Intersection of irreducible curves and the Hermitian curve

Peter Beelen, Mrinmoy Datta, Maria Montanucci and *Jonathan Niemann*

Technical University of Denmark (DTU)

DTU Compute
Department of Applied Mathematics and Computer Science

Introduction and motivation

Motivation: Understanding the intersection of projective algebraic varieties is relevant, e.g., in coding theory.

Introduction and motivation

Motivation: Understanding the intersection of projective algebraic varieties is relevant, e.g., in coding theory.

Theorem (Bézout)

Let $\mathcal{X}$ and $\mathcal{Y}$ be plane projective curves of degree d_1 and d_2 respectively, and suppose that they do not share a common component. Then,

$$|\mathcal{X} \cap \mathcal{Y}| \leq d_1 \cdot d_2.$$

Introduction and motivation

Motivation: Understanding the intersection of projective algebraic varieties is relevant, e.g., in coding theory.

Theorem (Bézout)

Let $\mathcal{X}$ and $\mathcal{Y}$ be plane projective curves of degree d_1 and d_2 respectively, and suppose that they do not share a common component. Then,

$$|\mathcal{X} \cap \mathcal{Y}| \leq d_1 \cdot d_2.$$

Question

Let $\mathcal{H}_q \subseteq \mathbb{P}^2$ denote the Hermitian curve and let $\mathcal{C}_d \subseteq \mathbb{P}^2$ be another irreducible curve of degree d, both defined over $\mathbb{F}_{q^2}$.

Is it possible that $\mathcal{H}_q$ and $\mathcal{C}_d$ intersect in $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points?

A bit of context - higher dimensional Hermitian varieties

For higher dimensional Hermitian varieties, it seems the number of rational intersection points is largest for highly reducible hypersurfaces:

A bit of context - higher dimensional Hermitian varieties

For higher dimensional Hermitian varieties, it seems the number of rational intersection points is largest for highly reducible hypersurfaces:

Conjecture (Sørensen, 1991)

For $d \leq q$, we have

$$|(S \cap \mathcal{H}_q^{(2)})(\mathbb{F}_{q^2})| \leq d(q^3 + q^2 - q) + q + 1,$$

and equality holds if and only if S is the union of d planes.

- $\mathcal{H}_q^{(2)}$: A nondegenerate Hermitian surface in $\mathbb{P}^3$ defined over $\mathbb{F}_{q^2}$.
- S : A surface of degree d in $\mathbb{P}^3$, also defined over $\mathbb{F}_{q^2}$.

A bit of context - higher dimensional Hermitian varieties

For higher dimensional Hermitian varieties, it seems the number of rational intersection points is largest for highly reducible hypersurfaces:

Conjecture (Sørensen, 1991)

For $d \leq q$, we have

$$|(S \cap \mathcal{H}_q^{(2)})(\mathbb{F}_{q^2})| \leq d(q^3 + q^2 - q) + q + 1,$$

and equality holds if and only if S is the union of d planes.

- $\mathcal{H}_q^{(2)}$: A nondegenerate Hermitian surface in $\mathbb{P}^3$ defined over $\mathbb{F}_{q^2}$.
- S : A surface of degree d in $\mathbb{P}^3$, also defined over $\mathbb{F}_{q^2}$.

Theorem (Beelen, Datta and Homma, 2021)

Sørensen's conjecture holds.

A bit of context - higher dimensional Hermitian varieties

For higher dimensional Hermitian varieties, it seems the number of rational intersection points is largest for highly reducible hypersurfaces:

Conjecture (Edoukou, 2009)

For $d \leq q$, we have

$$|(S \cap \mathcal{H}_q^{(3)})(\mathbb{F}_{q^2})| \leq d(q^5 + q^2) + q^3 + 1,$$

and equality holds if and only if S is the union of d hyperplanes.

- $\mathcal{H}_q^{(3)}$: A nondegenerate Hermitian threefold in $\mathbb{P}^4$ defined over $\mathbb{F}_{q^2}$.
- S : A hypersurface of degree d in $\mathbb{P}^4$, also defined over $\mathbb{F}_{q^2}$.

A bit of context - higher dimensional Hermitian varieties

For higher dimensional Hermitian varieties, it seems the number of rational intersection points is largest for highly reducible hypersurfaces:

Conjecture (Edoukou, 2009)

For $d \leq q$, we have

$$|(S \cap \mathcal{H}_q^{(3)})(\mathbb{F}_{q^2})| \leq d(q^5 + q^2) + q^3 + 1,$$

and equality holds if and only if S is the union of d hyperplanes.

- $\mathcal{H}_q^{(3)}$: A nondegenerate Hermitian threefold in $\mathbb{P}^4$ defined over $\mathbb{F}_{q^2}$.
- S : A hypersurface of degree d in $\mathbb{P}^4$, also defined over $\mathbb{F}_{q^2}$.

Theorem (Edoukou, 2009 & Datta and Manna, 2024)

The conjecture holds for $d = 2$, and for $d = 3$, $q \geq 7$.

The main question

Question

Can $\mathcal{H}_q$ and $\mathcal{C}_d$ intersect in exactly $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points?

- $\mathcal{H}_q$: The Hermitian curve in $\mathbb{P}^2$ defined over $\mathbb{F}_{q^2}$.
- $\mathcal{C}_d$: An irreducible plane projective curve of degree d in $\mathbb{P}^2$, also defined over $\mathbb{F}_{q^2}$.

Known results

Question

Can $\mathcal{H}_q$ and $\mathcal{C}_d$ intersect in exactly $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points?

The answer is $\boxed{\text{YES}}$ for

- $d = 1$: Any $\mathbb{F}_{q^2}$-secant of $\mathcal{H}_q$ will do.

Known results

Question

Can $\mathcal{H}_q$ and $\mathcal{C}_d$ intersect in exactly $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points?

The answer is $\boxed{\text{YES}}$ for

- $d = 1$: Any $\mathbb{F}_{q^2}$-secant of $\mathcal{H}_q$ will do.
- $d = q + 1$ and $q \geq 3$: Two distinct Hermitian curves *(Donati and Durante, 2003)*.

Known results

Question

Can $\mathcal{H}_q$ and $\mathcal{C}_d$ intersect in exactly $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points?

The answer is $\boxed{\text{YES}}$ for

- $d = 1$: Any $\mathbb{F}_{q^2}$-secant of $\mathcal{H}_q$ will do.
- $d = q + 1$ and $q \geq 3$: Two distinct Hermitian curves *(Donati and Durante, 2003)*.
- $d = 2$ and $q \geq 4$: Intersection is known *(Donati, Durante and Korchmáros, 2009)*.

Known results

Question

Can $\mathcal{H}_q$ and $\mathcal{C}_d$ intersect in exactly $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points?

The answer is $\boxed{\text{YES}}$ for

- $d = 1$: Any $\mathbb{F}_{q^2}$-secant of $\mathcal{H}_q$ will do.
- $d = q+1$ and $q \geq 3$: Two distinct Hermitian curves *(Donati and Durante, 2003)*.
- $d = 2$ and $q \geq 4$: Intersection is known *(Donati, Durante and Korchmáros, 2009)*.

The answer is $\boxed{\text{NO}}$ for

- $(q, d) \in \{(2,2), (3,2), (2,3)\}$, by an exhaustive computer search.

Our contribution

Question

Can $\mathcal{H}_q$ and $\mathcal{C}_d$ intersect in exactly $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points?

The answer is also $\boxed{\text{YES}}$ for

- $q \leq d \leq q^2 - q + 1$, for $q \geq 3$.

Our contribution

Question

Can $\mathcal{H}_q$ and $\mathcal{C}_d$ intersect in exactly $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points?

The answer is also $\boxed{\text{YES}}$ for

- $q \leq d \leq q^2 - q + 1$, for $q \geq 3$.
- $d = \lfloor (q+1)/2 \rfloor$.

Our contribution

Question

Can $\mathcal{H}_q$ and $\mathcal{C}_d$ intersect in exactly $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points?

The answer is also $\boxed{\text{YES}}$ for

- $q \leq d \leq q^2 - q + 1$, for $q \geq 3$.
- $d = \lfloor (q+1)/2 \rfloor$.
- $d = 3$ and $q \geq 3$.

Our contribution

Question

Can $\mathcal{H}_q$ and $\mathcal{C}_d$ intersect in exactly $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points?

The answer is also $\boxed{\text{YES}}$ for

- $q \leq d \leq q^2 - q + 1$, for $q \geq 3$.
- $d = \lfloor (q+1)/2 \rfloor$.
- $d = 3$ and $q \geq 3$.

Remark (Partial results)

We show that the answer is also often yes for $d = 4, 5, 6$ and generally for d small compared to q.

Results for large d

The answer is $\boxed{\text{NO}}$ for $d > q^2 - q + 1$, since

$$|\mathcal{H}_q(\mathbb{F}_{q^2})| = q^3 + 1 = (q+1)(q^2 - q + 1).$$

Results for large d

The answer is $\boxed{\text{NO}}$ for $d > q^2 - q + 1$, since

$$|\mathcal{H}_q(\mathbb{F}_{q^2})| = q^3 + 1 = (q+1)(q^2 - q + 1).$$

Theorem (Beelen, Datta, Montanucci, N.)

If $q + 1 \leq d \leq q^2 - q$, then there exists an absolutely irreducible curve $\mathcal{C}_d$ of degree d intersecting $\mathcal{H}_q$ in exactly $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points.

Results for large d

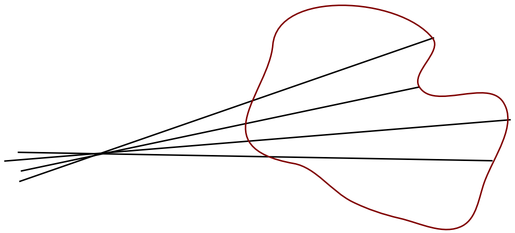
The answer is $\boxed{\text{NO}}$ for $d > q^2 - q + 1$, since

$$|\mathcal{H}_q(\mathbb{F}_{q^2})| = q^3 + 1 = (q+1)(q^2 - q + 1).$$

Theorem (Beelen, Datta, Montanucci, N.)

If $q + 1 \leq d \leq q^2 - q$, then there exists an absolutely irreducible curve $\mathcal{C}_d$ of degree d intersecting $\mathcal{H}_q$ in exactly $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points.

Proof idea:



Results for large d

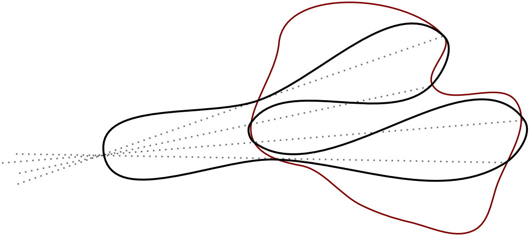
The answer is $\boxed{\text{NO}}$ for $d > q^2 - q + 1$, since

$$|\mathcal{H}_q(\mathbb{F}_{q^2})| = q^3 + 1 = (q+1)(q^2 - q + 1).$$

Theorem (Beelen, Datta, Montanucci, N.)

If $q + 1 \leq d \leq q^2 - q$, then there exists an absolutely irreducible curve $\mathcal{C}_d$ of degree d intersecting $\mathcal{H}_q$ in exactly $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points.

Proof idea:



Results for large d

The answer is $\boxed{\text{NO}}$ for $d > q^2 - q + 1$, since

$$|\mathcal{H}_q(\mathbb{F}_{q^2})| = q^3 + 1 = (q+1)(q^2 - q + 1).$$

Theorem (Beelen, Datta, Montanucci, N.)

If $q + 1 \leq d \leq q^2 - q$, then there exists an absolutely irreducible curve $\mathcal{C}_d$ of degree d intersecting $\mathcal{H}_q$ in exactly $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points.

Proof idea:

- Let $\mathcal{H}_q$ be given by $Y^q Z + Y Z^q = X^{q+1}$.

Results for large d

The answer is $\boxed{\text{NO}}$ for $d > q^2 - q + 1$, since

$$|\mathcal{H}_q(\mathbb{F}_{q^2})| = q^3 + 1 = (q+1)(q^2 - q + 1).$$

Theorem (Beelen, Datta, Montanucci, N.)

If $q + 1 \leq d \leq q^2 - q$, then there exists an absolutely irreducible curve $\mathcal{C}_d$ of degree d intersecting $\mathcal{H}_q$ in exactly $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points.

Proof idea:

- Let $\mathcal{H}_q$ be given by $Y^q Z + Y Z^q = X^{q+1}$.
- Choose $b_1, \ldots, b_d$ to be distinct elements from the set

$$S := \{b \in \mathbb{F}_{q^2} \mid b^q + b \neq 0\}.$$

Results for large d

The answer is $\boxed{\text{NO}}$ for $d > q^2 - q + 1$, since

$$|\mathcal{H}_q(\mathbb{F}_{q^2})| = q^3 + 1 = (q+1)(q^2 - q + 1).$$

Theorem (Beelen, Datta, Montanucci, N.)

If $q + 1 \leq d \leq q^2 - q$, then there exists an absolutely irreducible curve $\mathcal{C}_d$ of degree d intersecting $\mathcal{H}_q$ in exactly $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points.

Proof idea:

- Let $\mathcal{H}_q$ be given by $Y^qZ + YZ^q = X^{q+1}$.
- Choose $b_1, \ldots, b_d$ to be distinct elements from the set

$$S := \{b \in \mathbb{F}_{q^2} \mid b^q + b \neq 0\}.$$

- For $\alpha \in \mathbb{F}_{q^2} \setminus \{0\}$ consider the curve given by the equation

$$(X^{q+1} - Y^qZ - YZ^q)Z^{d-q-1} = \alpha \prod_{i=1}^{d}(Y - b_iZ).$$

Results for small d

Consider

$$\mathcal{H}_q : \; X^{q+1} + Y^{q+1} + Z^{q+1} = 0 \quad \text{and} \quad \mathcal{C}_d^{(\alpha)} : \; XZ^{d-1} = \alpha Y^d,$$

for $\alpha \in \mathbb{F}_{q^2} \setminus \{0\}$.

Results for small d

Consider

$$\mathcal{H}_q : \; X^{q+1} + Y^{q+1} + Z^{q+1} = 0 \quad \text{and} \quad \mathcal{C}_d^{(\alpha)} : \; XZ^{d-1} = \alpha Y^d,$$

for $\alpha \in \mathbb{F}_{q^2} \setminus \{0\}$.

- There are no intersection points at infinity ($Z = 0$).

Results for small d

Consider

$$\mathcal{H}_q : \ X^{q+1} + Y^{q+1} + Z^{q+1} = 0 \quad \text{and} \quad \mathcal{C}_d^{(\alpha)} : \ XZ^{d-1} = \alpha Y^d,$$

for $\alpha \in \mathbb{F}_{q^2} \setminus \{0\}$.

- There are no intersection points at infinity ($Z = 0$).
- There are $d(q+1)$ rational intersection points if and only if

  $$\alpha^{q+1} Y^{d(q+1)} + Y^{q+1} + 1 \in \mathbb{F}_{q^2}[Y]$$

  has $d(q+1)$ distinct roots in $\mathbb{F}_{q^2}$.

Results for small d

Consider

$$\mathcal{H}_q : \; X^{q+1} + Y^{q+1} + Z^{q+1} = 0 \quad \text{and} \quad \mathcal{C}_d^{(\alpha)} : \; XZ^{d-1} = \alpha Y^d,$$

for $\alpha \in \mathbb{F}_{q^2} \setminus \{0\}$.

- There are no intersection points at infinity ($Z = 0$).
- There are $d(q+1)$ rational intersection points if and only if

$$\alpha^{q+1} Y^{d(q+1)} + Y^{q+1} + 1 \in \mathbb{F}_{q^2}[Y]$$

  has $d(q+1)$ distinct roots in $\mathbb{F}_{q^2}$.

Lemma

For $\alpha \in \mathbb{F}_{q^2} \setminus \{0\}$, let $A := \alpha^{q+1} \in \mathbb{F}_q \setminus \{0\}$. Then,

$$\left|(\mathcal{H}_q \cap \mathcal{C}_d^{(\alpha)})(\mathbb{F}_{q^2})\right| = d(q+1) \;\Leftrightarrow\; At^d + t + 1 \in \mathbb{F}_q[t] \text{ splits over } \mathbb{F}_q.$$

Galois theory

Goal: Find $A \in \mathbb{F}_q \setminus \{0\}$ such that $At^d + t + 1 \in \mathbb{F}_q[t]$ splits over $\mathbb{F}_q$.

Galois theory

Goal: Find $A \in \mathbb{F}_q \setminus \{0\}$ such that $At^d + t + 1 \in \mathbb{F}_q[t]$ splits over $\mathbb{F}_q$.

Strategy: Consider A as a transcendental element and study the extension

$$\begin{array}{c} \mathbb{F}_q(A,T) \\ | \\ \mathbb{F}_q(A) \end{array} \qquad (\textit{with } AT^d + T + 1 = 0)$$

Galois theory

Goal: Find $A \in \mathbb{F}_q \setminus \{0\}$ such that $At^d + t + 1 \in \mathbb{F}_q[t]$ splits over $\mathbb{F}_q$.

Strategy: Consider A as a transcendental element and study the extension

$$\begin{array}{lcl}
F_d & & (\textit{the splitting field of } At^d + t + 1 \in \mathbb{F}_q(A)[t]) \\
\quad | & & \\
\mathbb{F}_q(A,T) & & (\textit{with } AT^d + T + 1 = 0) \\
\quad | & & \\
\mathbb{F}_q(A) & &
\end{array}$$

Adding one root

We have $A = -(1+T)/T^d$.

$$\begin{tikzcd}[arrows=dash]
\mathbb{F}_q(A,T) = \mathbb{F}_q(T) \arrow[d] & Q_0 \arrow[d, "d"] & Q_\infty \arrow[dr, "d-1"'] & & Q_{-1} \arrow[dl, "1"] \\
\mathbb{F}_q(A) & P_\infty & & P_0 &
\end{tikzcd}$$

Adding one root

We have $A = -(1+T)/T^d$.

$$
\begin{tikzcd}
\mathbb{F}_q(A,T) = \mathbb{F}_q(T) \arrow[d, dash] & Q_0 \arrow[d, dash, "d"] & Q_\infty \arrow[dr, dash, "d-1"'] & & Q_{-1} \arrow[dl, dash, "1"] & Q_{\alpha'} \arrow[d, dash, "2"] \\
\mathbb{F}_q(A) & P_\infty & & P_0 & & P_\alpha
\end{tikzcd}
$$

$$\gcd(q, d(d-1)) = 1$$

Adding two roots

Proposition

Let T_1 and T_2 be two distinct roots of the polynomial $At^d + t + 1$ in an algebraic closure of the function field $\mathbb{F}_q(A)$. Then $\mathbb{F}_q(A, T_1, T_2) = \mathbb{F}_q(\rho)$, where $\rho = T_2/T_1$. Moreover,

$$T_1 = -\frac{\rho^{d-1} + \cdots + \rho + 1}{\rho^{d-1} + \cdots + \rho} = -\frac{\rho^d - 1}{\rho^d - \rho},$$

$$T_2 = T_1 \cdot \rho = -\frac{\rho^{d-1} + \cdots + \rho + 1}{\rho^{d-2} + \cdots + 1} = -\frac{\rho^d - 1}{\rho^{d-1} - 1},$$

and

$$A = -\frac{T_1 + 1}{T_1^d} = (-1)^d \frac{(\rho - 1)(\rho^d - \rho)^{d-1}}{(\rho^d - 1)^d} = (-1)^d \frac{\rho^{d-1}(\rho^{d-2} + \cdots + \rho + 1)^{d-1}}{(\rho^{d-1} + \cdots + \rho + 1)^d}.$$

In particular, $\mathbb{F}_q$ is the full constant field of $\mathbb{F}_q(\rho)$ and $[\mathbb{F}_q(\rho) : \mathbb{F}_q(A)] = d(d-1)$.

Adding two roots - $d = 3$

Corollary

The splitting field F_3 of the polynomial $At^3 + t + 1 \in \mathbb{F}_q(A)[t]$ is the rational function field $\mathbb{F}_q(\rho)$. In particular, the Galois group of $At^3 + t + 1$ is isomorphic to the symmetric group S_3.

Adding two roots - $d = 3$

Corollary

The splitting field F_3 of the polynomial $At^3 + t + 1 \in \mathbb{F}_q(A)[t]$ is the rational function field $\mathbb{F}_q(\rho)$. In particular, the Galois group of $At^3 + t + 1$ is isomorphic to the symmetric group S_3.

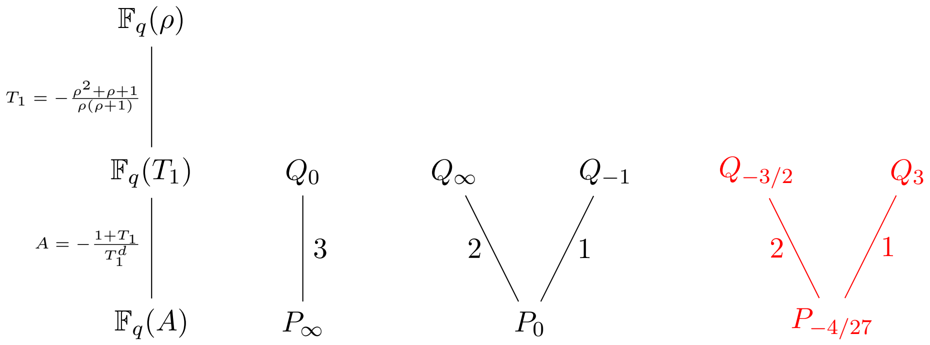
$$\begin{tikzcd} \mathbb{F}_q(T_1) \arrow[d, dash, "A = -\frac{1+T_1}{T_1^d}"'] \\ \mathbb{F}_q(A) \end{tikzcd} \qquad \begin{tikzcd} Q_0 \arrow[d, dash, "3"] \\ P_\infty \end{tikzcd} \qquad \begin{tikzcd} Q_\infty \arrow[dr, dash, "2"'] & & Q_{-1} \arrow[dl, dash, "1"] \\ & P_0 & \end{tikzcd} \qquad \begin{tikzcd} Q_{-3/2} \arrow[dr, dash, "2"'] & & Q_3 \arrow[dl, dash, "1"] \\ & P_{-4/27} & \end{tikzcd}$$

$$\gcd(q, d(d-1)) = 1$$

Adding two roots - $d = 3$

Corollary

The splitting field F_3 of the polynomial $At^3 + t + 1 \in \mathbb{F}_q(A)[t]$ is the rational function field $\mathbb{F}_q(\rho)$. In particular, the Galois group of $At^3 + t + 1$ is isomorphic to the symmetric group S_3.

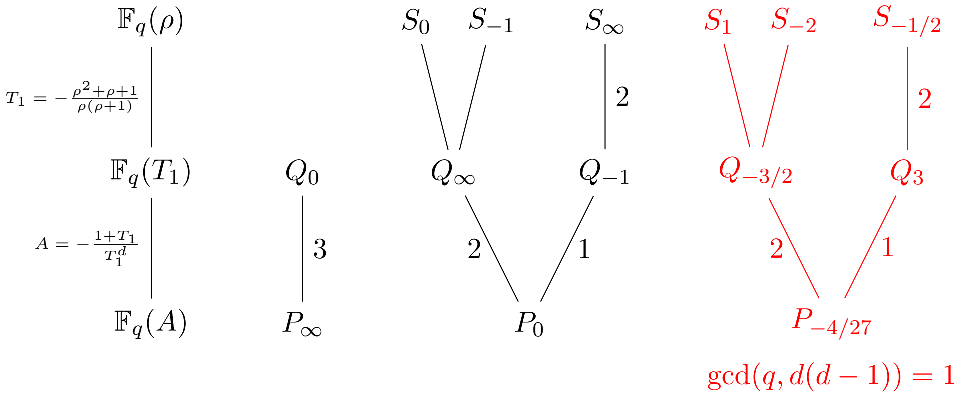


$\gcd(q, d(d-1)) = 1$

Adding two roots - $d = 3$

Corollary

The splitting field F_3 of the polynomial $At^3 + t + 1 \in \mathbb{F}_q(A)[t]$ is the rational function field $\mathbb{F}_q(\rho)$. In particular, the Galois group of $At^3 + t + 1$ is isomorphic to the symmetric group S_3.



Adding two roots - $d = 3$

Corollary

The splitting field F_3 of the polynomial $At^3 + t + 1 \in \mathbb{F}_q(A)[t]$ is the rational function field $\mathbb{F}_q(\rho)$. In particular, the Galois group of $At^3 + t + 1$ is isomorphic to the symmetric group S_3.

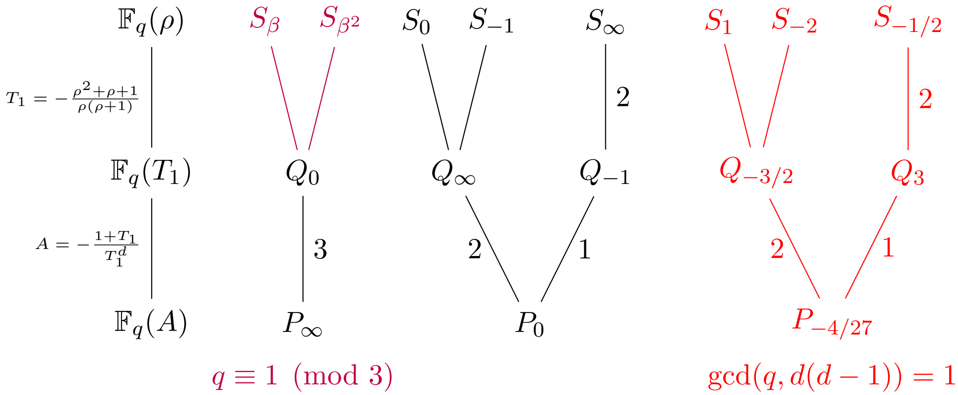
$$
\begin{tikzcd}
\mathbb{F}_q(\rho) \arrow[d, dash, "T_1 = -\frac{\rho^2+\rho+1}{\rho(\rho+1)}"'] & S_1 \arrow[d, dash, "2"] & S_0 \arrow[dr, dash] & & S_{-1} \arrow[dl, dash] & & S_\infty \arrow[d, dash, "2"] \\
\mathbb{F}_q(T_1) \arrow[d, dash, "A = -\frac{1+T_1}{T_1^d}"'] & Q_0 \arrow[d, dash, "3"] & & Q_\infty \arrow[drr, dash, "2"'] & & & Q_{-1} \arrow[dl, dash, "1"] \\
\mathbb{F}_q(A) & P_\infty & & & & P_0 &
\end{tikzcd}
$$

$q \equiv 0 \pmod 3$

Adding two roots - $d = 3$

Corollary

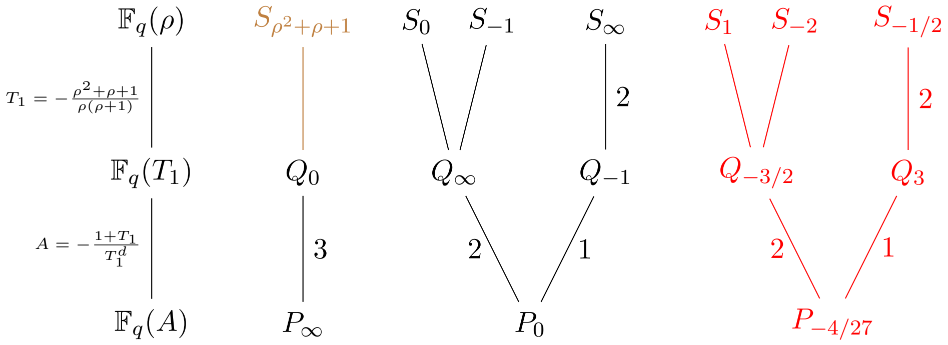
The splitting field F_3 of the polynomial $At^3 + t + 1 \in \mathbb{F}_q(A)[t]$ is the rational function field $\mathbb{F}_q(\rho)$. In particular, the Galois group of $At^3 + t + 1$ is isomorphic to the symmetric group S_3.



Adding two roots - $d = 3$

Corollary

The splitting field F_3 of the polynomial $At^3 + t + 1 \in \mathbb{F}_q(A)[t]$ is the rational function field $\mathbb{F}_q(\rho)$. In particular, the Galois group of $At^3 + t + 1$ is isomorphic to the symmetric group S_3.



$q \equiv 2 \pmod 3$ $\quad$ $\gcd(q, d(d-1)) = 1$

Adding two roots - $d = 3$

Corollary

The splitting field F_3 of the polynomial $At^3 + t + 1 \in \mathbb{F}_q(A)[t]$ is the rational function field $\mathbb{F}_q(\rho)$. In particular, the Galois group of $At^3 + t + 1$ is isomorphic to the symmetric group S_3.

Lemma

The polynomial $At^3 + t + 1 \in \mathbb{F}_q[t]$ splits over $\mathbb{F}_q$ for exactly $\lfloor (q-2)/6 \rfloor$ values of $A \in \mathbb{F}_q \setminus \{0\}$.

Conclusion for $d = 3$

Theorem (Beelen, Datta, Montanucci, N.)

For $q \geq 3$, there exists an absolutely irreducible cubic curve defined over $\mathbb{F}_{q^2}$ that intersects $\mathcal{H}_q$ in $3(q+1)$ many distinct $\mathbb{F}_{q^2}$-rational points.

Conclusion for $d = 3$

Theorem (Beelen, Datta, Montanucci, N.)

For $q \geq 3$, there exists an absolutely irreducible cubic curve defined over $\mathbb{F}_{q^2}$ that intersects $\mathcal{H}_q$ in $3(q+1)$ many distinct $\mathbb{F}_{q^2}$-rational points.

Proof: For $q \geq 8$ we use $\mathcal{C}_3^{(\alpha)}$, where $\alpha^{q+1} = A$ for some $A \in \mathbb{F}_q \setminus \{0\}$ as in the previous lemma. For $q \in \{3, 4, 5, 7\}$ we use a computer search. In fact, define

$$f(X,Y,Z) := \begin{cases} X^3 + Y^3 + Z^3 + XY^2 + X^2Z - YZ^2, & \text{if } q = 3 \\ X^3 + Y^3 + Z^3 + XY^2 + X^2Z + YZ^2 + XZ^2, & \text{if } q = 4 \\ X^3 + Z^3 - Y^2Z, & \text{if } q = 5 \\ X^3 + 4XY^2 + YZ^2, & \text{if } q = 7. \end{cases}$$

Then the cubic given by the equation $f(X,Y,Z) = 0$ satisfies the desired property.

The case $\gcd(q,(d-1)d)=1$

Theorem (Beelen, Datta, Montanucci, N.)

If $\gcd(q,(d-1)d)=1$*, then the Galois group of* $At^d+t+1 \in \mathbb{F}_q(A)[t]$ *is isomorphic to the symmetric group* S_d*. Moreover, in this case, the splitting field* F_d *of* At^d+t+1 *has full constant field* $\mathbb{F}_q$ *and its genus* g_d *is given by*

$$g_d = 1 + \frac{d^2-5d+2}{4}(d-2)!.$$

The case $\gcd(q, (d-1)d) = 1$

Theorem (Beelen, Datta, Montanucci, N.)

If $\gcd(q, (d-1)d) = 1$, *then the Galois group of* $At^d + t + 1 \in \mathbb{F}_q(A)[t]$ *is isomorphic to the symmetric group* S_d. *Moreover, in this case, the splitting field* F_d *of* $At^d + t + 1$ *has full constant field* $\mathbb{F}_q$ *and its genus* g_d *is given by*

$$g_d = 1 + \frac{d^2 - 5d + 2}{4}(d-2)!.$$

Proof (sketch): Consider $\overline{G} := \mathrm{Gal}\left(\overline{\mathbb{F}}_q F_d / \overline{\mathbb{F}}_q(A)\right)$.

The case $\gcd(q, (d-1)d) = 1$

Theorem (Beelen, Datta, Montanucci, N.)

If $\gcd(q, (d-1)d) = 1$, then the Galois group of $At^d + t + 1 \in \mathbb{F}_q(A)[t]$ is isomorphic to the symmetric group S_d. Moreover, in this case, the splitting field F_d of $At^d + t + 1$ has full constant field $\mathbb{F}_q$ and its genus g_d is given by

$$g_d = 1 + \frac{d^2 - 5d + 2}{4}(d-2)!.$$

Proof (sketch): Consider $\overline{G} := \mathrm{Gal}\left(\overline{\mathbb{F}}_q F_d / \overline{\mathbb{F}}_q(A)\right)$.

- $\overline{G}$ acts 2-transitively on the roots ($[\overline{\mathbb{F}}_q(A, T_1, T_2) : \overline{\mathbb{F}}_q(A, T_1)] = d - 1$).

The case $\gcd(q,(d-1)d)=1$

Theorem (Beelen, Datta, Montanucci, N.)

If $\gcd(q,(d-1)d)=1$, then the Galois group of $At^d+t+1 \in \mathbb{F}_q(A)[t]$ is isomorphic to the symmetric group S_d. Moreover, in this case, the splitting field F_d of At^d+t+1 has full constant field $\mathbb{F}_q$ and its genus g_d is given by

$$g_d = 1 + \frac{d^2-5d+2}{4}(d-2)!.$$

Proof (sketch): Consider $\overline{G} := \mathrm{Gal}\left(\overline{\mathbb{F}}_q F_d/\overline{\mathbb{F}}_q(A)\right)$.

- $\overline{G}$ acts 2-transitively on the roots ($[\overline{\mathbb{F}}_q(A,T_1,T_2) : \overline{\mathbb{F}}_q(A,T_1)] = d-1$).
- $\overline{G}$ contains a transposition ("Cycle lemma").

The case $\gcd(q,(d-1)d)=1$

Theorem (Beelen, Datta, Montanucci, N.)

If $\gcd(q,(d-1)d)=1$, then the Galois group of $At^d+t+1 \in \mathbb{F}_q(A)[t]$ is isomorphic to the symmetric group S_d. Moreover, in this case, the splitting field F_d of At^d+t+1 has full constant field $\mathbb{F}_q$ and its genus g_d is given by

$$g_d = 1 + \frac{d^2-5d+2}{4}(d-2)!.$$

Proof (sketch): Consider $\overline{G} := \mathrm{Gal}\left(\overline{\mathbb{F}}_q F_d/\overline{\mathbb{F}}_q(A)\right)$.

- $\overline{G}$ acts 2-transitively on the roots ($[\overline{\mathbb{F}}_q(A,T_1,T_2):\overline{\mathbb{F}}_q(A,T_1)]=d-1$).
- $\overline{G}$ contains a transposition ("Cycle lemma").
- $\overline{G}$ is isomorphic to a subgroup of $\mathrm{Gal}(F_d/\mathbb{F}_q(A))$.

The case $\gcd(q,(d-1)d)=1$

Theorem (Beelen, Datta, Montanucci, N.)

If $\gcd(q,(d-1)d)=1$, then the Galois group of $At^d+t+1 \in \mathbb{F}_q(A)[t]$ is isomorphic to the symmetric group S_d. Moreover, in this case, the splitting field F_d of At^d+t+1 has full constant field $\mathbb{F}_q$ and its genus g_d is given by

$$g_d = 1+\frac{d^2-5d+2}{4}(d-2)!.$$

Proof (sketch): Consider $\overline{G} := \mathrm{Gal}\left(\overline{\mathbb{F}}_q F_d/\overline{\mathbb{F}}_q(A)\right)$.

- $\overline{G}$ acts 2-transitively on the roots ($[\overline{\mathbb{F}}_q(A,T_1,T_2):\overline{\mathbb{F}}_q(A,T_1)]=d-1$).
- $\overline{G}$ contains a transposition ("Cycle lemma").
- $\overline{G}$ is isomorphic to a subgroup of $\mathrm{Gal}(F_d/\mathbb{F}_q(A))$.
- Apply Abhyankar's lemma (all ramification is tame).

The case $\gcd(q, (d-1)d) = 1$

Theorem (Beelen, Datta, Montanucci, N.)

If $\gcd(q, (d-1)d) = 1$, then the Galois group of $At^d + t + 1 \in \mathbb{F}_q(A)[t]$ is isomorphic to the symmetric group S_d. Moreover, in this case, the splitting field F_d of $At^d + t + 1$ has full constant field $\mathbb{F}_q$ and its genus g_d is given by

$$g_d = 1 + \frac{d^2 - 5d + 2}{4}(d-2)!.$$

Corollary (Beelen, Datta, Montanucci, N.)

Suppose that $\gcd(q, (d-1)d) = 1$. Then there exists $A \in \mathbb{F}_q$ such that the polynomial $At^d + t + 1$ splits over $\mathbb{F}_q$ if

$$q + 1 - \lfloor 2\sqrt{q} \rfloor \left(1 + \frac{d^2 - 5d + 2}{4}(d-2)!\right) - \left(\frac{1}{d} + \frac{1}{d-1} + \frac{1}{2}\right) d! > 0. \qquad (1)$$

Some results for $\gcd(q, d(d-1)) > 1$

From Abhyankar's "*Nice equations for nice groups*" (1994) we get information on the Galois group in some cases:

Some results for $\gcd(q, d(d-1)) > 1$

From Abhyankar's "*Nice equations for nice groups*" (1994) we get information on the Galois group in some cases:

Theorem

If $d = p^e$, then the splitting field of $At^d + t + 1$ over $\mathbb{F}_q(A)$ is the composite of $\mathbb{F}_q(T_1, T_2) = \mathbb{F}_q(\rho)$ and the finite field with p^e elements.

Some results for $\gcd(q, d(d-1)) > 1$

From Abhyankar's "*Nice equations for nice groups*" (1994) we get information on the Galois group in some cases:

Theorem

If $d = p^e$, then the splitting field of $At^d + t + 1$ over $\mathbb{F}_q(A)$ is the composite of $\mathbb{F}_q(T_1, T_2) = \mathbb{F}_q(\rho)$ and the finite field with p^e elements.

Corollary

If $d = p^e$, then there exists $A \in \mathbb{F}_q \setminus \{0\}$ such that $At^d + t + 1$ splits over $\mathbb{F}_q$ if and only if $\mathbb{F}_{p^e} \subseteq \mathbb{F}_q$ and $[\mathbb{F}_q : \mathbb{F}_{p^e}] > 1$.

Some results for $\gcd(q, d(d-1)) > 1$

From Abhyankar's "*Nice equations for nice groups*" (1994) we get information on the Galois group in some cases:

Theorem

If $d = p^e + 1$, then the splitting field of $At^d + t + 1$ over $\mathbb{F}_q(A)$ is the composite of the finite field with p^e elements and $\mathbb{F}_q(T_1, T_2, T_3) = \mathbb{F}_q((\sigma - 1)/(\sigma - \rho))$, where $\rho = T_2/T_1$ and $\sigma = T_3/T_1$.

Some results for $\gcd(q, d(d-1)) > 1$

From Abhyankar's "*Nice equations for nice groups*" (1994) we get information on the Galois group in some cases:

Theorem

If $d = p^e + 1$, then the splitting field of $At^d + t + 1$ over $\mathbb{F}_q(A)$ is the composite of the finite field with p^e elements and $\mathbb{F}_q(T_1, T_2, T_3) = \mathbb{F}_q((\sigma - 1)/(\sigma - \rho))$, where $\rho = T_2/T_1$ and $\sigma = T_3/T_1$.

Corollary

Let $d = p^e + 1$ where p is the characteristic. Then there exists $A \in \mathbb{F}_q \setminus \{0\}$ such that $At^d + t + 1$ splits over $\mathbb{F}_q$ if and only if $\mathbb{F}_{p^e} \subseteq \mathbb{F}_q$ and $[\mathbb{F}_q : \mathbb{F}_{p^e}] > 2$.

The case $d = 4$

Lemma

Let N_4 denote the number of $A \in \mathbb{F}_q \setminus \{0\}$ for which the polynomial $At^4 + t + 1$ splits over $\mathbb{F}_q$. Then

$$N_4 = \begin{cases} 0 & \text{if } q = 2^e \text{ and } e \text{ is odd,} \\ \frac{q-4}{12} & \text{if } q = 2^e \text{ and } e \text{ is even,} \\ \frac{q+1}{24} & \text{if } q \equiv 23 \pmod{24} \text{ and} \\ \left\lfloor \frac{q-2}{24} \right\rfloor & \text{otherwise.} \end{cases}$$

The case $d = 4$

Lemma

Let N_4 denote the number of $A \in \mathbb{F}_q \setminus \{0\}$ for which the polynomial $At^4 + t + 1$ splits over $\mathbb{F}_q$. Then

$$N_4 = \begin{cases} 0 & \text{if } q = 2^e \text{ and } e \text{ is odd,} \\ \frac{q-4}{12} & \text{if } q = 2^e \text{ and } e \text{ is even,} \\ \frac{q+1}{24} & \text{if } q \equiv 23 \pmod{24} \text{ and} \\ \left\lfloor \frac{q-2}{24} \right\rfloor & \text{otherwise.} \end{cases}$$

Theorem

Suppose q is a prime power, but not an odd power of two larger than 8. Then, there exists an absolutely irreducible quartic curve defined over $\mathbb{F}_{q^2}$ that intersects $\mathcal{H}_q$ in $4(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points.

The case $d = 4$

Lemma

Let N_4 denote the number of $A \in \mathbb{F}_q \setminus \{0\}$ for which the polynomial $At^4 + t + 1$ splits over $\mathbb{F}_q$. Then

$$N_4 = \begin{cases} 0 & \text{if } q = 2^e \text{ and } e \text{ is odd,} \\ \frac{q-4}{12} & \text{if } q = 2^e \text{ and } e \text{ is even,} \\ \frac{q+1}{24} & \text{if } q \equiv 23 \pmod{24} \text{ and} \\ \left\lfloor \frac{q-2}{24} \right\rfloor & \text{otherwise.} \end{cases}$$

Theorem

Suppose q is a prime power, but not an odd power of two larger than 8. Then, there exists an absolutely irreducible quartic curve defined over $\mathbb{F}_{q^2}$ that intersects $\mathcal{H}_q$ in $4(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points.

Open: $q = 2^e$ for $e > 3$ odd.

The cases $d = 5$ and $d = 6$

For $d = 5$, the answer is $\boxed{\text{YES}}$ in the following cases:

- $q \in \{3, 4, 9\}$ by "large d" results.

The cases $d = 5$ and $d = 6$

For $d = 5$, the answer is $\boxed{\text{YES}}$ in the following cases:

- $q \in \{3, 4, 9\}$ by "large d" results.
- $q > 131$, with $\gcd(q, 20) = 1$.

The cases $d = 5$ and $d = 6$

For $d = 5$, the answer is $\boxed{\text{YES}}$ in the following cases:

- $q \in \{3, 4, 9\}$ by "large d" results.
- $q > 131$, with $\gcd(q, 20) = 1$.
- $q = 5^e$ for $e > 1$, and $q = 2^e$ for $e > 2$ even.

The cases $d = 5$ and $d = 6$

For $d = 5$, the answer is $\boxed{\text{YES}}$ in the following cases:

- $q \in \{3, 4, 9\}$ by "large d" results.
- $q > 131$, with $\gcd(q, 20) = 1$.
- $q = 5^e$ for $e > 1$, and $q = 2^e$ for $e > 2$ even.

For $d = 6$, the answer is $\boxed{\text{YES}}$ in the following cases:

- $q \in \{3, 4, 5, 11\}$ by "large d" results.
- $q > 1877$, with $\gcd(q, 20) = 1$.
- $q = 5^e$, $e > 2$.

Conclusion

Question

Can $\mathcal{H}_q$ and $\mathcal{C}_d$ intersect in exactly $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points?

The answer is $\boxed{\text{YES}}$ for

- $d = 1$.
- $d = 2$ and $q \geq 4$.
- $d = q + 1$ and $q \geq 3$.

The answer is $\boxed{\text{NO}}$ for

- $(q, d) \in \{(2, 2), (3, 2), (2, 3)\}$.
- $d > q^2 - q + 1$.

Conclusion

Question

Can $\mathcal{H}_q$ and $\mathcal{C}_d$ intersect in exactly $d(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points?

The answer is $\boxed{\text{YES}}$ for

- $d = 1$.
- $d = 2$ and $q \geq 4$.
- $d = q + 1$ and $q \geq 3$.

The answer is also $\boxed{\text{YES}}$ for

- $d = 3$ and $q \geq 3$.
- $d = \lfloor (q+1)/2 \rfloor$.
- $q \leq d \leq q^2 - q + 1$, for $q \geq 3$.

The answer is $\boxed{\text{NO}}$ for

- $(q, d) \in \{(2,2), (3,2), (2,3)\}$.
- $d > q^2 - q + 1$.

The answer is $\boxed{\text{often YES}}$ for

- $d = 4, 5, 6$.
- $q >> d$ and $\gcd(q, d(d-1)) = 1$.

Thank you for your attention!

Results for large d

Theorem (Beelen, Datta, Montanucci, N.)

Let $\mathcal{C}_{q^2-q+1}$ be the curve defined over $\mathbb{F}_{q^2}$ given by the equation

$$X\left((Y^q+YZ^{q-1})^{q-1}-Z^{q^2-q}\right)+X^{q+1}Z^{q^2-2q}-Y^qZ^{q^2-2q+1}-YZ^{q^2-q}=0.$$

Then $\mathcal{C}_{q^2-q+1}$ is an absolutely irreducible curve of degree q^2-q+1 intersecting the Hermitian curve in exactly q^3+1 distinct $\mathbb{F}_{q^2}$-rational points.

Theorem (Beelen, Datta, Montanucci, N.)

For $q>2$ and $\alpha \in \mathbb{F}_{q^2}\setminus\mathbb{F}_q$, the curve $\mathcal{C}_q$ of degree q given by the equation

$$Y^q+YZ^{q-1}=(\alpha+\alpha^2)X^q-\alpha^3X^{q-1}Z+X^2Z^{q-2}-(\alpha+\alpha^2)XZ^{q-1}-\alpha^3Z^q$$

is absolutely irreducible and it intersects $\mathcal{H}_q$ in $q(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points.

Degree $d = \lfloor (q+1)/2 \rfloor$ for q even

Corollary

Suppose q is even and let $\alpha \in \mathbb{F}_{q^2}$ be an element satisfying $\alpha^q + \alpha = 1$. Then the curve $\mathcal{C}_{q/2}$ with equation

$$(Y + \alpha^q X)^{q/2} + \cdots + (Y + \alpha^q X)^2 Z^{q/2-2} + (Y + \alpha^q X) Z^{q/2-1} = X Z^{q/2-1}$$

is absolutely irreducible, and it intersects the Hermitian curve $\mathcal{H}_q$ in $q(q+1)/2$ distinct $\mathbb{F}_{q^2}$-rational points.

Degree $d = \lfloor (q+1)/2 \rfloor$ for q odd

Consider

$$\mathcal{H}_q : \; X^{q+1} + Y^{q+1} + Z^{q+1} = 0,$$

and

$$C_{\alpha,\beta} : \; \alpha X^{\frac{q+1}{2}} + Y^{\frac{q+1}{2}} + \beta Z^{\frac{q+1}{2}} = 0.$$

Degree $d = \lfloor (q+1)/2 \rfloor$ for q odd

Consider

$$\mathcal{H}_q : \ X^{q+1} + Y^{q+1} + Z^{q+1} = 0,$$

and

$$C_{\alpha,\beta} : \ \alpha X^{\frac{q+1}{2}} + Y^{\frac{q+1}{2}} + \beta Z^{\frac{q+1}{2}} = 0.$$

Let $Z = 1$ and eliminate Y to obtain

$$(\alpha^2 + 1)X^{q+1} + 2\alpha\beta X^{\frac{q+1}{2}} + (\beta^2 + 1) = 0.$$

Degree $d = \lfloor (q+1)/2 \rfloor$ for q odd

Consider

$$\mathcal{H}_q : \; X^{q+1} + Y^{q+1} + Z^{q+1} = 0,$$

and

$$C_{\alpha,\beta} : \; \alpha X^{\frac{q+1}{2}} + Y^{\frac{q+1}{2}} + \beta Z^{\frac{q+1}{2}} = 0.$$

Let $Z = 1$ and eliminate Y to obtain

$$(\alpha^2 + 1) X^{q+1} + 2\alpha\beta X^{\frac{q+1}{2}} + (\beta^2 + 1) = 0.$$

Claim:

> *For $q > 13$, there exists a pair $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q$, with $\alpha\beta \neq 0$, such that the above equation has two distinct solutions in $\mathbb{F}_q \setminus \{0\}$, when considered as a quadratic polynomial in $X^{\frac{q+1}{2}}$.*

The case $d = 4$

Lemma

Let N_4 denote the number of $A \in \mathbb{F}_q \setminus \{0\}$ for which the polynomial $At^4 + t + 1$ splits over $\mathbb{F}_q$. Then

$$N_4 = \begin{cases} 0 & \text{if } q = 2^e \text{ and } e \text{ is odd,} \\ \frac{q-4}{12} & \text{if } q = 2^e \text{ and } e \text{ is even,} \\ \frac{q+1}{24} & \text{if } q \equiv 23 \pmod{24} \text{ and} \\ \left\lfloor \frac{q-2}{24} \right\rfloor & \text{otherwise.} \end{cases}$$

The case $d = 4$

Lemma

Let N_4 denote the number of $A \in \mathbb{F}_q \setminus \{0\}$ for which the polynomial $At^4 + t + 1$ splits over $\mathbb{F}_q$. Then

$$N_4 = \begin{cases} 0 & \text{if } q = 2^e \text{ and } e \text{ is odd,} \\ \frac{q-4}{12} & \text{if } q = 2^e \text{ and } e \text{ is even,} \\ \frac{q+1}{24} & \text{if } q \equiv 23 \pmod{24} \text{ and} \\ \left\lfloor \frac{q-2}{24} \right\rfloor & \text{otherwise.} \end{cases}$$

Theorem

Suppose that either $q \in \{16, 23\}$ or $q \geq 27$ is a prime power, but not an odd power of two. Then there exists an absolutely irreducible quartic curve defined over $\mathbb{F}_{q^2}$ that intersects $\mathcal{H}_q$ in $4(q+1)$ distinct $\mathbb{F}_{q^2}$-rational points.

The case $d = 4$

- Our previous results imply the existence of such a quartic for $q \in \{3, 4, 7, 8\}$.

The case $d = 4$

- Our previous results imply the existence of such a quartic for $q \in \{3, 4, 7, 8\}$.
- For $q \in \{5, 9, 11, 13, 17, 19, 25\}$ one can choose the quartic given by $f(X, Y, Z) = 0$ with

$$f(X,Y,Z) := \begin{cases} X^3Y + 2Y^2Z^2 + Z^4, & \text{if } \ q = 5 \\ X^4 + Y^3Z - Y^2Z^2 + YZ^3, & \text{if } \ q = 9 \\ X^4 - Y^4 - \omega^{16}Z^4, & \text{if } \ q = 11 \\ X^3Y + Y^3Z + XZ^3, & \text{if } \ q = 13 \\ X^4 + 13Y^3Z + 14Y^3Z^2, & \text{if } \ q = 17 \\ X^4 - \omega^4Y^4 - \omega^{24}Z^4, & \text{if } \ q = 19 \\ X^2Y^2 + X^2Z^2 + Y^2Z^2, & \text{if } \ q = 25, \end{cases}$$

where ω is a primitive element of $\mathbb{F}_{q^2}$.

The case $d = 4$

- Our previous results imply the existence of such a quartic for $q \in \{3, 4, 7, 8\}$.
- For $q \in \{5, 9, 11, 13, 17, 19, 25\}$ one can choose the quartic given by $f(X, Y, Z) = 0$ with

$$f(X,Y,Z) := \begin{cases} X^3Y + 2Y^2Z^2 + Z^4, & \text{if } \; q = 5 \\ X^4 + Y^3Z - Y^2Z^2 + YZ^3, & \text{if } \; q = 9 \\ X^4 - Y^4 - \omega^{16}Z^4, & \text{if } \; q = 11 \\ X^3Y + Y^3Z + XZ^3, & \text{if } \; q = 13 \\ X^4 + 13Y^3Z + 14Y^3Z^2, & \text{if } \; q = 17 \\ X^4 - \omega^4Y^4 - \omega^{24}Z^4, & \text{if } \; q = 19 \\ X^2Y^2 + X^2Z^2 + Y^2Z^2, & \text{if } \; q = 25, \end{cases}$$

  where ω is a primitive element of $\mathbb{F}_{q^2}$.
- The case $d = 4$ is settled, except if $q > 8$ is an odd power of two.