Finite Fields and Their Applications 88 (2023) 102179

Contents lists available at ScienceDirect

Finite Fields and Their Applications

journal homepage: www.elsevier.com/locate/ffa

New results on permutation binomials of finite fields

Xiang-dong Hou *, Vincenzo Pallozzi Lavorante

Department of Mathematics and Statistics, University of South Florida, Tampa, FL 33620, United States of America

ARTICLE INFO

Article history:
Received 25 November 2021
Received in revised form 12 November 2022
Accepted 17 January 2023
Available online 1 March 2023
Communicated by Gary L. Mullen

MSC:
11T06
11T55
14H05

Keywords:
Finite field
Hasse–Weil bound
Permutation binomial

ABSTRACT

After a brief review of the existing results on permutation binomials of finite fields, we introduce the notion of equivalence among permutation binomials (PBs) and describe how to bring a PB to its canonical form under equivalence. We then focus on PBs of $\mathbb{F}_{q^2}$ of the form $X^n(X^{d(q-1)}+a)$, where n and d are positive integers and $a \in \mathbb{F}_{q^2}^*$. Our contributions include two nonexistence results: (1) If q is even and sufficiently large and $a^{q+1} \neq 1$, then $X^n(X^{3(q-1)}+a)$ is not a PB of $\mathbb{F}_{q^2}$. (2) If $2 \leq d \mid q+1$, q is sufficiently large and $a^{q+1} \neq 1$, then $X^n(X^{d(q-1)}+a)$ is not a PB of $\mathbb{F}_{q^2}$ under certain additional conditions. (1) partially confirms a recent conjecture by Tu et al. (2) is an extension of a previous result with $n = 1$.

1. Introduction

Let $\mathbb{F}_q$ be the finite field with q elements and $\mathbb{F}_q^*$ be its multiplicative group. A polynomial $f \in \mathbb{F}_q[X]$ is called a permutation polynomial (PP) of $\mathbb{F}_q$ if it induces a permutation of $\mathbb{F}_q$. A permutation binomial (PB) of $\mathbb{F}_q$ is a PP of the form aX^m+bX^n, where $a, b \in \mathbb{F}_q^*$, $m \not\equiv 0$, $n \not\equiv 0$ and $m \not\equiv n \pmod{q-1}$. Permutation binomials are an active topic that

* Corresponding author.
E-mail addresses: xhou@usf.edu (X.-d. Hou), vincenzo@usf.edu (V. Pallozzi Lavorante).

https://doi.org/10.1016/j.ffa.2023.102179

has attracted much attention. We refer the reader to [1] for a survey on PBs and to [2] for a survey on PPs. Permutation binomials are complex objects; in general, one can not expect a simple criterion on the parameters q, m, n, a, b for $aX^m + bX^n$ to be a PB of $\mathbb{F}_q$. In this paper, we focus on PBs of $\mathbb{F}_{q^e}$ of the form

$$f_{q,e,n,d,a}(X) = X^n(X^{d(q-1)} + a) \in \mathbb{F}_{q^e}[X], \tag{1.1}$$

where $n, d \in \mathbb{Z}^+$, $n \not\equiv 0$, $d(q-1) \not\equiv 0$, $n + d(q-1) \not\equiv 0 \pmod{q^e - 1}$, and $a \in \mathbb{F}_{q^e}^*$. Here is an overview of our current knowledge on such PBs.

Result 1.1 *([14, Corollary 5.3]).* Assume $e = 2$ and $a^{q+1} = 1$. Then $f_{q,2,n,d,a} = X^n(X^{d(q-1)} + a)$ is a PB of $\mathbb{F}_{q^2}$ if and only if $\gcd(n, q-1) = 1$, $\gcd(n-d, q+1) = 1$ and $(-a)^{(q+1)/\gcd(q+1,d)} \neq 1$.

Result 1.2 *([3, Theorem A]).* Assume $e = 2$, $n = 1$, $d = 2$ and $a^{q+1} \neq 1$. Then $f_{q,2,1,2,a} = X(X^{2(q-1)} + a)$ is a PB of $\mathbb{F}_{q^2}$ if and only if q is odd and $(-a)^{(q+1)/2} = 3$.

Result 1.3 *([5, Theorem 1.1]).* Assume $e = 2$, $n = 1$, $d > 2$, $a^{q+1} \neq 1$, and q is large relative to d. Then $f_{q,2,1,d,a} = X(X^{d(q-1)} + a)$ is not a PB of $\mathbb{F}_{q^2}$.

Result 1.4 *([6,7]).* Assume $e = 2$, $n = 3$, $d = 2$ and $a^{q+1} \neq 1$. Then $f_{q,2,3,2,a} = X^3(X^{2(q-1)} + a)$ is a PB of $\mathbb{F}_{q^2}$ if and only if q is odd, $q \equiv -1 \pmod 3$ and $(-a)^{(q+1)/2} = 1/3$.

Result 1.5 *([11, Theorem 1]).* Assume $e = 2$, $q = 2^{2m}$ and $d = 3$. Then $f_{q,2,n,3,a} = X^n(X^{3(q-1)} + a)$ is a PB of $\mathbb{F}_{q^2}$ if and only if $\gcd(n, q-1) = 1$, $n \equiv 3 \pmod{q+1}$ and $a^{q+1} \neq 1$.

(Note: In the original statement of Result 1.5 in [11], it is assumed that $m \geq 2$. However, the result also holds for $m = 1$; see Example 2.4.)

Result 1.6 *([4, Theorem 4.2]).* Assume $e = 2$ and $d = 1$. Then $f_{q,2,n,1,a} = X^n(X^{q-1} + a)$ is a PB of $\mathbb{F}_{q^2}$ if and only if $\gcd(n, q-1) = 1$, $n \equiv 1 \pmod{q+1}$ and $a^{q+1} \neq 1$.

Result 1.7 *([8]).* Assume $e \geq 2$, $d = 1$ and $n < q^e - q$. For the special cases $(q, e) = (q, 2), (q, 3), (q, 4), (p, 5), (p, 6)$, where p is a prime, the following statement is true: If $f_{q,e,n,1,a} = X^n(X^{q-1} + a)$ is a PB of $\mathbb{F}_{q^e}$, then $f_{q,e,n,1,a} \equiv X^{nq^h} + aX^n \pmod{X^{q^e} - X}$ for some integer $h > 0$. It is conjectured that the statement is true for all q.

(Note: In Result 1.7, when $q = 2$, $f_{2,e,n,1,a} = X^n(X + a)$ is never a PB of $\mathbb{F}_{2^e}$, so the statement is vacuously true.)

Through these results, we begin to understand the roles played by the parameters in the PBs of the form (1.1). At the same time, as more results on PBs gather, one feels a need for a properly defined notion of *equivalence* of PBs that allows us to categorize the existing results and channel future efforts to PBs that are new under equivalence. Section 2 is included for this purpose. We define the equivalence among all PBs (not just those of the form (1.1)). We show that every PB can be brought to a canonical form which is uniquely determined by a triple of invariants. In particular, we see that the PB in Result 1.4 is equivalent to a PB in Result 1.2 and the PB in Result 1.5 is equivalent to a PB in Result 1.6.

Regarding Result 1.5, if we assume $e = 2$, $q = 2^{2m+1}$, $d = 3$ and $a^{q+1} \neq 1$, [11] conjectured that $f_{q,2,n,3,a} = X^n(X^{3(q-1)} + a)$ is not a PB of $\mathbb{F}_{q^2}$ and provided strong evidence for this conjecture. Note that in this case, $d \mid q+1$. As we will see in Section 2, when the PB in (1.1) is brought to its canonical form, we always have $d \mid (q^e-1)/(q-1)$.

Let us further focus on the case $e = 2$, and we assume $d \mid q+1$ by the above comment. In this case, if $a^{q+1} = 1$ or $d = 1$, all PBs are given by Results 1.1 and 1.6. Therefore, we assume $e = 2$, $2 \le d \mid q+1$ and $a^{q+1} \neq 1$. Under these assumptions and up to equivalence, the PBs in Result 1.2 form the only known class that contains infinitely many q's. This leads to the following question.

Question 1.8. Fix integers $n \ge 1$ and $d \ge 2$. If there are infinitely many pairs (q, a) such that $d \mid q+1$, $a \in \mathbb{F}_{q^2}^*$, $a^{q+1} \neq 1$, and $f(X) = f_{q,2,n,d,a}(X) = X^n(X^{d(q-1)} + a)$ is a PB of $\mathbb{F}_{q^2}$, can we conclude that when q is sufficiently large, f is equivalent the PB in Result 1.2?

In this paper, we prove two nonexistence results that support an affirmative answer to the above question.

Theorem 1.9. *Let $q = 2^m$, $n \ge 1$ and $a \in \mathbb{F}_{q^2}^*$ be such that $q \ge (2\max\{n, 6-n\})^4$ and $a^{q+1} \neq 1$. Then $f(X) = f_{q,2,n,3,a}(X) = X^n(X^{3(q-1)} + a)$ is not a PB of $\mathbb{F}_{q^2}$.*

Theorem 1.9 proves the conjecture of [11] when q is large relative to n.

Theorem 1.10. *Let $n \ge 1$, $d \ge 2$ and $a \in \mathbb{F}_{q^2}^*$ be such that $d \mid q+1$, $q \ge (2\max\{n, 2d-n\})^4$ and $a^{q+1} \neq 1$. Then $f(X) = f_{q,2,n,d,a}(X) = X^n(X^{d(q-1)} + a)$ is not a PB of $\mathbb{F}_{q^2}$ if one of the following conditions is satisfied.*

(i) *$d - n > 1$ and either $d - n$ is not a power of p ($= \operatorname{char} \mathbb{F}_q$) or $\gcd(d, n+1)$ is a power of 2.*
(ii) *$d + 2 \le n < 2d$ and either $n - d$ is not a power of p or $\gcd(d, n-1)$ is a power of 2.*
(iii) *$n \ge 2d$, $\gcd(n-d, q-1) = 1$ and either $n - d$ is not a power of p or $\gcd(d, n-1)$ is a power of 2.*

Remark 1.11. In Theorem 1.10, one can replace the assumption that $d \mid q+1$ with $\gcd(n, d) = 1$. If the f in Theorem 1.10 is a PB of $\mathbb{F}_{q^2}$, then $d \mid q+1$ implies $\gcd(n, d) = 1$.

However, as we will see in Section 4, the proof of Theorem 1.10 only uses $\gcd(n, d) = 1$. Moreover, the assumption that $\gcd(n, d) = 1$ causes no loss of generality. If $f_{q,2,n,d,a}$ is a PB of $\mathbb{F}_{q^2}$ with $\gcd(n, d) = \delta$, then $\gcd(\delta, q^2 - 1) = 1$. Let $\delta' \in \mathbb{Z}^+$ be such that $\delta\delta' \equiv 1 \pmod{q^2 - 1}$. Then

$$f_{q,2,n,d,a}(X^{\delta'}) \equiv f_{q,2,n/\delta,d/\delta,a}(X) \pmod{X^{q^2} - X},$$

where $\gcd(n/\delta, d/\delta) = 1$.

Result 1.3 is a special case of Theorem 1.10 (i) with $n = 1$. In fact, the conditions in Theorem 1.10 are quite general; they cover almost all cases such that $|d - n|$ is not a power of p.

Theorems 1.9 and 1.10 are proved in Sections 3 and 4, respectively. The method is similar to that in [5]. Here we recall the basic strategy.

Let

$$f(X) = f_{q,2,n,d,a}(X) = X^n(X^{d(q-1)} + a) \in \mathbb{F}_{q^2}[X], \tag{1.2}$$

where $n \geq 1$, $2 \leq d \mid q+1$ and $a \in \mathbb{F}_{q^2}^*$. The following theorem follows from a well-known folklore [9,12,13].

Theorem 1.12. *The binomial $f(X)$ in (1.2) is PB of $\mathbb{F}_{q^2}$ if and only if*

(i) $\gcd(n, d(q-1)) = 1$ *and*
(ii) $X^n(X^d + a)^{q-1}$ *permutes* $\mu_{q+1} := \{x \in \mathbb{F}_{q^2}^* : x^{q+1} = 1\}$.

Assume that $f(X)$ in (1.2) is a PB of $\mathbb{F}_{q^2}$. Then for $x \in \mu_{q+1}$,

$$x^n(x^d + a)^{q-1} = \frac{x^n(x^{dq} + a^q)}{x^d + a} = \frac{x^n(a^q x^d + 1)}{x^d(x^d + a)} = G(x),$$

where

$$G(X) = \frac{a^q X^n + X^{n-d}}{X^d + a}. \tag{1.3}$$

Write

$$G(X) = \frac{P(X)}{Q(X)},$$

where

$$\begin{cases} P(X) = a^q X^n + X^{n-d}, \\ Q(X) = X^d + a, \end{cases} \qquad \text{if } n \geq d,$$

$$\begin{cases} P(X) = a^q X^d + 1, \\ Q(X) = X^{2d-n} + aX^{d-n}, \end{cases} \quad \text{if } n < d.$$

We assume that $a^{q+1} \neq 1$, which implies that $\gcd(P, Q) = 1$. Thus

$$\deg G = \begin{cases} n & \text{if } n \geq d, \\ 2d - n & \text{if } n < d. \end{cases}$$

Let

$$N(G) = \frac{P(X)Q(Y) - P(Y)Q(X)}{X - Y} \in \mathbb{F}_{q^2}[X, Y], \tag{1.4}$$

which is the numerator of $(G(X) - G(Y))/(X - Y)$. We have

$$\deg N(G) \leq \begin{cases} n + d - 1 & \text{if } n \geq d, \\ 3d - n - 1 & \text{if } n < d. \end{cases}$$

Theorem 1.13. *Assume that $f(X)$ in (1.2) is a PB of $\mathbb{F}_{q^2}$, where $q \geq (2\max\{n, 2d-n\})^4$. Then $N(G)$ in (1.4) is reducible in $\overline{\mathbb{F}}_q[X, Y]$, where $\overline{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$.*

Proof. We only give a sketch of the proof; the omitted details are given in [5, §3].

There exist $l_1, l_2 \in \mathbb{F}_{q^2}(X)$ of degree one such that $H := l_1 \circ G \circ l_2$ permutes $\mathbb{F}_q$. Since $\deg H = \deg G < q$, by [5, Lemma 3.2], $H \in \mathbb{F}_q(X)$. Let $A(X, Y) = N(H) \in \mathbb{F}_q[X, Y]$, the numerator of $(H(X) - H(Y))/(X - Y)$. Assume to the contrary that $N(G)$ is irreducible over $\overline{\mathbb{F}}_q$. Then by [5, Lemma 3.1], $A(X, Y)$ is also irreducible over $\overline{\mathbb{F}}_q$. We have

$$\delta := \deg A(X, Y) \leq 2\deg H - 2 = 2\deg G - 2.$$

By the Hasse-Weil bound, the number of zeros of $A(X, Y)$ in the projective plane $\mathbb{P}^2(\mathbb{F}_q)$ is at least

$$q + 1 - (\delta - 1)(\delta - 2)q^{1/2}.$$

Excluding the zeros at infinity of $\mathbb{P}^2(\mathbb{F}_q)$ and on the diagonal $\{(x, x) : x \in \mathbb{F}_q\}$ of the affine plane $\mathbb{F}_q^2$, we have

$$|\{(x, y) \in \mathbb{F}_q^2 : x \neq y,\ A(x, y) = 0\}| \geq q - (\delta - 1)(\delta - 2)q^{1/2} - 2\delta.$$

The right side is positive since $q \geq \delta^4$. Hence there exists $(x, y) \in \mathbb{F}_q^2$ with $x \neq y$ such that $A(x, y) = 0$. Then $H(x) = H(y)$, which is a contradiction. $\square$

2. Canonical forms of permutation binomials

For our purpose, a binomial over $\mathbb{F}_q$ is a polynomial of the

$$f(X) = aX^m + bX^n \in \mathbb{F}_q[X],$$

where $a, b \in \mathbb{F}_q^*$, $m, n > 0$, $m \not\equiv 0$, $n \not\equiv 0$ and $m \not\equiv n \pmod{q-1}$. We treat $f(X)$ as a function from $\mathbb{F}_q$ to $\mathbb{F}_q$, that is, we identify $f(X)$ with its image in the quotient ring $\mathbb{F}_q[X]/\langle X^q - X\rangle$. Let $\mathcal{B}_q$ denote the set of all such binomials. Two members $f, g \in \mathcal{B}_q$ are considered *equivalent*, denoted as $f \sim g$, if one can be obtained from the other through a combination of the following transformations of $\mathcal{B}_q$:

$$\alpha_u : \mathcal{B}_q \to \mathcal{B}_q,\ f(X) \mapsto uf(X), \quad u \in \mathbb{F}_q^*, \tag{2.1}$$

$$\beta : \mathcal{B}_q \to \mathcal{B}_q,\ f(X) \mapsto f(X)^p, \quad p = \operatorname{char} \mathbb{F}_q, \tag{2.2}$$

$$\gamma_{v,s} : \mathcal{B}_q \to \mathcal{B}_q,\ f(X) \mapsto f(vX^s), \quad v \in \mathbb{F}_q^*,\ s \in \mathbb{Z}^+,\ \gcd(s, q-1) = 1. \tag{2.3}$$

If $f, g \in \mathcal{B}_q$ are equivalent, then f permutes $\mathbb{F}_q$ if and only if g does. It is clear that $\gamma_{v,s}$ commutes with α_u and β, and $\beta \circ \alpha_u = \alpha_{u^p} \circ \beta$. Therefore, for $f, g \in \mathcal{B}_q$, $f \sim g$ if and only if

$$g(X) = uf(vX^s)^{p^i} \tag{2.4}$$

for some $u, v \in \mathbb{F}_q^*$, $i \geq 0$ and $s > 0$ with $\gcd(s, q-1) = 1$.

For $d \mid q-1$, define

$$N_d = \{1 \leq n \leq q-1 : n = n^*\}, \tag{2.5}$$

where

$$\begin{aligned} n^* = \min\bigl\{1 \leq n' \leq q-1 : {} & n' \equiv tn \pmod{q-1} \text{ for some } t \in \mathbb{Z}_{q-1}^\times \\ & \text{with } t \equiv 1 \pmod{(q-1)/d} \text{ or} \\ & n' \equiv tn - d \pmod{q-1} \text{ for some } t \in \mathbb{Z}_{q-1}^\times \\ & \text{with } t \equiv -1 \pmod{(q-1)/d}\bigr\}. \end{aligned}$$

(Here $\mathbb{Z}_{q-1}^\times$ denotes the multiplicative group of $\mathbb{Z}_{q-1}$.) Let $\theta : \mathbb{Z}_{q-1}^\times \to \mathbb{Z}_{(q-1)/d}^\times$ be the natural homomorphism (which is onto). Then $G := \theta^{-1}(\{\pm 1\})$ acts on $\mathbb{Z}_{q-1}$ as follows: For $t \in G$ and $n \in \mathbb{Z}_{q-1}$,

$$t(n) = \begin{cases} tn & \text{if } \theta(t) = 1, \\ tn - d & \text{if } \theta(t) = -1. \end{cases}$$

Write $\mathbb{Z}_{q-1} = \{1, 2, \dots, q-1\}$. Then for $n \in \mathbb{Z}_{q-1}$, n^* is the least element in the G-orbit of n. Therefore N_d is the set of least elements of the G-orbits in $\mathbb{Z}_{q-1}$.

Example 2.1. Let $q = 2^4$ and $d = 3$. We have $\theta : \mathbb{Z}_{15}^\times \to \mathbb{Z}_5^\times$, $\theta^{-1}(1) = \{1, 11\}$, $\theta^{-1}(-1) = \{-1, 4\}$ and $G = \{1, 11, -1, 4\}$. The G-orbits of $\mathbb{Z}_{15}$ are $\{1, 11\}$, $\{2, 7, 10, 5\}$, $\{3, 9\}$, $\{4, 14, 8, 13\}$, $\{6\}$, $\{15\}$. Hence $N_d = \{1, 2, 3, 4, 6, 15\}$.

For $d \mid q-1$ and $n \in N_d$, let

$$G_{d,n} = \text{the subgroup of } \mathbb{Z}_d^\times \text{ generated by} \qquad (2.6)$$
$$\begin{cases} \{p, -1\} & \text{if } d \equiv -2n \pmod{(q-1)/d} \text{ and } \gcd(n, q-1) = 1, \\ \{p\} & \text{otherwise,} \end{cases}$$

where $p = \operatorname{char} \mathbb{F}_q$. Let $G_{d,n}$ act on $\mathbb{F}_q^*/(\mathbb{F}_q^*)^d$, where $(\mathbb{F}_q^*)^d = \{x^d : x \in \mathbb{F}_q^*\}$, as follows:

$$\begin{array}{ccc} G_{d,n} \times \mathbb{F}_q^*/(\mathbb{F}_q^*)^d & \longrightarrow & \mathbb{F}_q^*/(\mathbb{F}_q^*)^d \\ (s, a(\mathbb{F}_q^*)^d) & \longmapsto & a^s(\mathbb{F}_q^*)^d, \quad a \in \mathbb{F}_q^*. \end{array}$$

Let $A_{d,n} \subset \mathbb{F}_q^*$ be such that $\{a(\mathbb{F}_q^*)^d : a \in A_{d,n}\}$ is a system of representatives of the $G_{d,n}$-orbits in $\mathbb{F}_q^*/(\mathbb{F}_q^*)^d$. Equivalently, let $G_{d,n}$ act on $\mathbb{Z}_d$ through multiplication and let ξ be a primitive element of $\mathbb{F}_q$. Then $A_{d,n} = \{\xi^e : e \in E_{d,n}\}$, where $E_{d,n}$ is a system of representatives of the $G_{d,n}$-orbits in $\mathbb{Z}_d$.

We now are ready to state and prove the main result of this section.

Theorem 2.2. *Assume that $f \in \mathcal{B}_q$ permutes $\mathbb{F}_q$. Then there is a unique triple (d, n, a), where $d \mid q-1$, $n \in N_d$ and $a \in A_{d,n}$, such that*

$$f(X) \sim X^n(X^d + a). \qquad (2.7)$$

We call the right side of (2.7) the canonical form *of f.*

Proof. *Existence of (d, n, a).*

Write $f(X) = a_0X^{m_0} + b_0X^{n_0}$, where $a_0, b_0 \in \mathbb{F}_q^*$ and $m_0 > n_0$. Let $d = \gcd(m_0 - n_0, q-1)$. Let $r \in \mathbb{Z}^+$ be such that

$$r\frac{m_0 - n_0}{d} \equiv 1 \pmod{\frac{q-1}{d}}.$$

Since $\gcd(r, (q-1)/d) = 1$, there exists an integer $k \geq 0$ such that $s := r + k(q-1)/d$ is relatively prime to $q-1$. (To see this, use Dirichlet's theorem on primes in arithmetic progression or the following simple argument: Let $p_1, \dots, p_l$ be the prime divisors of $q-1$ that do not divide r and let $k = p_1 \cdots p_l$.) Then

$$f(X) \sim f(X^s) = X^{sn_0}(a_0X^{s(m_0-n_0)} + b_0) = X^{n_1}(a_0X^d + b_0),$$

where $n_1 = sn_0$. We now assume $f(X) = X^{n_1}(a_0X^d + b_0)$.

Let $n = n_1^* \in N_d$. We claim that

$$f(X) \sim X^n(a_1X^d + b_1) \tag{2.8}$$

for some $a_1, b_1 \in \mathbb{F}_q^*$. To prove this claim, we consider two cases.

Case 1. Assume that $n \equiv tn_1 \pmod{q-1}$ for some $t \in \mathbb{Z}_{q-1}^\times$ with $t \equiv 1 \pmod{(q-1)/d}$. Then

$$f(X) \sim f(X^t) = X^{tn_1}(a_0X^{td} + b_0) = X^n(a_0X^d + b_0).$$

Case 2. Assume that $n \equiv tn_1 - d \pmod{q-1}$ for some $t \in \mathbb{Z}_{q-1}^\times$ with $t \equiv -1 \pmod{(q-1)/d}$. Then

$$\begin{aligned} f(X) \sim f(X^t) &= X^{tn_1}(a_0X^{td} + b_0) = a_0X^{tn_1+td} + b_0X^{tn_1} \\ &= a_0X^n + b_0X^{n+d} = X^n(b_0X^d + a_0). \end{aligned}$$

Hence (2.8) is proved.

By (2.8), we may assume

$$f(X) = X^n(X^d + c),$$

where $c \in \mathbb{F}_q^*$. To prove that $f(X) \sim X^n(X^d + a)$ for some $a \in A_{d,n}$, again, we consider two cases.

Case 1. Assume that $d \not\equiv -2n \pmod{(q-1)/d}$ or $\gcd(n, q-1) \neq 1$. By (2.6), $G_{d,n} = \langle p \rangle < \mathbb{Z}_d^\times$. Then by the definition of $A_{d,n}$, there exist $i \in \mathbb{N}$, $a \in A_{d,n}$ and $b \in \mathbb{F}_q^*$ such that $c^{p^i} = ab^d$. Write $b = b_1^{p^i}$, where $b_1 \in \mathbb{F}_q^*$. Let $s \in \mathbb{Z}^+$ be such that $sp^i \equiv 1 \pmod{q-1}$. Then

$$\begin{aligned} f(X) &\sim f(b_1X^s)^{p^i} = (b_1X^s)^{np^i}((b_1X^s)^{dp^i} + c^{p^i}) \\ &\sim X^n(b_1^{dp^i}X^d + c^{p^i}) = X^n(b^dX^d + c^{p^i}) \\ &\sim X^n(X^d + c^{p^i}b^{-d}) = X^n(X^d + a). \end{aligned}$$

Case 2. Assume that $d \equiv -2n \pmod{(q-1)/d}$ and $\gcd(n, q-1) = 1$. Then $G_{d,n} = \langle p, -1 \rangle < \mathbb{Z}_d^\times$. So there exist $i \in \mathbb{N}$, $a \in A_{d,n}$ and $b \in \mathbb{F}_q^*$ such that either $c^{p^i} = ab^d$ or $c^{-p^i} = ab^d$. In the former case, the proof is identical to Case 1. In the latter case, write $b = b_1^{p^i}$, where $b_1 \in \mathbb{F}_q^*$. Let $k \in \mathbb{Z}^+$ be such that $kn \equiv 1 \pmod{q-1}$, and let $s = 1 + kd$. Then

$$\begin{aligned} sn = n + nkd &\equiv n + d \pmod{q-1} \\ &\equiv -n \pmod{(q-1)/d}. \end{aligned}$$

Hence $s \equiv -1 \pmod{(q-1)/d}$. It follows that $\gcd(s, (q-1)/d) = 1$. We also have $\gcd(s, d) = \gcd(1 + kd, d) = 1$. Therefore $\gcd(s, q-1) = 1$. We have

$$f(X) \sim f(X^s) = X^{sn}(X^{sd} + c) = X^{sn+sd} + cX^{sn}.$$

In the above,

$$sn = n + nkd \equiv n + d \pmod{q-1}$$

and

$$sd = (1 + kd)d \equiv (1 + k(-2n))d \equiv -d \pmod{q-1}.$$

Hence

$$f(X) \sim X^n + cX^{n+d} \sim X^n(X^d + c^{-1}),$$

where $(c^{-1})^{p^i} = ab^d$. It follows from Case 1 that

$$X^n(X^d + c^{-1}) \sim X^n(X^d + a).$$

Uniqueness of (d, n, a).

Assume that

$$f(X) = X^n(X^d + a) \sim X^{n_1}(X^{d_1} + a_1), \tag{2.9}$$

where $d \mid q-1$, $n \in N_d$, $a \in A_{d,n}$, $d_1 \mid q-1$, $n_1 \in N_{d_1}$, $a_1 \in A_{d_1,n_1}$.

In general, for $bX^m + cX^l \in \mathcal{B}_q$, $\gcd(m-l, q-1)$ is invariant under equivalence. Therefore, in (2.9), we have $d = d_1$.

By (2.9),

$$X^{n_1}(X^d + a_1) = uf(vX^s)^{p^i} \tag{2.10}$$

for some $u, v \in \mathbb{F}_q^*$, $i \ge 0$ and $s > 0$ with $\gcd(s, q-1) = 1$. Expanding (2.10) gives

$$X^{n_1+d} + a_1X^{n_1} = \alpha X^{t(n+d)} + \beta X^{tn},$$

where $t = sp^i$ and $\alpha, \beta \in \mathbb{F}_q^*$. It follows that

$$\begin{cases} n_1 + d \equiv t(n+d) \pmod{q-1}, \\ n_1 \equiv tn \pmod{q-1}, \end{cases} \tag{2.11}$$

or

$$\begin{cases} n_1 + d \equiv tn \pmod{q-1}, \\ n_1 \equiv t(n+d) \pmod{q-1}. \end{cases} \tag{2.12}$$

Note that (2.11) is equivalent to

$$\begin{cases} t \equiv 1 \pmod{(q-1)/d}, \\ n_1 \equiv tn \pmod{q-1}, \end{cases} \tag{2.13}$$

and (2.12) is equivalent to

$$\begin{cases} t \equiv -1 \pmod{(q-1)/d}, \\ n_1 \equiv tn - d \pmod{q-1}. \end{cases} \tag{2.14}$$

Since $n \in N_d$, it follows from (2.13), (2.14) and the definition of N_d ((2.5)) that $n \le n_1$. By symmetry, $n_1 \le n$, whence $n = n_1$.

Now (2.10) becomes

$$\begin{aligned} X^{n+d} + a_1 X^n &= u\big[(vX^s)^{n+d} + a(vX^s)^n\big]^{p^i} \\ &= uv^{p^i(n+d)} X^{sp^i(n+d)} + ua^{p^i} v^{p^i n} X^{sp^i n}. \end{aligned}$$

Let $t = sp^i$. Then there are two possibilities.

Case 1. (2.13) holds with $n = n_1$ and

$$(uv^{p^i(n+d)},\, ua^{p^i} v^{p^i n}) = (1, a_1). \tag{2.15}$$

Case 2. (2.14) holds with $n = n_1$ and

$$(ua^{p^i} v^{p^i n},\, uv^{p^i(n+d)}) = (1, a_1). \tag{2.16}$$

It suffices to show that in both cases, a and a_1 are in the same $G_{d,n}$-orbit. (Then $a = a_1$.)

First, assume Case 1. We have

$$a_1 = \frac{ua^{p^i} v^{p^i n}}{uv^{p^i(n+d)}} = a^{p^i} v^{-p^i d},$$

which is in the $G_{d,n}$-orbit of a.

Next, assume Case 2. (2.14) with $n = n_1$ gives

$$\begin{cases} t \equiv -1 \pmod{(q-1)/d}, \\ n \equiv tn - d \pmod{q-1}. \end{cases}$$

It follows that $n \equiv tn - d \equiv -n - d \pmod{(q-1)/d}$, i.e., $d \equiv -2n \pmod{(q-1)/d}$. Since $f(X)$ permutes $\mathbb{F}_q$, we have $\gcd(n, d) = 1$. From $n \equiv tn - d \pmod{q-1}$, we have $(t-1)n - d \equiv 0 \pmod{q-1}$, whence $d \mid t - 1$ and

$$\frac{t-1}{d}n - 1 \equiv 0 \pmod{\frac{q-1}{d}}.$$

In particular, $\gcd(n, (q-1)/d) = 1$. Combining this with $\gcd(n, d) = 1$, we have $\gcd(n, q-1) = 1$. Therefore $G_{d,n} = \langle p, -1\rangle$. Now by (2.16),

$$a_1 = \frac{uv^{p^i(n+d)}}{ua^{p^i}v^{p^in}} = a^{-p^i}v^{p^id},$$

which is in the $G_{d,n}$-orbit of a. □

Example 2.3. Assume that $n, d \in \mathbb{Z}^+$ are such that $d \mid q+1$, $n < 2d$, $\gcd(n, q^2-1) = 1$ and $\gcd(2d-n, q-1) = 1$, and let $a \in \mathbb{F}_{q^2}^*$. Since $\gcd(dq-n+d, q-1) = \gcd(2d-n, q-1) = 1$ and $\gcd(dq - n + d, q + 1) = \gcd(n, q + 1) = 1$, we have $\gcd(dq - n + d, q^2 - 1) = 1$. Then in $\mathcal{B}_q$,

$$\begin{aligned}
X^n(X^{d(q-1)} + a) &= X^{dq+n-d} + aX^n \\
&\sim X^{(dq-n+d)(dq+n-d)} + aX^{(dq-n+d)n} \qquad (X \mapsto X^{dq-n+d}) \\
&= X^{d^2q^2-(n-d)^2} + aX^{(dq-n+d)n} \\
&= X^{d^2-(n-d)^2} + aX^{(dq-n+d)n} \\
&= X^{n(2d-n)} + aX^{(dq-n+d)n} \\
&\sim X^{2d-n} + aX^{dq-n+d} \qquad (X^n \mapsto X) \\
&= X^{2d-n}(1 + aX^{d(q-1)}) \\
&\sim X^{2d-n}(X^{d(q-1)} + a^{-1}).
\end{aligned}$$

In particular, when $n = 1$, $d = 2$, q is odd and $q \not\equiv 1 \pmod 3$, we have

$$X(X^{2(q-1)} + a) \sim X^3(X^{2(q-1)} + a^{-1}).$$

This shows that the PB in Result 1.4 is equivalent to a PB in Result 1.2.

Example 2.4. We show that the PB in Result 1.5 is equivalent to a PB in Result 1.6. Let $e = 2$, $q = 2^{2m}$, $n \in \mathbb{Z}^+$, $d = 3$, $a \in \mathbb{F}_{q^2}^*$, and consider $f = f_{q,2,n,3,a} = X^n(X^{3(q-1)} + a)$.

Let $s = (q + 2)/3 + k(q + 1)$, where

$$k = \begin{cases} 0 & \text{if } m \equiv 0, 1 \pmod 3, \\ 1 & \text{if } m \equiv -1 \pmod 3. \end{cases}$$

We claim that $\gcd(s, q^2-1)=1$. Clearly, $\gcd(s, q+1)=1$. We have

$$\begin{aligned}\gcd(s, q-1) &= \gcd\Big(\frac{q+2}{3}+2k,\ q-1\Big)\\ &= \frac{1}{3}\gcd(q+2+6k,\ 3q-3)\\ &= \frac{1}{3}\gcd(q+2+6k,\ 3(-2-6k)-3)\\ &= \frac{1}{3}\gcd(q+2+6k,\ 9(2k+1)).\end{aligned}$$

In the above, $9(2k+1)=3^2$ or 3^3, and

$$\begin{aligned}q+2+6k &= (3-1)^{2m}+2+6k\\ &\equiv 1-2m\cdot 3+2+6k \pmod{3^2}\\ &= 3+6(k-m)\\ &\not\equiv 0 \pmod{3^2}.\end{aligned}$$

So $\gcd(s, q-1)=1$ and the claim is proved.

Now we have

$$f(X)\sim f(X^s)=X^{sn}(X^{s\cdot 3(q-1)}+a)=X^{sn}(X^{q-1}+a).$$

By Result 1.6, $X^{sn}(X^{q-1}+a)$ permutes $\mathbb{F}_{q^2}$ if and only if

$$\gcd(sn, q-1)=1,\quad sn\equiv 1 \pmod{q+1},\quad \text{and } a^{q+1}\neq 1,$$

i.e.,

$$\gcd(n, q-1)=1,\quad n\equiv 3 \pmod{q+1},\quad \text{and } a^{q+1}\neq 1,$$

which are precisely the conditions in Result 1.5.

3. Proof of Theorem 1.9

Theorem 1.9. *Let $q=2^m$, $n\geq 1$ and $a\in\mathbb{F}_{q^2}^*$ be such that $q\geq(2\max\{n, 6-n\})^4$ and $a^{q+1}\neq 1$. Then $f(X)=f_{q,2,n,3,a}(X)=X^n(X^{3(q-1)}+a)$ is not a PB of $\mathbb{F}_{q^2}$.*

Assume to the contrary that f is a PB of $\mathbb{F}_{q^2}$. If m is even, by Result 1.5, $n\geq q+4$, which is a contradiction. So m is odd, and $3\mid q+1$. By (1.3),

$$G(X)=\frac{a^qX^n+X^{n-3}}{X^3+a}. \tag{3.1}$$

Let

$$N(X,Y) = \text{the numerator of } \frac{G(X)+G(Y)}{X+Y}. \tag{3.2}$$

By Theorem 1.13, $N(X,Y)$ is reducible over $\overline{\mathbb{F}}_q$. However, we will show that $N(X,Y)$ is irreducible over $\overline{\mathbb{F}}_q$, a contradiction. We consider two cases, $n \ge 3$ and $n \le 2$, separately.

3.1. Case 1. $n \ge 3$

Since $\gcd(n, 3(q-1)) = 1$ (Theorem 1.12), we have $n > 3$. We have

$$\begin{aligned} N(X,Y) &= \frac{1}{X+Y}\Big[(a^qX^n + X^{n-3})(Y^3+a) + (a^qY^n + Y^{n-3})(X^3+a)\Big] \\ &= a\frac{X^{n-3}+Y^{n-3}}{X+Y} + \Big[a^{q+1}\frac{X^n+Y^n}{X+Y} + X^3Y^3\frac{X^{n-6}+Y^{n-6}}{X+Y}\Big] \\ &\quad + a^qX^3Y^3\frac{X^{n-3}+Y^{n-3}}{X+Y}. \end{aligned}$$

The homogenization of $N(X,Y)$ is

$$\begin{aligned} N^*(X,Y,Z) &= a\frac{X^{n-3}+Y^{n-3}}{X+Y}Z^6 + \Big[a^{q+1}\frac{X^n+Y^n}{X+Y} + X^3Y^3\frac{X^{n-6}+Y^{n-6}}{X+Y}\Big]Z^3 \\ &\quad + a^qX^3Y^3\frac{X^{n-3}+Y^{n-3}}{X+Y} \\ &= Q(Z^3), \end{aligned}$$

where

$$\begin{aligned} Q(Z) &= a\frac{X^{n-3}+Y^{n-3}}{X+Y}Z^2 + \Big[a^{q+1}\frac{X^n+Y^n}{X+Y} + X^3Y^3\frac{X^{n-6}+Y^{n-6}}{X+Y}\Big]Z \\ &\quad + a^qX^3Y^3\frac{X^{n-3}+Y^{n-3}}{X+Y}. \end{aligned}$$

It suffices to show that $N^*(X,Y,Z)$ is irreducible over $\overline{\mathbb{F}}_q$. We first show that $N^*(X,Y,Z)$, as a polynomial in Z over $\overline{\mathbb{F}}_q[X,Y]$, is primitive, i.e., the gcd of its coefficients is 1; that is,

$$\gcd\Big(\frac{X^{n-3}+Y^{n-3}}{X+Y},\, a^{q+1}\frac{X^n+Y^n}{X+Y} + X^3Y^3\frac{X^{n-6}+Y^{n-6}}{X+Y}\Big) = 1. \tag{3.3}$$

Since the polynomials in (3.3) are homogeneous, it suffices to prove (3.3) with $Y = 1$, i.e.,

$$\gcd\Big(\frac{X^{n-3}+1}{X+1},\ a^{q+1}\frac{X^n+1}{X+1}+X^3\frac{X^{n-6}+1}{X+1}\Big)=1. \tag{3.4}$$

Let $\zeta\in\overline{\mathbb{F}}_q$ be a root of $(X^{n-3}+1)/(X+1)$. If $\zeta\neq 1$, then $\zeta^{n-3}+1=0$. Thus

$$\begin{aligned}
&\Big(a^{q+1}\frac{X^n+1}{X+1}+X^3\frac{X^{n-6}+1}{X+1}\Big)\Big|_{X=\zeta}\\
&=\frac{1}{\zeta+1}\big(a^{q+1}(\zeta^n+1)+\zeta^3(\zeta^{n-6}+1)\big)\\
&=\frac{1}{\zeta+1}\big(a^{q+1}(\zeta^3+1)+1+\zeta^3\big)\\
&=\frac{1}{\zeta+1}(a^{q+1}+1)(\zeta^3+1)\neq 0.
\end{aligned}$$

(Note: $\zeta^3\neq 1$ since $\zeta^{n-3}=1$ and $\gcd(n,3(q-1))=1$.) If $\zeta=1$, then n must be odd, in which case,

$$\Big(a^{q+1}\frac{X^n+1}{X+1}+X^3\frac{X^{n-6}+1}{X+1}\Big)\Big|_{X=1}=a^{q+1}n+n-6=n(a^{q+1}+1)\neq 0.$$

This proves (3.4) and hence (3.3).

With (3.3), to prove that $N^*(X,Y,Z)$ is irreducible in $\overline{\mathbb{F}}_q[X,Y,Z]$, it suffices to show that it is irreducible in $\overline{\mathbb{F}}_q(X,Y)[Z]$. Let w be a root of $N^*(X,Y,Z)\in\overline{\mathbb{F}}_q(X,Y)[Z]$ and let $z=w^3$. Then z is a root of $Q(Z)$. It suffices to show that $[\overline{\mathbb{F}}_q(X,Y,z):\overline{\mathbb{F}}_q(X,Y)]=2$ and $[\overline{\mathbb{F}}_q(X,Y,w):\overline{\mathbb{F}}_q(X,Y,z)]=3$.

$$\begin{array}{c}
\overline{\mathbb{F}}_q(X,Y,w)\\
\Big|\,3\\
\overline{\mathbb{F}}_q(X,Y,z)\\
\Big|\,2\\
\overline{\mathbb{F}}_q(X,Y)
\end{array}$$

3.1.1. Proof that $[\overline{\mathbb{F}}_q(X,Y,z):\overline{\mathbb{F}}_q(X,Y)]=2$

Assume to the contrary that $Q(Z)$ is reducible over $\overline{\mathbb{F}}_q(X,Y)$. Then there exists $A/B\in\overline{\mathbb{F}}_q(X,Y)$ ($A,B\in\overline{\mathbb{F}}_q[X,Y]$, $\gcd(A,B)=1$) such that

$$\frac{a^{q+1}X^3Y^3\Big(\dfrac{X^{n-3}+Y^{n-3}}{X+Y}\Big)^2}{\Big(a^{q+1}\dfrac{X^n+Y^n}{X+Y}+X^3Y^3\dfrac{X^{n-6}+Y^{n-6}}{X+Y}\Big)^2}=\Big(\frac{A}{B}\Big)^2+\frac{A}{B}=\frac{A(A+B)}{B^2}. \tag{3.5}$$

In the above equation, the numerator and the denominator on the left side are relatively prime (by (3.3)), so

$$B = a^{q+1}\frac{X^n + Y^n}{X+Y} + X^3Y^3\frac{X^{n-6}+Y^{n-6}}{X+Y} \tag{3.6}$$

and

$$A(A+B) = a^{q+1}X^3Y^3\Big(\frac{X^{n-3}+Y^{n-3}}{X+Y}\Big)^2.$$

Since $\gcd(A, A+B) = 1$, we may assume that

$$\begin{cases} A = X^3U^2, \\ A+B = Y^3V^2, \end{cases} \tag{3.7}$$

for some $U, V \in \overline{\mathbb{F}}_q[X,Y]$ with $UV = (X^{n-3}+Y^{n-3})/(X+Y)$. Therefore,

$$B = X^3U^2 + Y^3V^2. \tag{3.8}$$

By (3.8), the coefficient of XY^{n-2} in B is 0. However, by (3.6), the coefficient of XY^{n-2} in B is either a^{q+1} or $a^{q+1}+1$, a contradiction.

3.1.2. Proof that $[\overline{\mathbb{F}}_q(X,Y,w) : \overline{\mathbb{F}}_q(X,Y,z)] = 3$

Assume the contrary. Then z is a third power in $\overline{\mathbb{F}}_q(X,Y,z)$, that is, there exists $A, B \in \overline{\mathbb{F}}_q(X,Y)$ such that

$$z = (A+Bz)^3,$$

i.e.,

$$(A+BZ)^3 - Z \equiv 0 \pmod{Q(Z)}. \tag{3.9}$$

Setting $Y=1$ in (3.9) gives

$$(A_1+B_1Z)^3 - Z \equiv 0 \pmod{Q_1(Z)}, \tag{3.10}$$

where $A_1(X) = A(X,1)$, $B_1(X) = B(X,1)$ and

$$\begin{aligned} &Q_1(Z) = Q(Z)|_{Y=1} = \\ &a\frac{X^{n-3}+1}{X+1}Z^2 + \Big[a^{q+1}\frac{X^n+1}{X+1} + X^3\frac{X^{n-6}+1}{X+1}\Big]Z + a^qX^3\frac{X^{n-3}+1}{X+1}. \end{aligned} \tag{3.11}$$

We find that

$$(A_1+B_1Z)^3-Z\equiv\frac{f_0(X)}{a^2(X^3+X^n)}+\frac{f_1(X)}{a^2(X^3+X^n)^2}Z \pmod{Q_1(Z)},$$

where

$$\begin{aligned}f_0(X)=\,&a^2A_1^3X^3+a^{1+q}A_1B_1^2X^6+a^{1+2q}B_1^3X^6+a^qB_1^3X^9+a^2A_1^3X^n\\&+a^{1+q}A_1B_1^2X^{3+n}+a^qB_1^3X^{3+n}+a^{1+2q}B_1^3X^{6+n},\\f_1(X)=\,&a^2X^6+a^2A_1^2B_1X^6+a^{2+q}A_1B_1^2X^6+a^{2+2q}B_1^3X^6+aA_1B_1^2X^9\\&+a^{1+q}B_1^3X^9+B_1^3X^{12}+a^2X^{2n}+a^2A_1^2B_1X^{2n}+aA_1B_1^2X^{2n}+B_1^3X^{2n}\\&+aA_1B_1^2X^{3+n}+a^{2+q}A_1B_1^2X^{3+n}+aA_1B_1^2X^{6+n}+a^{2+q}A_1B_1^2X^{6+n}\\&+a^{2+q}A_1B_1^2X^{3+2n}+a^{1+q}B_1^3X^{3+2n}+a^{2+2q}B_1^3X^{6+2n}.\end{aligned}\tag{3.12}$$

Therefore, $f_0(X)=f_1(X)=0$. (We will not need the fact that $f_1(X)=0$.) From (3.10), $B_1\neq 0$. Then $f_0(X)=0$ implies $A_1\neq 0$. Let $C=B_1/A_1$. Then $f_0(X)=0$ becomes

$$(a^2+a^{1+q}X^3C^2)(1+X^{n-3})=a^qX^3(a^{1+q}+X^3+X^{n-3}+a^{1+q}X^n)C^3.\tag{3.13}$$

In the above

$$\begin{aligned}&\gcd(1+X^{n-3},\,a^{1+q}+X^3+X^{n-3}+a^{1+q}X^n)\\=\,&\gcd(1+X^{n-3},\,a^{1+q}+X^3+1+a^{1+q}X^3)\\=\,&\gcd(1+X^{n-3},\,(a^{1+q}+1)(1+X^3))\\=\,&1+X.\end{aligned}$$

Let $C=D/E$, where $D,E\in\overline{\mathbb{F}}_q[X]$, E is monic and $\gcd(D,E)=1$. Then (3.13) becomes

$$(a^2E^3+a^{1+q}X^3D^2E)\frac{1+X^{n-3}}{1+X}=a^qX^3D^3\,\frac{a^{1+q}+X^3+X^{n-3}+a^{1+q}X^n}{1+X}.\tag{3.14}$$

It follows that

$$\frac{1+X^{n-3}}{1+X}\,\Big|\,D\quad\text{and}\quad D\,\Big|\,\frac{1+X^{n-3}}{1+X}.\tag{3.15}$$

(3.14) and (3.15) force $D\in\overline{\mathbb{F}}_q^*$ and $n=4$. So

$$a^2E^3+a^{1+q}D^2X^3E=a^qD^3X^3(a^{1+q}(1+X)^3+X(1+X)).$$

Then $X\mid E$, say $E=XE_1$. Thus

$$a^2E_1^3+a^{1+q}D^2XE_1=a^qD^3(1+X)(a^{1+q}X^2+X+a^{1+q}).\tag{3.16}$$

It follows that $\deg E_1 = 1$, say $E_1 = X + \epsilon$, $\epsilon \in \overline{\mathbb{F}}_q$. Comparing the coefficients of X^3 and X^0 in the above gives

$$\begin{aligned} a^2 &= a^{1+2q} D^3, \\ a^2\epsilon^3 &= a^{1+2q} D^3. \end{aligned} \tag{3.17}$$

Hence $\epsilon^3 = 1$. Then $(a^{1+q}X^2 + X + a^{1+q})|_{X=\epsilon} = a^{1+q}(1+\epsilon^2) + \epsilon \neq 0$ since $a^{1+q} \neq 1$. It follows from (3.16) that $E_1 \mid 1 + X$, that is, $E_1 = X + 1$. Now (3.16) becomes

$$a^2(X+1)^2 + a^{1+q}D^2X = a^qD^3(a^{1+q}X^2 + X + a^{1+q}).$$

Comparing the coefficients of X in the above gives $a^{1+q}D^2 = a^qD^3$, i.e., $D = a$. But then (3.17) gives $a^{1+q} = 1$, which is a contradiction.

3.2. Case 2. $n \leq 2$

When $n = 1$, the absolute irreducibility (irreducibility over $\overline{\mathbb{F}}_q$) of $N(X, Y)$ follows from [5, §3]. So we assume $n = 2$. The arguments are similar to those in Case 1. We have

$$G(X) = \frac{a^qX^3 + 1}{X(X^3 + a)}, \tag{3.18}$$

$$N(X, Y) = a^qX^3Y^3 + a^{q+1}XY(X + Y) + (X + Y)^3 + a, \tag{3.19}$$

and

$$Q(Z) = aZ^2 + (a^{q+1}XY(X + Y) + (X + Y)^3)Z + a^qX^3Y^3. \tag{3.20}$$

When proving $[\overline{\mathbb{F}}_q(X, Y, z) : \overline{\mathbb{F}}_q(X, Y)] = 2$, Equations (3.5), (3.6) and (3.7) are replaced by

$$\begin{aligned} \frac{a^{q+1}X^3Y^3}{(a^{q+1}XY(X+Y) + (X+Y)^3)^2} &= \frac{A(A+B)}{B^2}, \\ B = a^{q+1}XY(X+Y) + (X+Y)^3&, \end{aligned} \tag{3.21}$$

and

$$\begin{cases} A = uX^3, \\ A + B = vY^3, \end{cases} \qquad u, v \in \overline{\mathbb{F}}_q^*.$$

Then $B = uX^3 + vY^3$, which contradicts (3.21) since $a^{1+q} \neq 1$.

When proving $[\overline{\mathbb{F}}_q(X,Y,w):\overline{\mathbb{F}}_q(X,Y,z)]=3$, Equation (3.12) is replaced by

$$\begin{aligned} f_0(X) = & a^2A_1^3 + a^{1+q}A_1B_1^2X^3 + a^qB_1^3X^3 + a^qB_1^3X^4 + a^{1+2q}B_1^3X^4 + a^qB_1^3X^5 \\ & + a^{1+2q}B_1^3X^5 + a^qB_1^3X^6. \end{aligned} \tag{3.22}$$

Setting $E = A_1/B_1$, the equation $f_0(X) = 0$ becomes

$$a^2E^3 + a^{1+q}X^3E + a^qX^3(1+X)(1+a^{1+q}X+X^2) = 0.$$

It follows that $E \in \overline{\mathbb{F}}_q[X]$ and $X \mid E$. Write $E = XE_1$. Then

$$a^2E_1^3 + a^{1+q}XE_1 + a^q(1+X)(1+a^{1+q}X+X^2) = 0. \tag{3.23}$$

Thus $\deg E_1 = 1$, say $E_1 = e(X+\epsilon)$, $e \in \overline{\mathbb{F}}_q^*$, $\epsilon \in \overline{\mathbb{F}}_q$. Comparing the coefficients of X^3 and X^0 in the above gives

$$\begin{aligned} a^2e^3 + a^q &= 0, \\ a^2e^3\epsilon^3 + a^q &= 0. \end{aligned} \tag{3.24}$$

Hence $\epsilon^3 = 1$. Then $(1+a^{1+q}X+X^2)|_{X=\epsilon} \neq 0$. It follows form (3.23) that $E_1 \mid 1+X$, whence $E_1 = e(X+1)$. Then (3.23) becomes

$$a^2e^3(X+1)^2 + a^{1+q}eX + a^q(1+a^{1+q}X+X^2) = 0.$$

Comparing the coefficients of X in the above gives $e = a^q$. But then (3.24) gives $a^{1+q} = 1$, which is a contradiction.

Remark 3.1. Most likely, Theorem 1.9 also holds for odd q.

4. Proof of Theorem 1.10

Theorem 1.10. *Let $n \ge 1$, $d \ge 2$ and $a \in \mathbb{F}_{q^2}^*$ be such that $d \mid q+1$, $q \ge (2\max\{n, 2d-n\})^4$ and $a^{q+1} \neq 1$. Then $f(X) = f_{q,2,n,d,a}(X) = X^n(X^{d(q-1)} + a)$ is not a PB of $\mathbb{F}_{q^2}$ if one of the following conditions is satisfied.*

(i) *$d - n > 1$ and $\gcd(d, n+1)$ is a power of 2.*
(ii) *$d + 2 \le n < 2d$ and $\gcd(d, n-1)$ is a power of 2.*
(iii) *$n \ge 2d$, $\gcd(d, n-1)$ is a power of 2, and $\gcd(n-d, q-1) = 1$.*

Assume to the contrary that $f(X)$ is a PB of $\mathbb{F}_{q^2}$. Recall that

$$G(X) = \frac{a^qX^n + X^{n-d}}{X^d + a}.$$

Let

$$N(X,Y) = \text{the numerator of } \frac{G(X)-G(Y)}{X-Y}$$

and

$$N^*(X,Y,Z) = \text{the homogenization of } N(X,Y).$$

Our objective is to show that $N^*(X,Y,Z)$ is irreducible over $\overline{\mathbb{F}}_q$ under the conditions in Theorem 1.10. We consider two cases: the case $d-n>1$, which corresponds to (i) in Theorem 1.10, and the case $n-d>1$, which corresponds to (ii) and (iii) in Theorem 1.10.

4.1. The case $d-n>1$

We have

$$\begin{aligned} G(X) &= \frac{a^qX^d+1}{X^{d-n}(X^d+a)}, \\ N(X,Y) &= -a\frac{X^{d-n}-Y^{d-n}}{X-Y} + \Big[a^{q+1}X^{d-n}Y^{d-n}\frac{X^n-Y^n}{X-Y} - \frac{X^{2d-n}-Y^{2d-n}}{X-Y}\Big] \\ &\quad - a^qX^dY^d\frac{X^{d-n}-Y^{d-n}}{X-Y}, \\ N^*(X,Y,Z) &= Q(Z^d), \end{aligned}$$

where

$$\begin{aligned} Q(Z) = &-a\frac{X^{d-n}-Y^{d-n}}{X-Y}Z^2 + \Big[a^{q+1}X^{d-n}Y^{d-n}\frac{X^n-Y^n}{X-Y} - \frac{X^{2d-n}-Y^{2d-n}}{X-Y}\Big]Z \\ &- a^qX^dY^d\frac{X^{d-n}-Y^{d-n}}{X-Y}. \end{aligned} \tag{4.1}$$

We claim that

$$\gcd\Big(\frac{X^{d-n}-Y^{d-n}}{X-Y},\ a^{q+1}X^{d-n}Y^{d-n}\frac{X^n-Y^n}{X-Y} - \frac{X^{2d-n}-Y^{2d-n}}{X-Y}\Big) = 1. \tag{4.2}$$

Since the polynomials in (4.2) are homogeneous, it suffices to prove (4.2) with $Y=1$, i.e.,

$$\gcd\Big(\frac{X^{d-n}-1}{X-1},\ a^{q+1}X^{d-n}\frac{X^n-1}{X-1} - \frac{X^{2d-n}-1}{X-1}\Big) = 1. \tag{4.3}$$

Let ζ be a root of $(X^{d-n}-1)/(X-1)$. If $\zeta\ne 1$, then $\zeta^{d-n}=1$. It follows that

$$
\begin{aligned}
&\Bigl(a^{q+1}X^{d-n}\frac{X^n-1}{X-1}-\frac{X^{2d-n}-1}{X-1}\Bigr)\Big|_{X=\zeta}\\
&=\frac{1}{\zeta-1}\bigl(a^{q+1}(\zeta^n-1)-(\zeta^n-1)\bigr)=\frac{1}{\zeta-1}(a^{q+1}-1)(\zeta^n-1)\neq 0.
\end{aligned}
$$

(Note: $\zeta^n \neq 1$ since $\zeta^{d-n}=1$ and $\gcd(n,d)=1$.) If $\zeta=1$, then $d-n\equiv 0 \pmod p$, where $p=\operatorname{char}\mathbb{F}_q$, whence

$$
\Bigl(a^{q+1}X^{d-n}\frac{X^n-1}{X-1}-\frac{X^{2d-n}-1}{X-1}\Bigr)\Big|_{X=1}=a^{q+1}n-(2d-n)=(a^{q+1}-1)n\neq 0.
$$

This proves (4.3) and hence (4.2). By (4.2), $N^*(X,Y,Z)$ is a primitive polynomial in Z over $\overline{\mathbb{F}}_q[X,Y]$, i.e., the gcd of its coefficients in $\overline{\mathbb{F}}_q[X,Y]$ is 1. Thus, to prove that $N^*(X,Y,Z)$ is irreducible in $\overline{\mathbb{F}}_q[X,Y,Z]$, it suffices to show that it is irreducible in $\overline{\mathbb{F}}_q(X,Y)[Z]$. Let w be a root of $N^*(X,Y,Z)$ for Z and let $z=w^d$. Then z is a root of $Q(Z)$, and it suffices to show that $[\overline{\mathbb{F}}_q(X,Y,z):\overline{\mathbb{F}}_q(X,Y)]=2$ and $[\overline{\mathbb{F}}_q(X,Y,w):\overline{\mathbb{F}}_q(X,Y,z)]=d$.

$$
\begin{array}{c}
\overline{\mathbb{F}}_q(X,Y,w)\\
\Big| \, d\\
\overline{\mathbb{F}}_q(X,Y,z)\\
\Big| \, 2\\
\overline{\mathbb{F}}_q(X,Y)
\end{array}
$$

4.1.1. Proof that $[\overline{\mathbb{F}}_q(X,Y,z):\overline{\mathbb{F}}_q(X,Y)]=2$

Assume to the contrary that $Q(Z)$ is reducible over $\overline{\mathbb{F}}_q(X,Y)$.

First assume that q is odd. The discriminant of Q is

$$
D=\Bigl[a^{q+1}X^{d-n}Y^{d-n}\frac{X^n-Y^n}{X-Y}-\frac{X^{2d-n}-Y^{2d-n}}{X-Y}\Bigr]^2-4a^{q+1}X^dY^d\Bigl(\frac{X^{d-n}-Y^{d-n}}{X-Y}\Bigr)^2.
$$

By assumption, $D=\Delta^2$ for some $\Delta\in\overline{\mathbb{F}}_q[X,Y]$. Then

$$
\begin{aligned}
&4a^{q+1}X^dY^d\Bigl(\frac{X^{d-n}-Y^{d-n}}{X-Y}\Bigr)^2=\\
&\Bigl[a^{q+1}X^{d-n}Y^{d-n}\frac{X^n-Y^n}{X-Y}-\frac{X^{2d-n}-Y^{2d-n}}{X-Y}+\Delta\Bigr]\\
&\cdot\Bigl[a^{q+1}X^{d-n}Y^{d-n}\frac{X^n-Y^n}{X-Y}-\frac{X^{2d-n}-Y^{2d-n}}{X-Y}-\Delta\Bigr].
\end{aligned}
\tag{4.4}
$$

Let δ be the gcd of the two factors on the right side of (4.4). Then

$$\delta \;\Big|\; a^{q+1}X^{d-n}Y^{d-n}\frac{X^n-Y^n}{X-Y}-\frac{X^{2d-n}-Y^{2d-n}}{X-Y}$$

and

$$\delta \;\Big|\; \frac{X^{d-n}-Y^{d-n}}{X-Y}.$$

It follows from (4.2) that $\delta = 1$.

Now from (4.4), we have

$$\begin{cases} a^{q+1}X^{d-n}Y^{d-n}\dfrac{X^n-Y^n}{X-Y}-\dfrac{X^{2d-n}-Y^{2d-n}}{X-Y}+\Delta = X^dU, \\ a^{q+1}X^{d-n}Y^{d-n}\dfrac{X^n-Y^n}{X-Y}-\dfrac{X^{2d-n}-Y^{2d-n}}{X-Y}-\Delta = Y^dV, \end{cases}$$

for some $U, V \in \overline{\mathbb{F}}_q[X, Y]$. It follows that

$$2a^{q+1}X^{d-n}Y^{d-n}\frac{X^n-Y^n}{X-Y}-2\frac{X^{2d-n}-Y^{2d-n}}{X-Y} = X^dU + Y^dV. \tag{4.5}$$

The coefficient of $X^{d-1}Y^{d-n}$ on the left side of (4.5) is $2(a^{q+1}-1) \neq 0$, while the coefficient of the same term on the right side of (4.5) is 0. This is a contradiction.

Next, assume that q is even. Since $Q(Z)$ is assumed to be reducible over $\overline{\mathbb{F}}_q(X, Y)$, we have

$$\frac{a^{q+1}X^dY^d\Big(\dfrac{X^{d-n}+Y^{d-n}}{X+Y}\Big)^2}{\Big[a^{q+1}X^{d-n}Y^{d-n}\dfrac{X^n+Y^n}{X+Y}+\dfrac{X^{2d-n}+Y^{2d-n}}{X+Y}\Big]^2} = \Big(\frac{A}{B}\Big)^2+\frac{A}{B} = \frac{A(A+B)}{B^2},$$

where $A, B \in \overline{\mathbb{F}}_q[X, Y]$, $\gcd(A, B) = 1$. By (4.2), the numerator and the denominator on the left side are relatively prime. Therefore we may assume

$$\begin{aligned} B &= a^{q+1}X^{d-n}Y^{d-n}\frac{X^n+Y^n}{X+Y}+\frac{X^{2d-n}+Y^{2d-n}}{X+Y}, \\ A(A+B) &= a^{q+1}X^dY^d\Big(\frac{X^{d-n}+Y^{d-n}}{X+Y}\Big)^2. \end{aligned} \tag{4.6}$$

Since $\gcd(A, A+B) = 1$, we have

$$\begin{cases} A = X^dU^2, \\ A+B = Y^dV^2, \end{cases}$$

where $U, V \in \overline{\mathbb{F}}_q[X, Y]$, $UV = (X^{d-n}+Y^{d-n})/(X+Y)$. Then

$$B = X^d U^2 + Y^d V^2. \tag{4.7}$$

The coefficient of $X^{d-1}Y^{d-n}$ in (4.6) is $a^{q+1} + 1 \neq 0$. However, the coefficient of $X^{d-1}Y^{d-n}$ in (4.7) is 0, which is a contradiction.

4.1.2. Proof that $[\overline{\mathbb{F}}_q(X, Y, w) : \overline{\mathbb{F}}_q(X, Y, z)] = d$

To prove this claim, it suffices to show that for each prime divisor t of d, z is not a t-th power in $\overline{\mathbb{F}}_q(X, Y, z)$. In (4.1), divide $Q(Z)$ by its leading coefficient and set $Y = 1$, the result is

$$Q_1(Z) = Z^2 - \frac{a^{q+1}X^{d-n}\dfrac{X^n - 1}{X - 1} - \dfrac{X^{2d-n} - 1}{X - 1}}{a\dfrac{X^{d-n} - 1}{X - 1}} Z + a^{q-1}X^d, \tag{4.8}$$

which is irreducible in $\overline{\mathbb{F}}_q(X)[Z]$. Let z_1 be a root of $Q_1(Z)$. By [5, §3.3, Claim II′], it suffices to show that for each prime divisor t of d, z_1 is not a t-th power in $\overline{\mathbb{F}}_q(X, z_1)$.

Let $\overline{(\ )}$ denote the nonidentity automorphism in $\mathrm{Aut}(\overline{\mathbb{F}}_q(X, z_1)/\overline{\mathbb{F}}_q(X))$. We have

$$z_1\bar{z}_1 = a^{q-1}X^d, \tag{4.9}$$

$$z_1 + \bar{z}_1 = \frac{a^{q+1}X^{d-n}\dfrac{X^n - 1}{X - 1} - \dfrac{X^{2d-n} - 1}{X - 1}}{a\dfrac{X^{d-n} - 1}{X - 1}}. \tag{4.10}$$

Let $d - n = p^m d'$, where $p = \mathrm{char}\,\mathbb{F}_q$, $p \nmid d'$. Let $\zeta \in \overline{\mathbb{F}}_q$ be a primitive d'th root of unity. Let $\mathfrak{p}$ be the place of the rational function field $\overline{\mathbb{F}}_q(X)$ which is the zero of $X - \zeta$, and let $\mathfrak{P}$ be a place of $\overline{\mathbb{F}}_q(X, z_1)$ such that $\mathfrak{P} \mid \mathfrak{p}$. Then $\mathfrak{P}$ is unramified over $\mathfrak{p}$ ([10, III 7.3 (b) and 7.8 (b)]). From (4.9) and (4.10), we have

$$\nu_{\mathfrak{p}}(z_1\bar{z}_1) = 0, \tag{4.11}$$

$$\nu_{\mathfrak{p}}(z_1 + \bar{z}_1) = \begin{cases} -p^m & \text{if } d' > 1, \\ -p^m + 1 & \text{if } d' = 1, \end{cases} \tag{4.12}$$

where $\nu_{\mathfrak{p}}$ is the valuation of $\overline{\mathbb{F}}_q(X)$ at $\mathfrak{p}$. Equation (4.12) is derived as follows: First, note that in (4.10),

$$\nu_{\mathfrak{p}}\Big(\frac{X^{d-n} - 1}{X - 1}\Big) = \begin{cases} p^m & \text{if } d' > 1, \\ p^m - 1 & \text{if } d' = 1. \end{cases} \tag{4.13}$$

Next, write

$$a^{q+1}X^{d-n}\frac{X^n-1}{X-1}-\frac{X^{2d-n}-1}{X-1}=(a^{q+1}X^{d-n}-1)\frac{X^n-1}{X-1}-X^n\frac{X^{2(d-n)}-1}{X-1}. \quad (4.14)$$

If $d'>1$, the value of (4.14) at $X=\zeta$ is

$$(a^{q+1}-1)\frac{\zeta^n-1}{\zeta-1}\neq 0.$$

If $d'=1$, we have $m>0$ (since $d-n>1$), whence $d-n\equiv 0 \pmod p$. Then $n\not\equiv 0$ since $\gcd(n,d)=1$. Therefore, the value of (4.14) at $X=\zeta$ $(=1)$ is

$$(a^{q+1}-1)n-2(d-n)=(a^{q+1}-1)n\neq 0.$$

Hence we always have

$$\nu_{\mathfrak{p}}\Big(a^{q+1}X^{d-n}\frac{X^n-1}{X-1}-\frac{X^{2d-n}-1}{X-1}\Big)=0. \quad (4.15)$$

Combining (4.10), (4.13) and (4.15) gives (4.12).

Write (4.11) and (4.12) as

$$\nu_{\mathfrak{P}}(z_1)+\nu_{\mathfrak{P}}(\bar z_1)=0,$$
$$\nu_{\mathfrak{P}}(z_1+\bar z_1)=\begin{cases}-p^m & \text{if } d'>1,\\ -p^m+1 & \text{if } d'=1,\end{cases}$$

where $\nu_{\mathfrak{P}}$ is the valuation of $\overline{\mathbb{F}}_q(X,z_1)$ at $\mathfrak{P}$. It follows that

$$\{\nu_{\mathfrak{P}}(z_1),\nu_{\mathfrak{P}}(\bar z_1)\}=\begin{cases}\{\pm p^m\} & \text{if } d'>1,\\ \{\pm(p^m-1)\} & \text{if } d'=1.\end{cases} \quad (4.16)$$

Assume to the contrary that z_1 is a t-th power in $\overline{\mathbb{F}}_q(X,z_1)$. Then $t\mid\nu_{\mathfrak{P}}(z_1)$. If $d'>1$, then by (4.16), $t\mid p^m$, whence $t\mid d-n$. This is impossible since $t\mid d$ and $\gcd(n,d)=1$. Therefore, $d'=1$ and $d-n=p^m$. By (4.16), $t\mid p^m-1=d-n-1$. Since $t\mid \gcd(d,d-n-1)=\gcd(d,n+1)$ and $\gcd(d,n+1)$ is a power of 2, we have $t=2$. It follows that p is odd.

Recall that $Q_1(z_1)=0$, where $Q_1(Z)$ is given in (4.8). Using (4.14) and $d-n=p^m$, the equation $Q_1(z_1)=0$ can be written as

$$u^2=\delta,$$

where

$$u=z_1-\gamma,$$

$$\gamma = \frac{1}{2}\frac{(a^{q+1}X^{p^m}-1)\dfrac{X^n-1}{X-1} - X^n(X+1)^{p^m}(X-1)^{p^m-1}}{a(X-1)^{p^m-1}},$$

and

$$\delta = \gamma^2 - a^{q-1}X^{p^m+n}.$$

By assumption, there exist $\alpha, \beta \in \overline{\mathbb{F}}_q(X)$ such that

$$(\alpha u + \beta)^2 = u + \gamma,$$

i.e.,

$$\alpha^2\delta + \beta^2 + 2\alpha\beta u = u + \gamma.$$

Since u is of degree 2 over $\overline{\mathbb{F}}_q(X)$, we have

$$\begin{cases} \alpha^2\delta + \beta^2 = \gamma, \\ 2\alpha\beta = 1. \end{cases}$$

Letting $\tau = \alpha/\beta$, we have

$$1 + \delta\tau^2 - 2\gamma\tau = 0 \tag{4.17}$$

and

$$\tau = 2\alpha^2. \tag{4.18}$$

Fortunately, (4.17) has an explicit solution

$$\tau = \frac{1}{\delta}(\gamma \pm a^{(q-1)/2}X^{(p^m+n)/2}) = \frac{1}{\gamma \mp a^{(q-1)/2}X^{(p^m+n)/2}}.$$

In the above,

$$\begin{aligned} &\gamma \mp a^{(q-1)/2}X^{(p^m+n)/2} = \\ &\frac{1}{2a(X-1)^{p^m-1}}\Big[(a^{q+1}X^{p^m}-1)\frac{X^n-1}{X-1} - X^n(X+1)^{p^m}(X-1)^{p^m-1} \\ &\qquad \mp 2a^{(q+1)/2}X^{(p^m+n)/2}(X-1)^{p^m-1}\Big]. \end{aligned}$$

Since τ is square in $\overline{\mathbb{F}}_q(X)$ (by (4.18)),

$$h := (1 - a^{q+1}X^{p^m})\frac{X^n-1}{X-1} + X^n(X+1)^{p^m}(X-1)^{p^m-1} + 2\epsilon X^{(p^m+n)/2}(X-1)^{p^m-1},$$

where $\epsilon = \pm a^{(q+1)/2}$, is a square in $\overline{\mathbb{F}}_q(X)$, say $h = g^2$, where $g \in \overline{\mathbb{F}}_q[X]$ is monic of degree $p^m + (n-1)/2$. Note that

$$\begin{aligned} h =& \frac{X^n-1}{X-1} + (X^n + X^{p^m+n})\frac{X^{p^m}-1}{X-1} - a^{q+1}X^{p^m}\frac{X^n-1}{X-1} + 2\epsilon X^{(p^m+n)/2}\frac{X^{p^m}-1}{X-1} \\ =& (1+\cdots+X^{2p^m+n-1}) \\ &- a^{q+1}(X^{p^m}+\cdots+X^{p^m+n-1}) \\ &+ 2\epsilon(X^{(p^m+n)/2}+\cdots+X^{(3p^m+n)/2-1}), \end{aligned}$$

which is self-reciprocal. Hence $g^* = \pm g$, where g^* is the reciprocal polynomial of g. (In fact, if $g^* = g$, but we do not need to be precise.) Let

$$\begin{aligned} H &= (X-1)h \\ &= (1-a^{q+1}X^{p^m})(X^n-1) + X^n(X+1)^{p^m}(X-1)^{p^m} + 2\epsilon X^{(p^m+n)/2}(X-1)^{p^m}. \end{aligned}$$

Then

$$H' = (1-a^{q+1}X^{p^m})nX^{n-1} + nX^{n-1}(X+1)^{p^m}(X-1)^{p^m} + \epsilon nX^{(p^m+n)/2-1}(X-1)^{p^m}.$$

(When computing H', we used the assumption that $m > 0$.) Let

$$\begin{aligned} K = H - n^{-1}XH' &= -(1-a^{q+1}X^{p^m}) + \epsilon X^{(p^m+n)/2}(X-1)^{p^m} \\ &= -1 + a^{q+1}X^{p^m} - \epsilon X^{(p^m+n)/2} + \epsilon X^{(p^m+n)/2+p^m}. \end{aligned}$$

The reciprocal of K is

$$K^* = \epsilon - \epsilon X^{p^m} + a^{q+1}X^{(p^m+n)/2} - X^{(p^m+n)/2+p^m}.$$

Since $g \mid K$ and g is self-reciprocal, we also have $g = \pm g^* \mid K^*$. Thus g divides

$$K + \epsilon K^* = -1 + \epsilon^2 + (-\epsilon + \epsilon a^{q+1})X^{(p^m+n)/2} = (a^{q+1}-1)(1+\epsilon X^{(p^m+n)/2}).$$

This is a contradiction since

$$\frac{p^m+n}{2} < p^m + \frac{n-1}{2} = \deg g.$$

4.2. The case $n - d > 1$

In this case,

$$G(X) = \frac{a^qX^n + X^{n-d}}{X^d + a},$$

$$\begin{aligned} N(X,Y) &= a\frac{X^{n-d}-Y^{n-d}}{X-Y} + \Big[a^{q+1}\frac{X^n-Y^n}{X-Y} + X^dY^d\frac{X^{n-2d}-Y^{n-2d}}{X-Y}\Big] \\ &\quad + a^qX^dY^d\frac{X^{n-d}-Y^{n-d}}{X-Y}, \end{aligned}$$

$$N^*(X,Y,Z) = Q(Z^d),$$

where

$$\begin{aligned} Q(Z) &= a\frac{X^{n-d}-Y^{n-d}}{X-Y}Z^2 + \Big[a^{q+1}\frac{X^n-Y^n}{X-Y} + X^dY^d\frac{X^{n-2d}-Y^{n-2d}}{X-Y}\Big]Z \\ &\quad + a^qX^dY^d\frac{X^{n-d}-Y^{n-d}}{X-Y}. \end{aligned}$$

We claim that

$$\gcd\Big(\frac{X^{n-d}-Y^{n-d}}{X-Y},\ a^{q+1}\frac{X^n-Y^n}{X-Y} + X^dY^d\frac{X^{n-2d}-Y^{n-2d}}{X-Y}\Big) = 1, \tag{4.19}$$

equivalently,

$$\gcd\Big(\frac{X^{n-d}-1}{X-1},\ a^{q+1}\frac{X^n-1}{X-1} + X^d\frac{X^{n-2d}-1}{X-1}\Big) = 1. \tag{4.20}$$

Let ζ be a root of $(X^{n-d}-1)/(X-1)$. If $\zeta \neq 1$, then

$$\begin{aligned} \Big(a^{q+1}\frac{X^n-1}{X-1} + X^d\frac{X^{n-2d}-1}{X-1}\Big)\Big|_{X=\zeta} &= \frac{1}{\zeta-1}\big(a^{q+1}(\zeta^n-1) + \zeta^d(\zeta^{n-2d}-1)\big) \\ &= \frac{1}{\zeta-1}(a^{q+1}-1)(\zeta^n-1) \neq 0. \end{aligned}$$

If $\zeta = 1$, then $n-d \equiv 0 \pmod p$, and

$$\Big(a^{q+1}\frac{X^n-1}{X-1} + X^d\frac{X^{n-2d}-1}{X-1}\Big)\Big|_{X=1} = a^{q+1}n + n - 2d = n(a^{q+1}-1) \neq 0.$$

So (4.20) and (4.19) hold. Therefore $Q(Z)$ is a primitive polynomial over $\overline{\mathbb{F}}_q[X,Y]$.

Let

$$\begin{aligned} Q_1(Z) &= \Big[\Big(a\frac{X^{n-d}-Y^{n-d}}{X-Y}\Big)^{-1}Q(Z)\Big]\Big|_{Y=1} \\ &= Z^2 + \frac{a^{q+1}\frac{X^n-1}{X-1} + X^d\frac{X^{n-2d}-1}{X-1}}{a\frac{X^{n-d}-1}{X-1}}Z + a^{q-1}X^d \in \overline{\mathbb{F}}_q(X)[Z]. \end{aligned} \tag{4.21}$$

Following the arguments in Section 4.1, we only have to prove the following two claims:

Claim 1. $Q(Z)$ is irreducible in $\overline{\mathbb{F}}_q(X,Y)[Z]$.

Claim 2. Let z be a root of $Q_1(Z)$ and t be a prime divisor of d. Then z is not a t-th power in $\overline{\mathbb{F}}_q(X,z)$.

4.2.1. Proof of Claim 1

Assume to the contrary that $Q(Z)$ is reducible in $\overline{\mathbb{F}}_q(X,Y)[Z]$.

First, assume that q is odd. The discriminant of $Q(Z)$ is

$$D=\Big[\frac{a^{q+1}(X^n-Y^n)}{X-Y}+\frac{X^dY^d(X^{n-2d}-Y^{n-2d})}{X-Y}\Big]^2-\frac{4a^{q+1}X^dY^d(X^{n-d}-Y^{n-d})^2}{(X-Y)^2}.$$

By assumption, $D=\Delta^2$ for some $\Delta\in\overline{\mathbb{F}}_q[X,Y]$. Then

$$\begin{aligned}\frac{4a^{q+1}X^dY^d\left(X^{n-d}-Y^{n-d}\right)^2}{(X-Y)^2}&=\Big(a^{q+1}\frac{X^n-Y^n}{X-Y}+X^dY^d\frac{X^{n-2d}-Y^{n-2d}}{X-Y}+\Delta\Big)\\&\quad\cdot\Big(a^{q+1}\frac{X^n-Y^n}{X-Y}+X^dY^d\frac{X^{n-2d}-Y^{n-2d}}{X-Y}-\Delta\Big).\end{aligned}$$

In the above, the two factors on the right side are relatively prime. (This follows from (4.19).) Therefore, we may assume

$$\begin{cases}a^{q+1}\dfrac{X^n-Y^n}{X-Y}+X^dY^d\dfrac{X^{n-2d}-Y^{n-2d}}{X-Y}+\Delta=2a^{(q+1)/2}X^dU^2,\\ a^{q+1}\dfrac{X^n-Y^n}{X-Y}+X^dY^d\dfrac{X^{n-2d}-Y^{n-2d}}{X-Y}-\Delta=2a^{(q+1)/2}Y^dV^2,\end{cases}\tag{4.22}$$

for some $U,V\in\overline{\mathbb{F}}_q[X,Y]$ with

$$UV=\frac{X^{n-d}-Y^{n-d}}{X-Y}.\tag{4.23}$$

Then

$$\frac{a^{q+1}\left(X^n-Y^n\right)}{X-Y}+\frac{X^dY^d\left(X^{n-2d}-Y^{n-2d}\right)}{X-Y}=a^{(q+1)/2}(X^dU^2+Y^dV^2).\tag{4.24}$$

Let L denote the left side of (4.24). We have

$$\begin{aligned}L&=a^{q+1}(Y^{n-1}+XY^{n-2}+\cdots+X^{n-1})\\&\quad+\begin{cases}X^dY^{n-d-1}+X^{d+1}Y^{n-d-2}+\cdots+X^{n-d-1}Y^d & \text{if } n\ge 2d,\\ -X^{n-d}Y^{d-1}-X^{n-d+1}Y^{d-2}-\cdots-X^{d-1}Y^{n-d} & \text{if } d+2\le n<2d.\end{cases}\end{aligned}$$

If $d+2 \le n < 2d$, the coefficient of $X^{d-1}Y^{n-d}$ in L is $a^{q+1}-1 \ne 0$, while the coefficient of $X^{d-1}Y^{n-d}$ on the right side of (4.24) is 0, which is a contradiction. Hence Theorem 1.10 (iii) holds. In particular, $\gcd(n-d, q-1) = 1$.

Since

$$\Delta(Y,X)^2 = D(Y,X) = D(X,Y) = \Delta(X,Y)^2,$$

we have $\Delta(Y,X) = \pm\Delta(X,Y)$. If $\Delta(Y,X) = \Delta(X,Y)$, then by (4.22), $X^dU(X,Y)^2 = Y^dU(Y,X)^2$. Then $Y \mid U(X,Y)$, which is a contradiction to (4.23). Hence $\Delta(Y,X) = -\Delta(X,Y)$, and by (4.22),

$$U(Y,X)^2 = V(X,Y)^2. \tag{4.25}$$

By (4.25) and (4.23), we have

$$U(X,Y)^2 = \alpha \prod_{i=1}^{(n-d-1)/2} (X - \epsilon_i Y)^2, \tag{4.26}$$

$$V(X,Y)^2 = \alpha^{-1} \prod_{i=1}^{(n-d-1)/2} (X - \epsilon_i^{-1} Y)^2, \tag{4.27}$$

where $\alpha, \beta \in \overline{\mathbb{F}}_q$ and $\epsilon_i \in \overline{\mathbb{F}}_q^*$ are such that

$$\frac{X^{n-d} - Y^{n-d}}{X - Y} = \prod_{i=1}^{(n-d-1)/2} \big[(X - \epsilon_i Y)(X - \epsilon_i^{-1} Y)\big].$$

We have

$$\begin{aligned} \alpha &= U(1,0)^2 && \text{(by (4.26))} \\ &= V(0,1)^2 && \text{(by (4.25))} \\ &= \alpha^{-1} \prod_{i=1}^{(n-d-1)/2} \epsilon_i^{-2} && \text{(by (4.27))}. \end{aligned}$$

It follows that

$$\alpha^2 = \prod_{i=1}^{(n-d-1)/2} \epsilon_i^{-2}. \tag{4.28}$$

On the other hand, comparing the coefficients of X^{n-1} in (4.24) gives $a^{q+1} = a^{(q+1)/2} \cdot \alpha$, i.e., $\alpha = a^{(q+1)/2}$. Since the ϵ_i's are roots of $X^{n-d} - 1$, we have

$$a^{(q+1)(n-d)} = \alpha^{2(n-d)} = 1 \qquad \text{(by (4.28))}.$$

This, combined with $a^{(q+1)(q-1)} = 1$ and $\gcd(n-d, q-1) = 1$, implies that $a^{q+1} = 1$, which is a contradiction.

Next, assume that q is even. Since $Q(Z)$ is assumed to be reducible over $\overline{\mathbb{F}}_q(X,Y)$, there are $A, B \in \overline{\mathbb{F}}_q[X,Y]$, relatively prime, such that

$$\frac{a^{q+1}X^dY^d\Big(\dfrac{X^{n-d}+Y^{n-d}}{X+Y}\Big)^2}{\Big(a^{q+1}\dfrac{X^n+Y^n}{X+Y} + X^dY^d\dfrac{X^{n-2d}+Y^{n-2d}}{X+Y}\Big)^2} = \Big(\frac{A}{B}\Big)^2 + \frac{A}{B} = \frac{A(A+B)}{B^2}.$$

In the above, the numerator and the denominator on the left side are relatively prime (by (4.19)). Thus

$$B = a^{q+1}\frac{X^n+Y^n}{X+Y} + X^dY^d\frac{X^{n-2d}+Y^{n-2d}}{X+Y} \tag{4.29}$$

and

$$A(A+B) = a^{q+1}X^dY^d\Big(\frac{X^{n-d}+Y^{n-d}}{X+Y}\Big)^2.$$

We may assume that

$$\begin{cases} A = X^dU^2, \\ A+B = Y^dV^2, \end{cases}$$

for some $U, V \in \overline{\mathbb{F}}_q[X,Y]$ such that $UV = (X^{n-d}+Y^{n-d})/(X+Y)$. Then

$$B = X^dU^2 + Y^dV^2. \tag{4.30}$$

By (4.29),

$$\begin{aligned} B = {} & a^{q+1}(Y^{n-1} + XY^{n-2} + \cdots + X^{n-1}) \\ & + \begin{cases} X^dY^{n-d-1} + X^{d+1}Y^{n-d-2} + \cdots + X^{n-d-1}Y^d & \text{if } n \ge 2d, \\ X^{n-d}Y^{d-1} + X^{n-d+1}Y^{d-2} + \cdots + X^{d-1}Y^{n-d} & \text{if } d+2 \le n < 2d. \end{cases} \end{aligned} \tag{4.31}$$

Since we assume $d > 1$ and $n - d > 1$, the coefficient of XY^{n-2} in (4.31) is $a^{q+1} \ne 0$. (Even if we allowed $d = 1$ or $n - d = 1$, the coefficient of XY^{n-2} in (4.31) would be $a^{q+1} + 1$, which is still nonzero.) However, the coefficient of XY^{n-2} in (4.30) is 0, which is a contradiction.

4.2.2. Proof of Claim 2

Recall that $Q_1(Z)$ is given in (4.21). Let z be a root of $Q_1(Z)$ and t be a prime divisor of d. Assume to the contrary that z is a t-th power in $\overline{\mathbb{F}}_q(X,z)$. Let $\overline{(\ )}$ be the nonidentity automorphism in $\mathrm{Aut}(\overline{\mathbb{F}}_q(X,z)/\overline{\mathbb{F}}_q(X))$. Then

$$z\bar{z} = a^{q-1}X^d, \tag{4.32}$$

$$\begin{aligned} z+\bar{z} &= -\frac{a^{q+1}\dfrac{X^n-1}{X-1} + X^d\dfrac{X^{n-2d}-1}{X-1}}{a\dfrac{X^{n-d}-1}{X-1}} \\ &= -\frac{(a^{q+1}-1)\dfrac{X^d-1}{X-1} + (a^{q+1}X^d+1)\dfrac{X^{n-d}-1}{X-1}}{a\dfrac{X^{n-d}-1}{X-1}}. \end{aligned} \tag{4.33}$$

Write $n-d = p^m d'$, where $p \nmid d'$, and let ζ be a primitive d'th root of unity. Let $\mathfrak{p}$ be the place of the rational function field $\overline{\mathbb{F}}_q(X)$ which is the zero of $X-\zeta$, and let $\mathfrak{P}$ be a place of $\overline{\mathbb{F}}_q(X,z)$ such that $\mathfrak{P} \mid \mathfrak{p}$. Then $\mathfrak{P}$ is unramified over $\mathfrak{p}$ ([10, III 7.3 (b) and 7.8 (b)]). From (4.32) and (4.33), we have

$$\nu_{\mathfrak{p}}(z\bar{z}) = 0, \tag{4.34}$$

$$\nu_{\mathfrak{p}}(z+\bar{z}) = \begin{cases} -p^m & \text{if } d' > 1, \\ -p^m+1 & \text{if } d' = 1. \end{cases} \tag{4.35}$$

(The proof of (4.35) is similar to that of (4.12) and uses the assumption $n-d>1$ in the case $d'=1$.) Therefore,

$$\nu_{\mathfrak{P}}(z) + \nu_{\mathfrak{P}}(\bar{z}) = 0,$$

$$\nu_{\mathfrak{P}}(z+\bar{z}) = \begin{cases} -p^m & \text{if } d' > 1, \\ -p^m+1 & \text{if } d' = 1, \end{cases}$$

and it follows that

$$\{\nu_{\mathfrak{P}}(z), \nu_{\mathfrak{P}}(\bar{z})\} = \begin{cases} \{\pm p^m\} & \text{if } d' > 1, \\ \{\pm(p^m-1)\} & \text{if } d' = 1. \end{cases}$$

Since z is t-th power in $\overline{\mathbb{F}}_q(X,z)$, we have $t \mid \nu_{\mathfrak{P}}(z)$. If $d'>1$, then $t=p$. It follows from $t \mid d$ and $t \mid n-d$ that $\gcd(n,d) \neq 1$, which is a contradiction. So we must have $d'=1$ and $n-d=p^m$, $m>0$. Then $t \mid p^m-1 = n-d-1$. Since $t \mid \gcd(n-d-1,d) = \gcd(n-1,d)$, where $\gcd(n-1,d)$ is a power of 2 (by assumption), we have $t=2$. Consequently, p is odd.

The equation $Q_1(z) = 0$ can be written as

$$u^2 = \delta,$$

where

$$u = z - \gamma,$$

$$\gamma = -\frac{1}{2}\frac{(a^{q+1}-1)\dfrac{X^d-1}{X-1} + (a^{q+1}X^d+1)(X-1)^{p^m-1}}{a(X-1)^{p^m-1}},$$

and

$$\delta = \gamma^2 - a^{q-1}X^d.$$

By assumption, there exist $\alpha, \beta \in \overline{\mathbb{F}}_q(X)$ such that

$$(\alpha u + \beta)^2 = u + \gamma,$$

i.e.,

$$\alpha^2\delta + \beta^2 + 2\alpha\beta u = u + \gamma.$$

So

$$\begin{cases} \alpha^2\delta + \beta^2 = \gamma, \\ 2\alpha\beta = 1. \end{cases}$$

Letting $\tau = \alpha/\beta$, we have

$$1 + \delta\tau^2 - 2\gamma\tau = 0 \tag{4.36}$$

and

$$\tau = 2\alpha^2. \tag{4.37}$$

Equation (4.36) has an explicit solution

$$\tau = \frac{1}{\delta}(\gamma \pm a^{(q-1)/2}X^{d/2}) = \frac{1}{\gamma \mp a^{(q-1)/2}X^{d/2}} = \frac{-2a(X-1)^{p^m-1}}{h(X)},$$

where

$$h(X) = (a^{q+1}-1)\frac{X^d-1}{X-1} + (a^{q+1}X^d+1)(X-1)^{p^m-1} + 2\epsilon X^{d/2}(X-1)^{p^m-1}$$

and $\epsilon = \pm a^{(q+1)/2}$. By (4.37), $h(X)$ is a square in $\overline{\mathbb{F}}_q[X]$, say $h = g^2$ for some $g \in \overline{\mathbb{F}}_q[X]$ with $\deg g = (d + p^m - 1)/2$. Note that

$$\begin{aligned} h(X) &= a^{q+1}\Bigl(\frac{X^d-1}{X-1} + X^d\frac{X^{p^m}-1}{X-1}\Bigr) + \Bigl(\frac{X^{p^m}-1}{X-1} - \frac{X^d-1}{X-1}\Bigr) + 2\epsilon X^{d/2}\frac{X^{p^m}-1}{X-1} \\ &= a^{q+1}(1 + \cdots + X^{p^m+d-1}) + (X^d + \cdots + X^{p^m-1}) + 2\epsilon(X^{d/2} + \cdots + X^{p^m+d/2-1}), \end{aligned}$$

which is self-reciprocal. It follows that $g^* = \pm g$, where g^* is the reciprocal polynomial of g. Let

$$H = (X-1)h = (a^{q+1}-1)(X^d-1) + (a^{q+1}X^d+1)(X-1)^{p^m} + 2\epsilon X^{d/2}(X-1)^{p^m}.$$

Then

$$H' = (a^{q+1}-1)dX^{d-1} + a^{q+1}dX^{d-1}(X-1)^{p^m} + \epsilon dX^{d/2-1}(X-1)^{p^m}.$$

Let

$$K = -H + d^{-1}XH' = a^{q+1} - X^{p^m} + \epsilon X^{d/2} - \epsilon X^{p^m+d/2}.$$

The reciprocal of K is

$$K^* = -\epsilon + \epsilon X^{p^m} - X^{d/2} + a^{q+1}X^{p^m+d/2}.$$

Since $g \mid K$, we have $g = \pm g^* \mid K^*$. Hence g divides

$$\epsilon K + K^* = (a^{q+1}-1)(\epsilon + X^{d/2}).$$

This is a contradiction since

$$\frac{d}{2} < \frac{d+p^m-1}{2} = \deg g.$$

The proof of Theorem 1.10 is now complete.

4.3. Final remarks

Theorem 1.10 leaves ample room for improvement, by which we mean nonexistence results of PB under conditions that are weaker than or not covered by (i) – (iii) in Theorem 1.10. While some improvements may be obtained by fine tuning the techniques demonstrated in the present paper, breakthroughs may require new methods or substantially new elements in the current approach.

The cases $d - n = \pm 1$ appear to be special. These are the two cases not covered by Theorem 1.10 and there are indeed infinite classes of PBs in these two cases with $e = 2$ (Results 1.2 and 1.4). A natural question is this: When $d - n = \pm 1$ and $e > 2$, are there infinite classes of PBs of the form $f_{q,e,n,d,a}(X) = X^n(X^{d(q-1)} + a)$ of $\mathbb{F}_{q^e}$?

Data availability

No data was used for the research described in the article.

Acknowledgments

The authors thank the anonymous referee for the careful reading and insightful comments.

Vincenzo Palozzi Lavorante was partially supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

References

[1] X. Hou, A survey of permutation binomials and trinomials over finite fields, in: Proceedings of the 11th International Conference on Finite Fields and Their Applications, Magdeburg, Germany, 2013, in: Contemporary Mathematics, vol. 632, 2015, pp. 177–191.

[2] X. Hou, Permutation polynomials over finite fields — a survey of recent advances, Finite Fields Appl. 32 (2015) 82–119.

[3] X. Hou, Determination of a type of permutation trinomials over finite fields, II, Finite Fields Appl. 35 (2015) 16–35.

[4] X. Hou, Permutation polynomials of the form $X^r(a + X^{2(q-1)})$ — a nonexistence result, arXiv:1609.03662.

[5] X. Hou, Applications of the Hasse-Weil bound to permutation polynomials, Finite Fields Appl. 54 (2018) 113–132.

[6] S.D. Lappano, Some Results Concerning Permutation Polynomials over Finite Fields, Ph.D. Dissertation, University of South, Florida, 2016.

[7] S.D. Lappano, A family of permutation trinomials over $\mathbb{F}_{q^2}$, private communication.

[8] A.M. Masuda, I. Rubio, J. Santiago, Permutation binomials of index $q^{e-1} + \cdots + q + 1$ over $\mathbb{F}_{q^e}$, arXiv:2009.10851.

[9] Y.H. Park, J.B. Lee, Permutation polynomials and group permutation polynomials, Bull. Aust. Math. Soc. 63 (2001) 67–74.

[10] H. Stichtenoth, Algebraic Function Fields and Codes, Springer, Berlin, 1993.

[11] Z. Tu, X. Zeng, Y. Jiang, Y. Li, Binomial permutations over finite fields with even characteristic, Des. Codes Cryptogr. 89 (2021) 2869–2888.

[12] Q. Wang, Cyclotomic mapping permutation polynomials over finite fields, in: S.W. Golomb, G. Gong, T. Helleseth, H.-Y. Song (Eds.), Sequences, Subsequences, and Consequences, in: Lecture Notes in Comput. Sci., vol. 4893, Springer, Berlin, 2007, pp. 119–128.

[13] M.E. Zieve, On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$, Proc. Am. Math. Soc. 137 (2009) 2209–2216.

[14] M.E. Zieve, Permutation polynomials on $\mathbb{F}_q$ induced from Rédei function bijections on subgroups of $\mathbb{F}_q^*$, arXiv:1310.0776.