

A Note on Plane Pointless Curves

Sergey Yekhanin
MIT
yekhanin@mit.edu

Abstract

Let $d(q)$ denote the minimal degree of a smooth projective plane curve that is defined over the finite field \mathbb{F}_q and does not contain \mathbb{F}_q rational points. We are interested in the asymptotic behavior of $d(q)$ for $q \rightarrow \infty$. To the best of the author's knowledge the problem of estimating the asymptotic behavior of $d(q)$ was not considered previously. In this note we establish the following bounds:

$$\frac{1}{4} \leq \varliminf_{q \rightarrow \infty} \log_q d(q) \leq \frac{1}{3}. \quad (1)$$

More specifically, for every characteristic $p > 3$ we construct a sequence of pointless Fermat curves

$$x^{d_k} + y^{d_k} + z^{d_k} = 0, \text{ over } \mathbb{F}_{p^{m_k}},$$

such that $\lim_{k \rightarrow \infty} \log_{p^{m_k}} d_k = 1/3$.

1 Lower bound

Let χ be a smooth projective plane pointless curve of degree $d(q)$ over \mathbb{F}_q . From the Hasse-Weil bound we have:

$$|N_q(\chi) - (q + 1)| \leq (d(q) - 1)(d(q) - 2)\sqrt{q}. \quad (2)$$

Combining (2) with $N_q(\chi) = 0$, we obtain:

$$q + 1 \leq (d(q) - 1)(d(q) - 2)\sqrt{q}.$$

This implies $d(q) \geq q^{1/4}$ and the left-hand side of (1) follows.

2 Cyclic three independent subsets of \mathbb{F}_q^m and pointless Fermat curves

In this section we introduce the notion of cyclic three independent subsets of \mathbb{F}_q^m . We demonstrate that large cyclic three independent sets yield low degree pointless Fermat curves.

Definition 1 Let $C \subseteq \mathbb{F}_q^m \setminus \{0\}$. We say that C is a three independent set if for any three elements $x, y, z \in C \cup \{0\}$, $x + y + z = 0$ implies $x = y = z = 0$.

Note that nonempty three independent subsets of \mathbb{F}_q^m exist only if $\text{char } \mathbb{F}_q > 3$.

Definition 2 Let $C \subseteq \mathbb{F}_q^m$ be a three independent subset. We say that C is a cyclic three independent subset if C is a subgroup of $\mathbb{F}_{q^m}^*$ (under the standard bijection between \mathbb{F}_q^m and \mathbb{F}_{q^m}), i.e., for some integer D that divides $q^m - 1$, we have:

$$C = \{x \in \mathbb{F}_{q^m} \mid x^D = 1\}. \quad (3)$$

Lemma 3 Let C be a subset of \mathbb{F}_q^m defined by (3). Let $d = (q^m - 1)/D$. Consider the regular projective curve χ defined by

$$X^d + Y^d + Z^d = 0 \quad (4)$$

over the field \mathbb{F}_{q^m} . Suppose C is a cyclic three independent set; then χ is pointless over \mathbb{F}_{q^m} .

Proof: Assume to the contrary that there exist $X, Y, Z \in \mathbb{F}_{q^m}$ (not all simultaneously zero) such that (4) holds. Denote $x = X^d$, $y = Y^d$ and $z = Z^d$. Clearly, $x, y, z \in C \cup \{0\}$. Now (4) can be rewritten as

$$x + y + z = 0. \quad (5)$$

Thus we arrive at a contradiction. ■

In the next section we present a construction of cyclic three independent subsets of \mathbb{F}_q^m with $D \approx q^{2m/3}$, that works for $\text{char } \mathbb{F}_q > 3$. Lemma 3 translates our subsets into Fermat curves of degree $d \approx q^{m/3}$ that are pointless over \mathbb{F}_{q^m} . This way the upper bound in (1) is proven.

Three independent subsets of \mathbb{F}_q^m are related to caps in the projective space $\text{PG}(m - 1, q)$. A cap is simply a set of points in $\text{PG}(m - 1, q)$, such that no three points are collinear. A three independent subset $C \subseteq \mathbb{F}_q^m$ satisfying a stronger constraint that any three elements of C are linearly independent over \mathbb{F}_q defines a cap in $\text{PG}(m - 1, q)$. Three independent sets that we construct do satisfy this constraint. Projective caps have an extensive literature. For instance see [1, 2, 3, 4].

3 The construction

We start with a very simple lemma:

Lemma 4 Let $x \in \mathbb{F}_q$, where q is odd. Then

$$x^{\frac{(q^2+1)}{2}} = x^{(q-1)\frac{(q+1)}{2}+1} = x.$$

We need the following lemma [5, theorem 7.23]:

Lemma 5 Consider the projective Hermitian curve H defined by

$$x^{q+1} + y^{q+1} + z^{q+1} = 0. \quad (6)$$

The set of \mathbb{F}_{q^4} rational points of H is exactly the set of \mathbb{F}_{q^2} rational points of H .

Now we define a subgroup $S_q \subseteq \mathbb{F}_{q^4}^*$. Understanding the structure of S_q will lead us to several results concerning cyclic three independent sets. Let

$$S_q = \{x \in \mathbb{F}_{q^4} \mid x^{(q^2+1)(q-1)} = 1\}. \quad (7)$$

The following theorem has previously appeared in [3] and [7]. We present a new short proof.

Theorem 6 (Decomposition) *The set S_q can be partitioned into $q^2 + 1$ sets C_i*

$$S_q = \bigcup_{i=1}^{q^2+1} C_i, \quad (8)$$

such that the following two conditions are satisfied:

- Each C_i has the form $C_i = c_i * F_q^*$ for some $c_i \in \mathbb{F}_{q^4}$.
- Let a, b, c be three elements of S_q that are linearly dependent over \mathbb{F}_q ; then there exists a set C_i (in decomposition (8)) such that $\{a, b, c\} \in C_i$.

Proof: Let a, b, c be elements of S_q that are linearly dependent over \mathbb{F}_q . Our goal is to demonstrate that b/a and c/a are in \mathbb{F}_q . Note that $\{a, b, c\} \subseteq S_q$ implies that for some $A, B, C \in \mathbb{F}_{q^4}$ we have $a = A^{q+1}$, $b = B^{q+1}$ and $c = C^{q+1}$. Thus for some λ_a, λ_b and λ_c in \mathbb{F}_q (not all simultaneously zero) we have

$$\lambda_a A^{q+1} + \lambda_b B^{q+1} + \lambda_c C^{q+1} = 0. \quad (9)$$

Using the basic properties of the norm function we conclude that there exist L_a, L_b, L_c in \mathbb{F}_{q^2} such that $\lambda_a = L_a^{q+1}$, $\lambda_b = L_b^{q+1}$ and $\lambda_c = L_c^{q+1}$. Therefore we can rewrite (9) as

$$(L_a A)^{q+1} + (L_b B)^{q+1} + (L_c C)^{q+1} = 0. \quad (10)$$

Without loss of generality we assume that L_a is nonzero. Lemma 5 implies that $L_b B / L_a A$ and $L_c C / L_a A$ are in \mathbb{F}_{q^2} . This in turn implies $\{B/A, C/A\} \subseteq \mathbb{F}_{q^2}$, and finally $\{b/a, c/a\} \subseteq \mathbb{F}_q$. ■

Let W be a subgroup of $S_{q^t} \subseteq \mathbb{F}_{q^{4t}}$, for some integer $t \geq 1$. Theorem 6 implies that in order to verify that W is a three independent set it suffices to verify that $W \cap \mathbb{F}_{q^t}$ is a three independent set.

Corollary 7 *Let $\text{char } \mathbb{F}_q > 3$; then $V = \{x \in \mathbb{F}_{q^4} \mid x^{(q^2+1)/2} = 1\}$ is a cyclic three independent set.*

Proof: Clearly, $V \subseteq S_q$. According to Theorem 6 it suffices to verify that $V \cap \mathbb{F}_q$ is a three independent set. However every $x \in V \cap \mathbb{F}_q$ should satisfy

$$x^{\frac{(q^2+1)}{2}} = 1.$$

By Lemma 4 this implies $x = 1$. Using the assumption that $\text{char } \mathbb{F}_q > 3$ we conclude that $V \cap \mathbb{F}_q$ is a three independent set. ■

Now we are ready to present our main construction. This construction can be viewed as a result of recursive application of the following folklore construction for projective caps. Let C be a cap in $\text{PG}(m-1, q^n)$ represented by elements of $\mathbb{F}_{q^{mn}}$. Let D be cap in $\text{PG}(n-1, q)$ represented by elements of \mathbb{F}_{q^n} . Then $CD = \{cd \mid c \in C, d \in D\}$ is a cap in $\text{PG}(nm-1, q)$.

Theorem 8 *Let $k \geq 0$ and $\text{char } \mathbb{F}_q > 3$. Consider the subgroup $W \subseteq \mathbb{F}_{q^{4*4^k}}^*$ defined by:*

$$W = \{x \in \mathbb{F}_{q^{4*4^k}} \mid x^{((q^{2*4^k}+1)/2)((q^{2*4^{k-1}}+1)/2)\dots((q^2+1)/2)} = 1\}. \quad (11)$$

Our claim is that W is a cyclic three independent set.

Proof: The proof is by induction on k . Suppose $k = 0$; then (11) states that the set $\{x \in \mathbb{F}_{q^4} \mid x^{(q^2+1)/2} = 1\}$ is a cyclic three independent set, which is true by corollary 7. Assume we have proved our claim for $k^* = k - 1$. Let us establish it for k .

It is easy to verify that

$$\frac{(q^{4*4^k} - 1)}{((q^{2*4^k} + 1)/2)((q^{2*4^{k-1}} + 1)/2) \dots ((q^2 + 1)/2)} = 2^{k+1}(q^{4^k} + 1)(q^{4^{k-1}} + 1) \dots (q^4 + 1)(q^2 - 1) \quad (12)$$

is an integer divisible by $(q^{4^k} + 1)$. Therefore $W \subseteq S_{q^{4^k}}$. Theorem 6 implies that in order to prove that W is a three independent set it suffices to prove that $W \cap \mathbb{F}_{q^{4^k}} = W \cap \mathbb{F}_{q^{4*4^{k-1}}}$ is a three independent set. By Lemma 4 for every $x \in \mathbb{F}_{q^{4^k}}$:

$$x^{((q^{2*4^k} + 1)/2)((q^{2*4^{k-1}} + 1)/2) \dots ((q^2 + 1)/2)} = x^{((q^{2*4^{k-1}} + 1)/2) \dots ((q^2 + 1)/2)}.$$

Therefore W restricted to $\mathbb{F}_{q^{4*4^{k-1}}}$ takes the form:

$$W \cap \mathbb{F}_{q^{4*4^{k-1}}} = \{x \in \mathbb{F}_{q^{4*4^{k-1}}} \mid x^{((q^{2*4^{k-1}} + 1)/2) \dots ((q^2 + 1)/2)} = 1\}. \quad (13)$$

Using the inductive assumption we conclude that $W \cap \mathbb{F}_{q^{4*4^{k-1}}}$ is a three independent set. Therefore W is a three independent set. ■

An application of Lemma 3 to sets from Theorem 8 yields the following

Theorem 9 *Suppose $\text{char } \mathbb{F}_q > 3$ and $k \geq 0$; then the Fermat curve:*

$$x^{d_k} + y^{d_k} + z^{d_k} = 0$$

with

$$d_k = 2^{k+1}(q^{4^k} + 1)(q^{4^{k-1}} + 1) \dots (q^4 + 1)(q^2 - 1)$$

is pointless over the field $\mathbb{F}_{q^{4^{k+1}}}$.

It remains to estimate the asymptotic parameters of the family of pointless curves coming from Theorem 9. Clearly,

$$\lim_{k \rightarrow \infty} \log_{q^{4^{k+1}}} \left(2^{k+1} \left(\prod_{i=1}^k (q^{4^i} + 1) \right) (q^2 - 1) \right) = 1/3.$$

This completes the proof of the right hand side of (1).

References

- [1] J. Bierbrauer, A. Cossidente, Y. Edel, "Caps on classical varieties and their projections," *European Journal of Combinatorics* vol. 22, pp. 135-143, 2001.
- [2] A. Cossidente, L. Storme, "Cyclic and Elementary Abelian Caps in Projective Spaces," *Discrete Mathematics* vol. 208/209, pp. 139-156, 1999.

- [3] G. L. Ebert, "Partitioning projective geometries into caps," *Can. J. Math.* vol. 37, pp. 1163-1175, 1985.
- [4] Y. Edel, J. Bierbrauer, "Recursive Constructions for Large Caps," *Bulletin of the Belgian Mathematical Society - Simon Stevin* vol. 6, pp. 249-258, 1999.
- [5] J.W.P. Hirschfeld, *Projective Geometries Over Finite Fields*. Oxford University Press, second edition, 1998.
- [6] G. Korchmáros, T. Szonyi "Fermat Curves over Finite Fields and Cyclic Subsets in High-Dimensional Projective Spaces," *Finite Fields and Their Applications* vol. 5, pp. 206-217, 1999.
- [7] T. Szőnyi, "On Cyclic Caps in Projective Spaces," *Designs, Codes and Cryptography* vol 8, pp. 327-332, 1996.