On the linear bounds on the genus of pointless curves

Pogildiakov Ivan

Université de la Polynésie française,
Tahiti, Polynésie française

Arithmetic, Geometry, Cryptography and Coding Theory
Marseille, June 19 - 23, 2017

Overview

Motivation

Let $\mathcal{C}$ be a smooth genus g curve $\mathcal{C}$ over $\mathbb{F}_q$. The number of rational points on $\mathcal{C}$ satisfies the well known Weil-Serre bound:

$$q + 1 - g\lfloor 2\sqrt{q}\rfloor \leq N_1(\mathcal{C}) \leq q + 1 + g\lfloor 2\sqrt{q}\rfloor.$$

Let q, g be such that $q+1-g\lfloor 2\sqrt{q}\rfloor \leq 0$, i.e. $g \geq (q+1)/\lfloor 2\sqrt{q}\rfloor$.
Question: Does there exist a curve over $\mathbb{F}_q$ of genus g with no rational points (which is called *pointless*)?
Main directions:

1. g is fixed (E. W. Howe, K. E. Lauter, J. Top, 2005),
2. q is fixed (R. Becker, D. Glass, 2013).

Motivation

Let $\mathcal{C}$ be a smooth genus g curve $\mathcal{C}$ over $\mathbb{F}_q$. The number of rational points on $\mathcal{C}$ satisfies the well known Weil-Serre bound:

$$q+1-g\lfloor 2\sqrt{q}\rfloor \leq N_1(\mathcal{C}) \leq \boldsymbol{q+1+g\lfloor 2\sqrt{q}\rfloor}\ .$$

Let q, g be such that $q+1-g\lfloor 2\sqrt{q}\rfloor \leq 0$, i.e. $g \geq (q+1)/\lfloor 2\sqrt{q}\rfloor$.
Question: Does there exist a curve over $\mathbb{F}_q$ of genus g with no rational points (which is called *pointless*)?
Main directions:

1. g is fixed (E. W. Howe, K. E. Lauter, J. Top, 2005),
2. q is fixed (R. Becker, D. Glass, 2013).

Motivation

Let $\mathcal{C}$ be a smooth genus g curve $\mathcal{C}$ over $\mathbb{F}_q$. The number of rational points on $\mathcal{C}$ satisfies the well known Weil-Serre bound:

$$\boldsymbol{q + 1 - g\lfloor 2\sqrt{q} \rfloor} \leq N_1(\mathcal{C}) \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor.$$

Let q, g be such that $q+1-g\lfloor 2\sqrt{q}\rfloor \leq 0$, i.e. $g \geq (q+1)/\lfloor 2\sqrt{q}\rfloor$.
Question: Does there exist a curve over $\mathbb{F}_q$ of genus g with no rational points (which is called *pointless*)?
Main directions:

1. g is fixed (E. W. Howe, K. E. Lauter, J. Top, 2005),
2. q is fixed (R. Becker, D. Glass, 2013).

Motivation

Let $\mathcal{C}$ be a smooth genus g curve $\mathcal{C}$ over $\mathbb{F}_q$. The number of rational points on $\mathcal{C}$ satisfies the well known Weil-Serre bound:

$$\boldsymbol{q+1-g\lfloor 2\sqrt{q}\rfloor} \le N_1(\mathcal{C}) \le q+1+g\lfloor 2\sqrt{q}\rfloor.$$

Let q, g be such that $q+1-g\lfloor 2\sqrt{q}\rfloor \le 0$, i.e. $g \ge (q+1)/\lfloor 2\sqrt{q}\rfloor$.

Question: Does there exist a curve over $\mathbb{F}_q$ of genus g with no rational points (which is called *pointless*)?

Main directions:

1. g is fixed (E. W. Howe, K. E. Lauter, J. Top, 2005),
2. q is fixed (R. Becker, D. Glass, 2013).

Motivation

Let $\mathcal{C}$ be a smooth genus g curve $\mathcal{C}$ over $\mathbb{F}_q$. The number of rational points on $\mathcal{C}$ satisfies the well known Weil-Serre bound:

$$\boldsymbol{q+1-g\lfloor 2\sqrt{q}\rfloor} \leq N_1(\mathcal{C}) \leq q+1+g\lfloor 2\sqrt{q}\rfloor.$$

Let q, g be such that $q+1-g\lfloor 2\sqrt{q}\rfloor \leq 0$, i.e. $g \geq (q+1)/\lfloor 2\sqrt{q}\rfloor$.
Question: Does there exist a curve over $\mathbb{F}_q$ of genus g with no rational points (which is called *pointless*)?
Main directions:

1. g is fixed (E. W. Howe, K. E. Lauter, J. Top, 2005),
2. q is fixed (R. Becker, D. Glass, 2013).

Motivation

Let $\mathcal{C}$ be a smooth genus g curve $\mathcal{C}$ over $\mathbb{F}_q$. The number of rational points on $\mathcal{C}$ satisfies the well known Weil-Serre bound:

$$\boldsymbol{q+1-g\lfloor 2\sqrt{q}\rfloor} \leq N_1(\mathcal{C}) \leq q+1+g\lfloor 2\sqrt{q}\rfloor.$$

Let q, g be such that $q+1-g\lfloor 2\sqrt{q}\rfloor \leq 0$, i.e. $g \geq (q+1)/\lfloor 2\sqrt{q}\rfloor$.
Question: Does there exist a curve over $\mathbb{F}_q$ of genus g with no rational points (which is called *pointless*)?
Main directions:

1. g is fixed (E. W. Howe, K. E. Lauter, J. Top, 2005),
2. q is fixed (R. Becker, D. Glass, 2013).

The case of fixed q

Given q, denote by g_q^{min} the number such that for all $g \geq g_q^{min}$ there is a smooth pointless genus g curve over $\mathbb{F}_q$.

Theorem (R. Becker and D. Glass, 2013)

Let a be the least residue of $g \mod p$. Suppose that

$$g \geq (p-a-1)(q-1), \text{ if } a < p-1,$$

or

$$g \geq (p-2a-2)(q-1), \text{ if } 0 \leq a \leq (p-3)/2.$$

Then there is a non-singular hyperelliptic pointless curve of genus g defined over $\mathbb{F}_q$.

Remarks. This result shows that $g_q^{min} \leq O(pq)$ when q is odd. However, under special assumptions they obtain that $g_q^{min} \leq O(q)$.

The case of fixed q

Given q, denote by g_q^{min} the number such that for all $g \geq g_q^{min}$ there is a smooth pointless genus g curve over $\mathbb{F}_q$.

Theorem (R. Becker and D. Glass, 2013)

Let a be the least residue of $g \mod p$. Suppose that

$$g \geq (p-a-1)(q-1), \text{ if } a < p-1,$$

or

$$g \geq (p-2a-2)(q-1), \text{ if } 0 \leq a \leq (p-3)/2.$$

Then there is a non-singular hyperelliptic pointless curve of genus g defined over $\mathbb{F}_q$.

Remarks. This result shows that $g_q^{min} \leq O(pq)$ when q is odd. However, under special assumptions they obtain that $g_q^{min} \leq O(q)$.

The case of fixed q

Given q, denote by g_q^{min} the number such that for all $g \geq g_q^{min}$ there is a smooth pointless genus g curve over $\mathbb{F}_q$.

Theorem (R. Becker and D. Glass, 2013)

Let a be the least residue of $g \mod p$. Suppose that

$$g \geq (p-a-1)(q-1), \textit{ if } a < p-1,$$

or

$$g \geq (p-2a-2)(q-1), \textit{ if } 0 \leq a \leq (p-3)/2.$$

Then there is a non-singular hyperelliptic pointless curve of genus g defined over $\mathbb{F}_q$.

Remarks. This result shows that $g_q^{min} \leq O(pq)$ when q is odd. However, under special assumptions they obtain that $g_q^{min} \leq O(q)$.

The case of fixed q

The result of R. Becker and D. Glass possesses a generalization.

Theorem (I. Pogildiakov, 2017)

Let q be a prime power. Set

$$g_q = \begin{cases} \max\{2, (q-3)/2\}, & q \text{ is odd}, \\ \max\{2, q-1\}, & q \text{ is even}. \end{cases}$$

Suppose that $g \geq g_q$. Then there is a smooth genus g hyperelliptic curve over $\mathbb{F}_q$ having no $\mathbb{F}_q$-points.

This implies a **linear bound** on the number g_q^{min} **for all** q.

Like R. Becker and D. Glass, we use explicit constructions, but

1. consider more cases (less assumptions),
2. involve more families of polynomials.

The case of fixed q

The result of R. Becker and D. Glass possesses a generalization.

Theorem (I. Pogildiakov, 2017)

Let q be a prime power. Set

$$g_q = \begin{cases} \max\{2, (q-3)/2\}, & q \text{ is odd}, \\ \max\{2, q-1\}, & q \text{ is even}. \end{cases}$$

Suppose that $g \geq g_q$. Then there is a smooth genus g hyperelliptic curve over $\mathbb{F}_q$ having no $\mathbb{F}_q$-points.

This implies a **linear bound** on the number g_q^{min} **for all** q.

Like R. Becker and D. Glass, we use explicit constructions, but

1. consider more cases (less assumptions),
2. involve more families of polynomials.

The case of fixed q

The result of R. Becker and D. Glass possesses a generalization.

Theorem (I. Pogildiakov, 2017)

Let q be a prime power. Set

$$g_q = \begin{cases} \max\{2, (q-3)/2\}, & q \text{ is odd}, \\ \max\{2, q-1\}, & q \text{ is even}. \end{cases}$$

Suppose that $g \geq g_q$. Then there is a smooth genus g hyperelliptic curve over $\mathbb{F}_q$ having no $\mathbb{F}_q$-points.

This implies a **linear bound** on the number g_q^{min} **for all** q.

Like R. Becker and D. Glass, we use explicit constructions, but

1. consider more cases (less assumptions),
2. involve more families of polynomials.

Hyperelliptic curves over $\mathbb{F}_q$

Let $\mathcal{C}$ be a hyperelliptic curve over $\mathbb{F}_q$ of genus g. It can be defined by an affine model $y^2 + h(x)y = f(x)$, where

$$2g + 1 \leq \max\{2 \deg h(x), \deg f(x)\} \leq 2g + 2.$$

As a projective curve, $\mathcal{C}$ is the union of two affine patches:

$$y^2 + h(x)y = f(x), \text{ and } y^2 + x^{g+1}h(1/x)y = x^{2g+2}f(1/x).$$

The curve $\mathcal{C}$ is smooth if and only if

$$h(x) \text{ and } h'(x)^2 f(x) + f'(x)^2 \text{ are comprime.}$$

Special case: if q is odd, then we can let $h(x) = 0$.

Hyperelliptic curves over $\mathbb{F}_q$

Let $\mathcal{C}$ be a hyperelliptic curve over $\mathbb{F}_q$ of genus g. It can be defined by an affine model $y^2 + h(x)y = f(x)$, where

$$2g + 1 \leq \max\{2 \deg h(x), \deg f(x)\} \leq 2g + 2.$$

As a projective curve, $\mathcal{C}$ is the union of two affine patches:

$$y^2 + h(x)y = f(x), \text{ and } y^2 + x^{g+1}h(1/x)y = x^{2g+2}f(1/x).$$

The curve $\mathcal{C}$ is smooth if and only if

$$h(x) \text{ and } h'(x)^2 f(x) + f'(x)^2 \text{ are comprime.}$$

Special case: if q is odd, then we can let $h(x) = 0$.

Hyperelliptic curves over $\mathbb{F}_q$

Let $\mathcal{C}$ be a hyperelliptic curve over $\mathbb{F}_q$ of genus g. It can be defined by an affine model $y^2 + h(x)y = f(x)$, where

$$2g + 1 \leq \max\{2 \deg h(x), \deg f(x)\} \leq 2g + 2.$$

As a projective curve, $\mathcal{C}$ is the union of two affine patches:

$$y^2 + h(x)y = f(x), \text{ and } y^2 + x^{g+1}h(1/x)y = x^{2g+2}f(1/x).$$

The curve $\mathcal{C}$ is smooth if and only if

$$h(x) \text{ and } h'(x)^2 f(x) + f'(x)^2 \text{ are comprime.}$$

Special case: if q is odd, then we can let $h(x) = 0$.

Hyperelliptic curves over $\mathbb{F}_q$

Let $\mathcal{C}$ be a hyperelliptic curve over $\mathbb{F}_q$ of genus g. It can be defined by an affine model $y^2 + h(x)y = f(x)$, where

$$2g + 1 \leq \max\{2 \deg h(x), \deg f(x)\} \leq 2g + 2.$$

As a projective curve, $\mathcal{C}$ is the union of two affine patches:

$$y^2 + h(x)y = f(x), \text{ and } y^2 + x^{g+1}h(1/x)y = x^{2g+2}f(1/x).$$

The curve $\mathcal{C}$ is smooth if and only if

$$h(x) \text{ and } h'(x)^2 f(x) + f'(x)^2 \text{ are comprime.}$$

Special case: if q is odd, then we can let $h(x) = 0$.

Hyperelliptic curves over $\mathbb{F}_q$, odd q.

Let $\mathcal{C}$ be a hyperelliptic curve $y^2 = f(x)$ over $\mathbb{F}_q$, where q is odd. We have the following information :

1. $\mathcal{C}$ is the union of two affine patches
$$y^2 = f(x) \text{ and } y^2 = x^{2g+2} f(1/x).$$
2. $\mathcal{C}$ is smooth if and only if $f(x)$ is square-free.
3. The number of rational points of $\mathcal{C}$ is
$$N_1(\mathcal{C}) = N_1(\mathcal{C})^{aff} + N_1(\mathcal{C})^{\infty},$$
where
   - $N_1(\mathcal{C})^{aff}$ is the number of affine points in $\mathcal{C}(\mathbb{F}_q)$.
   - $N_1(\mathcal{C})^{\infty}$ is the number of points in $\mathcal{C}(\mathbb{F}_q)$ that lie at ∞.

Counting rational points on $\mathcal{C}$, odd q.

Let us define

$$N^0 = \#\{\alpha \in \mathbb{F}_q \mid f(\alpha) = 0\},$$
$$N^r = \#\{\alpha \in \mathbb{F}_q \mid f(\alpha) \text{ is a q.r.}\}.$$

Then $N_1(\mathcal{C})^{aff} = N^0 + 2N^r$. Note, that $N_1(\mathcal{C})^{aff} \leq 2q$.

Points at infinity belong to the affine patch $y^2 = x^{2g+2}f(1/x)$ and correspond to the solutions with $x = 0$, i.e. $y^2 = LT(f(x))$.

1. If $\deg f(x) = 2g + 1$, then $N_1(\mathcal{C})^{\infty} = 1$.
2. If $\deg f(x) = 2g + 2$ and $LT(f)$ is a q.r., then $N_1(\mathcal{C})^{\infty} = 2$.
3. If $\deg f(x) = 2g + 2$ and $LT(f)$ is a q.n.r, then $N_1(\mathcal{C})^{\infty} = 0$.

Counting rational points on $\mathcal{C}$, odd q.

Let us define

$$N^0 = \#\{\alpha \in \mathbb{F}_q \mid f(\alpha) = 0\},$$
$$N^r = \#\{\alpha \in \mathbb{F}_q \mid f(\alpha) \text{ is a q.r.}\}.$$

Then $N_1(\mathcal{C})^{aff} = N^0 + 2N^r$. Note, that $N_1(\mathcal{C})^{aff} \leq 2q$.

Points at infinity belong to the affine patch $y^2 = x^{2g+2}f(1/x)$ and correspond to the solutions with $x = 0$, i.e. $y^2 = LT(f(x))$.

1. If $\deg f(x) = 2g + 1$, then $N_1(\mathcal{C})^\infty = 1$.
2. If $\deg f(x) = 2g + 2$ and $LT(f)$ is a q.r., then $N_1(\mathcal{C})^\infty = 2$.
3. If $\deg f(x) = 2g + 2$ and $LT(f)$ is a q.n.r, then $N_1(\mathcal{C})^\infty = 0$.

Counting rational points on $\mathcal{C}$, odd q.

Let us define

$$N^0 = \#\{\alpha \in \mathbb{F}_q \mid f(\alpha) = 0\},$$
$$N^r = \#\{\alpha \in \mathbb{F}_q \mid f(\alpha) \text{ is a q.r.}\}.$$

Then $N_1(\mathcal{C})^{aff} = N^0 + 2N^r$. Note, that $N_1(\mathcal{C})^{aff} \leq 2q$.

Points at infinity belong to the affine patch $y^2 = x^{2g+2} f(1/x)$ and correspond to the solutions with $x = 0$, i.e. $y^2 = LT(f(x))$.

1. If $\deg f(x) = 2g + 1$, then $N_1(\mathcal{C})^\infty = 1$.
2. If $\deg f(x) = 2g + 2$ and $LT(f)$ is a q.r., then $N_1(\mathcal{C})^\infty = 2$.
3. If $\deg f(x) = 2g + 2$ and $LT(f)$ is a q.n.r, then $N_1(\mathcal{C})^\infty = 0$.

$\mathbb{F}_q$-maximal hyperelliptic curves

Let us call $f(x)$ to be a *good polynomial*, if it satisfies the following conditions:

1. $\deg f(x) = 2g + 2$ is even,
2. $f(x)$ is squarefree,
3. $LT(f(x))$ is a quadratic residue,
4. $f(\alpha)$ is a q.r. for all $\alpha \in \mathbb{F}_q$ ($\Rightarrow N^0_{f(x)} = 0,\ N^r_{f(x)} = 2q$).

Let $\mathcal{C}$ be a curve $y^2 = f(x)$ over $\mathbb{F}_q$, where $f(x)$ is good.
Then $\mathcal{C}$ is smooth of genus g having

$$N_1(\mathcal{C}) = N_1(\mathcal{C})^{aff} + N_1(\mathcal{C})^{\infty} = N^0_{f(x)} + 2N^r_{f(x)} + N_1(\mathcal{C})^{\infty} = 2q + 2.$$

We will call such a curve $\mathbb{F}_q$-*maximal*, since $N_1 \leq 2q + 2$ for every hyperelliptic curve over $\mathbb{F}_q$.

$\mathbb{F}_q$-maximal hyperelliptic curves

Let us call $f(x)$ to be a *good polynomial*, if it satisfies the following conditions:

1. $\deg f(x) = 2g + 2$ is even,
2. $f(x)$ is squarefree,
3. $LT(f(x))$ is a quadratic residue,
4. $f(\alpha)$ is a q.r. for all $\alpha \in \mathbb{F}_q$ ($\Rightarrow N^0_{f(x)} = 0,\ N^r_{f(x)} = 2q$).

Let $\mathcal{C}$ be a curve $y^2 = f(x)$ over $\mathbb{F}_q$, where $f(x)$ is good.
Then $\mathcal{C}$ is smooth of genus g having

$$N_1(\mathcal{C}) = N_1(\mathcal{C})^{aff} + N_1(\mathcal{C})^{\infty} = N^0_{f(x)} + 2N^r_{f(x)} + N_1(\mathcal{C})^{\infty} = 2q + 2.$$

We will call such a curve $\mathbb{F}_q$-*maximal*, since $N_1 \leq 2q + 2$ for every hyperelliptic curve over $\mathbb{F}_q$.

$\mathbb{F}_q$-maximal hyperelliptic curves

Let us call $f(x)$ to be a *good polynomial*, if it satisfies the following conditions :

1. $\deg f(x) = 2g + 2$ is even,
2. $f(x)$ is squarefree,
3. $LT(f(x))$ is a quadratic residue,
4. $f(\alpha)$ is a q.r. for all $\alpha \in \mathbb{F}_q$ ($\Rightarrow N^0_{f(x)} = 0$, $N^r_{f(x)} = 2q$).

Let $\mathcal{C}$ be a curve $y^2 = f(x)$ over $\mathbb{F}_q$, where $f(x)$ is good. Then $\mathcal{C}$ is smooth of genus g having

$$N_1(\mathcal{C}) = N_1(\mathcal{C})^{aff} + N_1(\mathcal{C})^{\infty} = N^0_{f(x)} + 2N^r_{f(x)} + N_1(\mathcal{C})^{\infty} = 2q + 2.$$

We will call such a curve $\mathbb{F}_q$-*maximal*, since $N_1 \leq 2q + 2$ for every hyperelliptic curve over $\mathbb{F}_q$.

$\mathbb{F}_q$-maximal hyperelliptic curves

Let us call $f(x)$ to be a *good polynomial*, if it satisfies the following conditions:

1. $\deg f(x) = 2g + 2$ is even,
2. $f(x)$ is squarefree,
3. $LT(f(x))$ is a quadratic residue,
4. $f(\alpha)$ is a q.r. for all $\alpha \in \mathbb{F}_q$ ($\Rightarrow N^0_{f(x)} = 0$, $N^r_{f(x)} = 2q$).

Let $\mathcal{C}$ be a curve $y^2 = f(x)$ over $\mathbb{F}_q$, where $f(x)$ is good. Then $\mathcal{C}$ is smooth of genus g having

$$N_1(\mathcal{C}) = N_1(\mathcal{C})^{aff} + N_1(\mathcal{C})^{\infty} = N^0_{f(x)} + 2N^r_{f(x)} + N_1(\mathcal{C})^{\infty} = 2q + 2.$$

We will call such a curve $\mathbb{F}_q$*-maximal*, since $N_1 \leq 2q + 2$ for every hyperelliptic curve over $\mathbb{F}_q$.

$\mathbb{F}_q$-maximal hyperelliptic curves

Let us call $f(x)$ to be a *good polynomial*, if it satisfies the following conditions:

1. $\deg f(x) = 2g + 2$ is even,
2. $f(x)$ is squarefree,
3. $LT(f(x))$ is a quadratic residue,
4. $f(\alpha)$ is a q.r. for all $\alpha \in \mathbb{F}_q$ ($\Rightarrow N^0_{f(x)} = 0,\ N^r_{f(x)} = 2q$).

Let $\mathcal{C}$ be a curve $y^2 = f(x)$ over $\mathbb{F}_q$, where $f(x)$ is good. Then $\mathcal{C}$ is smooth of genus g having

$$N_1(\mathcal{C}) = N_1(\mathcal{C})^{aff} + N_1(\mathcal{C})^{\infty} = N^0_{f(x)} + 2N^r_{f(x)} + N_1(\mathcal{C})^{\infty} = 2q + 2.$$

We will call such a curve $\mathbb{F}_q$-*maximal*, since $N_1 \leq 2q + 2$ for every hyperelliptic curve over $\mathbb{F}_q$.

$\mathbb{F}_q$-maximal hyperelliptic curves

Let us call $f(x)$ to be a *good polynomial*, if it satisfies the following conditions:

1. $\deg f(x) = 2g + 2$ is even,
2. $f(x)$ is squarefree,
3. $LT(f(x))$ is a quadratic residue,
4. $f(\alpha)$ is a q.r. for all $\alpha \in \mathbb{F}_q$ ($\Rightarrow N^0_{f(x)} = 0,\ N^r_{f(x)} = 2q$).

Let $\mathcal{C}$ be a curve $y^2 = f(x)$ over $\mathbb{F}_q$, where $f(x)$ is good.
Then $\mathcal{C}$ is smooth of genus g having

$$N_1(\mathcal{C}) = N_1(\mathcal{C})^{aff} + N_1(\mathcal{C})^{\infty} = N^0_{f(x)} + 2N^r_{f(x)} + N_1(\mathcal{C})^{\infty} = 2q + 2.$$

We will call such a curve $\mathbb{F}_q$-*maximal*, since $N_1 \leq 2q + 2$ for every hyperelliptic curve over $\mathbb{F}_q$.

$\mathbb{F}_q$-maximal hyperelliptic curves

Let us call $f(x)$ to be a *good polynomial*, if it satisfies the following conditions:

1. $\deg f(x) = 2g + 2$ is even,
2. $f(x)$ is squarefree,
3. $LT(f(x))$ is a quadratic residue,
4. $f(\alpha)$ is a q.r. for all $\alpha \in \mathbb{F}_q$ ($\Rightarrow N^0_{f(x)} = 0,\ N^r_{f(x)} = 2q$).

Let $\mathcal{C}$ be a curve $y^2 = f(x)$ over $\mathbb{F}_q$, where $f(x)$ is good.
Then $\mathcal{C}$ is smooth of genus g having

$$N_1(\mathcal{C}) = N_1(\mathcal{C})^{aff} + N_1(\mathcal{C})^{\infty} = N^0_{f(x)} + 2N^r_{f(x)} + N_1(\mathcal{C})^{\infty} = 2q + 2.$$

We will call such a curve $\mathbb{F}_q$-*maximal*, since $N_1 \leq 2q + 2$ for every hyperelliptic curve over $\mathbb{F}_q$.

Construction of a pointless curve over $\mathbb{F}_q$, odd q

Let $\mathcal{C}$ be a smooth $\mathbb{F}_q$-maximal hyperelliptic curve over $\mathbb{F}_q$. It can be defined by $y^2 = f(x)$, where $f(x)$ is good of degree $2g+2$, where g is the genus of $\mathcal{C}$.

Let $\mathcal{C}'$ be its quadratic twist: $\alpha y^2 = f(x)$, α is a q.n.r.

The Weil theorem implies that

$$\mathrm{Tr}(Fr_{\mathcal{C}}) = q + 1 - N_1(\mathcal{C}) = -q - 1,$$
$$N_1(\mathcal{C}') = q + 1 - \mathrm{Tr}(Fr_{\mathcal{C}'}) = q + 1 + \mathrm{Tr}(Fr_{\mathcal{C}}) = 0,$$

where Fr stands for Frobenius endomorphism.

Thus, $\mathcal{C}'$ is smooth pointless hyperelliptic genus g curve over $\mathbb{F}_q$.

The idea of the search of pointless curves:

good polynomial $f(x)$ over $\mathbb{F}_q \Leftrightarrow$

$\mathbb{F}_q$-maximal curve $y^2 = f(x) \Leftrightarrow$

pointless curve over $\mathbb{F}_q$.

Construction of a pointless curve over $\mathbb{F}_q$, odd q

Let $\mathcal{C}$ be a smooth $\mathbb{F}_q$-maximal hyperelliptic curve over $\mathbb{F}_q$. It can be defined by $y^2 = f(x)$, where $f(x)$ is good of degree $2g+2$, where g is the genus of $\mathcal{C}$.

Let $\mathcal{C}'$ be its quadratic twist: $\alpha y^2 = f(x)$, α is a q.n.r.

The Weil theorem implies that

$$\mathrm{Tr}(Fr_{\mathcal{C}}) = q + 1 - N_1(\mathcal{C}) = -q - 1,$$
$$N_1(\mathcal{C}') = q + 1 - \mathrm{Tr}(Fr_{\mathcal{C}'}) = q + 1 + \mathrm{Tr}(Fr_{\mathcal{C}}) = 0,$$

where Fr stands for Frobenius endomorphism.

Thus, $\mathcal{C}'$ is smooth pointless hyperelliptic genus g curve over $\mathbb{F}_q$.

The idea of the search of pointless curves:

good polynomial $f(x)$ over $\mathbb{F}_q$ $\Leftrightarrow$

$\mathbb{F}_q$-maximal curve $y^2 = f(x)$ $\Leftrightarrow$

pointless curve over $\mathbb{F}_q$.

Construction of a pointless curve over $\mathbb{F}_q$, odd q

Let $\mathcal{C}$ be a smooth $\mathbb{F}_q$-maximal hyperelliptic curve over $\mathbb{F}_q$. It can be defined by $y^2 = f(x)$, where $f(x)$ is good of degree $2g+2$, where g is the genus of $\mathcal{C}$.

Let $\mathcal{C}'$ be its quadratic twist: $\alpha y^2 = f(x)$, α is a q.n.r.

The Weil theorem implies that

$$\mathrm{Tr}(Fr_{\mathcal{C}}) = q + 1 - N_1(\mathcal{C}) = -q - 1,$$
$$N_1(\mathcal{C}') = q + 1 - \mathrm{Tr}(Fr_{\mathcal{C}'}) = q + 1 + \mathrm{Tr}(Fr_{\mathcal{C}}) = 0,$$

where Fr stands for Frobenius endomorphism.

Thus, $\mathcal{C}'$ is smooth pointless hyperelliptic genus g curve over $\mathbb{F}_q$.

The idea of the search of pointless curves:

good polynomial $f(x)$ over $\mathbb{F}_q$ $\Leftrightarrow$

$\mathbb{F}_q$-maximal curve $y^2 = f(x)$ $\Leftrightarrow$

pointless curve over $\mathbb{F}_q$.

Construction of a pointless curve over $\mathbb{F}_q$, odd q

Let $\mathcal{C}$ be a smooth $\mathbb{F}_q$-maximal hyperelliptic curve over $\mathbb{F}_q$. It can be defined by $y^2 = f(x)$, where $f(x)$ is good of degree $2g+2$, where g is the genus of $\mathcal{C}$.

Let $\mathcal{C}'$ be its quadratic twist: $\alpha y^2 = f(x)$, α is a q.n.r.

The Weil theorem implies that

$$\mathrm{Tr}(Fr_{\mathcal{C}}) = q + 1 - N_1(\mathcal{C}) = -q - 1,$$
$$N_1(\mathcal{C}') = q + 1 - \mathrm{Tr}(Fr_{\mathcal{C}'}) = q + 1 + \mathrm{Tr}(Fr_{\mathcal{C}}) = 0,$$

where Fr stands for Frobenius endomorphism.

Thus, $\mathcal{C}'$ is smooth pointless hyperelliptic genus g curve over $\mathbb{F}_q$.

The idea of the search of pointless curves:

good polynomial $f(x)$ over $\mathbb{F}_q$ $\Leftrightarrow$

$\mathbb{F}_q$-maximal curve $y^2 = f(x)$ $\Leftrightarrow$

pointless curve over $\mathbb{F}_q$.

Construction of a pointless curve over $\mathbb{F}_q$, odd q

Let $\mathcal{C}$ be a smooth $\mathbb{F}_q$-maximal hyperelliptic curve over $\mathbb{F}_q$. It can be defined by $y^2 = f(x)$, where $f(x)$ is good of degree $2g+2$, where g is the genus of $\mathcal{C}$.

Let $\mathcal{C}'$ be its quadratic twist: $\alpha y^2 = f(x)$, α is a q.n.r.

The Weil theorem implies that

$$\mathrm{Tr}(Fr_{\mathcal{C}}) = q + 1 - N_1(\mathcal{C}) = -q - 1,$$
$$N_1(\mathcal{C}') = q + 1 - \mathrm{Tr}(Fr_{\mathcal{C}'}) = q + 1 + \mathrm{Tr}(Fr_{\mathcal{C}}) = 0,$$

where Fr stands for Frobenius endomorphism.

Thus, $\mathcal{C}'$ is smooth pointless hyperelliptic genus g curve over $\mathbb{F}_q$.

The idea of the search of pointless curves:

good polynomial $f(x)$ over $\mathbb{F}_q \Leftrightarrow$

$\mathbb{F}_q$-maximal curve $y^2 = f(x) \Leftrightarrow$

pointless curve over $\mathbb{F}_q$.

Linear bound on the genus for odd q

Theorem

Given odd q, for all $g \geq (q-3)/2$ (or $g \geq 2$) there is a pointless smooth hyperelliptic curve over $\mathbb{F}_q$ of genus g.

Idea: for each step find a monic polynomial of degree $2g+2$ having good values and then check whether it is square-free or not.

The proof is divided into three parts, depending on a family of good polynomials.

Note:

1. We omit technical details of proofs of smoothness.
2. We pay attention on the values of polynomials.
3. Some times polynomials can be defined over $\mathbb{F}_p$!

Linear bound on the genus for odd q

Theorem

Given odd q, for all $g \geq (q-3)/2$ (or $g \geq 2$) there is a pointless smooth hyperelliptic curve over $\mathbb{F}_q$ of genus g.

Idea: for each step find a monic polynomial of degree $2g+2$ having good values and then check whether it is square-free or not.

The proof is divided into three parts, depending on a family of good polynomials.

Note:

1. We omit technical details of proofs of smoothness.
2. We pay attention on the values of polynomials.
3. Some times polynomials can be defined over $\mathbb{F}_p$!

Linear bound on the genus for odd q

Theorem

Given odd q, for all $g \geq (q-3)/2$ (or $g \geq 2$) there is a pointless smooth hyperelliptic curve over $\mathbb{F}_q$ of genus g.

Idea: for each step find a monic polynomial of degree $2g+2$ having good values and then check whether it is square-free or not.

The proof is divided into three parts, depending on a family of good polynomials.

Note:

1. We omit technical details of proofs of smoothness.
2. We pay attention on the values of polynomials.
3. Some times polynomials can be defined over $\mathbb{F}_p$!

Linear bound on the genus for odd q

Theorem

Given odd q, for all $g \geq (q-3)/2$ (or $g \geq 2$) there is a pointless smooth hyperelliptic curve over $\mathbb{F}_q$ of genus g.

Idea: for each step find a monic polynomial of degree $2g+2$ having good values and then check whether it is square-free or not.

The proof is divided into three parts, depending on a family of good polynomials.

Note:

1. We omit technical details of proofs of smoothness.
2. We pay attention on the values of polynomials.
3. Some times polynomials can be defined over $\mathbb{F}_p$!

Sketch of proof: part I

Let $g \geq (q-1)/2$.

Special condition on q and g:

1. $\mathcal{D}(q,g) > 2$, or $\mathcal{D}(q,g) = 2$ and $\mathcal{L}(q,g) > 1$, or
2. $\mathcal{D}(q,g) = 2$ and $\mathcal{L}(q,g) = 1$, but one of the following holds:

$$q = p^{2n} \text{ or } q = p^{2n+1},\ p \equiv 1 \pmod 8 \text{ or } 2g+2 \not\equiv -1/2 \pmod p,$$

where $\mathcal{D}(q,g) = \gcd(2g+2, q-1)$, $\mathcal{L}(q,g) = \lfloor (2g+2)/(q-1) \rfloor$.

The polynomial

$$f(x) = x^{2g+2} - x^{2g+2-l(q-1)} + a^2, \quad a \in \mathbb{F}_q^*, \quad 1 \leq l \leq \mathcal{L}(q,g).$$

1. is monic of even degree,
2. has good values over $\mathbb{F}_q$, since $f(x) = \left(x^{l(q-1)} - 1\right) x^* + a^2$,
3. is square-free, when q and g satisfy the condition, which is implied by computation of the discriminant of $f(x)$.

Sketch of proof: part I

Let $g \geq (q-1)/2$.

Special condition on q and g:

1. $\mathcal{D}(q,g) > 2$, or $\mathcal{D}(q,g) = 2$ and $\mathcal{L}(q,g) > 1$, or
2. $\mathcal{D}(q,g) = 2$ and $\mathcal{L}(q,g) = 1$, but one of the following holds:

$$q = p^{2n} \text{ or } q = p^{2n+1},\ p \equiv 1 \pmod 8 \text{ or } 2g+2 \not\equiv -1/2 \pmod p,$$

where $\mathcal{D}(q,g) = \gcd(2g+2, q-1)$, $\mathcal{L}(q,g) = \lfloor (2g+2)/(q-1) \rfloor$.

The polynomial

$$f(x) = x^{2g+2} - x^{2g+2-l(q-1)} + a^2, \quad a \in \mathbb{F}_q^*, \quad 1 \leq l \leq \mathcal{L}(q,g).$$

1. is monic of even degree,
2. has good values over $\mathbb{F}_q$, since $f(x) = (x^{l(q-1)} - 1)\, x^* + a^2$,
3. is square-free, when q and g satisfy the condition, which is implied by computation of the discriminant of $f(x)$.

Sketch of proof: part I

Let $g \geq (q-1)/2$.

Special condition on q and g:

1. $\mathcal{D}(q,g) > 2$, or $\mathcal{D}(q,g) = 2$ and $\mathcal{L}(q,g) > 1$, or
2. $\mathcal{D}(q,g) = 2$ and $\mathcal{L}(q,g) = 1$, but one of the following holds:

$$q = p^{2n} \text{ or } q = p^{2n+1},\ p \equiv 1 \pmod 8 \text{ or } 2g+2 \not\equiv -1/2 \pmod p,$$

where $\mathcal{D}(q,g) = \gcd(2g+2, q-1)$, $\mathcal{L}(q,g) = \lfloor (2g+2)/(q-1) \rfloor$.

The polynomial

$$f(x) = x^{2g+2} - x^{2g+2-l(q-1)} + a^2, \quad a \in \mathbb{F}_q^*, \quad 1 \leq l \leq \mathcal{L}(q,g).$$

1. is monic of even degree,
2. has good values over $\mathbb{F}_q$, since $f(x) = \left(x^{l(q-1)} - 1\right) x^* + a^2$,
3. is square-free, when q and g satisfy the condition, which is implied by computation of the discriminant of $f(x)$.

Sketch of proof: part I

Let $g \geq (q-1)/2$.

Special condition on q and g:

1. $\mathcal{D}(q,g) > 2$, or $\mathcal{D}(q,g) = 2$ and $\mathcal{L}(q,g) > 1$, or
2. $\mathcal{D}(q,g) = 2$ and $\mathcal{L}(q,g) = 1$, but one of the following holds:

$$q = p^{2n} \text{ or } q = p^{2n+1},\ p \equiv 1 \pmod 8 \text{ or } 2g+2 \not\equiv -1/2 \pmod p,$$

where $\mathcal{D}(q,g) = \gcd(2g+2, q-1)$, $\mathcal{L}(q,g) = \lfloor (2g+2)/(q-1) \rfloor$.

The polynomial

$$f(x) = x^{2g+2} - x^{2g+2-l(q-1)} + a^2, \quad a \in \mathbb{F}_q^*, \quad 1 \leq l \leq \mathcal{L}(q,g).$$

1. is monic of even degree,
2. has good values over $\mathbb{F}_q$, since $f(x) = \left(x^{l(q-1)} - 1\right) x^* + a^2$,
3. is square-free, when q and g satisfy the condition, which is implied by computation of the discriminant of $f(x)$.

Sketch of proof: part I

Let $g \geq (q-1)/2$.

Special condition on q and g:

1. $\mathcal{D}(q,g) > 2$, or $\mathcal{D}(q,g) = 2$ and $\mathcal{L}(q,g) > 1$, or
2. $\mathcal{D}(q,g) = 2$ and $\mathcal{L}(q,g) = 1$, but one of the following holds:

$$q = p^{2n} \text{ or } q = p^{2n+1},\ p \equiv 1 \pmod 8 \text{ or } 2g+2 \not\equiv -1/2 \pmod p,$$

where $\mathcal{D}(q,g) = \gcd(2g+2, q-1)$, $\mathcal{L}(q,g) = \lfloor (2g+2)/(q-1) \rfloor$.

The polynomial

$$f(x) = x^{2g+2} - x^{2g+2-l(q-1)} + a^2, \quad a \in \mathbb{F}_q^*, \quad 1 \leq l \leq \mathcal{L}(q,g).$$

1. is monic of even degree,
2. has good values over $\mathbb{F}_q$, since $f(x) = \left(x^{l(q-1)} - 1\right) x^* + a^2$,
3. is square-free, when q and g satisfy the condition, which is implied by computation of the discriminant of $f(x)$.

Sketch of proof: part II

Let $g \geq (q-1)/2$ and the special condition does not hold.

Let $n = 2g + 2 - (q-1)$, and $b, \xi \in \mathbb{F}_p^*$, ξ is a q.n.r.
The polynomial

$$f(x) = x^{q-1+n} + b^2x^{2n} - (2b^2\xi + 1)x^n + b^2\xi^2$$
$$= (x^{q-1} - 1)x^n + b^2(x^n - \xi)^2$$

1. is monic of even degree,
2. has good values (since n is even and ξ is not a q.n.r),
3. is square-free, if one chooses b, given ξ, in the way that

$$s^2 = b^4\xi^2 + 4b^2\xi + 1$$

and $s \neq 0$, $b \neq 0$.

Remark. We have treated all cases for $g \geq (q-1)/2$, so that it suffices to prove the theorem for $g = (q-3)/2$.

Sketch of proof: part II

Let $g \geq (q-1)/2$ and the special condition does not hold.

Let $n = 2g + 2 - (q-1)$, and b, $\xi \in \mathbb{F}_p^*$, ξ is a q.n.r.
The polynomial

$$f(x) = x^{q-1+n} + b^2x^{2n} - (2b^2\xi + 1)x^n + b^2\xi^2$$
$$= (x^{q-1} - 1)x^n + b^2(x^n - \xi)^2$$

1. is monic of even degree,
2. has good values (since n is even and ξ is not a q.n.r),
3. is square-free, if one chooses b, given ξ, in the way that

$$s^2 = b^4\xi^2 + 4b^2\xi + 1$$

and $s \neq 0$, $b \neq 0$.

Remark. We have treated all cases for $g \geq (q-1)/2$, so that it suffices to prove the theorem for $g = (q-3)/2$.

Sketch of proof: part II

Let $g \geq (q-1)/2$ and the special condition does not hold.

Let $n = 2g + 2 - (q-1)$, and b, $\xi \in \mathbb{F}_p^*$, ξ is a q.n.r.
The polynomial

$$f(x) = x^{q-1+n} + b^2x^{2n} - (2b^2\xi + 1)x^n + b^2\xi^2$$
$$= (x^{q-1} - 1)x^n + b^2(x^n - \xi)^2$$

1. is monic of even degree,
2. has good values (since n is even and ξ is not a q.n.r),
3. is square-free, if one chooses b, given ξ, in the way that

$$s^2 = b^4\xi^2 + 4b^2\xi + 1$$

and $s \neq 0$, $b \neq 0$.

Remark. We have treated all cases for $g \geq (q-1)/2$, so that it suffices to prove the theorem for $g = (q-3)/2$.

Sketch of proof: part II

Let $g \geq (q-1)/2$ and the special condition does not hold.

Let $n = 2g + 2 - (q-1)$, and b, $\xi \in \mathbb{F}_p^*$, ξ is a q.n.r.
The polynomial

$$\begin{aligned} f(x) &= x^{q-1+n} + b^2 x^{2n} - (2b^2\xi + 1)x^n + b^2\xi^2 \\ &= (x^{q-1} - 1)x^n + b^2(x^n - \xi)^2 \end{aligned}$$

1. is monic of even degree,
2. has good values (since n is even and ξ is not a q.n.r),
3. is square-free, if one chooses b, given ξ, in the way that

$$s^2 = b^4\xi^2 + 4b^2\xi + 1$$

and $s \neq 0$, $b \neq 0$.

Remark. We have treated all cases for $g \geq (q-1)/2$, so that it suffices to prove the theorem for $g = (q-3)/2$.

Sketch of proof: part II

Let $g \geq (q-1)/2$ and the special condition does not hold.

Let $n = 2g + 2 - (q-1)$, and b, $\xi \in \mathbb{F}_p^*$, ξ is a q.n.r.
The polynomial

$$\begin{aligned} f(x) &= x^{q-1+n} + b^2x^{2n} - (2b^2\xi + 1)x^n + b^2\xi^2 \\ &= (x^{q-1} - 1)x^n + b^2(x^n - \xi)^2 \end{aligned}$$

1. is monic of even degree,
2. has good values (since n is even and ξ is not a q.n.r),
3. is square-free, if one chooses b, given ξ, in the way that

$$s^2 = b^4\xi^2 + 4b^2\xi + 1$$

and $s \neq 0$, $b \neq 0$.

Remark. We have treated all cases for $g \geq (q-1)/2$, so that it suffices to prove the theorem for $g = (q-3)/2$.

Sketch of proof: part II

Let $g \geq (q-1)/2$ and the special condition does not hold.

Let $n = 2g + 2 - (q-1)$, and $b, \xi \in \mathbb{F}_p^*$, ξ is a q.n.r.
The polynomial

$$f(x) = x^{q-1+n} + b^2 x^{2n} - (2b^2\xi + 1)x^n + b^2\xi^2$$
$$= (x^{q-1} - 1)x^n + b^2(x^n - \xi)^2$$

1. is monic of even degree,
2. has good values (since n is even and ξ is not a q.n.r),
3. is square-free, if one chooses b, given ξ, in the way that

$$s^2 = b^4\xi^2 + 4b^2\xi + 1$$

and $s \neq 0$, $b \neq 0$.

Remark. We have treated all cases for $g \geq (q-1)/2$, so that it suffices to prove the theorem for $g = (q-3)/2$.

Sketch of proof: part III

Let $g = (q-3)/2$. We can assume that $q > 5$.

The curve $x^2 + y^2 = \delta^2$ over $\mathbb{F}_q$ has a rational point (x, y) such that $xy \neq 0$.

Let α, β, $\gamma \in \mathbb{F}_q$ be residues such that $\alpha + \beta = \gamma$.

The polynomial

$$f(x) = \frac{\alpha}{\gamma}\left(x^{(q-1)/2} + 1\right)^2 + \frac{\beta}{\gamma}\left(x^{(q-1)/2} - 1\right)^2$$
$$= x^{q-1} + 2\frac{\alpha - \beta}{\gamma}x^{(q-1)/2} + 1.$$

is monic, of even degree and has good values (we have either $f(a) = 4\alpha/\gamma$, or $f(a) = 4\beta/\gamma$, or $f(a) = 1$ for all $a \in \mathbb{F}_q$).

The condition $\alpha\beta \neq 0$ implies that $f(x)$ is square-free. □

Sketch of proof: part III

Let $g = (q-3)/2$. We can assume that $q > 5$.

The curve $x^2 + y^2 = \delta^2$ over $\mathbb{F}_q$ has a rational point (x, y) such that $xy \neq 0$.

Let α, β, $\gamma \in \mathbb{F}_q$ be residues such that $\alpha + \beta = \gamma$.

The polynomial

$$f(x) = \frac{\alpha}{\gamma}\left(x^{(q-1)/2} + 1\right)^2 + \frac{\beta}{\gamma}\left(x^{(q-1)/2} - 1\right)^2$$
$$= x^{q-1} + 2\frac{\alpha-\beta}{\gamma}x^{(q-1)/2} + 1.$$

is monic, of even degree and has good values (we have either $f(a) = 4\alpha/\gamma$, or $f(a) = 4\beta/\gamma$, or $f(a) = 1$ for all $a \in \mathbb{F}_q$).

The condition $\alpha\beta \neq 0$ implies that $f(x)$ is square-free. □

Sketch of proof: part III

Let $g = (q-3)/2$. We can assume that $q > 5$.

The curve $x^2 + y^2 = \delta^2$ over $\mathbb{F}_q$ has a rational point (x, y) such that $xy \neq 0$.

Let α, β, $\gamma \in \mathbb{F}_q$ be residues such that $\alpha + \beta = \gamma$.

The polynomial

$$f(x) = \frac{\alpha}{\gamma}\left(x^{(q-1)/2} + 1\right)^2 + \frac{\beta}{\gamma}\left(x^{(q-1)/2} - 1\right)^2$$
$$= x^{q-1} + 2\frac{\alpha - \beta}{\gamma}x^{(q-1)/2} + 1.$$

is monic, of even degree and has good values (we have either $f(a) = 4\alpha/\gamma$, or $f(a) = 4\beta/\gamma$, or $f(a) = 1$ for all $a \in \mathbb{F}_q$).

The condition $\alpha\beta \neq 0$ implies that $f(x)$ is square-free. □

Sketch of proof: part III

Let $g = (q-3)/2$. We can assume that $q > 5$.

The curve $x^2 + y^2 = \delta^2$ over $\mathbb{F}_q$ has a rational point (x, y) such that $xy \neq 0$.

Let α, β, $\gamma \in \mathbb{F}_q$ be residues such that $\alpha + \beta = \gamma$.

The polynomial

$$f(x) = \frac{\alpha}{\gamma}\left(x^{(q-1)/2} + 1\right)^2 + \frac{\beta}{\gamma}\left(x^{(q-1)/2} - 1\right)^2$$
$$= x^{q-1} + 2\frac{\alpha - \beta}{\gamma}x^{(q-1)/2} + 1.$$

is monic, of even degree and has good values (we have either $f(a) = 4\alpha/\gamma$, or $f(a) = 4\beta/\gamma$, or $f(a) = 1$ for all $a \in \mathbb{F}_q$).

The condition $\alpha\beta \neq 0$ implies that $f(x)$ is square-free. □

Sketch of proof: part III

Let $g = (q-3)/2$. We can assume that $q > 5$.

The curve $x^2 + y^2 = \delta^2$ over $\mathbb{F}_q$ has a rational point (x, y) such that $xy \neq 0$.

Let α, β, $\gamma \in \mathbb{F}_q$ be residues such that $\alpha + \beta = \gamma$.

The polynomial

$$\begin{aligned} f(x) &= \frac{\alpha}{\gamma}\left(x^{(q-1)/2} + 1\right)^2 + \frac{\beta}{\gamma}\left(x^{(q-1)/2} - 1\right)^2 \\ &= x^{q-1} + 2\frac{\alpha - \beta}{\gamma}x^{(q-1)/2} + 1. \end{aligned}$$

is monic, of even degree and has good values (we have either $f(a) = 4\alpha/\gamma$, or $f(a) = 4\beta/\gamma$, or $f(a) = 1$ for all $a \in \mathbb{F}_q$).

The condition $\alpha\beta \neq 0$ implies that $f(x)$ is square-free. □

Hyperelliptic curves over $\mathbb{F}_q$, q is even

This is a completely different case: for every hyperelliptic curve over $\mathbb{F}_{2^n}$

$$y^2 + h(x)y = f(x)$$

we can not let $h(x) = 0$ and it is not trivial to count rational points.

The existence of pointless curves over $\mathbb{F}_2$ is known.

Theorem (H. Stichtenoth, 2011)

For every $g \geq 2$ there is a non-singular pointless curve over $\mathbb{F}_2$.

Goal: study the case $q > 2$.

Hyperelliptic curves over $\mathbb{F}_q$, q is even

This is a completely different case: for every hyperelliptic curve over $\mathbb{F}_{2^n}$

$$y^2 + h(x)y = f(x)$$

we can not let $h(x) = 0$ and it is not trivial to count rational points.

The existence of pointless curves over $\mathbb{F}_2$ is known.

Theorem (H. Stichtenoth, 2011)

For every $g \geq 2$ there is a non-singular pointless curve over $\mathbb{F}_2$.

Goal: study the case $q > 2$.

Hyperelliptic curves over $\mathbb{F}_q$, q is even

This is a completely different case: for every hyperelliptic curve over $\mathbb{F}_{2^n}$

$$y^2 + h(x)y = f(x)$$

we can not let $h(x) = 0$ and it is not trivial to count rational points.

The existence of pointless curves over $\mathbb{F}_2$ is known.

Theorem (H. Stichtenoth, 2011)

For every $g \geq 2$ there is a non-singular pointless curve over $\mathbb{F}_2$.

Goal: study the case $q > 2$.

Linear bound on the genus for even q

Theorem

Let $q = 2^n$, $q > 2$. For every $g \geq q - 1$ there is a pointless smooth curve over $\mathbb{F}_q$ of the form $y^2 + a\,f(x)y = b\,h(x)$, where

$$f(x) = x^{g+1} + x^{g+1-(q-1)} + c, \quad h(x) = x^{2g+2} + x^{2g+2-2(q-1)} + d,$$

for some a, b, c, $d \in \mathbb{F}_q^*$.

The goal: find auxiliary a, b, c, and d in $\mathbb{F}_q^*$.

Proof steps:

1. The smoothness implies a condition on c and d.
2. Choose b, d by a, c (and by two good elements in $\mathbb{F}_q^*$) in order to guaranty the pointlessness.

The condition $q > 2$ is essential for the last step.

Linear bound on the genus for even q

Theorem

Let $q = 2^n$, $q > 2$. For every $g \geq q - 1$ there is a pointless smooth curve over $\mathbb{F}_q$ of the form $y^2 + a\, f(x) y = b\, h(x)$, where

$$f(x) = x^{g+1} + x^{g+1-(q-1)} + c, \quad h(x) = x^{2g+2} + x^{2g+2-2(q-1)} + d,$$

for some a, b, c, $d \in \mathbb{F}_q^*$.

The goal: find auxiliary a, b, c, and d in $\mathbb{F}_q^*$.

Proof steps:

1. The smoothness implies a condition on c and d.
2. Choose b, d by a, c (and by two good elements in $\mathbb{F}_q^*$) in order to guaranty the pointlessness.

The condition $q > 2$ is essential for the last step.

Linear bound on the genus for even q

Theorem

Let $q = 2^n$, $q > 2$. For every $g \geq q - 1$ there is a pointless smooth curve over $\mathbb{F}_q$ of the form $y^2 + a\,f(x)y = b\,h(x)$, where

$$f(x) = x^{g+1} + x^{g+1-(q-1)} + c, \quad h(x) = x^{2g+2} + x^{2g+2-2(q-1)} + d,$$

for some a, b, c, $d \in \mathbb{F}_q^*$.

The goal: find auxiliary a, b, c, and d in $\mathbb{F}_q^*$.

Proof steps:

1. The smoothness implies a condition on c and d.
2. Choose b, d by a, c (and by two good elements in $\mathbb{F}_q^*$) in order to guaranty the pointlessness.

The condition $q > 2$ is essential for the last step.

Sketch of proof: the smoothness

Let $\mathcal{C}$ be a hyperellptic curve over $\mathbb{F}_q$, $q = 2^n$, of the form $y^2 + a\,f(x)y = b\,h(x)$, where

$$f(x) = x^{g+1} + x^{g+1-(q-1)} + c, \quad h(x) = x^{2g+2} + x^{2g+2-2(q-1)} + d,$$

for some $a,\ b,\ c,\ d \in \mathbb{F}_q^*$.

The curve $\mathcal{C}$ is smooth $\Leftrightarrow$ $R(x)$ and $Q(x)$ are comprime, where

$$R(x) = a^2 b\,f'(x)h(x) + b^2\,h'(x)^2, \quad Q(x) = a\,f(x).$$

One can show that

$$\gcd\big(R(x), Q(x)\big) = \gcd\big(h(x), f(x)\big) = \gcd\big(f(x)^2 + c^2 + d, f(x)\big).$$

This implies a condition for the smoothness: $c^2 \neq d$.

Sketch of proof: the smoothness

Let $\mathcal{C}$ be a hyperellptic curve over $\mathbb{F}_q$, $q = 2^n$, of the form $y^2 + a\,f(x)y = b\,h(x)$, where

$$f(x) = x^{g+1} + x^{g+1-(q-1)} + c, \quad h(x) = x^{2g+2} + x^{2g+2-2(q-1)} + d,$$

for some a, b, c, $d \in \mathbb{F}_q^*$.

The curve $\mathcal{C}$ is smooth $\Leftrightarrow$ $R(x)$ and $Q(x)$ are comprime, where

$$R(x) = a^2 b\,f'(x)h(x) + b^2\,h'(x)^2, \quad Q(x) = a\,f(x).$$

One can show that

$$\gcd\big(R(x), Q(x)\big) = \gcd\big(h(x), f(x)\big) = \gcd\big(f(x)^2 + c^2 + d, f(x)\big).$$

This implies a condition for the smoothness: $c^2 \neq d$.

Sketch of proof: the smoothness

Let $\mathcal{C}$ be a hyperellptic curve over $\mathbb{F}_q$, $q = 2^n$, of the form $y^2 + a\,f(x)y = b\,h(x)$, where

$$f(x) = x^{g+1} + x^{g+1-(q-1)} + c, \quad h(x) = x^{2g+2} + x^{2g+2-2(q-1)} + d,$$

for some $a,\ b,\ c,\ d \in \mathbb{F}_q^*$.

The curve $\mathcal{C}$ is smooth $\Leftrightarrow$ $R(x)$ and $Q(x)$ are comprime, where

$$R(x) = a^2 b\, f'(x)h(x) + b^2\, h'(x)^2, \quad Q(x) = a\, f(x).$$

One can show that

$$\gcd\big(R(x), Q(x)\big) = \gcd\big(h(x), f(x)\big) = \gcd\big(f(x)^2 + c^2 + d, f(x)\big).$$

This implies a condition for the smoothness: $c^2 \neq d$.

Sketch of proof : the smoothness

Let $\mathcal{C}$ be a hyperellptic curve over $\mathbb{F}_q$, $q = 2^n$, of the form $y^2 + a\,f(x)y = b\,h(x)$, where

$$f(x) = x^{g+1} + x^{g+1-(q-1)} + c, \quad h(x) = x^{2g+2} + x^{2g+2-2(q-1)} + d,$$

for some $a,\ b,\ c,\ d \in \mathbb{F}_q^*$.

The curve $\mathcal{C}$ is smooth $\Leftrightarrow$ $R(x)$ and $Q(x)$ are comprime, where

$$R(x) = a^2 b\,f'(x)h(x) + b^2\,h'(x)^2, \quad Q(x) = a\,f(x).$$

One can show that

$$\gcd\big(R(x), Q(x)\big) = \gcd\big(h(x), f(x)\big) = \gcd\big(f(x)^2 + c^2 + d, f(x)\big).$$

This implies a condition for the smoothness : $c^2 \neq d$.

Sketch of proof: the lack of $\mathbb{F}_q$-points

$\mathcal{C}$ is the union of

$$y^2 + a\,f(x)y = b\,g(x), \quad y^2 + a\,x^{g+1}f(x)y = b\,x^{2g+2}g(x),$$

$$f(x) = x^{g+1} + x^{g+1-(q-1)} + c, \quad h(x) = x^{2g+2} + x^{2g+2-2(q-1)} + d.$$

Any rational point corresponds to a solution of

$$\text{either } y^2 + y + bd(ac)^{-2} = 0, \text{ or } y^2 + y + ba^{-2} = 0.$$

By Hilbert'90, $\mathcal{C}$ has no rational points iff

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{b}{a^2}\cdot\frac{d}{c^2}\right) = 1 \text{ and } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{b}{a^2}\right) = 1.$$

Set $b = a^2\alpha$ and $d = c^2\beta/\alpha$, where $\alpha, \beta \in \mathbb{F}_q^*$ are distinct of the trace 1 (recall that $q > 2$!). $\square$

Sketch of proof: the lack of $\mathbb{F}_q$-points

$\mathcal{C}$ is the union of

$$y^2 + a\,f(x)y = b\,g(x), \quad y^2 + a\,x^{g+1}f(x)y = b\,x^{2g+2}g(x),$$

$$f(x) = x^{g+1} + x^{g+1-(q-1)} + c, \quad h(x) = x^{2g+2} + x^{2g+2-2(q-1)} + d.$$

Any rational point corresponds to a solution of

$$\text{either } y^2 + y + bd(ac)^{-2} = 0, \text{ or } y^2 + y + ba^{-2} = 0.$$

By Hilbert'90, $\mathcal{C}$ has no rational points iff

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{b}{a^2}\cdot\frac{d}{c^2}\right) = 1 \text{ and } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{b}{a^2}\right) = 1.$$

Set $b = a^2\alpha$ and $d = c^2\beta/\alpha$, where $\alpha, \beta \in \mathbb{F}_q^*$ are distinct of the trace 1 (recall that $q > 2$!). $\square$

Sketch of proof: the lack of $\mathbb{F}_q$-points

$\mathcal{C}$ is the union of

$$y^2 + a\,f(x)y = b\,g(x), \quad y^2 + a\,x^{g+1}f(x)y = b\,x^{2g+2}g(x),$$

$$f(x) = x^{g+1} + x^{g+1-(q-1)} + c, \quad h(x) = x^{2g+2} + x^{2g+2-2(q-1)} + d.$$

Any rational point corresponds to a solution of

$$\text{either } y^2 + y + bd(ac)^{-2} = 0, \text{ or } y^2 + y + ba^{-2} = 0.$$

By Hilbert'90, $\mathcal{C}$ has no rational points iff

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{b}{a^2}\cdot\frac{d}{c^2}\right) = 1 \text{ and } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{b}{a^2}\right) = 1.$$

Set $b = a^2\alpha$ and $d = c^2\beta/\alpha$, where $\alpha, \beta \in \mathbb{F}_q^*$ are distinct of the trace 1 (recall that $q > 2$!). $\square$

Sketch of proof: the lack of $\mathbb{F}_q$-points

$\mathcal{C}$ is the union of

$$y^2 + a\,f(x)y = b\,g(x), \quad y^2 + a\,x^{g+1}f(x)y = b\,x^{2g+2}g(x),$$

$$f(x) = x^{g+1} + x^{g+1-(q-1)} + c, \quad h(x) = x^{2g+2} + x^{2g+2-2(q-1)} + d.$$

Any rational point corresponds to a solution of

$$\text{either } y^2 + y + bd(ac)^{-2} = 0, \text{ or } y^2 + y + ba^{-2} = 0.$$

By Hilbert'90, $\mathcal{C}$ has no rational points iff

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{b}{a^2}\cdot\frac{d}{c^2}\right) = 1 \text{ and } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{b}{a^2}\right) = 1.$$

Set $b = a^2\alpha$ and $d = c^2\beta/\alpha$, where $\alpha, \beta \in \mathbb{F}_q^*$ are distinct of the trace 1 (recall that $q > 2!$). $\square$

The gap

Question: Given q, g, does there exist a smooth curve over $\mathbb{F}_q$ of genus g having no rational points?

1. The Weil-Serre bound implies that if $g < (q+1)/\lfloor 2\sqrt{q} \rfloor$, then the answer is NO.
2. The result implies that if

$$g \geq (q-3)/2, \ q \text{ is odd, or } g \geq q-1, \ q \text{ is even,}$$

   then the answer is YES.

It remains to resolve the question in the case when, given odd or even q, the number g belongs to the gap

$$\left(\frac{q+1}{\lfloor 2\sqrt{q} \rfloor}, \frac{q-3}{2} \right) \text{ or } \left(\frac{q+1}{\lfloor 2\sqrt{q} \rfloor}, q-1 \right), \text{ resp.}$$

The gap

Question: Given q, g, does there exist a smooth curve over $\mathbb{F}_q$ of genus g having no rational points?

1. The Weil-Serre bound implies that if $g < (q+1)/\lfloor 2\sqrt{q} \rfloor$, then the answer is NO.
2. The result implies that if

$$g \geq (q-3)/2,\ q \text{ is odd, or } g \geq q-1,\ q \text{ is even,}$$

then the answer is YES.

It remains to resolve the question in the case when, given odd or even q, the number g belongs to the gap

$$\left(\frac{q+1}{\lfloor 2\sqrt{q} \rfloor}, \frac{q-3}{2} \right) \text{ or } \left(\frac{q+1}{\lfloor 2\sqrt{q} \rfloor}, q-1 \right), \text{ resp.}$$

The gap

Question: Given q, g, does there exist a smooth curve over $\mathbb{F}_q$ of genus g having no rational points?

1. The Weil-Serre bound implies that if $g < (q+1)/\lfloor 2\sqrt{q} \rfloor$, then the answer is NO.
2. The result implies that if

$$g \geq (q-3)/2,\ q \text{ is odd, or } g \geq q-1,\ q \text{ is even,}$$

then the answer is YES.

It remains to resolve the question in the case when, given odd or even q, the number g belongs to the gap

$$\left(\frac{q+1}{\lfloor 2\sqrt{q} \rfloor}, \frac{q-3}{2}\right) \text{ or } \left(\frac{q+1}{\lfloor 2\sqrt{q} \rfloor}, q-1\right), \text{ resp.}$$

The gap

Question: Given q, g, does there exist a smooth curve over $\mathbb{F}_q$ of genus g having no rational points?

1. The Weil-Serre bound implies that if $g < (q+1)/\lfloor 2\sqrt{q} \rfloor$, then the answer is NO.
2. The result implies that if

$$g \geq (q-3)/2,\ q \text{ is odd, or } g \geq q-1,\ q \text{ is even,}$$

   then the answer is YES.

It remains to resolve the question in the case when, given odd or even q, the number g belongs to the gap

$$\left(\frac{q+1}{\lfloor 2\sqrt{q} \rfloor}, \frac{q-3}{2} \right) \text{ or } \left(\frac{q+1}{\lfloor 2\sqrt{q} \rfloor}, q-1 \right), \text{ resp.}$$

More good polynomials

Let q be odd. Let $g(x)$, $h(x)$ be two monic polynomials of degree n and m, an let $b \in \mathbb{F}_q$.
Define

$$F_{g,h}(x) = \frac{g(x)^2 - b^2 h(x)^2}{2} x^{\frac{q-1}{2}} + \frac{g(x)^2 + b^2 h(x)^2}{2}.$$

It has almost good value set:

$$F_{g,h}(\alpha) = \begin{cases} g(\alpha)^2, & \alpha \text{ is a q.r.,} \\ b^2 h(\alpha)^2, & \alpha \text{ is a q.n.r.,} \\ \frac{g(0)^2 + b^2 h(0)^2}{2}, & \alpha = 0. \end{cases}$$

- We can choose m compare to n, depending on $q \pmod 4$.
- We can choose b using the intersection of two quadrics in $\mathbb{F}_q^3$ (to make $F_{g,h}(0)$ and $LT(F_{g,h}(x))$ to be q.rr.), that is — an elliptic curve over $\mathbb{F}_q$!
- Is $F_{g,h}(x)$ square-free? In the greate majority of cases - YES (experiments).

More good polynomials

Let q be odd. Let $g(x)$, $h(x)$ be two monic polynomials of degree n and m, an let $b \in \mathbb{F}_q$.
Define

$$F_{g,h}(x) = \frac{g(x)^2 - b^2 h(x)^2}{2} x^{\frac{q-1}{2}} + \frac{g(x)^2 + b^2 h(x)^2}{2}.$$

It has almost good value set:

$$F_{g,h}(\alpha) = \begin{cases} g(\alpha)^2, & \alpha \text{ is a q.r.,} \\ b^2 h(\alpha)^2, & \alpha \text{ is a q.n.r.,} \\ \frac{g(0)^2 + b^2 h(0)^2}{2}, & \alpha = 0. \end{cases}$$

- We can choose m compare to n, depending on $q \pmod 4$.
- We can choose b using the intersection of two quadrics in $\mathbb{F}_q^3$ (to make $F_{g,h}(0)$ and $LT(F_{g,h}(x))$ to be q.rr.), that is — an elliptic curve over $\mathbb{F}_q$!
- Is $F_{g,h}(x)$ square-free? In the greate majority of cases - YES (experiments).

More good polynomials

Let q be odd. Let $g(x)$, $h(x)$ be two monic polynomials of degree n and m, an let $b \in \mathbb{F}_q$.
Define

$$F_{g,h}(x) = \frac{g(x)^2 - b^2 h(x)^2}{2} x^{\frac{q-1}{2}} + \frac{g(x)^2 + b^2 h(x)^2}{2}.$$

It has almost good value set:

$$F_{g,h}(\alpha) = \begin{cases} g(\alpha)^2, & \alpha \text{ is a q.r.,} \\ b^2 h(\alpha)^2, & \alpha \text{ is a q.n.r.,} \\ \frac{g(0)^2 + b^2 h(0)^2}{2}, & \alpha = 0. \end{cases}$$

- We can choose m compare to n, depending on $q \pmod 4$.
- We can choose b using the intersection of two quadrics in $\mathbb{F}_q^3$ (to make $F_{g,h}(0)$ and $LT(F_{g,h}(x))$ to be q.rr.), that is — an elliptic curve over $\mathbb{F}_q$!
- Is $F_{g,h}(x)$ square-free? In the greate majority of cases - YES (experiments).

More good polynomials

Let q be odd. Let $g(x)$, $h(x)$ be two monic polynomials of degree n and m, an let $b \in \mathbb{F}_q$.
Define

$$F_{g,h}(x) = \frac{g(x)^2 - b^2 h(x)^2}{2} x^{\frac{q-1}{2}} + \frac{g(x)^2 + b^2 h(x)^2}{2}.$$

It has almost good value set:

$$F_{g,h}(\alpha) = \begin{cases} g(\alpha)^2, & \alpha \text{ is a q.r.,} \\ b^2 h(\alpha)^2, & \alpha \text{ is a q.n.r.,} \\ \frac{g(0)^2 + b^2 h(0)^2}{2}, & \alpha = 0. \end{cases}$$

- We can choose m compare to n, depending on $q \pmod 4$.
- We can choose b using the intersection of two quadrics in $\mathbb{F}_q^3$ (to make $F_{g,h}(0)$ and $LT(F_{g,h}(x))$ to be q.rr.), that is — an elliptic curve over $\mathbb{F}_q$!
- Is $F_{g,h}(x)$ square-free? In the greate majority of cases - YES (experiments).

More good polynomials

Let q be odd. Let $g(x)$, $h(x)$ be two monic polynomials of degree n and m, an let $b \in \mathbb{F}_q$.
Define

$$F_{g,h}(x) = \frac{g(x)^2 - b^2 h(x)^2}{2} x^{\frac{q-1}{2}} + \frac{g(x)^2 + b^2 h(x)^2}{2}.$$

It has almost good value set:

$$F_{g,h}(\alpha) = \begin{cases} g(\alpha)^2, & \alpha \text{ is a q.r.,} \\ b^2 h(\alpha)^2, & \alpha \text{ is a q.n.r.,} \\ \frac{g(0)^2 + b^2 h(0)^2}{2}, & \alpha = 0. \end{cases}$$

- We can choose m compare to n, depending on $q \pmod 4$.
- We can choose b using the intersection of two quadrics in $\mathbb{F}_q^3$ (to make $F_{g,h}(0)$ and $LT(F_{g,h}(x))$ to be q.rr.), that is — an elliptic curve over $\mathbb{F}_q$!
- Is $F_{g,h}(x)$ square-free? In the greate majority of cases - YES (experiments).

Work in progress

Let q be odd.

1. There is a binary linear code over $\mathbb{F}_q$ defined by parity-check matrix such that:
   - This matrix depends only on the arithmetic of $\mathbb{F}_q$ possessing several properties.
   - Each codeword of weight w corresponds to a pointless smooth curve over $\mathbb{F}_q$ of genus $w-1$.
   - **Problem**: find the minimum distance, the weight enumerator and so on.
2. The generation function $\sum a_n z^n$ of the class of polynomials with good values.
   - a_n, $n \geq q$, are computed.
   - $a_n > 0$, $(q-1)/2 \leq n \leq q-1$ (more explicit constructions!).
   - a_n, $0 \leq n \leq q-1$ depends only on the generation function $\sum b_n z^n$ of the class of square-free polynomials with good values.
   - **Problem**: find the minimal n_0 such that for all $n \geq n_0$ we have $b_n > 0$.