On monomial complete permutation polynomials

Daniele Bartoli, Massimo Giulietti and Giovanni Zini *

This is a post-peer-review, pre-copyedit version of an article published in Finite Fields and Their Applications. The final authenticated version is available online at `https://doi.org/10.1016/j.ffa.2016.06.005`
Copyright © 2016. This manuscript version is made available under the CC BY-NC-ND 4.0 license `http://creativecommons.org/licenses/by-nc-nd/4.0`

Abstract

We investigate monomials ax^d over the finite field with q elements $\mathbb{F}_q$, in the case where the degree d is equal to $\frac{q-1}{q'-1}+1$ with $q=(q')^n$ for some n. For $n=6$ we explicitly list all a's for which ax^d is a complete permutation polynomial (CPP) over $\mathbb{F}_q$. Some previous characterization results by Wu et al. for $n=4$ are also made more explicit by providing a complete list of a's such that ax^d is a CPP. For odd n, we show that if q is large enough with respect to n then ax^d cannot be a CPP over $\mathbb{F}_q$, unless q is even, $n \equiv 3 \pmod 4$, and the trace $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q'}}(a^{-1})$ is equal to 0.

Keywords: Permutation polynomials; Complete permutation polynomials; Bent-negabent boolean functions.

1 Introduction

Let $\mathbb{F}_\ell$, $\ell = p^h$, p prime, denote the finite field of order ℓ. A *permutation polynomial* (or PP) $f(x) \in \mathbb{F}_\ell[x]$ is a bijection of $\mathbb{F}_\ell$ onto itself. A polynomial $f(x) \in \mathbb{F}_\ell[x]$ is a *complete permutation polynomial* (or CPP), if both $f(x)$ and $f(x)+x$ are permutation polynomials of $\mathbb{F}_\ell$. Both permutation polynomials and complete permutation polynomials have been

*The research of D. Bartoli, M. Giulietti, and G. Zini was supported in part by Ministry for Education, University and Research of Italy (MIUR) (Project PRIN 2012 "Geometrie di Galois e strutture di incidenza" - Prot. N. 2012XZE22K_005) and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

extensively studied also because of their applications to cryptography and combinatorics; see for instance [6, 8, 11, 12, 16, 20] and the references therein. In particular, CPPs over fields of characteristic 2 give rise to bent-negabent boolean functions, which are a useful tool in cryptography; see [14].

Some families of CPPs are obtained in [6, 8, 11, 13, 18, 20]. Nevertheless, CPPs seem to be very rare objects, even if we restrict to the monomial case. It is easily seen that a monomial ax^d is a CPP if and only if $(d, \ell - 1) = 1$ and $x^d + \frac{x}{a}$ is a PP. This motivates the investigation of permutation binomials of type $x^d + bx$ for $d = (\ell - 1)/m + 1$ with m a divisor of $\ell - 1$.

In [3–5, 20, 21] PPs of type $f_b(x) = x^{\frac{q^n-1}{q-1}+1} + bx$ over $\mathbb{F}_{q^n}$ are thoroughly investigated for $n = 2$, $n = 3$, and $n = 4$. For $n = 6$, sufficient conditions for f_b to be a PP of $\mathbb{F}_{q^6}$ are provided in [20, 21] in the special cases of characteristic $p \in \{2, 3, 5\}$. The case $p = n + 1$ is dealt with in [10].

In this paper, we provide a complete classification of permutation polynomials f_b in the case $n = 6$, for arbitrary q. Theorems 1.1 and 1.2 list explicitely for $q \geq 421$ all elements $b \in \mathbb{F}_{q^6} \setminus \mathbb{F}_q$ such that f_b is a PP. For smaller values of q, Theorems 1.1 and 1.2 provide families of PPs of type f_b. We also determine the number of PPs of type f_b for $q \geq 421$; see Corollary 3.3. It should be noted that for $p = 7$, the sufficient condition in [10] for f_b to be a PP is that $b^{q-1} = -1$; our results show that this is not a necessary condition.

Our methods also work for $n = 4$. This allows us to list PPs of type f_b for $n = 4$; see Remark 3.4. In this way, a more explicit description of the necessary and sufficient conditions of [21, Theorem 4.1] is given.

In the paper the case n odd is dealt with as well. Note that for n odd f_b being a PP implies that $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is a CPP only for $p = 2$. We show that if p does not divide $(n+1)/2$ or $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q'}}(b) \neq 0$, then for q large enough with respect to n the polynomial f_b is never a PP; see Theorem 4.2. This shows that for n odd the monomial $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is never a CPP unless $n \equiv 3 \pmod 4$. For $n = 3$ Theorem 4.2 provides a shorter proof of the results of [5, Section 3].

A key tool in our investigation is the following criterion from [13], which relates the existence of a suitable $\mathbb{F}_q$-rational point of some algebraic curve to f_b being a PP or not.

Niederreiter-Robinson Criterion. *The polynomial*

$$f_b(x) = x^{\frac{q^n-1}{q-1}+1} + bx \tag{1}$$

is a PP of $\mathbb{F}_{q^n}$ *if and only if* $b \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ *and the following inequality*

$$x(x+b)^{\frac{q^n-1}{q-1}} \neq y(y+b)^{\frac{q^n-1}{q-1}} \tag{2}$$

holds for all $x, y \in \mathbb{F}_q$ *such that* $x \neq 0$, $y \neq 0$, *and* $x \neq y$.

The well-known Hasse-Weil bound will be applied to an algebraic curve related to Condition (2).

Hasse-Weil Bound. [17, Theorem 5.2.3] *Let $\mathcal{X}$ be an absolutely irreducible curve defined over $\mathbb{F}_q$ with genus g. The number N of $\mathbb{F}_q$-rational places of $\mathcal{X}$ satisfies*

$$|N-(q+1)| \leq 2g\sqrt{q}.$$

Our results for $n=6$ are Theorems 1.1 and 1.2 below.

Theorem 1.1. *Let $q=p^h$ with $p \neq 7$, and let ξ be a primitive 7-th root of unity in $\mathbb{F}_{q^6}$; define $\alpha=\xi^4-\xi^3$. Let ϵ be a primitive element of $\mathbb{F}_q$. If $q \geq 421$, then f_b is a PP if and only if one of the following cases occurs.*

- $q \equiv 3,5 \pmod 7$,
$$b \in \left\{ \frac{t(1-\xi^i)}{7} \;\middle|\; i=1,\ldots,6,\, t \in \mathbb{F}_q^* \right\}. \tag{3}$$

- q *odd,* $q \equiv 3 \pmod 7$,
$$b \in \left\{ \frac{-\alpha^{2q}u+\alpha s}{14}, \frac{-\alpha^{2q^2}u+\alpha^q s}{14}, \frac{-\alpha^2 u+\alpha^{q^2} s}{14} \;\middle|\; u,s \in \mathbb{F}_q, u \neq \pm s \right\}. \tag{4}$$

- q *odd,* $q \equiv 5 \pmod 7$,
$$b \in \left\{ \frac{-\alpha^{2q^2}u+\alpha s}{14}, \frac{-\alpha^2 u+\alpha^q s}{14}, \frac{-\alpha^{2q} u+\alpha^{q^2} s}{14} \;\middle|\; u,s \in \mathbb{F}_q, u \neq \pm s \right\}. \tag{5}$$

- q *odd,* $q \equiv 2 \pmod 7$,
$$b \in \left\{ \frac{-\alpha^{2q^2}u+\alpha s\sqrt{\epsilon}}{14}, \frac{-\alpha^2 u+\alpha^q s\sqrt{\epsilon}}{14}, \frac{-\alpha^{2q} u+\alpha^{q^2} s\sqrt{\epsilon}}{14} \;\middle|\; (u,s) \in \mathbb{F}_q^2 \setminus \{(0,0)\} \right\}. \tag{6}$$

- q *odd,* $q \equiv 4 \pmod 7$,
$$b \in \left\{ \frac{-\alpha^{2q}u+\alpha s\sqrt{\epsilon}}{14}, \frac{-\alpha^{2q^2} u+\alpha^q s\sqrt{\epsilon}}{14}, \frac{-\alpha^{2} u+\alpha^{q^2} s\sqrt{\epsilon}}{14} \;\middle|\; (u,s) \in \mathbb{F}_q^2 \setminus \{(0,0)\} \right\}. \tag{7}$$

- q *even,* $q \equiv 2,4 \pmod 7$.
$$b \in \left\{ (\xi+1)t, (\xi+1)^2 t, (\xi+1)^4 t \;\middle|\; t \in \mathbb{F}_q^* \right\}. \tag{8}$$

- $q=2^h$, $q\equiv 2,4 \pmod 7$. *Assume without loss of generality that* ξ *satisfies* $\xi^3=\xi+1$, *and fix an element* k *such that* $\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_2}(k)=1$. *Define* $\delta_i(u,v)=\frac{v}{u^2}+(\xi+1)^{2^i}$, $i=0,1,2$, *and* $y_i=y_i(u,v)=k\delta_i^2(u,v)+(k+k^2)\delta_i^4(u,v)+\cdots+(k+k^2+\cdots+k^{2^{6h-2}})\delta_i^{2^{6h-1}}(u,v)$; *then*

$$b\in\left\{y_i(\xi+1)^{2^{i+1}}u,(y_i+1)(\xi+1)^{2^{i+1}}u\Big|u\in\mathbb{F}_q^*,\ \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\big(\frac{v}{u^2}\big)\equiv(h-1)\pmod 2\right\} \quad (9)$$

  for some $i=0,1,2$.

If $q<421$, *then the above conditions are sufficient for* f_b *to be a permutation polynomial.*

Theorem 1.2. *Let* $q=7^h$. *Let* $\xi\in\mathbb{F}_{343}$ *be such that* $\xi^{18}=1$ *and let* z *be a* 6*-th root of a fixed primitive element of* $\mathbb{F}_q$. *If* $q\geq 421$, *then the polynomial* f_b *is a PP in* $\mathbb{F}_{q^6}$ *if and only if one of the following cases occurs.*

- $$b\in\left\{tz,tz^5\ \mid\ t\in\mathbb{F}_q^*\right\}. \quad (10)$$

- h *is even and*

$$b\in\left\{-2\xi t+\epsilon\frac{3s}{t}\ \Big|\ 3t^3 \text{ is not a cube in } \mathbb{F}_q,\ s\in\mathbb{F}_q\right\}. \quad (11)$$

- h *is odd and*

$$b\in\left\{-2\xi t+\epsilon\frac{3s}{t}\ \Big|\ 3t^3 \text{ is not a cube in } \mathbb{F}_q,\ s\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q,\ s^2\in\mathbb{F}_q\right\}. \quad (12)$$

- $$b\in\left\{-\xi t\mid 3t^3 \text{ is not a cube in } \mathbb{F}_q\right\}. \quad (13)$$

- $$b\in\left\{3t\mid t\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q,\ t^2\in\mathbb{F}_q^*\right\}. \quad (14)$$

- $$b\in\left\{3t+3s+\frac{s^2}{t}\ \Big|\ t\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q,\ s\in\mathbb{F}_{q^3}\setminus\mathbb{F}_q,\ t^2\in\mathbb{F}_q^*,\ s^3\in\mathbb{F}_q^*\right\}. \quad (15)$$

If $q<421$, *then the above conditions are sufficient for* f_b *to be a permutation polynomial.*

The paper is organized as follows. In Section 2 we provide necessary and sufficient conditions for f_b to be a PP of $\mathbb{F}_{q^6}$ when $q \geq 421$; to this aim, we study the reducibility of an algebraic curve associated to f_b and discuss the existence of some $\mathbb{F}_q$-rational points. In Section 3 we present the proofs of Theorems 1.1 and 1.2; as a consequence, Corollary 3.3 gives the exact number of PPs of type f_b for $q \geq 421$, and a lower bound for $q < 421$. Remark 3.4 shows that the techniques used in Section 3 can be applied also to other types of permutation polynomials; in particular, PPs of $\mathbb{F}_{q^4}$ of type $x^{\frac{q^4-1}{q-1}+1} + bx$ are listed. In this way, the characterization given in [21, Theorem 4.1] is made more explicit. Finally, in Section 4 we deal with the odd n case.

2 Some auxiliary curves associated to f_b for $n = 6$

Our results on polynomials f_b, for $b \in \mathbb{F}_{q^6} \setminus \mathbb{F}_q$, involve elementary symmetric polynomials in b^{q^j}, for $j = 0, \ldots, 5$. Throughout the paper, let

$$\begin{aligned} A &= \sum_{0\leq j\leq 5} b^{q^j}, \qquad B = \sum_{0\leq j_1<j_2\leq 5} b^{q^{j_1}+q^{j_2}}, \qquad C = \sum_{0\leq j_1<j_2<j_3\leq 5} b^{q^{j_1}+q^{j_2}+q^{j_3}} \\ D &= \sum_{0\leq j_1<\ldots<j_4\leq 5} b^{q^{j_1}+q^{j_2}+q^{j_3}+q^{j_4}}, \qquad E = \sum_{0\leq j_1<\ldots<j_5\leq 5} b^{q^{j_1}+q^{j_2}+q^{j_3}+q^{j_4}+q^{j_5}}, \end{aligned} \tag{16}$$

and

$$F = b^{1+q+q^2+q^3+q^4+q^5}.$$

Note that $A, B, C, D, E, F \in \mathbb{F}_q$. The aim of this section is to prove the following theorems which characterize PPs of type f_b.

Theorem 2.1. *Let $p \neq 7$, $b \in \mathbb{F}_{q^6} \setminus \mathbb{F}_q$. Suppose that one of the following conditions holds.*

1. $q \not\equiv 1 \pmod 7$ *and*

$$B = \frac{3}{7}A^2, \qquad C = \frac{5}{7^2}A^3, \qquad D = \frac{5}{7^3}A^4, \qquad E = \frac{3}{7^4}A^5, \qquad F = \frac{1}{7^5}A^6;$$

2. $q \not\equiv 1 \pmod 7$, $7B - 3A^2 \neq 0$, *and*

$$C = \frac{1}{7^2}(-10A^3 + 35AB), \qquad D = \frac{1}{7^2}(14B^2 - A^4 - 2A^2B),$$

$$E = \frac{1}{7^4}(27A^5 - 182A^3B + 294AB^2), \qquad F = \frac{1}{7^5}(13A^6 - 28A^4B - 147A^2B^2 + 343B^3).$$

Then f_b is a PP of $\mathbb{F}_{q^6}$. Viceversa, if $q \geq 421$ and f_b is a PP of $\mathbb{F}_{q^6}$, then either Condition 1 *or Condition* 2 *holds.*

Theorem 2.2. *Let $p = 7$, $b \in \mathbb{F}_{q^6} \setminus \mathbb{F}_q$. Suppose that one of the following conditions holds.*

1. $$b \in \left\{(0, \lambda, 0, 0, 0, 0), (0, 0, 0, 0, 0, \lambda) \mid \lambda \in \mathbb{F}_q^*\right\} ;$$

2. $$A = B = 0\,, \quad C \neq 0\,, \quad E = \frac{3D^2}{C}\,, \quad F = \frac{2C^4 + 4D^3}{C^2}\,; \tag{17}$$

3. $$A = 0\,, \quad \sqrt{B} \notin \mathbb{F}_q\,, \quad D = \frac{5B^3 + 6C^2}{B}\,, \quad E = \frac{C(3B^3 + 4C^2)}{B^2}\,, \quad F = \frac{6(B^3 + 6C^2)^2}{B^3}\,. \tag{18}$$

Then f_b is a PP of $\mathbb{F}_{q^6}$. Viceversa, if $q \geq 421$ and f_b is a PP of $\mathbb{F}_{q^6}$, then Condition 1*, Condition* 2 *or Condition* 3 *holds.*

It is easily seen that for $x, y \in \mathbb{F}_q$ Condition (2) in Niederreiter-Robinson criterion reads as follows:

$$\big(x - y\big)\big[x^6 + x^5y + x^4y^2 + x^3y^3 + x^2y^4 + xy^5 + y^6 + A(x^5 + x^4y + x^3y^2 + x^2y^3 + xy^4 + y^5)$$
$$+B(x^4+x^3y+x^2y^2+xy^3+y^4)+C(x^3+x^2y+xy^2+y^3)+D(x^2+xy+y^2)+E(x+y)+F\big] \neq 0.$$

Let $\mathcal{S}_b$ be the sextic plane curve defined over $\mathbb{F}_q$ with affine equation $F_b(X, Y) = 0$, where

$$\begin{aligned} F_b(X,Y) = {} & X^6 + X^5Y + X^4Y^2 + X^3Y^3 + X^2Y^4 + XY^5 + Y^6 \\ & +A(X^5 + X^4Y + X^3Y^2 + X^2Y^3 + XY^4 + Y^5) + B(X^4 + X^3Y + X^2Y^2 + XY^3 + Y^4) \\ & +C(X^3 + X^2Y + XY^2 + Y^3) + D(X^2 + XY + Y^2) + E(X + Y) + F. \end{aligned}$$

Remark 2.3. *By Niederreiter-Robinson Criterion, f_b is a PP of $\mathbb{F}_{q^6}$ if and only if $b \in \mathbb{F}_{q^6} \setminus \mathbb{F}_q$ and $\mathcal{S}_b$ has no $\mathbb{F}_q$-rational affine points off the lines $X = Y$, $X = 0$, and $Y = 0$.*

Lemma 2.4. *If $\mathcal{S}_b$ has no $\mathbb{F}_q$-rational affine points off the lines $X = Y$, $X = 0$, and $Y = 0$, then one of the following cases occurs.*

i) The prime power q is at most 421*.*

ii) The curve $\mathcal{S}_b$ has a linear component not defined over $\mathbb{F}_q$.

iii) The curve $\mathcal{S}_b$ splits into three absolutely irreducible conics not defined over $\mathbb{F}_q$ but over $\mathbb{F}_{q^3}$.

iv) The curve $\mathcal{S}_b$ splits into two absolutely irreducible cubics not defined over $\mathbb{F}_q$ but over $\mathbb{F}_{q^2}$.

Proof. Assume that $\mathcal{S}_b$ is absolutely irreducible; then its genus is at most 10. Also, $\mathcal{S}_b$ has at most 6 places centered on the ideal line ℓ_∞, at most 6 places centered on the line $X = Y$, and no $\mathbb{F}_q$-rational affine points (x, y) with $x = 0$ or $y = 0$; this is easily seen by (2). By the Hasse-Weil Bound, $q + 1 - 20\sqrt{q} \leq 12$, that is, $q \leq 421$. If $\mathcal{S}_b$ is reducible but has an irreducible component defined over $\mathbb{F}_q$, then the same argument yields $q \leq 13$.

We can now assume that $\mathcal{S}_b$ splits into absolutely irreducible components not defined over $\mathbb{F}_q$. Let $\varphi_q : (a, b, c) \mapsto (a^q, b^q, c^q)$ be the Frobenius collineation of the projective plane over the algebraic closure of $\mathbb{F}_q$ and let $\mathcal{C}$ be a component of $\mathcal{S}_b$. Then $\varphi_q(\mathcal{C})$ is a component of $\mathcal{S}_b$ different from $\mathcal{C}$; hence, the degree of $\mathcal{C}$ is smaller than 4. If $\mathcal{S}_b$ has no linear components, then either $\mathcal{C}$ is a conic, whose orbit under φ_q has length 3; or $\mathcal{C}$ is a cubic, whose orbit under φ_q has length 2. In the former case $\mathcal{C}$ is defined over $\mathbb{F}_{q^3}$, otherwise over $\mathbb{F}_{q^2}$. □

2.1 The case $p \neq 7$

Theorem 2.1 is implied by the following result.

Proposition 2.5. *Let $p \neq 7$.*

1. *If $\mathcal{S}_b$ has a linear component not defined over $\mathbb{F}_q$, then $\mathcal{S}_b$ splits into six linear components not defined over $\mathbb{F}_q$. This happens if and only if $q \not\equiv 1 \pmod 7$ and*

$$7B - 3A^2 = 49C - 5A^3 = 343D - 5A^4 = 2401E - 3A^5 = 16807F - A^6 = 0. \quad (19)$$

   In this case, $\mathcal{S}_b$ has no $\mathbb{F}_q$-rational affine points off the line $X = Y$.

2. *The curve $\mathcal{S}_b$ splits into three absolutely irreducible conics not defined over $\mathbb{F}_q$ if and only if $q \not\equiv 1 \pmod 7$, $7B - 3A^2 \neq 0$, and*

$$\begin{aligned} &A^4 + 2A^2B - 14B^2 + 49D = 27A^5 - 182A^3B + 294AB^2 - 2401E \\ &= 10A^3 - 35AB + 49C = 13A^6 - 28A^4B - 147A^2B^2 + 343B^3 - 16807F = 0. \end{aligned} \quad (20)$$

   In this case, $\mathcal{S}_b$ has no $\mathbb{F}_q$-rational affine points.

3. *The curve $\mathcal{S}_b$ does not split into two absolutely irreducible cubics not defined over $\mathbb{F}_q$.*

Proof. Let ξ denote a primitive 7-th root of unity; the curve $\mathcal{S}_b$ has 6 non-singular ideal points $P_i = (1, \xi^i, 0)$, $i = 1, \ldots, 6$. We denote by ℓ_i the tangent line to $\mathcal{S}_b$ at P_i, which has affine equation $L_i(X, Y) = 0$, where

$$L_i(X, Y) = Y - \xi^i X - w_i, \qquad \text{with} \qquad w_i = \frac{A\xi^{6i}}{6\xi^{5i} + 5\xi^{4i} + 4\xi^{3i} + 3\xi^{2i} + 2\xi^i + 1}.$$

Let $\Phi_7(X) = \frac{X^7-1}{X-1} \in \mathbb{F}_q[X]$ be the 7-th cyclotomic polynomial. For a polynomial $F(X) \in \mathbb{F}_q[X]$ we denote by $R(F) \in \mathbb{F}_q$ the resultant of Φ_7 and F with respect to X. Therefore, $R(F) \neq 0$ implies $F(\xi) \neq 0$.

1. A linear component s_i of $\mathcal{S}_b$ must have affine equation $Y = \xi^i X + \alpha_i$, for some $i \in \{1, \ldots, 6\}$, $\alpha_i \in \overline{\mathbb{F}}_q$.

   By straightforward computations, $s_i \subset \mathcal{S}_b$ reads

$$\begin{cases} (5\xi^{4i} + 4\xi^{3i} + 3\xi^{2i} + 2\xi^i + 1)A\alpha_i + (\xi^{4i} + \xi^{3i} + \xi^{2i} + \xi^i + 1)B \\ \qquad +(15\xi^{4i} + 10\xi^{3i} + 6\xi^{2i} + 3\xi^i + 1)\alpha_i^2 = 0 \\ A(\xi^{5i} + \xi^{4i} + \xi^{3i} + \xi^{2i} + \xi^i + 1) + (6\xi^{5i} + 5\xi^{4i} + 4\xi^{3i} + 3\xi^{2i} + 2\xi^i + 1)\alpha_i = 0 \\ (10\xi^{3i} + 6\xi^{2i} + 3A\xi^i + 1)A\alpha_i^2 + (4\xi^{3i} + 3\xi^{2i} + 2\xi^i + 1)B\alpha_i \\ \qquad +(\xi^{3i} + \xi^{2i} + \xi^i + 1)C + (20\xi^{3i} + 10\xi^{2i} + 4\xi^i + 1)\alpha_i^3 = 0 \\ (10\xi^{2i} + 4\xi^i + 1)A\alpha_i^3 + (6\xi^{2i} + 3\xi^i + 1)B\alpha_i^2 + (3\xi^{2i} + 2\xi^i + 1)C\alpha_i \\ \qquad +(\xi^{2i} + \xi^i + 1)D + 15\alpha_i^4\xi^{2i} + 5\alpha_i^4\xi^i + \alpha_i^4 = 0 \\ (5\xi^i + 1)A\alpha_1^4 + (4\xi^i + 1)B\alpha_i^3 + (3\xi^i + 1)C\alpha_i^2 + (2\xi^i + 1)D\alpha_i \\ \qquad +(\xi^i + 1)E + 6\alpha_i^5\xi + \alpha_i^5 = 0 \\ A\alpha_i^5 + B\alpha_i^4 + C\alpha_i^3 + D\alpha_i^2 + E\alpha_i + F + \alpha_i^6 = 0 \end{cases} . \tag{21}$$

   From the first two equations we obtain

$$(3A^2 - 7B)(\xi^{5i} + 4\xi^{4i} + 9\xi^{3i} + 9\xi^{2i} + 4\xi^i + 1) = 0.$$

   For each $i \in \{1, \ldots, 6\}$ we have $R(X^{5i} + 4X^{4i} + 9X^{3i} + 9X^{2i} + 4X^i + 1) = 7^4$, and hence $\xi^{5i} + 4\xi^{4i} + 9\xi^{3i} + 9\xi^{2i} + 4\xi^i + 1 \neq 0$. Combining $3A^2 - 7B = 0$ with the second and the third equation in (21), we get

$$(5A^3 - 49C)(2\xi^{5i} + 7\xi^{4i} + 12\xi^{3i} + 14\xi^{2i} + 10\xi^i + 4) = 0.$$

   For each $i \in \{1, \ldots, 6\}$, we have $R(2X^{5i} + 7X^{4i} + 12X^{3i} + 14X^{2i} + 10X^i + 4) = 7^3$, and hence $5A^3 - 49C = 0$. Similarly, from the other equations in (21), we obtain

$$343D - 5A^4 = 2401E - 3A^5 = 16807F - A^6 = 0.$$

   Also,

$$\alpha_i = \frac{A\xi^{6i}}{6\xi^{5i} + 5\xi^{4i} + 4\xi^{3i} + 3\xi^{2i} + 2\xi^i + 1}. \tag{22}$$

   Therefore s_i is not defined over $\mathbb{F}_q$ if and only if $\xi^i \notin \mathbb{F}_q$. Equivalently, $q \not\equiv 1 \pmod 7$; in fact, Φ_7 factorizes over $\mathbb{F}_q$ into $6/d$ irreducible polynomials, where d is the multiplicative order of q modulo 7.

On the other hand, direct calculations show that, if Conditions (19) hold and α_i is defined by (22) for $i = 1, \ldots, 6$, then $\mathcal{S}_b$ splits into the six lines $\ell_1, \ldots, \ell_6$.

If $\mathcal{S}_b$ has a component not defined over $\mathbb{F}_q$ containing an $\mathbb{F}_q$-rational point, then this point lies on at least another component of $\mathcal{S}_b$. As $\ell_1 \cap \ldots \cap \ell_6 = \{(\frac{-A}{7}, \frac{-A}{7})\}$, the thesis follows.

2. If $\mathcal{S}_b$ splits into three absolutely irreducible conics, then $\mathcal{S}_b$ has equation $S(X,Y) = 0$, where

$$S(X,Y) = (L_{i_1}(X,Y)L_{j_1}(X,Y) + \beta_1) \cdot (L_{i_2}(X,Y)L_{j_2}(X,Y) + \beta_2) \cdot (L_{i_3}(X,Y)L_{j_3}(X,Y) + \beta_3)$$

for some $\beta_1, \beta_2, \beta_3 \in \overline{\mathbb{F}}_q^*$, with $\{i_1, j_1, i_2, j_2, i_3, j_3\} = \{1, \ldots, 6\}$. There are 15 possible distinct choises of the indexes $i_1, j_1, i_2, j_2, i_3, j_3$. For instance, let $(i_1, j_1, i_2, j_2, i_3, j_3) = (1, 2, 3, 4, 5, 6)$. Using the fact that the three conics are in the same orbit under the Frobenius collineation φ_q, and comparing the coefficients of $S(X,Y)$ with the coefficients of $F_b(X,Y)$, we get

$$\begin{cases} (\xi^5+\xi^4+3\xi^3+\xi^2+\xi)\beta_1 + (-2\xi^5-2\xi^4-2\xi^3-2\xi^2+1)\beta_2 + (2\xi^4-\xi-1)\beta_3 \\ \qquad = 21A^2-49B \\ (-2\xi^5-2\xi^4-\xi^2-\xi-1)\beta_1 + (-\xi^4-\xi^3+2)\beta_2 + (\xi^4-\xi^3-\xi^2+\xi)\beta_3 = 21A^2-49B \\ (\xi^4+2\xi^3+\xi^2+2\xi+1)\beta_1 + (\xi^5+2\xi^4+2\xi^3+\xi^2+1)\beta_2 - \xi^5-\xi^3-2\xi^2-2\xi-1)\beta_3 \\ \qquad = 21A^2-49B \\ (\xi^3-\xi^2-\xi+1)\beta_1 + (-\xi^4-\xi^3+2)\beta_2 + (2\xi^4+\xi^3+\xi^2+\xi+2)\beta_3 = 21A^2-49B \\ (\xi^5+\xi^3-\xi-1)\beta_1 + (\xi^5+2\xi^4+2\xi^3+\xi^2+1)\beta_2 + (\xi^5+2\xi^4+\xi^3+2\xi^2+\xi)\beta_3 \\ \qquad = 21A^2-49B \end{cases}. \tag{23}$$

System (23) has a solution $(\beta_1, \beta_2, \beta_3)$ if and only if

$$\begin{cases} 6A^2\xi^5 - 15A^2\xi^4 - 45A^2\xi^3 - 66A^2\xi^2 - 60A^2\xi - 30A^2 \\ -14B\xi^5 + 35B\xi^4 + 105B\xi^3 + 154B\xi^2 + 140B\xi + 70B = 0 \\ 6A^2\xi^5 - 6A^2\xi^4 - 24A^2\xi^3 - 36A^2\xi^2 - 30A^2\xi - 15A^2 \\ -14B\xi^5 + 14B\xi^4 + 56B\xi^3 + 84B\xi^2 + 70B\xi + 35B = 0 \end{cases},$$

that is

$$\begin{cases} (3A^2-7B)(2\xi^5-5\xi^4-15\xi^3-22\xi^2-20\xi-10) = 0 \\ (3A^2-7B)(2\xi^5-2\xi^4-8\xi^3-12\xi^2-10\xi-5) = 0 \end{cases}.$$

Since $R(2X^5-2X^4-8X^3-12X^2-10X-5) = 7^3$, we have $3A^2-7B=0$. Then, by

(23),

$$\begin{cases} (-2\xi^5-2\xi^4-\xi^2-\xi-1)\beta_1+(-\xi^4-\xi^3+2)\beta_2+(\xi^4-\xi^3-\xi^2+\xi)\beta_3=0\\ (\xi^4+2\xi^3+\xi^2+2\xi+1)\beta_1+(\xi^5+2\xi^4+2\xi^3+\xi^2+1)\beta_2-\xi^5-\xi^3-2\xi^2-2\xi-1)\beta_3=0\\ (\xi^5+\xi^3-\xi-1)\beta_1+(\xi^5+2\xi^4+2\xi^3+\xi^2+1)\beta_2+(\xi^5+2\xi^4+\xi^3+2\xi^2+\xi)\beta_3=0 \end{cases}. \tag{24}$$

System (24) is linear and homogeneous in the β_i's. Since $R(X^5+3X^4+3X^3+5X^2+6X+3)=7^3$, it has a unique solution $\beta_1=\beta_2=\beta_3=0$, a contradiction.

When $\{\{i_1,j_1\},\{i_2,j_2\},\{i_3,j_3\}\}\neq\{\{1,6\},\{2,5\},\{3,4\}\}$, an analogous argument yields a contradiction. Now assume $(i_1,j_1,i_2,j_2,i_3,j_3)=(1,6,2,5,3,4)$. By direct calculations,

$$\begin{array}{l}\beta_1=(\xi^5+\xi^4+\xi^3+\xi^2-1)(3A^2-7B)\,,\\ \beta_2=\beta_3=(-\xi^5-\xi^2-2)(3A^2-7B)\,;\end{array} \tag{25}$$

in particular, $3A^2-7B\neq 0$, since $R(X^5+X^4+X^3+X^2-1)=R(-X^5-X^2-2)=1$. Also, we get that Conditions (20) hold. Since the conic components of $\mathcal{S}_b$ are not defined over $\mathbb{F}_q$, $\xi\notin\mathbb{F}_q$, i.e. $q\not\equiv 1 \pmod 7$.

On the other hand, if $3A^2-7B\neq 0$ and Conditions (20) hold, then $\mathcal{S}_b$ has equation

$$(L_1(X,Y)L_6(X,Y)+\beta_1)\cdot(L_2(X,Y)L_5(X,Y)+\beta_2)\cdot(L_3(X,Y)L_4(X,Y)+\beta_3)=0\,,$$

where the β_i's are non-zero and defined as in (25).

In this case, it is easy to check that two conic components of $\mathcal{S}_b$ intersect in an $\mathbb{F}_q$-rational point if and only if $q\equiv 1 \pmod 7$ or $3A^2-7B=0$, which is not possible. Hence, $\mathcal{S}_b$ has no $\mathbb{F}_q$-rational points.

3. If $\mathcal{S}_b$ splits into two absolutely irreducible cubics $\mathcal{C}_1$ and $\mathcal{C}_2$ not defined over $\mathbb{F}_q$, then $\mathcal{C}_1$, $\mathcal{C}_2$ have affine equation $C_1(X,Y)=0$, $C_2(X,Y)=0$, where

$$\begin{array}{rl} C_1(X,Y)= & (Y-\xi^{i_1}X)(Y-\xi^{i_2}X)(Y-\xi^{i_3}X)+(w_{i_1}\xi^{i_2}\xi^{i_3}+w_{i_2}\xi^{i_1}\xi^{i_3}+w_{i_3}\xi^{i_1}\xi^{i_2})X^2\\ & +(w_{i_1}(\xi^{i_2}+\xi^{i_3})+w_{i_2}(\xi^{i_1}+\xi^{i_3})+w_{i_3}(\xi^{i_1}+\xi^{i_2}))XY\\ & -(w_{i_1}+w_{i_2}+w_{i_3})Y^2+\alpha X+\beta Y+\gamma\,,\\ C_2(X,Y)= & (Y-\xi^{i_4}X)(Y-\xi^{i_5}X)(Y-\xi^{i_6}X)+(w_{i_4}\xi^{i_5}\xi^{i_6}+w_{i_5}\xi^{i_4}\xi^{i_6}+w_{i_6}\xi^{i_4}\xi^{i_5})X^2\\ & +(w_{i_4}(\xi^{i_5}+\xi^{i_6})+w_{i_5}(\xi^{i_4}+\xi^{i_6})+w_{i_6}(\xi^{i_4}+\xi^{i_5}))XY\\ & -(w_{i_4}+w_{i_5}+w_{i_6})Y^2+\alpha' X+\beta' Y+\gamma'\,.\end{array} \tag{26}$$

Since $\mathcal{C}_1$ and $\mathcal{C}_2$ are switched by the Frobenius collineation φ_q, there exists $\lambda\in\overline{\mathbb{F}}_q^*$ such that $C_1^q(X,Y)=\lambda C_2(X,Y)$. Let $u\in\{1,\ldots,6\}$ be such that $q\equiv u \pmod 7$; then

$(\xi^i)^q = \xi^{iu}$. By comparing the coefficients of $C_1(X,Y)\cdot C_2(X,Y)$ with the coefficients of $F_b(X,Y)$, we have that the indexes $\{\{i_1,i_2,i_3\},\{i_4,i_5,i_6\},u\}$ belong to

$$\begin{aligned}\Big\{&\{\{1,2,3\},\{4,5,6\},6\},\quad \{\{1,2,4\},\{3,5,6\},3\},\quad \{\{1,2,4\},\{3,5,6\},5\},\\ &\{\{1,2,4\},\{3,5,6\},6\},\quad \{\{1,3,5\},\{2,4,6\},6\},\quad \{\{1,4,5\},\{2,3,6\},6\}\Big\}.\end{aligned} \tag{27}$$

Also, in these cases we have $\lambda = 1$. Hence $\alpha' = \alpha^q$, $\beta' = \beta^q$, and $\gamma' = \gamma^q$.

The projectivity $\psi : (X,Y,T) \mapsto (Y,X,T)$ is an isomorphism of $\mathcal{S}_b$ and ψ either fixes or switches the components $\mathcal{C}_1$ and $\mathcal{C}_2$. It is easy to check that the former case cannot occur, for any case in (27). Together with $\mathcal{C}_1\mathcal{C}_2 = \mathcal{S}_b$, this yields

$$\gamma^q = \mu\gamma\,,\quad \alpha^q = \mu\beta\,,\quad \beta^q = \mu\alpha\,,\quad \gamma^{q+1} = 16807F\,,\quad \alpha\gamma^q + \alpha^q\gamma = \beta\gamma^q + \beta^q\gamma = 16807E\,,$$

for some $\mu \in \overline{\mathbb{F}}_q$. Consider the case $(i_1,i_2,i_3,i_4,i_5,i_6,u) = (1,2,4,3,5,6,3)$; by direct computation $\mu = 1$, and $\mathcal{C}_1\mathcal{C}_2 = \mathcal{S}_b$ is equivalent to

$$\begin{cases} \alpha\gamma + \beta\gamma = 16807E \\ A(\alpha-\beta)(\xi^4+\xi^2+\xi-2) - 5A\beta - 343C - 7\gamma = 0 \\ \gamma^2 = 16807F \\ A(\beta-\alpha)(\xi^4+\xi^2+\xi) - A\alpha - 343C = 0 \\ 98A^2 - 343B + (\alpha-\beta)(\xi^4+\xi^2+\xi-3) - 7\beta = 0 \\ -196A\gamma - 16807D + \alpha^2 + \beta^2 = 0 \\ -49A\gamma - 16807D + \alpha\beta = 0 \\ 98A^2 - 343B + (\beta-\alpha)(2\xi^4+2\xi^2+2\xi+1) = 0 \\ 49A^2 - 343B + (\alpha-\beta)(2\xi^4+2\xi^2+2\xi-6) - 14\beta = 0 \end{cases}.$$

By eliminating α, β, and γ, the system yields

$$\begin{cases} (3A^2-7B)(2\xi^4+2\xi^2+2\xi+1) = 0 \\ (2A^3+7AB-49C)(2\xi^4+2\xi^2+2\xi+1) = 0 \\ -15A^4 + 56A^2B - 49AC - 49B^2 + 343D = 0 \\ (-33A^5 + 259A^3B - 147A^2C - 490AB^2 + 686BC - 2401E)(2\xi^4+2\xi^2+2\xi+1) = 0 \\ -121A^6 + 770A^4B - 1078A^3C - 1225A^2B^2 + 3430ABC - 2401C^2 + 16807F = 0 \\ -45A^4 + 182A^2B - 196AC - 98B^2 + 343D = 0 \end{cases}.$$

Since $R(2X^4+2X^2+2X+1) = 7^3$, we obtain

$$7B - 3A^2 = 49C - 5A^3 = 343D - 5A^4 = 2401E - 3A^5 = 16807F - A^6 = 0.$$

Then $\mathcal{S}_b$ splits into lines as shown above, contradiction.

If $(\{i_1,i_2,i_3\},\{i_4,i_5,i_6\},u) \in \{(\{1,2,4\},\{3,5,6\},6),(\{1,2,4\},\{3,5,6\},6)\}$, then $\mu=1$ and analogous arguments yield a contradiction.

Now consider the case $(\{i_1,i_2,i_3\},\{i_4,i_5,i_6\},u) = (\{1,2,3\},\{4,5,6\},6)$. We get $\mu=\xi^5$, and $\mathcal{C}_1\mathcal{C}_2=\mathcal{S}_b$ implies

$$\begin{cases} A^2(22\xi^5-5\xi^4-4\xi^3+11\xi^2+26\xi+27)-49B(2\xi^5+\xi^2+2\xi+2)+\alpha\xi^5-\beta\xi=0 \\ A^2(22\xi^5-5\xi^4-4\xi^3+11\xi^2+26\xi+27)-49B(2\xi^5+\xi^2+2\xi+2)+\alpha\xi^2-\beta\xi^4=0 \\ -A^2(70\xi^4+14\xi+14)+343B\xi^4+\alpha(8\xi^5+6\xi^4+9\xi^3+4\xi^2-\xi+2)=0 \\ -A^2(70\xi^4+14\xi+14)+343B\xi^4-\alpha(6\xi^5+8\xi^4+5\xi^3+3\xi^2+\xi-2)=0 \\ 343C\xi^4+\gamma(2\xi^5+\xi^3-2\xi^2-2\xi+1)=0 \\ 343C\xi^4+\gamma(-\xi^5+3\xi^3+\xi^2+\xi+3)=0 \end{cases},$$

whence

$$\begin{cases} (\xi^4-\xi)(\alpha\xi+\beta)=0 \\ (14\xi^5+14\xi^4+14\xi^3+7\xi^2)\alpha=0 \\ (3\xi^5-2\xi^3-3\xi^2-3\xi-2)\gamma=0. \end{cases}.$$

Therefore $\gamma=0$ and $F=\gamma^2/16807=0$, a contradiction.

Finally, for $(\{i_1,i_2,i_3\},\{i_4,i_5,i_6\},u) \in \{(\{1,3,5\},\{2,4,6\},6),(\{1,4,5\},\{2,3,6\},6)\}$, analogous arguments yield a contradiction.

□

2.2 The case $p=7$

Theorem 2.2 is implied by the following result.

Proposition 2.6. *Let $p=7$.*

1. *If $\mathcal{S}_b$ has a linear component not defined over $\mathbb{F}_q$, then $\mathcal{S}_b$ splits into six linear components not defined over $\mathbb{F}_q$. This happens if and only if*

$$b \in \left\{(0,\lambda,0,0,0,0),(0,0,0,0,0,\lambda) \mid \lambda \in \mathbb{F}_q^*\right\}. \tag{28}$$

   In this case, $\mathcal{S}_b$ has no $\mathbb{F}_q$-rational affine points.

2. *The curve $\mathcal{S}_b$ splits into three absolutely irreducible conics not defined over $\mathbb{F}_q$ if and only if*

$$A=B=0\,,\quad C\neq 0\,,\quad E=\frac{3D^2}{C}\,,\quad F=\frac{2C^4+4D^3}{C^2}\,. \tag{29}$$

   In this case, $\mathcal{S}_b$ has no $\mathbb{F}_q$-rational affine points off the line $X=Y$.

3. *The curve* $\mathcal{S}_b$ *splits into two absolutely irreducible cubics not defined over* $\mathbb{F}_q$ *if and only if*

$$A = 0\,, \quad \sqrt{B} \notin \mathbb{F}_q\,, \quad D = \frac{5B^3+6C^2}{B}\,, \quad E = \frac{C(3B^3+4C^2)}{B^2}\,, \quad F = \frac{6(B^3+6C^2)^2}{B^3}\,. \tag{30}$$

In this case $\mathcal{S}_b$ *has no* $\mathbb{F}_q$*-rational affine points off the line* $X = Y$*.*

Proof. The unique ideal point of $\mathcal{S}_b$ is $P_\infty = (1, 1, 0)$. The point P_∞ is singular if and only if $A = 0$. Suppose $A \neq 0$. The tangent line to $\mathcal{S}_b$ at P_∞ is the ideal line ℓ_∞. Since ℓ_∞ is not a component of $\mathcal{S}_b$, there is no linear component of $\mathcal{S}_b$ passing through P_∞. Hence, $\mathcal{S}_b$ is absolutely irreducible by a criterion due to Segre; see [15] and [2, Lemma 8].

Therefore, a necessary condition for $\mathcal{S}_b$ to be reducible is $A = 0$.

1. Let s_1 be a linear component of the curve $\mathcal{S}_b$, then it has affine equation $Y = X + \alpha$ and the system

$$\begin{cases} A = 0 \\ A\alpha + 5B = 0 \\ 6A\alpha^2 + 3B\alpha + 4C = 0 \\ A\alpha^3 + 3B\alpha^2 + 6C\alpha + 3D = 0 \\ 6A\alpha^4 + 5B\alpha^3 + 4C\alpha^2 + 3D\alpha + 2E = 0 \\ A\alpha^5 + B\alpha^4 + C\alpha^3 + D\alpha^2 + E\alpha + F + \alpha^6 = 0 \end{cases}$$

holds. This happens if and only if $A = B = C = D = E = 0$ and $\alpha^6 = -F$. On the other hand, these conditions imply that $\mathcal{S}_b$ splits into the six lines $s_i : Y = X + i\alpha$, $i = 1, \ldots, 6$.

Let k be such that $q = 6k + 1$. Recall that ζ is a primitive element of $\mathbb{F}_q$ and z is a root of the polynomial $T^6 - \zeta$. In particular $z^{6(q-1)} = 1$ and $\{1, z, z^2, z^3, z^4, z^5\}$ is a basis of $\mathbb{F}_{q^6}$ over $\mathbb{F}_q$.

If $b = (b_0, b_1, b_2, b_3, b_4, b_5), c = (c_0, c_1, c_2, c_3, c_4, c_5) \in \mathbb{F}_{q^6}$, then

$$\begin{aligned}
b^q &= (b_0, b_1\zeta^k, b_2\zeta^k - b_2, -b_3, -b_4\zeta^k, -b^5\zeta^k + b_5),\\
b^{q^2} &= (b_0, b_1\zeta^k - b_1, -b_2\zeta^k, b_3, b_4\zeta^k - b_4, -b^5\zeta^k),\\
b^{q^3} &= (b_0, -b_1, b_2, -b_3, b_4, -b_5),\\
b^{q^4} &= (b_0, -b_1\zeta^k, b_2\zeta^k - b_2, b_3, -b_4\zeta^k, b^5\zeta^k - b_5),\\
b^{q^5} &= (-b_0, -b_1\zeta^k + b_1, -b_2\zeta^k, -b_3, b_4\zeta^k - b_4, b^5\zeta^k),\\
bc &= \big(b_0c_0 + b_1c_5\zeta + b_2c_4\zeta + b_3c_3\zeta + b_4c_2\zeta + b_5c_1\zeta, b_0c_1 + b_1c_0 + b_2c_5\zeta + b_3c_4\zeta + b_4c_3\zeta + b_5c_2\zeta,\\
&\qquad b_0c_2 + b_1c_1 + b_2c_0 + b_3c_5\zeta + b_4c_4\zeta + b_5c_3\zeta, b_0c_3 + b_1c_2 + b_2c_1 + b_3c_0 + b_4c_5\zeta + b_5c_4\zeta,\\
&\qquad b_0c_4 + b_1c_3 + b_2c_2 + b_3c_1 + b_4c_0 + b_5c_5\zeta, b_0c_5 + b_1c_4 + b_2c_3 + b_3c_2 + b_4c_1 + b_5c_0\big),
\end{aligned}$$

hence

$$A=-b_0,\quad B=b_0^2+b_1b_5\zeta+b_2b_4\zeta+4b_3^2\zeta,$$

$$C=6b_0^3+4b_0b_1b_5\zeta+4b_0b_2b_4\zeta+2b_0b_3^2\zeta+6b_1^2b_4\zeta$$
$$+5b_1b_2b_3\zeta+2b_2^3\zeta+6b_2b_5^2\zeta^2+5b_3b_4b_5\zeta^2+2b_4^3\zeta^2,$$

$$D=b_0^4+6b_0^2b_1b_5\zeta+6b_0^2b_2b_4\zeta+3b_0^2b_3^2\zeta+4b_0b_1^2b_4\zeta+b_0b_1b_2b_3\zeta+6b_0b_2^3\zeta$$
$$+4b_0b_2b_5^2\zeta^2+b_0b_3b_4b_5\zeta^2+6b_0b_4^3\zeta^2+b_1^3b_3\zeta+5b_1^2b_2^2\zeta+2b_1^2b_5^2\zeta^2$$
$$+3b_1b_3b_4^2\zeta^2+3b_2^2b_3b_5\zeta^2+2b_2^2b_4^2\zeta^2+3b_3^4\zeta^2+b_3b_5^3\zeta^3+5b_4^2b_5^2\zeta^3,$$

$$E=6b_0^5+4b_0^3b_1b_5\zeta+4b_0^3b_2b_4\zeta+2b_0^3b_3^2\zeta+4b_0^2b_1^2b_4\zeta+b_0^2b_1b_2b_3\zeta+6b_0^2b_2^3\zeta+4b_0^2b_2b_5^2\zeta^2$$
$$+b_0^2b_3b_4b_5\zeta^2+6b_0^2b_4^3\zeta^2+2b_0b_1^3b_3\zeta+3b_0b_1^2b_2^2\zeta+4b_0b_1^2b_5^2\zeta^2+6b_0b_1b_3b_4^2\zeta^2+6b_0b_2^2b_3b_5\zeta^2$$
$$+4b_0b_2^2b_4^2\zeta^2+6b_0b_3^4\zeta^2+2b_0b_3b_5^3\zeta^3+3b_0b_4^2b_5^2\zeta^3+6b_1^4b_2\zeta+2b_1^3b_4b_5\zeta^2+4b_1^2b_3^2b_4\zeta^2$$
$$+5b_1b_2^3b_5\zeta^2+2b_1b_2b_3^3\zeta^2+2b_1b_2b_5^3\zeta^3+5b_1b_4^3b_5\zeta^3+b_2^4b_4\zeta^2+6b_2^3b_3^2\zeta^2+4b_2b_3^2b_5^2\zeta^3$$
$$+b_2b_4^4\zeta^3+2b_3^3b_4b_5\zeta^3+6b_3^2b_4^3\zeta^3+6b_4b_5^4\zeta^4.$$

It is easy to check that $A=B=C=D=E=0$ is equivalent to Condition (28). Since $b=\lambda z$ or $b=\lambda z^5$, with $\lambda\in\mathbb{F}_q^*$, the condition $\alpha^6=-b^{q^5+q^4+q^3+q^2+q+1}$, i.e. $\alpha^6=-F$, implies $\alpha\in\mathbb{F}_{q^6}\setminus\mathbb{F}_q$. Therefore, the six lines s_i, $i=1,\ldots,6$, have no $\mathbb{F}_q$-rational affine points.

2. Suppose that $\mathcal{S}_b$ splits into three absolutely irreducible conics $\mathcal{C}_1$, $\mathcal{C}_2$, and $\mathcal{C}_3$. Since $\psi:(X,Y,T)\mapsto(Y,X,T)$ is an automorphism of $\mathcal{S}_b$, either ψ fixes each $\mathcal{C}_i$, or (up to reordering the indexes) ψ fixes $\mathcal{C}_1$ and switches $\mathcal{C}_2$ and $\mathcal{C}_3$.

   In the latter case, the conics $\mathcal{C}_i$'s have affine equation

$$\begin{array}{ll}\mathcal{C}_1: & (X-Y)^2+\alpha X+\alpha Y+\beta=0\,,\\ \mathcal{C}_2: & (X-Y)^2+\gamma X+\delta Y+\epsilon=0\,,\\ \mathcal{C}_3: & (X-Y)^2+\delta X+\gamma Y+\zeta=0\,,\end{array}$$

   for some $\alpha,\beta,\gamma,\delta,\epsilon,\zeta\in\overline{\mathbb{F}}_q$. The conditions $\mathcal{C}_1\mathcal{C}_2\mathcal{C}_3=\mathcal{S}_b$ and $A=0$ yield

$$A=B=C=D=E=0\,.$$

   Hence, as above, $\mathcal{S}_b$ splits into six lines, a contradiction.

   In the former case, the conics $\mathcal{C}_i$'s have affine equation

$$\begin{array}{ll}\mathcal{C}_1: & (X-Y)^2+\alpha X+\alpha Y+\beta=0\,,\\ \mathcal{C}_2: & (X-Y)^2+\gamma X+\gamma Y+\delta=0\,,\\ \mathcal{C}_3: & (X-Y)^2+\epsilon X+\epsilon Y+\zeta=0\,,\end{array}\tag{31}$$

   for some $\alpha,\beta,\gamma,\delta,\epsilon,\zeta\in\overline{\mathbb{F}}_q$. Since the $\mathcal{C}_i$'s form a single orbit under the Frobenius collineation φ_q, the coefficients lie in $\mathbb{F}_{q^3}$ and $\gamma=\alpha^q$, $\epsilon=\alpha^{q^2}$, $\delta=\beta^q$, $\zeta=\beta^{q^2}$. By direct computation, $\mathcal{C}_1\mathcal{C}_2\mathcal{C}_3=\mathcal{S}_b$ and $A=0$ imply

$$B=0\,,\quad CE+4D^2=0\,,\quad C^2D+3DF+E^2=0\,,\quad C^3+3CF+3DE=0\,.$$

Hence Conditions (29) follow, beacause $C = 0$ would imply that $\mathcal{S}_b$ splits into lines, a contradiction. Conversely, if Conditions (29) hold, then $\mathcal{S}_b$ splits into irreducible conics defined by (31), where the $\mathcal{C}_i$'s form an orbit under φ_q, and α, β are defined by

$$\alpha^3 = 4C\,, \quad \beta = \frac{C\alpha + 2D}{\alpha^2}.$$

The conics $\mathcal{C}_i$'s are not defined over $\mathbb{F}_q$. Assume by contradiction that one of them is defined over $\mathbb{F}_q$. Then $\mathcal{S}_b = (\mathcal{C}_1)^3$, and the polynomial $\big((X-Y)^2 + \alpha(X+Y) + \beta\big)^3$ has no terms of degree either 5 or 4. Hence, by direct checking, $\alpha = \beta = 0$, which is impossible since $F \neq 0$.

Conditions (29), together with the condition $(x, y) \in \mathcal{C}_1 \cap \mathcal{C}_2 \cap \mathcal{C}_3$, yield $x = y$. This means that $\mathcal{S}_b$ has no $\mathbb{F}_q$-rational affine points off the line $X = Y$.

3. Suppose that $\mathcal{S}_b$ splits into two absolutely irreducible cubics $\mathcal{C}_1$ and $\mathcal{C}_2$. The automorphism $\psi : (X, Y, T) \mapsto (Y, X, T)$ either fixes or switches $\mathcal{C}_1$ and $\mathcal{C}_2$.

   In the former case, the cubics $\mathcal{C}_i$'s have affine equation

$$\begin{array}{ll} \mathcal{C}_1: & (X-Y)^3 + \alpha(X^2+Y^2) + \beta XY + \gamma(X+Y) + \delta = 0\,, \\ \mathcal{C}_2: & (X-Y)^3 + \alpha'(X^2+Y^2) + \beta' XY + \gamma'(X+Y) + \delta' = 0\,. \end{array}$$

   The conditions $\mathcal{C}_1\mathcal{C}_2 = \mathcal{S}_b$ and $A = 0$ yield $B = C = D = E = 0$; hence, as above, $\mathcal{S}_b$ splits into lines, a contradiction.

   In the latter case, the conditions $\mathcal{C}_1\mathcal{C}_2 = \mathcal{S}_b$, $A = 0$, and $\psi(\mathcal{C}_1) = \mathcal{C}_2$ yield in particular

$$\begin{cases} CF^2 + DEF + 2E^3 = 0 \\ BC^2 + 5BF + 4CE + 3D^2 = 0 \\ B^2E + CF + 5DE = 0 \\ B^2C + 3BE + 5CD = 0 \\ B^3 + 4BD + 4C^2 = 0 \end{cases}.$$

   Hence $B \neq 0$, otherwise $\mathcal{S}_b$ splits into lines; also,

$$A = 0\,, \quad D = \frac{5B^3 + 6C^2}{B}\,, \quad E = \frac{C(3B^3 + 4C^2)}{B^2}\,, \quad F = \frac{6(B^3 + 6C^2)^2}{B^3}\,. \tag{32}$$

   If Conditions (32) are satisfied, then $\mathcal{C}_1$ and $\mathcal{C}_2$ have equation

$$\begin{array}{ll} \mathcal{C}_1: & \alpha\left[(X-Y)^3 - B(X-Y)\right] + 4B(X+Y)^2 + 3C(X+Y) + \frac{3B^3+5BC^2+C^2}{B} = 0\,, \\ \mathcal{C}_2: & -\alpha\left[(X-Y)^3 - B(X-Y)\right] + 4B(X+Y)^2 + 3C(X+Y) + \frac{3B^3+5BC^2+C^2}{B} = 0\,, \end{array} \tag{33}$$

where $\alpha^2 = 4B$; therefore, $\mathcal{S}_b$ is not defined over $\mathbb{F}_q$ if and only if $\sqrt{B} \notin \mathbb{F}_q$.

Viceversa, if Conditions (30) are satisfied, then $\mathcal{S}_b = \mathcal{C}_1\mathcal{C}_2$, with $\mathcal{C}_1, \mathcal{C}_2$ defined as in (33).

If $\sqrt{B} \notin \mathbb{F}_q$, then $\mathcal{C}_1$ and $\mathcal{C}_2$ in (33) have no $\mathbb{F}_q$-rational affine points off the line $X = Y$. In fact, if an $\mathbb{F}_q$-rational point (x, y) lies on $\mathcal{C}_1$, then the coefficient $(X-Y)^3 - B(X-Y)$ of α must vanish at (x, y); this implies either $B = (x-y)^2$, which is impossible, or $x = y$.

$\square$

3 Proof of Theorems 1.1 and 1.2

Using the characterization results contained in Theorems 2.1 and 2.2 we are now in a position to prove our main Theorems.

Assume first that $p \neq 7$ and let $\xi \in \mathbb{F}_{q^6}$ denote a primitive 7-th root of unity.

Consider the following family of polynomials over $\mathbb{F}_q$.

$$\mathcal{F} = \Big\{ F_{u,v} = X^6 - uX^5 + vX^4 - \frac{(-10u^3 + 35uv)}{7^2} X^3 + \frac{(14v^2 - u^4 - 2u^2v)}{7^2} X^2$$

$$- \frac{(27u^5 - 182u^3v + 294uv^2)}{7^4} X + \frac{(13u^6 - 28u^4v - 147u^2v^2 + 343v^3)}{7^5} \mid u, v \in \mathbb{F}_q \Big\}.$$

Since by definition of $A, B, C, D, E,$ and F, the elements $b, b^q, \ldots, b^{q^5}$ are the zeros of the following polynomial over $\mathbb{F}_q$

$$X^6 - AX^5 + BX^4 - CX^3 + DX^2 - EX + F,$$

we have that f_b is a PP if and only if and only if $b, b^q, \ldots, b^{q^5}$ are the only zeros of $F_{u_b, v_b} \in \mathcal{F}$, for some u_b, v_b depending on b. More precisely, Condition 1 in Theorem 2.1 holds if and only if $b, b^q, \ldots, b^{q^5}$ are the zeros of $F_{A, \frac{3}{7}A^2}$, whereas Condition 2 in Theorem 2.1 is equivalent to $7B - 3A^2 \neq 0$ and $b, b^q, \ldots, b^{q^5}$ being the zeros of $F_{A,B}$.

We consider Condition 1 first. By direct computation,

$$F_{u, \frac{3}{7}u^2} = \prod_{i=1}^{6} \left(X - u\frac{1 - \xi^i}{7} \right).$$

Since the trace map is surjective, for each $u \in \mathbb{F}_q$ there exists $b \in \mathbb{F}_{q^6} \setminus \mathbb{F}_q$ such that $u = A$. Moreover, for each $i = 1, \ldots, 6$, the minimal polynomial of ξ^i over $\mathbb{F}_q$ has degree congruent to q modulo 7. Hence, $F_{u,\frac{3}{7}u^2}$ is irreducible over $\mathbb{F}_q$ if and only if $q \equiv 3,5 \pmod 7$; in this case, the roots b of $F_{u,\frac{3}{7}u^2}$ provide 6 permutation polynomials f_b. If $F_{u,\frac{3}{7}u^2}$ is reducible over $\mathbb{F}_q$, then the zeros of $F_{u,\frac{3}{7}u^2}$ do not form a single orbit under the Frobenius map, since they are all distinct; in this case, if b is a root of $F_{u,\frac{3}{7}u^2}$, then f_b is not a PP.

As to Condition 2 in Theorem 2.1, it is satisfied by b if and only if b is a root of some $F_{u,v}$, where $u,v \in \mathbb{F}_q$ are such that $7v-3u^2 \neq 0$ and either $F_{u,v}$ is irreducible over $\mathbb{F}_q$, or $F_{u,v}$ is the square of an irreducible polynomial over $\mathbb{F}_q$, or $F_{u,v}$ is the cube of an irreducible polynomial over $\mathbb{F}_q$.

By direct computation, $F_{u,v} = \frac{1}{7^6} \cdot G^{(1)}_{u,v} \cdot G^{(2)}_{u,v} \cdot G^{(3)}_{u,v}$, with

$$G^{(1)}_{u,v}(X) = 49X^2 + 7(\xi^4+\xi^3-2)uX - (3\xi^5+4\xi^4+4\xi^3+3\xi^2+7)u^2 + 7(\xi^5+\xi^4+\xi^3+\xi^2+3)v,$$

$$G^{(2)}_{u,v}(X) = 49X^2 - 7(\xi^5+\xi^4+\xi^3+\xi^2+3)uX + (4\xi^5+\xi^4+\xi^3+4\xi^2-3)u^2 - 7(\xi^5+\xi^2-2)v,$$

$$G^{(3)}_{u,v}(X) = 49X^2 + 7(\xi^5+\xi^2-2)uX - (\xi^5-3\xi^4-3\xi^3+\xi^2+4)u^2 - 7(\xi^4+\xi^3-2)v.$$

Also, the $G^{(i)}_{u,v}$'s are defined over $\mathbb{F}_{q^3}$ and form a single orbit under φ_q. The discriminant of $F_{u,v}(X)$ is $\Delta = 13u^6 - 28u^4v - 147u^2v^2 + 343v^3$ and it vanishes if and only if $u^2 = \delta \cdot v$, with $13\delta^3 - 28\delta^2 - 147\delta + 343 = 0$. For $p \neq 13$, δ is in

$$\left\{ \frac{21\xi^5+35\xi^4+35\xi^3+21\xi^2+28}{13}, \frac{14\xi^5-21\xi^4-21\xi^3+14\xi^2+7}{13}, \frac{-35\xi^5-14\xi^4-14\xi^3-35\xi^2-7}{13} \right\},$$

and it is easily seen that $\delta \notin \mathbb{F}_q$; hence $\Delta \neq 0$, since $u,v \in \mathbb{F}_q^*$. For $p=13$, $\delta \in \{8,11\}$. In this case, a direct computation shows that $F_{u,v}$ is not a power of an irreducible polynomial over $\mathbb{F}_q$, for any $(u,v) \in \mathbb{F}_q^2 \setminus \{(0,0)\}$; hence, f_b is not a PP for any root b of $F_{u,v}$.

Therefore, we can assume that $G^{(i)}_{u,v}$ and $G^{(j)}_{u,v}$ have no roots in common for $i \neq j$.

If $q \equiv 1,6 \pmod 7$, then $G^{(i)}_{u,v}$'s are defined over $\mathbb{F}_q$. Hence, f_b is not a PP of $\mathbb{F}_{q^6}$, for any root b of $F_{u,v}$.

Suppose now q odd and $q \equiv r \in \{2,3,4,5\} \pmod 7$. For $i=1,2,3$, the roots of $G^{(i)}_{u,v}$ are

$$x^{(i)}_{1,2} = (\alpha_i u \pm \rho_i)/14, \quad \text{with} \quad \rho_i^2 = \beta_i(28v - 11u^2), \tag{34}$$

where

$$\alpha_2 = \beta_1 = (\xi^4-\xi^3)^2, \ \alpha_3 = \beta_2 = (\xi^5+\xi^4+\xi^3+\xi^2+2\xi+1)^2, \ \alpha_1 = \beta_3 = (\xi^5-\xi^2)^2.$$

Note that $\xi^4-\xi^3$, $\xi^5+\xi^4+\xi^3+\xi^2+2\xi+1$, and $\xi^5-\xi^2$ belong to $\mathbb{F}_{q^3}$ if and only if $r \in \{2,4\}$. Therefore, for any $i=1,2,3$, $\beta_i^{q^3} = \beta_i$ when $r \in \{2,4\}$, and $\beta_i^{q^3} = -\beta_i$ when $r \in \{3,5\}$, whereas $\alpha_i^{q^3} = \alpha_i$.

Suppose $28v - 11u^2 = 0$. Then $x_1^{(i)} = x_2^{(i)}$, and $F_{u,v}$ is the square of an irreducible polynomial over $\mathbb{F}_q$. Hence, the three distinct roots b of $F_{u,v}$ provide PPs f_b.

Suppose $28v - 11u^2 \neq 0$, hence $\rho_i \neq 0$ for any $i = 1, 2, 3$. Then

$$\rho_i^{q^3} = (-1)^r \cdot (28v - 11u^2)^{\frac{q^3-1}{2}} \cdot \rho_i \,.$$

Note that $(28v - 11u^2)^{\frac{q^3-1}{2}} = 1$ if $28v - 11u^2$ is a square in $\mathbb{F}_q$ (and hence in $\mathbb{F}_{q^3}$), while $(28v - 11u^2)^{\frac{q^3-1}{2}} = -1$ if $28v - 11u^2$ is a non-square in $\mathbb{F}_q$.

If $r \in \{2, 4\}$ and $28v - 11u^2$ is a non-zero square in $\mathbb{F}_q$, then $\rho^{q^3} = \rho$; the same holds if $r \in \{3, 5\}$ and $28v - 11u^2$ is a non-square in $\mathbb{F}_q$. Therefore, $(x_1^{(i)})^{q^3} = x_1$, and $F_{u,v}$ factors over $\mathbb{F}_q$ into two distinct irreducible polynomials. Hence, for any root b of $F_{u,v}$, f_b is not a PP.

If $r \in \{2, 4\}$ and $28v - 11u^2$ is a non-square in $\mathbb{F}_q$, then $\rho^{q^3} = -\rho$; the same holds if $r \in \{3, 5\}$ and $28v - 11u^2$ is a non-zero square in $\mathbb{F}_q$. Therefore, $(x_1^{(i)})^{q^3} = x_2$, and $F_{u,v}$ is irreducible over $\mathbb{F}_q$. Hence, the roots b of $F_{u,v}$ provide PPs f_b.

Let $s, \epsilon \in \mathbb{F}_q$ with ϵ a primitive element of $\mathbb{F}_q$, such that $28v - 11u^2 = s^2$ when $28v - 11u^2$ is a square in $\mathbb{F}_q$, and $28v - 11u^2 = s^2\epsilon$ when $28v - 11u^2$ is a non-square in $\mathbb{F}_q$. Then the condition $7v - 3u^2 \neq 0$ reads $u \neq \pm s$ in the former case, while it is satisfied for all $(u, s) \neq (0, 0)$ in the latter case.

Suppose now $q = 2^h$. Then, $q \equiv 2, 4 \pmod 7$. The minimal polynomial of ξ is either $X^3 + X + 1$ or $X^3 + X^2 + 1$; assume without loss of generality that $\xi^3 = \xi + 1$. The factors of $F_{u,v}$ over $\mathbb{F}_{q^3}$ in this case are

$$X^2 + (\xi + 1)Xu + (\xi + 1)^2 v + (\xi^2 + \xi)u^2,$$

$$X^2 + (\xi + 1)^2 Xu + (\xi + 1)^4 v + \xi u^2,$$
$$X^2 + (\xi + 1)^4 Xu + (\xi + 1)v + \xi^2 u^2.$$

There exist roots of $F_{u,v}$ of multiplicity larger than one if and only if $u^6(u^2 + \xi v)^4(u^2 + \xi^2 v)^4(u^2 + (\xi^2 + \xi)v)^4 = 0$. Since $\xi \notin \mathbb{F}_q$, the only possibility is $u = 0$. In this case

$$F_{u,v} = \left[\left(X + (\xi + 1)\sqrt{v}\right) \cdot \left(X + (\xi^2 + 1)\sqrt{v}\right) \cdot \left(X + (\xi^2 + \xi + 1)\sqrt{v}\right)\right]^2 .$$

Hence, $F_{u,v}$ has three distinct zeros with multiplicity 2 and defined over $\mathbb{F}_{q^3}$, for any $v \in \mathbb{F}_q^*$, namely

$$(\xi + 1)\sqrt{v}, (\xi^2 + 1)\sqrt{v}, (\xi^2 + \xi + 1)\sqrt{v}$$

which form a unique orbit under the Frobenius map.

Suppose now $u \neq 0$, that is $F_{u,v}$ has six distinct zeros belonging to $\mathbb{F}_{q^6}$. They belong to $\mathbb{F}_{q^3}$ if and only if $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_2}\left(\frac{v}{u^2} + (\xi+1)^{2^i}\right) = 0$, $i = 0,1,2$, that is

$$\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_2}\left(\frac{v}{u^2} + (\xi+1)^{2^i}\right) = \mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_2}\left(\frac{v}{u^2}\right) + \mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_2}\left((\xi+1)^{2^i}\right) = 0,$$

where $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_2}(\alpha)$ denotes the trace function from $\mathbb{F}_{q^3}$ to $\mathbb{F}_2$. It is not hard to see that $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_2}\left((\xi+1)^{2^i}\right) = 1$ if and only if h is odd. Therefore the zeros of $F_{u,v}(X)$ correspond to PPs f_b if and only if one of the following cases occurs:

- h is odd and $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_2}\left(\frac{v}{u^2}\right) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{v}{u^2}\right) = 0$;
- h is even and $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_2}\left(\frac{v}{u^2}\right) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{v}{u^2}\right) = 1$.

In these cases, let $\delta_i = \frac{v}{u^2} + (\xi+1)^{2^i}$, $i = 0,1,2$, and let k be an element with $\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_2}(k) = 1$. Denote by y_i the quantity $k\delta_i^2 + (k+k^2)\delta_i^4 + \cdots + (k+k^2+\cdots+k^{2^{h-2}})\delta_i^{2^{h-1}}$, $i = 0,1,2$. The six roots are

$$b \in \left\{ y_i(\xi+1)^{2^{i+1}}u, (y_i+1)(\xi+1)^{2^{i+1}}u \;\middle|\; i = 0,1,2, \quad \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{v}{u^2}\right) = 0 \right\}$$

if h is odd,

$$b \in \left\{ y_i(\xi+1)^{2^{i+1}}u, (y_i+1)(\xi+1)^{2^{i+1}}u \;\middle|\; i = 0,1,2, \quad \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{v}{u^2}\right) = 1 \right\}$$

otherwise.

Therefore we have proved Theorem 1.1.

For the case $p = 7$, Propositions 3.1 and 3.2 imply Theorem 1.2.

Proposition 3.1. *Let $q = 7^h \geq 421$ and let $\xi \in \mathbb{F}_{7^3}$ be such that $\xi^{18} = 1$ and let $\epsilon \in \mathbb{F}_{7^3}$ be such that $\epsilon^2 = \xi$. The polynomial f_b is a PP in $\mathbb{F}_{q^6}$ of type* (17) *if and only if one of the following cases occurs.*

- *h is even and*

$$b \in \left\{ -2\xi\overline{C} + \epsilon\frac{3\overline{D}}{\overline{C}} \;\middle|\; 3\overline{C}^3 \text{ is not a cube in } \mathbb{F}_q,\ \overline{D} \in \mathbb{F}_q \right\}.$$

- *h is odd and*

$$b \in \left\{ -2\xi\overline{C} + \epsilon\frac{3\overline{D}}{\overline{C}} \;\middle|\; 3\overline{C}^3 \text{ is not a cube in } \mathbb{F}_q,\ \overline{D} \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q,\ \overline{D}^2 \in \mathbb{F}_q \right\}.$$

- $$b \in \left\{ -\xi\overline{C} \mid 3\overline{C}^3 \textit{ is not a cube in } \mathbb{F}_q \right\}.$$

Proof. We have that f_b is a PP if and only if $b, b^q, \ldots, b^{q^5}$ are the unique zeros of some polynomial $F_{C,D}(x)$, with $C, D \in \mathbb{F}_q$, $C \neq 0$, where

$$F_{C,D}(x) := C^2x^6 - C^3x^3 + C^2Dx^2 - 3D^2Cx + (2C^4 + 4D^3).$$

A polynomial of this type factorizes over $\mathbb{F}_{q^3}$ as

$$(\overline{C}^2x^2+\xi\overline{C}^3x+\xi^8\overline{C}^4+\xi^4D)(4\overline{C}^2x^2+\xi^7\overline{C}^3x+2\xi^2\overline{C}^4+\xi^{10}D)(2\overline{C}^2x^2+\xi^{13}\overline{C}^3x+4\xi^{14}\overline{C}^4+\xi^{16}D),$$

where $\overline{C}, 2\overline{C}, 4\overline{C} \in \mathbb{F}_{q^3}$ are the cubic roots of C. It is easily seen that the three factors above are defined over $\mathbb{F}_q$ if and only if $\xi\overline{C}$ belongs to $\mathbb{F}_q$, that is if and only if $3C$ is a cube in $\mathbb{F}_q$. Also, the polynomial $F_{D,C}(x)$ has roots of multiplicity greater than 1 if and only if $C^3D^{10}(C^4 + 2D^3)^4 = 0$. Since $C \neq 0$, the only possibilities are $D = 0$ and $C^4 + 2D^3 = 0$.

- $D = 0$. In this case $F_{C,D}(x) = C^2(x^3 + 3C)^2$, which has three roots not defined over $\mathbb{F}_q$ if and only if $3C$ is not a cube in $\mathbb{F}_q$.
- $C^4 + 2D^3 = 0$. This is equivalent to $D^3/C^3 = 3C$, which is not possible since $3C$ is not a cube in $\mathbb{F}_q$.

Suppose now that $F_{C,D}(x)$ has no roots of multiplicity greater than 1. Then, the six roots are

$$\left\{ \frac{-\xi\overline{C}^3 \pm \overline{C}\xi^3\sqrt{D\xi}}{2\overline{C}^2}, \frac{-\xi^7\overline{C}^3 \pm \overline{C}\xi^3\sqrt{D\xi}}{\overline{C}^2}, \frac{-\xi^{13}\overline{C}^3 \pm \overline{C}\xi^3\sqrt{D\xi}}{4\overline{C}^2} \right\}.$$

These six solutions belong to a unique orbit under Frobenius if and only if ξD is a square in $\mathbb{F}_{q^3}$. This happens if and only if h is even and D is a non-zero square in $\mathbb{F}_q$, or h is odd and D is a non-square in $\mathbb{F}_q$. □

Proposition 3.2. *Let $q = 7^h$. The polynomial f_b is a PP in $\mathbb{F}_{q^6}$ of type* (18) *if and only if one of the following cases occurs:*

- $$b \in \left\{ 3\overline{B} \mid \overline{B} \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q,\ \overline{B}^2 \in \mathbb{F}_q^* \right\};$$
- $$b \in \left\{ 3\overline{D} + 3\overline{C} + \frac{\overline{C}^2}{\overline{D}} \;\middle|\; \overline{D} \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q,\ \overline{C} \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q,\ \overline{D}^2 \in \mathbb{F}_q^*,\ \overline{C}^3 \in \mathbb{F}_q^* \right\}.$$

Proof. We need to determine if the roots in $\mathbb{F}_{q^6}$ of the polynomials

$$F_{B,C}(x) := B^3x^6 + B^4x^4 - B^3Cx^3 + (5B^3+6C^2)B^2x^2 - BC(3B^3+4C^2)x + 6(B^3+6C^2)^2,$$

with $B, C \in \mathbb{F}_q$, $B \neq 0$, are contained in a unique orbit under the Frobenius map. Such roots are

$$\Big\{4\overline{B} + 6\overline{C} + 3\overline{C}^2/\overline{B}, 4\overline{B} + 5\overline{C} + 5\overline{C}^2/\overline{B}, 4\overline{B} + 3\overline{C} + 6\overline{C}^2/\overline{B},$$
$$3\overline{B} + 6\overline{C} + 4\overline{C}^2/\overline{B}, 3\overline{B} + 5\overline{C} + 2\overline{C}^2/\overline{B}, 3\overline{B} + 3\overline{C} + \overline{C}^2/\overline{B}\Big\},$$

where $\overline{B} \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $\overline{C} \in \mathbb{F}_{q^3}$ are such that $\overline{B}^2 = B$ and $\overline{C}^3 = C$, respectively. There are roots of multiplicity larger than one if and only if $C^4B^{15}(B^3+6C^2)^8 = 0$. Note that $B \neq 0$ by hypothesis and $B^3 = C^2$ would imply $C = \pm\overline{B}B \notin \mathbb{F}_q$, impossible. Also, $C = 0$ implies that the two distinct solutions of $F_{B,0}(x) = 0$ are $\pm 3\overline{B} \notin \mathbb{F}_q$ and the corresponding polynomial f_b is a PP.

If $C^4B^{15}(B^3+6C^2)^8 \neq 0$, all the roots of $F_{B,C}(x)$ are distinct. If $\overline{C} \in \mathbb{F}_q$ then there are three orbits under Frobenius, namely

$$\Big\{4\overline{B} + 6\overline{C} + 3\overline{C}^2/\overline{B}, 3\overline{B} + 6\overline{C} + 4\overline{C}^2/\overline{B}\Big\},$$
$$\Big\{4\overline{B} + 5\overline{C} + 5\overline{C}^2/\overline{B}, 3\overline{B} + 5\overline{C} + 2\overline{C}^2/\overline{B}\Big\},$$
$$\Big\{4\overline{B} + 3\overline{C} + 6\overline{C}^2/\overline{B}, 3\overline{B} + 3\overline{C} + \overline{C}^2/\overline{B}\Big\}.$$

The corresponding f_b are not PPs.

If $\overline{C} \notin \mathbb{F}_q$ then the six roots are contained in a unique orbit and therefore the corresponding f_b are PPs. □

Note that if q is even, then $q \equiv 2, 4, 8, 16 \pmod{28}$, whereas $7 \mid q$ implies $q \equiv 7, 14 \pmod{28}$.

Corollary 3.3. *Let $q \geq 421$ and let n_q be the number of PPs of $\mathbb{F}_{q^6}$ of type f_b.*

- *If $q \equiv 0, 1, 6, 8, 13, 14, 15, 27 \pmod{28}$, then $n_q = 0$.*
- *If $q \equiv 2, 3, 4, 5, 9, 11, 16, 17, 18, 19, 23, 25 \pmod{28}$, then $n_q = 3(q^2-1)$.*
- *If $q \equiv 7, 21 \pmod{28}$, then $n_q = 4q^2 - 3q - 1$.*

Proof. Note first that the values of b listed in Theorems 1.1 and 1.2 are all distinct for a fixed q.

1. The solutions of type (4) - (7) are

$$\begin{cases} 3(q-1)(q-2)+3(q-1)=3(q-1)^2, & q\equiv 3,5,17,19 \pmod{28}, \\ 3(q-1)q+3(q-1)=3(q^2-1), & q\equiv 9,11,23,25 \pmod{28}, \end{cases}$$

   If $q \equiv 3,5,17,19 \pmod{28}$ the number of solutions of type (3) is $6(q-1)$.

2. If q is even and $q \equiv 2,4 \pmod 7$, that is $q \equiv 2,4,16,18 \pmod{28}$, there are $q/2$ elements with trace 1 and $q/2$ elements with trace 0. For a fixed element $t \in \mathbb{F}_q$ there are $q-1$ pairs (u,v), $u \neq 0$, such that $v/u^2 = t$. For each of them there exist 6 corresponding b's. If $u = 0$, there are 3 values of b for each choice of $v \in \mathbb{F}_q^*$. The solutions of type (9) are $6\frac{q}{2}(q-1)$, whereas the number of solutions of type (8) is $3(q-1)$.

3. If $7 \mid q$, that is $q \equiv 7,21 \pmod{28}$, then the solutions of types (10), (11), (12), (13), (14), (15) are respectively $2(q-1)$, $2(q-1)^2$, $2(q-1)^2$, $2(q-1)$, $(q-1)$, $2(q-1)^2$. Therefore the total number of solutions is

$$2(q-1)+2(q-1)^2+2(q-1)+(q-1)+2(q-1)^2 = 4(q-1)^2+5(q-1) = 4q^2-3q-1.$$

□

Remark 3.4. *By using the same methods, it is possible to obtain similar descriptions of the values $b \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q$ which provide permutation polynomials of $\mathbb{F}_{q^4}$ of the type $x^{q^3+q^2+q+2}+bx$. By straightforward computations, if $q \equiv 2,3 \pmod 5$, then the values b satisfying the first condition in* [21, Theorem 4.1] *are as follows. Let $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be such that $a^2+a+1/5=0$; for each pair $(A,B) \in \mathbb{F}_q^2$ distinct from $(0,0)$, if $7A^2-20B \neq 0$, then*

$$b \in \left\{ \frac{-(2a+1)aA \pm 5\sqrt{(a+1)(7A^2-20B)}}{2(2a+1)}, \frac{(2a+1)(a+1)A \pm 5\sqrt{-a(7A^2-20B)}}{2(2a+1)} \right\},$$

otherwise

$$b \in \left\{ \frac{-aA}{2}, \frac{(a+1)A}{2} \right\}.$$

As to the second condition in [21, Theorem 4.1]*, no $b \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q$ can satisfy it when $q \equiv 4 \pmod 5$. If $q \equiv 2,3 \pmod 5$, then for each $A \in \mathbb{F}_q^*$ we have*

$$b \in \left\{ \frac{-(2a+1)aA \pm 5A\sqrt{-(a+1)}}{2(2a+1)}, \frac{(2a+1)(a+1)A \pm 5A\sqrt{a}}{2(2a+1)} \right\},$$

where $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ is such that $a^2+a+1/5=0$.

4 Necessary conditions for PPs of type $x^{\frac{q^n-1}{q-1}+1}+bx$, n odd

The Niederreiter-Robinson Criterion can be applied to any binomial of type $f_{q,b,n} = x^{\frac{q^n-1}{q-1}+1} + bx$ for some $n \in \mathbb{N}$. The algebraic curve $\mathcal{C}_{q,b,n}$ associated to $f_{q,b,n}$ is given by

$$\sum_{i=0}^{n} A_{n-i} \frac{x^{i+1} - y^{i+1}}{x - y} = 0,$$

where $A_0 = 1$ and $A_i = \sum_{0 \le j_1 < j_2 < \cdots < j_i \le (n-1)} b^{q^{j_1}+q^{j_2}+\cdots+q^{j_i}}$. Note that

$$A_1 = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b).$$

When n is odd, it is easily seen that the point $(1, -1, 0)$ belongs to $\mathcal{C}_{q,b,n}$ for every q and $b \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$.

Proposition 4.1. *Let $\mathcal{C}$ be an algebraic curve defined over $\mathbb{F}_q$ having a simple $\mathbb{F}_q$-rational point P. Then there exists an absolutely irreducible $\mathbb{F}_q$-rational component passing through P.*

Proof. Let $\mathcal{C}'$ be an absolutely irreducible $\mathbb{F}_q$-rational component of $\mathcal{C}$ containing P. The image $\mathcal{C}''$ of $\mathcal{C}'$ under the Frobenius map φ_q contains P, since $\varphi_q(P) = P$. Also, P being a simple point implies the existence of a unique component of $\mathcal{C}$ through it. Therefore $\mathcal{C}'' = \varphi_q(\mathcal{C}') = \mathcal{C}'$, that is $\mathcal{C}'$ is defined over $\mathbb{F}_q$. □

The above criterion is useful to deduce necessary conditions for a polynomial $f_{q,b,n}$ to be a PP. Let p be the characteristic of $\mathbb{F}_q$.

Theorem 4.2. *Let n be odd. Suppose $q > \frac{\left((n-1)(n-2)+\sqrt{n^2+13n-2}\right)^2}{4}$. If $f_{q,b,n}$ is a PP then $p \mid \frac{n+1}{2}$ and $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b) = 0$.*

Proof. We already observed that the point $P = (1, -1, 0)$ always belongs to the curve $\mathcal{C}_{q,b,n}$. We now show that if $f_{q,b,n}$ is a PP then the point P is a singular point of $\mathcal{C}_{q,b,n}$. Assume on the contrary that P is simple. Then by Proposition 4.1 the curve $\mathcal{C}_{q,b,n}$ contains an absolutely irreducible component defined over $\mathbb{F}_q$. Since $q > \frac{\left((n-1)(n-2)+\sqrt{n^2+13n-2}\right)^2}{4}$ this component contains an affine $\mathbb{F}_q$-rational point not lying on $X = 0$, $Y = 0$, or $X = Y$. Therefore by the Niederreiter-Robinson Criterion $f_{q,b,n}$ cannot be a PP, a contradiction.

Let $F(X, Y, T) = \sum_{i=0}^{n} A_{n-i} \frac{X^{i+1}-Y^{i+1}}{X-Y} T^{n-i}$ the homogenization of the polynomial defining $\mathcal{C}_{q,b,n}$. As P is singular, we have

$$\frac{\partial F(X,Y,T)}{\partial X}(1,-1,0) = \frac{\partial F(X,Y,T)}{\partial Y}(1,-1,0) = \frac{\partial F(X,Y,T)}{\partial T}(1,-1,0) = 0.$$

This is equivalent to

$$p \mid \frac{n+1}{2} \quad \text{and} \quad A_1 = 0.$$

□

A consequence of Theorem 4.2 is that for a given n odd there are just a finite number of characteristics p for which there exists a PP of type $f_{q,b,n}$.

For $n = 3$, Theorem 4.2 implies that for $q \geq 23$ odd there cannot be a PP of type $x^{q^2+q+2} + bx$. This is the main result in [5, Section 3].

For $n = 7$, $p = 2$, it has been shown in [7] that for q large enough the values b for which $f_{2^h,b,7}$ is a PP are exactly the roots of irreducible polynomials of type $x^7 + ax^3 + bx + c$ for some $a, b, c \in \mathbb{F}_q$. Note that for such b's, the monomial $b^{-1}x^{\frac{q^7-1}{q-1}+1}$ is a CPP. In particular, for $q = 2$ the values of b are $\{\eta^{2^i} : i = 0 \ldots 6\} \cup \{(\eta^{11})^{2^i} : i = 0 \ldots 6\}$, where η is a primitive element of $\mathbb{F}_{2^7}$.

The cases $n = 5, 9, 11, 13, 15$ are currently under investigation in [1].

References

[1] D. Bartoli, E. Franzé, and G. Zini, *Permutation binomials of type* $x^{\frac{q^k-1}{q-1}+1} + bx$*, k odd*, in preparation.

[2] U. Bartocci, B. Segre, *Ovali ed altre curve nei piani di Galois di caratteristica* 2, Acta Arith. **XVIII** (1971), 423–449.

[3] L.A. Bassalygo, V.A. Zinoviev, *On complete permutation polynomials*, in: "Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory", September 7 -13, 2014, Svetlogorsk (Kaliningad region), Russia, Proceedings, 57 – 62.

[4] L.A. Bassalygo, V.A. Zinoviev, *On one class of permutation polynomials over finite fields of characteristic two.* Preprint.

[5] L.A. Bassalygo, V.A. Zinoviev, *Permutation and complete permutation polynomials*, Finite Fields Appl. **33** (2015) 198–211.

[6] P. Charpin, G.M. Kyureghyan, *Cubic monomial bent functions: a subclass of* $\mathcal{M}^*$, SIAM J. Discrete Math. **22** (2) (2008), 650–665.

[7] E. Franzè, *Polinomi di permutazione*, Master thesis, Università degli Studi di Perugia.

[8] X. Hou, *Permutation polynomials over finite fields - A survey of recent advances*, Finite Fields Appl. **32** (2015) 82–119.

[9] R. Lidl, H. Niederreiter, *Finite Fields*. Encyclopedia of Mathematics and Its Applications Vol. 20, Addison-Wesley Publishing Company, London 1983.

[10] J. Ma, T. Zhang, T. Feng, G. Ge, *New results on permutation polynomials over finite fields*, arXiv:1506.05525.

[11] G. L. Mullen, Q. Wang, *Permutation polynomials: one variable*, in "Handbook of Finite Fields", Eds. G. L. Mullen, D. Panario, Chapman and Hall/CRC, 2013.

[12] A. Muratovic-Ribic, E. Pasalic, *A note on complete polynomials over finite fields and their applications in cryptography*, Finite Fields Appl. **25** (2014) 306–315.

[13] H. Niederreiter, K.H. Robinson, *Complete mappings of finite fields*, J. Austral. Math. Soc. (Series A) **33** (1982) 197–212.

[14] P. Stanica, S. Gangopadhyay, A. Chaturvedi, A.K. Gangopadhyay, S. Maitra, *Investigation on Bent and Negabent Functions via the Nega-Hadamard Transform*, IEEE Trans. Inf Theory **58**(6) (2012) 4064–4072.

[15] B. Segre, *Ovali e curve σ nei piani di Galois di caratteristica* 2, Atti dell'Accad. Naz. Lincei **32**(8) (1962), 785–790.

[16] S. Sarkar, S. Bhattacharya, A. Cesmelioglu, *On Some Permutation binomials of the form $x^{(2^h-1)/k+1} + ax$ over $\mathbb{F}_{2^h}$: Existence and Count*, International Workshop on the Arithmetic of Finite Fields, WAIFI 2012, Springer LNCS 7369, (2012) 236–246.

[17] H. Stichtenoth, *Algebraic function fields and codes*, Graduate Texts in Mathematics Vol. 254, 2nd edn. Springer, Berlin 2009.

[18] Z. Tu, X. Zeng, L. Hu, *Several classes of complete permutation polynomials*, Finite Fields Appl. **25** (2014), 182–193.

[19] S.G. Vladüt, D.Yu. Nogin, M.A. Tsfasman, *Algebraic-geometric codes*, Moscow, Independent Moscow University, 2003.

[20] G. Wu, N. Li, T. Helleseth, Y. Zhang, *Some classes of monomial complete permutation polynomials over finite fields of characteristic two*, Finite Fields Appl. **28** (2014) 148–165.

[21] G. Wu, N. Li, T. Helleseth, Y. Zhang, *Some classes of complete permutation polynomials over $\mathbb{F}_q$*, Sci. China Math. **58** (10) (2015), 2081–2094.

Daniele Bartoli and Massimo Giulietti are with
Dipartimento di Matematica e Informatica
Università degli Studi di Perugia
Via Vanvitelli, 1 - 06123 Perugia - Italy
emails: daniele.bartoli,massimo.giulietti@unipg.it

Giovanni Zini is with
Dipartimento di Matematica e Informatica "Ulisse Dini"
Università degli Studi di Firenze
Viale Morgagni, 67/A - 50134 Firenze - Italy
email: gzini@math.unifi.it