

Example 1

Rational curve

Example 2

Hermitian curve (non-tangent plane section of $\mathcal{U}_3$)

Example 3 (Fuhrmann-Torres curve)

$\mathcal{U}_3$:=$X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0$;

Maximal curves

Maximal curve:= curve $\mathcal{X}$ whose number of points $N_{q^2}(\mathcal{X})$ attains the Hasse-Weil upper bound;
$N_{q^2}(\mathcal{X}) = q^2 + 1 + 2\mathfrak{g}(\mathcal{X})q$ where $\mathfrak{g}(\mathcal{X})$:=genus of $\mathcal{X}$.

Corollary to the Natural Embedding Theorem (G.K.-F. Torres, 2000) Every curve of degree $q+1$ lying on the Hermitian surface $\mathcal{U}_3$ is a maximal curve.

Example 1

Rational curve

Example 2

Hermitian curve (non-tangent plane section of $\mathcal{U}_3$)

Example 3 (Fuhrmann-Torres curve)

$\mathcal{U}_3$:=$X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0$;
$\mathcal{X}^+ := \{(1, u, v, v^2) | u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$.

Maximal curves

Maximal curve:= curve $\mathcal{X}$ whose number of points $N_{q^2}(\mathcal{X})$ attains the Hasse-Weil upper bound;
$N_{q^2}(\mathcal{X}) = q^2 + 1 + 2\mathfrak{g}(\mathcal{X})q$ where $\mathfrak{g}(\mathcal{X})$:=genus of $\mathcal{X}$.

Corollary to the Natural Embedding Theorem (G.K.-F. Torres, 2000) Every curve of degree $q+1$ lying on the Hermitian surface $\mathcal{U}_3$ is a maximal curve.

Example 1

Rational curve

Example 2

Hermitian curve (non-tangent plane section of $\mathcal{U}_3$)

Example 3 (Fuhrmann-Torres curve)

$\mathcal{U}_3 := X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0;$
$\mathcal{X}^+ := \{(1, u, v, v^2) | u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0,0,0,1\}.$
$\mathcal{X}^+$ has genus $\mathfrak{g}(\mathcal{X}) = \frac{1}{4}(q-1)^2;$

Maximal curves

Maximal curve:= curve $\mathcal{X}$ whose number of points $N_{q^2}(\mathcal{X})$ attains the Hasse-Weil upper bound;
$N_{q^2}(\mathcal{X}) = q^2 + 1 + 2\mathfrak{g}(\mathcal{X})q$ where $\mathfrak{g}(\mathcal{X})$:=genus of $\mathcal{X}$.

Corollary to the Natural Embedding Theorem (G.K.-F. Torres, 2000) Every curve of degree $q+1$ lying on the Hermitian surface $\mathcal{U}_3$ is a maximal curve.

Example 1

Rational curve

Example 2

Hermitian curve (non-tangent plane section of $\mathcal{U}_3$)

Example 3 (Fuhrmann-Torres curve)

$\mathcal{U}_3$:=$X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0$;
$\mathcal{X}^+ := \{(1, u, v, v^2) | u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$.
$\mathcal{X}^+$ has genus $\mathfrak{g}(\mathcal{X}) = \frac{1}{4}(q-1)^2$; $N_{q^2}(\mathcal{X}^+) = \frac{1}{2}(q^3 - q) + q + 1$.

Maximal curves

Maximal curve:= curve $\mathcal{X}$ whose number of points $N_{q^2}(\mathcal{X})$ attains the Hasse-Weil upper bound;
$N_{q^2}(\mathcal{X}) = q^2 + 1 + 2\mathfrak{g}(\mathcal{X})q$ where $\mathfrak{g}(\mathcal{X})$:=genus of $\mathcal{X}$.

Corollary to the Natural Embedding Theorem (G.K.-F. Torres, 2000) Every curve of degree $q+1$ lying on the Hermitian surface $\mathcal{U}_3$ is a maximal curve.

Example 1

Rational curve

Example 2

Hermitian curve (non-tangent plane section of $\mathcal{U}_3$)

Example 3 (Fuhrmann-Torres curve)

$\mathcal{U}_3$:=$X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0$;
$\mathcal{X}^+ := \{(1, u, v, v^2) | u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$.
$\mathcal{X}^+$ has genus $\mathfrak{g}(\mathcal{X}) = \frac{1}{4}(q-1)^2$; $N_{q^2}(\mathcal{X}^+) = \frac{1}{2}(q^3 - q) + q + 1$.
$\mathrm{Aut}(\mathcal{X}^+)$ has an index 2 subgroup $\cong PSL(2, q) \times C_{(q+1)/2}$

Combinatorial Properties of Maximal curves lying on $\mathcal{H}_3$

Apparently maximal curves are useless as a tool in the study of $\mathcal{U}_3$, as a polar space.

Apparently maximal curves are useless as a tool in the study of $\mathcal{U}_3$, as a polar space.
Wrong thesis!

Apparently maximal curves are useless as a tool in the study of $\mathcal{U}_3$, as a polar space.
Wrong thesis!
$\mathcal{X}$:=maximal curve naturally embedded in $\mathcal{U}_3$;

Apparently maximal curves are useless as a tool in the study of $\mathcal{U}_3$, as a polar space.
Wrong thesis!
$\mathcal{X}$:=maximal curve naturally embedded in $\mathcal{U}_3$;

real chord of $\mathcal{X}$:= any line meeting $\mathcal{X}$ in more than one point;

Apparently maximal curves are useless as a tool in the study of $\mathcal{U}_3$, as a polar space.

Wrong thesis!

$\mathcal{X}$:=maximal curve naturally embedded in $\mathcal{U}_3$;

real chord of $\mathcal{X}$:= any line meeting $\mathcal{X}$ in more than one point;

imaginary chord of $\mathcal{X}$:= any line through a point $P \in \mathcal{X}$ with $P \in PG(3, q^4) \setminus PG(3, q^2)$ and its Frobenius image $P' = \Phi_{q^2}(P)$.

Apparently maximal curves are useless as a tool in the study of $\mathcal{U}_3$, as a polar space.
Wrong thesis!
$\mathcal{X}$:=maximal curve naturally embedded in $\mathcal{U}_3$;

real chord of $\mathcal{X}$:= any line meeting $\mathcal{X}$ in more than one point;

imaginary chord of $\mathcal{X}$:= any line through a point $P \in \mathcal{X}$ with $P \in PG(3, q^4) \setminus PG(3, q^2)$ and its Frobenius image $P' = \Phi_{q^2}(P)$.

- the points of $\mathcal{X}$ form a partial ovoid of $\mathcal{U}_3$;
- every imaginary chord of $\mathcal{X}$ is a generator disjoint from $\mathcal{X}$.

Combinatorial Properties of Maximal curves lying on $\mathcal{H}_3$

Apparently maximal curves are useless as a tool in the study of $\mathcal{U}_3$, as a polar space.
Wrong thesis!
$\mathcal{X}$:=maximal curve naturally embedded in $\mathcal{U}_3$;

real chord of $\mathcal{X}$:= any line meeting $\mathcal{X}$ in more than one point;

imaginary chord of $\mathcal{X}$:= any line through a point $P \in \mathcal{X}$ with $P \in PG(3, q^4) \setminus PG(3, q^2)$ and its Frobenius image $P' = \Phi_{q^2}(P)$.

- the points of $\mathcal{X}$ form a partial ovoid of $\mathcal{U}_3$;
- every imaginary chord of $\mathcal{X}$ is a generator disjoint from $\mathcal{X}$.

Question Is there a hemisystem consisting of imaginary chords and generators which meet $\mathcal{X}$ (exactly one point)?

Apparently maximal curves are useless as a tool in the study of $\mathcal{U}_3$, as a polar space.
Wrong thesis!
$\mathcal{X}$:=maximal curve naturally embedded in $\mathcal{U}_3$;

real chord of $\mathcal{X}$:= any line meeting $\mathcal{X}$ in more than one point;

imaginary chord of $\mathcal{X}$:= any line through a point $P \in \mathcal{X}$ with $P \in PG(3, q^4) \setminus PG(3, q^2)$ and its Frobenius image $P' = \Phi_{q^2}(P)$.

- the points of $\mathcal{X}$ form a partial ovoid of $\mathcal{U}_3$;
- every imaginary chord of $\mathcal{X}$ is a generator disjoint from $\mathcal{X}$.

Question Is there a hemisystem consisting of imaginary chords and generators which meet $\mathcal{X}$ (exactly one point)?
Some evidence that the answer might be yes

Basic idea to construct hemisystems from maximal curves

$\mathcal{X}$:=Maximal curve naturally embedded in $\mathcal{U}_3$;
$\mathfrak{g} := \mathfrak{g}(\mathcal{X})$:=genus of $\mathcal{X}$;
N_1:=number of points of $\mathcal{X}$ in $PG(3, q^2)$;
$N_1 = q^2 + 1 + 2\mathfrak{g}q$;
S_1:=number of generators meeting $\mathcal{X}$;
$S_1 = (q+1)(q^2 + 1 + 2\mathfrak{g}q)$;
N_2:=number of points of $\mathcal{X}$ in $PG(3, q^4)$;
$N_2 = q^4 + 1 - 2\mathfrak{g}q^2$;
S_2:=number of imaginary chords;
$S_2 = \frac{1}{2}(N_2 - N_1) = \frac{1}{2}(q^2+q)((q^2-q) - 2\mathfrak{g})$;
$S_2 + \frac{1}{2}S_1 = \frac{1}{2}(q+1)(q^3+1)$;
Taking half of the generators on each point of $\mathcal{X}$ plus all imaginary chords may produce a hemisystem

Sufficient conditions

Sufficient conditions

$\forall\ P \in \mathcal{U}_3 \setminus \mathcal{X};$

Sufficient conditions

$\forall\ P \in \mathcal{U}_3 \setminus \mathcal{X}$;
n_P:=number of generators on P meeting $\mathcal{X}$.

Sufficient conditions

$\forall\ P \in \mathcal{U}_3 \setminus \mathcal{X}$;
n_P:=number of generators on P meeting $\mathcal{X}$.
$\mathcal{M}$:=set of generators is a *half-hemisystem on* $\mathcal{X}$ if:

Sufficient conditions

$\forall\ P \in \mathcal{U}_3 \setminus \mathcal{X}$;
n_P:=number of generators on P meeting $\mathcal{X}$.
$\mathcal{M}$:=set of generators is a *half-hemisystem on* $\mathcal{X}$ if:

(A) On each $Q \in \mathcal{X}$ there are exactly $\frac{1}{2}(q+1)$ generators from $\mathcal{M}$.

Sufficient conditions

$\forall\ P \in \mathcal{U}_3 \setminus \mathcal{X}$;

n_P:=number of generators on P meeting $\mathcal{X}$.

$\mathcal{M}$:=set of generators is a *half-hemisystem on* $\mathcal{X}$ if:

(A) On each $Q \in \mathcal{X}$ there are exactly $\frac{1}{2}(q+1)$ generators from $\mathcal{M}$.

(B) For any point $P \in \mathcal{U}_3 \setminus \mathcal{X}$, $\mathcal{M}$ has as many as $\frac{1}{2}n_P$ generators on P meeting $\mathcal{X}$.

Sufficient conditions

$\forall\ P \in \mathcal{U}_3 \setminus \mathcal{X}$;
n_P:=number of generators on P meeting $\mathcal{X}$.
$\mathcal{M}$:=set of generators is a *half-hemisystem on* $\mathcal{X}$ if:

(A) On each $Q \in \mathcal{X}$ there are exactly $\frac{1}{2}(q+1)$ generators from $\mathcal{M}$.

(B) For any point $P \in \mathcal{U}_3 \setminus \mathcal{X}$, $\mathcal{M}$ has as many as $\frac{1}{2}n_P$ generators on P meeting $\mathcal{X}$.

$\mathcal{H}$:= set of all imaginary chords of $\mathcal{X}$;

Sufficient conditions

$\forall\ P \in \mathcal{U}_3 \setminus \mathcal{X}$;
n_P:=number of generators on P meeting $\mathcal{X}$.
$\mathcal{M}$:=set of generators is a *half-hemisystem on* $\mathcal{X}$ if:

(A) On each $Q \in \mathcal{X}$ there are exactly $\frac{1}{2}(q+1)$ generators from $\mathcal{M}$.

(B) For any point $P \in \mathcal{U}_3 \setminus \mathcal{X}$, $\mathcal{M}$ has as many as $\frac{1}{2}n_P$ generators on P meeting $\mathcal{X}$.

$\mathcal{H}$:= set of all imaginary chords of $\mathcal{X}$;
Theorem
$\mathcal{M} \cup \mathcal{H}$ is a hemisystem of $\mathcal{U}_3$.

Rational (maximal) curves

Rational (maximal) curves

$$\mathcal{U}_3 := X_1^{q+1} + X_2^{q+1} = X_0^q X_3 + X_0 X_3^q;$$

Rational (maximal) curves

$\mathcal{U}_3 := X_1^{q+1} + X_2^{q+1} = X_0^q X_3 + X_0 X_3^q$;
$\mathcal{X}$:=rational curve (i.e. $\mathfrak{g}(\mathcal{X}) = 0$);

Rational (maximal) curves

$\mathcal{U}_3 := X_1^{q+1} + X_2^{q+1} = X_0^q X_3 + X_0 X_3^q$;
$\mathcal{X}$:=rational curve (i.e. $\mathfrak{g}(\mathcal{X}) = 0$);
$\mathcal{X} := \{P(1, t, t^q, t^{q+1}) | t \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$

Rational (maximal) curves

$\mathcal{U}_3 := X_1^{q+1} + X_2^{q+1} = X_0^q X_3 + X_0 X_3^q$;
$\mathcal{X}$:=rational curve (i.e. $\mathfrak{g}(\mathcal{X}) = 0$);
$\mathcal{X} := \{P(1, t, t^q, t^{q+1}) | t \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$
$N_1 = q^2 + 1$;

Rational (maximal) curves

$\mathcal{U}_3 := X_1^{q+1} + X_2^{q+1} = X_0^q X_3 + X_0 X_3^q$;
$\mathcal{X}$:=rational curve (i.e. $\mathfrak{g}(\mathcal{X}) = 0$);
$\mathcal{X} := \{P(1, t, t^q, t^{q+1}) | t \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$
$N_1 = q^2 + 1$;
G:=subgroup of $PGU(4, q)$ s.t. $G \cong PSL(2, q^2)$ and $G : \mathcal{X} \mapsto \mathcal{X}$.

Rational (maximal) curves

$\mathcal{U}_3 := X_1^{q+1} + X_2^{q+1} = X_0^q X_3 + X_0 X_3^q$;
$\mathcal{X}$:=rational curve (i.e. $\mathfrak{g}(\mathcal{X}) = 0$);
$\mathcal{X} := \{P(1, t, t^q, t^{q+1}) | t \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$
$N_1 = q^2 + 1$;
G:=subgroup of $PGU(4, q)$ s.t. $G \cong PSL(2, q^2)$ and $G : \mathcal{X} \mapsto \mathcal{X}$.
Take a point $Q \in \mathcal{X}$;

Rational (maximal) curves

$\mathcal{U}_3 := X_1^{q+1} + X_2^{q+1} = X_0^q X_3 + X_0 X_3^q$;
$\mathcal{X}$:=rational curve (i.e. $\mathfrak{g}(\mathcal{X}) = 0$);
$\mathcal{X} := \{P(1, t, t^q, t^{q+1}) | t \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$
$N_1 = q^2 + 1$;
G:=subgroup of $PGU(4, q)$ s.t. $G \cong PSL(2, q^2)$ and $G : \mathcal{X} \mapsto \mathcal{X}$.
Take a point $Q \in \mathcal{X}$;
The stabilizer G_Q has two orbits on the set of all generators on Q;

Rational (maximal) curves

$\mathcal{U}_3 := X_1^{q+1} + X_2^{q+1} = X_0^q X_3 + X_0 X_3^q$;
$\mathcal{X}$:=rational curve (i.e. $\mathfrak{g}(\mathcal{X}) = 0$);
$\mathcal{X} := \{P(1, t, t^q, t^{q+1}) | t \in \mathbb{F}_{q^2}\} \cup \{(0,0,0,1\}$
$N_1 = q^2 + 1$;
G:=subgroup of $PGU(4, q)$ s.t. $G \cong PSL(2, q^2)$ and $G : \mathcal{X} \mapsto \mathcal{X}$.
Take a point $Q \in \mathcal{X}$;
The stabilizer G_Q has two orbits on the set of all generators on Q;
Take a generator ℓ meeting $\mathcal{X}$, and

Rational (maximal) curves

$\mathcal{U}_3 := X_1^{q+1} + X_2^{q+1} = X_0^q X_3 + X_0 X_3^q$;
$\mathcal{X}$:=rational curve (i.e. $\mathfrak{g}(\mathcal{X}) = 0$);
$\mathcal{X} := \{P(1, t, t^q, t^{q+1}) | t \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$
$N_1 = q^2 + 1$;
G:=subgroup of $PGU(4, q)$ s.t. $G \cong PSL(2, q^2)$ and $G : \mathcal{X} \mapsto \mathcal{X}$.
Take a point $Q \in \mathcal{X}$;
The stabilizer G_Q has two orbits on the set of all generators on Q;
Take a generator ℓ meeting $\mathcal{X}$, and the orbit Λ of ℓ (under the action of G)

Rational (maximal) curves

$\mathcal{U}_3 := X_1^{q+1} + X_2^{q+1} = X_0^q X_3 + X_0 X_3^q$;
$\mathcal{X}$:=rational curve (i.e. $\mathfrak{g}(\mathcal{X}) = 0$);
$\mathcal{X} := \{P(1, t, t^q, t^{q+1}) | t \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$
$N_1 = q^2 + 1$;
G:=subgroup of $PGU(4, q)$ s.t. $G \cong PSL(2, q^2)$ and $G : \mathcal{X} \mapsto \mathcal{X}$.
Take a point $Q \in \mathcal{X}$;
The stabilizer G_Q has two orbits on the set of all generators on Q;
Take a generator ℓ meeting $\mathcal{X}$, and the orbit Λ of ℓ (under the action of G)
Conditions (A) and (B) are satisfied.

Rational (maximal) curves

$\mathcal{U}_3 := X_1^{q+1} + X_2^{q+1} = X_0^q X_3 + X_0 X_3^q$;
$\mathcal{X}$:=rational curve (i.e. $\mathfrak{g}(\mathcal{X}) = 0$);
$\mathcal{X} := \{P(1, t, t^q, t^{q+1}) | t \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$
$N_1 = q^2 + 1$;
G:=subgroup of $PGU(4, q)$ s.t. $G \cong PSL(2, q^2)$ and $G : \mathcal{X} \mapsto \mathcal{X}$.
Take a point $Q \in \mathcal{X}$;
The stabilizer G_Q has two orbits on the set of all generators on Q;
Take a generator ℓ meeting $\mathcal{X}$, and the orbit Λ of ℓ (under the action of G)
Conditions (A) and (B) are satisfied.

Remark

The arising hemisystem is isomorphic to the Cossidente-Penttila hemisystem.

Hemisystems from the FT maximal curve, $q \equiv 1 \pmod 4$

$$\mathcal{U}_3 := X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0;$$

Hemisystems from the FT maximal curve, $q \equiv 1 \pmod 4$

$$\mathcal{U}_3 := X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0;$$
$$\mathcal{X}^+ := \{(1, u, v, v^2) | u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}.$$

Hemisystems from the FT maximal curve, $q \equiv 1 \pmod 4$

$\mathcal{U}_3 := X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0;$
$\mathcal{X}^+ := \{(1, u, v, v^2) | u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}.$
$\mathfrak{G}$:=subgroup of $PGU(4, q)$ preserving $\mathcal{X}$;

Hemisystems from the FT maximal curve, $q \equiv 1 \pmod 4$

$\mathcal{U}_3 := X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0;$
$\mathcal{X}^+ := \{(1, u, v, v^2) | u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0,0,0,1\}.$
$\mathfrak{G}$:=subgroup of $PGU(4, q)$ preserving $\mathcal{X}$;
$\mathfrak{G}/C_{(q+1)/2} \cong PGL(2, q)$ $Z(\mathfrak{G}) = C_{(q+1)/2}$;

Hemisystems from the FT maximal curve, $q \equiv 1 \pmod 4$

$\mathcal{U}_3 := X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0;$
$\mathcal{X}^+ := \{(1, u, v, v^2) | u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}.$
$\mathfrak{G}$:=subgroup of $PGU(4, q)$ preserving $\mathcal{X}$;
$\mathfrak{G}/C_{(q+1)/2} \cong PGL(2, q)$ $Z(\mathfrak{G}) = C_{(q+1)/2}$;
$\mathfrak{H}$:=subgroup of $\mathfrak{G}$ of index 2, $\mathfrak{H} \cong PSL(2, q) \times C_{(q+1)/2}$;

$\mathcal{U}_3 := X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0;$
$\mathcal{X}^+ := \{(1, u, v, v^2) | u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}.$
$\mathfrak{G}$:=subgroup of $PGU(4, q)$ preserving $\mathcal{X}$;
$\mathfrak{G}/C_{(q+1)/2} \cong PGL(2, q)$ $Z(\mathfrak{G}) = C_{(q+1)/2}$;
$\mathfrak{H}$:=subgroup of $\mathfrak{G}$ of index 2, $\mathfrak{H} \cong PSL(2, q) \times C_{(q+1)/2}$;
$\mathfrak{G}$ fixes X_∞ and preserves the plane Π of equation $X = 0$;

Hemisystems from the FT maximal curve, $q \equiv 1 \pmod 4$

$\mathcal{U}_3 := X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0;$
$\mathcal{X}^+ := \{(1, u, v, v^2) | u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}.$
$\mathfrak{G}$:=subgroup of $PGU(4, q)$ preserving $\mathcal{X}$;
$\mathfrak{G}/C_{(q+1)/2} \cong PGL(2, q)$ $Z(\mathfrak{G}) = C_{(q+1)/2}$;
$\mathfrak{H}$:=subgroup of $\mathfrak{G}$ of index 2, $\mathfrak{H} \cong PSL(2, q) \times C_{(q+1)/2}$;
$\mathfrak{G}$ fixes X_∞ and preserves the plane Π of equation $X = 0$;
$\mathcal{X} = \Delta \cup \Omega$ with $\Omega = \mathcal{X} \cap \Pi$;

$\mathcal{U}_3 := X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0$;
$\mathcal{X}^+ := \{(1, u, v, v^2) | u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$.
$\mathfrak{G}$:=subgroup of $PGU(4, q)$ preserving $\mathcal{X}$;
$\mathfrak{G}/C_{(q+1)/2} \cong PGL(2, q)$ $Z(\mathfrak{G}) = C_{(q+1)/2}$;
$\mathfrak{H}$:=subgroup of $\mathfrak{G}$ of index 2, $\mathfrak{H} \cong PSL(2, q) \times C_{(q+1)/2}$;
$\mathfrak{G}$ fixes X_∞ and preserves the plane Π of equation $X = 0$;
$\mathcal{X} = \Delta \cup \Omega$ with $\Omega = \mathcal{X} \cap \Pi$;
Take a point $P_1 \in \Delta$, together with a generator ℓ_1 on P_1;

Hemisystems from the FT maximal curve, $q \equiv 1 \pmod 4$

$\mathcal{U}_3 {:=} X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0$;
$\mathcal{X}^+ := \{(1,u,v,v^2) | u^{(q+1)/2} = v^q - v; u,v \in \mathbb{F}_{q^2}\} \cup \{(0,0,0,1\}$.
$\mathfrak{G}$:=subgroup of $PGU(4,q)$ preserving $\mathcal{X}$;
$\mathfrak{G}/C_{(q+1)/2} \cong PGL(2,q)$ $Z(\mathfrak{G}) = C_{(q+1)/2}$;
$\mathfrak{H}$:=subgroup of $\mathfrak{G}$ of index 2, $\mathfrak{H} \cong PSL(2,q) \times C_{(q+1)/2}$;
$\mathfrak{G}$ fixes X_∞ and preserves the plane Π of equation $X = 0$;
$\mathcal{X} = \Delta \cup \Omega$ with $\Omega = \mathcal{X} \cap \Pi$;
Take a point $P_1 \in \Delta$, together with a generator ℓ_1 on P_1;
Then the orbit $\mathcal{M}_1$ of ℓ_1 (under the action of $\mathfrak{H}$) has size $\frac{1}{2}(q+1)(q^3-q)$;

$\mathcal{U}_3 := X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0$;
$\mathcal{X}^+ := \{(1, u, v, v^2) | u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$.
$\mathfrak{G}$:=subgroup of $PGU(4, q)$ preserving $\mathcal{X}$;
$\mathfrak{G}/C_{(q+1)/2} \cong PGL(2, q)$ $Z(\mathfrak{G}) = C_{(q+1)/2}$;
$\mathfrak{H}$:=subgroup of $\mathfrak{G}$ of index 2, $\mathfrak{H} \cong PSL(2, q) \times C_{(q+1)/2}$;
$\mathfrak{G}$ fixes X_∞ and preserves the plane Π of equation $X = 0$;
$\mathcal{X} = \Delta \cup \Omega$ with $\Omega = \mathcal{X} \cap \Pi$;
Take a point $P_1 \in \Delta$, together with a generator ℓ_1 on P_1;
Then the orbit $\mathcal{M}_1$ of ℓ_1 (under the action of $\mathfrak{H}$) has size $\frac{1}{2}(q + 1)(q^3 - q)$;
Take a point $P_2 \in \Omega$, together with a generator ℓ_2 on P_2;

$\mathcal{U}_3 := X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0$;
$\mathcal{X}^+ := \{(1, u, v, v^2) | u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$.
$\mathfrak{G}$:=subgroup of $PGU(4, q)$ preserving $\mathcal{X}$;
$\mathfrak{G}/C_{(q+1)/2} \cong PGL(2, q)$ $Z(\mathfrak{G}) = C_{(q+1)/2}$;
$\mathfrak{H}$:=subgroup of $\mathfrak{G}$ of index 2, $\mathfrak{H} \cong PSL(2, q) \times C_{(q+1)/2}$;
$\mathfrak{G}$ fixes X_∞ and preserves the plane Π of equation $X = 0$;
$\mathcal{X} = \Delta \cup \Omega$ with $\Omega = \mathcal{X} \cap \Pi$;
Take a point $P_1 \in \Delta$, together with a generator ℓ_1 on P_1;
Then the orbit $\mathcal{M}_1$ of ℓ_1 (under the action of $\mathfrak{H}$) has size $\frac{1}{2}(q+1)(q^3 - q)$;
Take a point $P_2 \in \Omega$, together with a generator ℓ_2 on P_2;
Then the orbit $\mathcal{M}_2$ of ℓ_2 (under the action of $\mathfrak{H}$) has size $\frac{1}{2}(q+1)^2$.

$\mathcal{U}_3 := X_3^q X_0 + X_3 X_0^q + 2X_2^{q+1} - X_1^{q+1} = 0$;
$\mathcal{X}^+ := \{(1, u, v, v^2) | u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$.
$\mathfrak{G}$:=subgroup of $PGU(4, q)$ preserving $\mathcal{X}$;
$\mathfrak{G}/C_{(q+1)/2} \cong PGL(2, q)$ $Z(\mathfrak{G}) = C_{(q+1)/2}$;
$\mathfrak{H}$:=subgroup of $\mathfrak{G}$ of index 2, $\mathfrak{H} \cong PSL(2, q) \times C_{(q+1)/2}$;
$\mathfrak{G}$ fixes X_∞ and preserves the plane Π of equation $X = 0$;
$\mathcal{X} = \Delta \cup \Omega$ with $\Omega = \mathcal{X} \cap \Pi$;
Take a point $P_1 \in \Delta$, together with a generator ℓ_1 on P_1;
Then the orbit $\mathcal{M}_1$ of ℓ_1 (under the action of $\mathfrak{H}$) has size $\frac{1}{2}(q+1)(q^3 - q)$;
Take a point $P_2 \in \Omega$, together with a generator ℓ_2 on P_2;
Then the orbit $\mathcal{M}_2$ of ℓ_2 (under the action of $\mathfrak{H}$) has size $\frac{1}{2}(q+1)^2$.
Is $\mathcal{M}$ a half-semisystem?
If "yes" then $\mathcal{M} \cup \mathcal{H}$ is a hemisystem.

Discussion

Discussion

$\mathcal{M}$ a half-semisystem if

(A) Each $Q \in \mathcal{X}$ is incident with exactly $\frac{1}{2}(q+1)$ generators in $\mathcal{M}$

Discussion

$\mathcal{M}$ a half-semisystem if

(A) Each $Q \in \mathcal{X}$ is incident with exactly $\frac{1}{2}(q+1)$ generators in $\mathcal{M}$

(B) For any point $P \in \mathcal{U}_3 \setminus \mathcal{X}$, $\mathcal{M}$ has as many as $\frac{1}{2}n_P$ generators on P meeting $\mathcal{X}$.

Discussion

$\mathcal{M}$ a half-semisystem if

(A) Each $Q \in \mathcal{X}$ is incident with exactly $\frac{1}{2}(q+1)$ generators in $\mathcal{M}$

(B) For any point $P \in \mathcal{U}_3 \setminus \mathcal{X}$, $\mathcal{M}$ has as many as $\frac{1}{2}n_P$ generators on P meeting $\mathcal{X}$.

- By construction (A) is satisfied.

Discussion

$\mathcal{M}$ a half-semisystem if

(A) Each $Q \in \mathcal{X}$ is incident with exactly $\frac{1}{2}(q+1)$ generators in $\mathcal{M}$

(B) For any point $P \in \mathcal{U}_3 \setminus \mathcal{X}$, $\mathcal{M}$ has as many as $\frac{1}{2}n_P$ generators on P meeting $\mathcal{X}$.

- By construction (A) is satisfied.
- If $\mathfrak{G}_P$ is nontrivial, then (B) is satisfied.

Discussion

$\mathcal{M}$ a half-semisystem if

(A) Each $Q \in \mathcal{X}$ is incident with exactly $\frac{1}{2}(q+1)$ generators in $\mathcal{M}$

(B) For any point $P \in \mathcal{U}_3 \setminus \mathcal{X}$, $\mathcal{M}$ has as many as $\frac{1}{2}n_P$ generators on P meeting $\mathcal{X}$.

- By construction (A) is satisfied.
- If $\mathfrak{G}_P$ is nontrivial, then (B) is satisfied.
- If $\mathfrak{G}_P$ is trivial, then (B) does not hold in general.

Discussion

$\mathcal{M}$ a half-semisystem if

(A) Each $Q \in \mathcal{X}$ is incident with exactly $\frac{1}{2}(q+1)$ generators in $\mathcal{M}$

(B) For any point $P \in \mathcal{U}_3 \setminus \mathcal{X}$, $\mathcal{M}$ has as many as $\frac{1}{2}n_P$ generators on P meeting $\mathcal{X}$.

- By construction (A) is satisfied.
- If $\mathfrak{G}_P$ is nontrivial, then (B) is satisfied.
- If $\mathfrak{G}_P$ is trivial, then (B) does not hold in general.

Assumption Either $q = p^h$ with $p \equiv 1 \pmod 8$, or q square.

Discussion

$\mathcal{M}$ a half-semisystem if

(A) Each $Q \in \mathcal{X}$ is incident with exactly $\frac{1}{2}(q+1)$ generators in $\mathcal{M}$

(B) For any point $P \in \mathcal{U}_3 \setminus \mathcal{X}$, $\mathcal{M}$ has as many as $\frac{1}{2}n_P$ generators on P meeting $\mathcal{X}$.

- By construction (A) is satisfied.
- If $\mathfrak{G}_P$ is nontrivial, then (B) is satisfied.
- If $\mathfrak{G}_P$ is trivial, then (B) does not hold in general.

Assumption Either $q = p^h$ with $p \equiv 1 \pmod 8$, or q square.
Theorem. Condition (B) is satisfied for $\forall P \in \mathcal{U}_3 \setminus \mathcal{X}$ if and only if the following Condition (U) is satisfies:

Discussion

$\mathcal{M}$ a half-semisystem if

(A) Each $Q \in \mathcal{X}$ is incident with exactly $\frac{1}{2}(q+1)$ generators in $\mathcal{M}$

(B) For any point $P \in \mathcal{U}_3 \setminus \mathcal{X}$, $\mathcal{M}$ has as many as $\frac{1}{2}n_P$ generators on P meeting $\mathcal{X}$.

- By construction (A) is satisfied.
- If $\mathfrak{G}_P$ is nontrivial, then (B) is satisfied.
- If $\mathfrak{G}_P$ is trivial, then (B) does not hold in general.

Assumption Either $q = p^h$ with $p \equiv 1 \pmod 8$, or q square.

Theorem. Condition (B) is satisfied for $\forall P \in \mathcal{U}_3 \setminus \mathcal{X}$ if and only if the following Condition (U) is satisfies:

(U) the elliptic curve $\mathcal{E}_3$ of equation $Y^2 = X^3 - X$ has exactly $q - 1$ point over $\mathbb{F}_q$.

Discussion

$\mathcal{M}$ a half-semisystem if

(A) Each $Q \in \mathcal{X}$ is incident with exactly $\frac{1}{2}(q+1)$ generators in $\mathcal{M}$

(B) For any point $P \in \mathcal{U}_3 \setminus \mathcal{X}$, $\mathcal{M}$ has as many as $\frac{1}{2}n_P$ generators on P meeting $\mathcal{X}$.

- By construction (A) is satisfied.
- If $\mathfrak{G}_P$ is nontrivial, then (B) is satisfied.
- If $\mathfrak{G}_P$ is trivial, then (B) does not hold in general.

Assumption Either $q = p^h$ with $p \equiv 1 \pmod 8$, or q square.
Theorem. Condition (B) is satisfied for $\forall P \in \mathcal{U}_3 \setminus \mathcal{X}$ if and only if the following Condition (U) is satisfies:

(U) the elliptic curve $\mathcal{E}_3$ of equation $Y^2 = X^3 - X$ has exactly $q-1$ point over $\mathbb{F}_q$.

Remark Some more computation should prove that Theorem holds true for $p \equiv 1 \pmod 4$.

Existence of hemisystems

Existence of hemisystems

Let $q = p$ with $p \equiv 1 \pmod 4$.

Existence of hemisystems

Let $q = p$ with $p \equiv 1 \pmod 4$. From earlier results on elliptic curves (Serre)

Let $q = p$ with $p \equiv 1 \pmod 4$. From earlier results on elliptic curves (Serre)
(U) is satisfied $\Leftrightarrow$ $p = 1 + n^2$ with $n \in \mathbb{Z}$.

Existence of hemisystems

Let $q = p$ with $p \equiv 1 \pmod 4$. From earlier results on elliptic curves (Serre)
(U) is satisfied $\Leftrightarrow p = 1 + n^2$ with $n \in \mathbb{Z}$.
$\Rightarrow$ Let $p \equiv 1 \pmod 8$. Then we obtain a hemisystem if and only if $p = 1 + 16n^2$.

Existence of hemisystems

Let $q = p$ with $p \equiv 1 \pmod 4$. From earlier results on elliptic curves (Serre)
(U) is satisfied $\Leftrightarrow p = 1 + n^2$ with $n \in \mathbb{Z}$.
$\Rightarrow$ Let $p \equiv 1 \pmod 8$. Then we obtain a hemisystem if and only if $p = 1 + 16n^2$.
Remark This should remain true for $p = 1 + n^2$

Existence of hemisystems

Let $q = p$ with $p \equiv 1 \pmod 4$. From earlier results on elliptic curves (Serre)
(U) is satisfied $\Leftrightarrow$ $p = 1 + n^2$ with $n \in \mathbb{Z}$.
$\Rightarrow$ Let $p \equiv 1 \pmod 8$. Then we obtain a hemisystem if and only if $p = 1 + 16n^2$.
Remark This should remain true for $p = 1 + n^2$
Landau's Conjecture

Existence of hemisystems

Let $q = p$ with $p \equiv 1 \pmod 4$. From earlier results on elliptic curves (Serre)
(U) is satisfied $\Leftrightarrow p = 1 + n^2$ with $n \in \mathbb{Z}$.
$\Rightarrow$ Let $p \equiv 1 \pmod 8$. Then we obtain a hemisystem if and only if $p = 1 + 16n^2$.
Remark This should remain true for $p = 1 + n^2$
Landau's Conjecture
$\exists$ infinite sequence of primes $p = 1 + n^2$.

More hemisystems for $q \equiv 1 \pmod 4$

More hemisystems for $q \equiv 1 \pmod 4$

Some more examples arise with a slight modification of the above procedure;

More hemisystems for $q \equiv 1 \pmod 4$

Some more examples arise with a slight modification of the above procedure;

The idea is to use the Fuhrmann-Torres curve $\mathcal{X}$ together with its twin curve;

$\mathcal{X}^+ := \{(1, u, v, v^2) | -u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$.

Some more examples arise with a slight modification of the above procedure;
The idea is to use the Fuhrmann-Torres curve $\mathcal{X}$ together with its twin curve;
$\mathcal{X}^+ := \{(1, u, v, v^2) | -u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}.$
The modified construction:

More hemisystems for $q \equiv 1 \pmod 4$

Some more examples arise with a slight modification of the above procedure;

The idea is to use the Fuhrmann-Torres curve $\mathcal{X}$ together with its twin curve;

$\mathcal{X}^+ := \{(1, u, v, v^2) | -u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0,0,0,1\}$.

The modified construction:

On each point of $\mathcal{X}$ take one half of the generators (using again the group $G \cong PSL(2,q) \times C_{(q+1)/2}$;

More hemisystems for $q \equiv 1 \pmod 4$

Some more examples arise with a slight modification of the above procedure;
The idea is to use the Fuhrmann-Torres curve $\mathcal{X}$ together with its twin curve;
$\mathcal{X}^+ := \{(1, u, v, v^2) | -u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$.
The modified construction:
On each point of $\mathcal{X}$ take one half of the generators (using again the group $G \cong PSL(2, q) \times C_{(q+1)/2}$;
Take a G-orbit Σ of imaginary chords of $\mathcal{X}$;

More hemisystems for $q \equiv 1 \pmod 4$

Some more examples arise with a slight modification of the above procedure;

The idea is to use the Fuhrmann-Torres curve $\mathcal{X}$ together with its twin curve;

$\mathcal{X}^+ := \{(1, u, v, v^2) | -u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0,0,0,1\}.$

The modified construction:

On each point of $\mathcal{X}$ take one half of the generators (using again the group $G \cong PSL(2, q) \times C_{(q+1)/2}$;

Take a G-orbit Σ of imaginary chords of $\mathcal{X}$;

Take a G-orbit Δ of imaginary chords of $\mathcal{Y}$;

More hemisystems for $q \equiv 1 \pmod 4$

Some more examples arise with a slight modification of the above procedure;
The idea is to use the Fuhrmann-Torres curve $\mathcal{X}$ together with its twin curve;
$\mathcal{X}^+ := \{(1, u, v, v^2) | -u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$.
The modified construction:
On each point of $\mathcal{X}$ take one half of the generators (using again the group $G \cong PSL(2, q) \times C_{(q+1)/2}$;
Take a G-orbit Σ of imaginary chords of $\mathcal{X}$;
Take a G-orbit Δ of imaginary chords of $\mathcal{Y}$;
The generators chosen in this way may form a hemisystem.

More hemisystems for $q \equiv 1 \pmod 4$

Some more examples arise with a slight modification of the above procedure;

The idea is to use the Fuhrmann-Torres curve $\mathcal{X}$ together with its twin curve;

$\mathcal{X}^+ := \{(1, u, v, v^2) | -u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$.

The modified construction:

On each point of $\mathcal{X}$ take one half of the generators (using again the group $G \cong PSL(2, q) \times C_{(q+1)/2}$;

Take a G-orbit Σ of imaginary chords of $\mathcal{X}$;

Take a G-orbit Δ of imaginary chords of $\mathcal{Y}$;

The generators chosen in this way may form a hemisystem.

For instance, this occurs for $q = 5, 13, 17, 25, 37, 41, 101$ (computer aided research);

More hemisystems for $q \equiv 1 \pmod 4$

Some more examples arise with a slight modification of the above procedure;

The idea is to use the Fuhrmann-Torres curve $\mathcal{X}$ together with its twin curve;

$\mathcal{X}^+ := \{(1, u, v, v^2) | -u^{(q+1)/2} = v^q - v; u, v \in \mathbb{F}_{q^2}\} \cup \{(0, 0, 0, 1\}$.

The modified construction:

On each point of $\mathcal{X}$ take one half of the generators (using again the group $G \cong PSL(2, q) \times C_{(q+1)/2}$;

Take a G-orbit Σ of imaginary chords of $\mathcal{X}$;

Take a G-orbit Δ of imaginary chords of $\mathcal{Y}$;

The generators chosen in this way may form a hemisystem.

For instance, this occurs for $q = 5, 13, 17, 25, 37, 41, 101$ (computer aided research);

Are these hemisystems members of an infinite family?