

# Classification of a class of planar quadrinomials

Chin Hei Chan and Maosheng Xiong

## Abstract

Let  $p$  be an odd prime,  $k, \ell$  be positive integers,  $q = p^k, Q = p^\ell$ . In this paper we characterise planar functions of the form  $f_{\underline{c}}(X) = c_0X^{qQ+q} + c_1X^{qQ+1} + c_2X^{Q+q} + c_3X^{Q+1}$  over  $\mathbb{F}_{q^2}$  for any  $\underline{c} = (c_0, c_1, c_2, c_3) \in \mathbb{F}_{q^2}^4$  in terms of linear equivalence.

**Index terms**— Planar polynomials, two-to-one polynomials, differential uniformity, linear equivalence, rational functions.

## I. INTRODUCTION

### A. Background and motivation

Let  $p$  be any prime number,  $k$  a positive integer,  $q = p^k$ , and  $\mathbb{F}_q$  the finite field of order  $q$ . A function  $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$  is called *planar* if all the equations

$$F(x + a) - F(x) = b, \quad \forall a, b \in \mathbb{F}_q, a \neq 0 \quad (1)$$

have exactly one solution. In other words, for any  $a \in \mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$ , the function

$$D_a F(x) = F(x + a) - F(x),$$

called the *derivative of  $F$  in the direction of  $a$* , is a permutation on  $\mathbb{F}_q$ .

In the above definition, only the additive operation is involved, so planar functions can also be defined on any finite dimensional vector space over  $\mathbb{F}_p$ .

Planar functions were originally introduced by Dembowski and Ostrom in the seminar paper [14] in connection with projective planes in finite geometry. This notion coincides with that of perfect nonlinear (PN) functions in odd characteristic introduced by Nyberg [26] from cryptography. From this perspective, planar functions have the best differential uniformity, hence if used as S-boxes, they offer the best resistance to differential cryptanalysis, one of the most powerful attacks known today used

against block ciphers. Besides their importance in cryptography, planar functions have applications in coding theory [10], [34], combinatorics [1], [32] and some engineering areas [16]. Planar functions also correspond to important algebraic and combinatorial structures such as commutative semifields [13], [35]. All of these make the study of planar functions fruitful and important in a much broader context in mathematics and computer science. Planar functions together with almost perfect nonlinear (APN) functions in characteristic two have become a central topic in design theory, coding theory and cryptography ([3], [8], [15], [28]).

Planar functions exist only for odd  $q$ . Currently there are less than 20 distinct infinite families of planar functions (see [21] for a list and [11] for a recent construction of planar functions). One of the main reasons why new planar functions are so difficult to construct and analyze is that planar functions are classified up to a certain notion of equivalence, namely linear equivalence, EA-equivalence or CCZ-equivalence, and to show that a given planar function is equivalent or inequivalent to some known ones is usually rather difficult, most of such verification involves quite technical computation. For a flavor of the techniques, interested readers may refer to a recent work [29].

Now let  $p$  be an odd prime,  $k, \ell$  be some positive integers,  $q = p^k$ ,  $Q = p^\ell$ , and  $\mathbb{F}_{q^2}$  the finite field of order  $q^2$ . For any  $\underline{c} := (c_0, c_1, c_2, c_3) \in \mathbb{F}_{q^2}^4$ , we define a quadrinomial  $f_{\underline{c}}(X) \in \mathbb{F}_{q^2}[X]$  given by

$$f_{\underline{c}}(X) = c_0 X^{qQ+q} + c_1 X^{qQ+1} + c_2 X^{Q+q} + c_3 X^{Q+1}. \quad (2)$$

In this paper we study planar functions from these  $f_{\underline{c}}(X)$  for all  $\underline{c} \in \mathbb{F}_{q^2}^4$ .

We remark that when  $q$  is even, this class of quadrinomials  $f_{\underline{c}}(X)$  and some variations have been studied extensively in the literature. In fact in this case these  $f_{\underline{c}}(X)$ 's have been the main object of study in more than 40 papers and by more than 60 authors (see [17]). Now we have reached somewhat satisfactory understanding of their various cryptographic properties. For example, when  $q$  is even, complete characterization as to when  $f_{\underline{c}}(X)$  is a permutation on  $\mathbb{F}_{q^2}$  was obtained in [17], [23]; complete characterization as to when  $f_{\underline{c}}(X)$  is a permutation with optimal Boomerang uniformity was obtained in [25], [33]. In another perspective,  $f_{\underline{c}}(X)$  satisfies the subfield property

$$f_{\underline{c}}(aX) = a^{Q+1} f_{\underline{c}}(X) \text{ for all } a \in \mathbb{F}_q.$$

By identifying  $(x, y) \in \mathbb{F}_q^2$  with  $X = x + \zeta y \in \mathbb{F}_{q^2}$  for a fixed element  $\zeta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ , one sees that the class of  $f_{\underline{c}}(X)$  is linear equivalent to the class of  $(Q, Q)$ -biprojective functions  $f^*(x, y) \in \mathbb{F}_q[x, y]^2$  given

by

$$f^*(x, y) = (a_0x^{Q+1} + a_1x^Qy + a_2xy^Q + a_3y^{Q+1}, b_0x^{Q+1} + b_1x^Qy + b_2xy^Q + b_3y^{Q+1}), \quad (3)$$

whose various properties were studied in depth in [19], [20]. In this language, in [20] Göloğlu provided a complete characterization of APN functions from  $f_{\underline{c}}(X)$  under linear equivalence, hence giving a satisfactory answer to a question of Carlet [7].

In view of all these papers and in particular of [7] and [20], it is natural for us to study and to characterize planar functions from  $f_{\underline{c}}(X)$  for odd  $q$ .

### B. Statement of main results

The main results of the paper are as follows.

**Theorem 1.** *Let  $p$  be an odd prime,  $k$  and  $\ell$  positive integers,  $q = p^k$  and  $Q = p^\ell$ . Consider the quadrinomial  $f_{\underline{c}}(X)$  given in (2) for any  $\underline{c} = (c_0, c_1, c_2, c_3) \in \mathbb{F}_{q^2}^4$ . Let  $\mu_{q+1}$  denote the set of  $(q+1)$ -th roots of unity in  $\mathbb{F}_{q^2}$ . If  $f_{\underline{c}}(X)$  is planar over  $\mathbb{F}_{q^2}$ , then it is linear equivalent to one of the polynomials listed below (which are either univariate over  $\mathbb{F}_{q^2}$  or  $(Q, Q)$ -biprojective over  $\mathbb{F}_q^2$ ):*

- 1)  $X^{Q+1}$ ;
- 2)  $X^{Q+q}$ ;
- 3)  $P_2(x, y) = (x^Qy, x^{Q+1} + \varepsilon y^{Q+1})$  for some  $\varepsilon \in \mathbb{F}_q^*$ ;
- 4)  $P_3(x, y) = (x^{Q+1} - x^Qy, xy^Q + \varepsilon y^{Q+1})$  for some  $\varepsilon \in \mathbb{F}_q^* \setminus \{-1\}$ ;
- 5)  $X^{Q+q} + \varepsilon X^{Q+1}$  for some  $\varepsilon \in \mathbb{F}_{q^2}^* \setminus \mu_{q+1}$ .

The next result gives criteria as to when the polynomials 1)-5) listed in Theorem 1 are indeed planar functions:

**Theorem 2.** *Let  $p$  be an odd prime,  $k$  and  $\ell$  positive integers,  $q = p^k$  and  $Q = p^\ell$ .*

(i) *For Families 1) to 3) in Theorem 1:*

- 1)  $X^{Q+1}$  is planar over  $\mathbb{F}_{q^2}$  if and only if  $\frac{\ell}{\gcd(k, \ell)}$  is even;
- 2)  $X^{Q+q}$  is planar over  $\mathbb{F}_{q^2}$  if and only if  $\frac{k\ell}{\gcd(k, \ell)^2}$  is odd;
- 3)  $P_2(x, y)$ ,  $\varepsilon \in \mathbb{F}_q^*$  is planar over  $\mathbb{F}_q^2$  if and only if  $\frac{k}{\gcd(k, \ell)}$  is odd and  $\varepsilon \in \mathbb{F}_q^*$  is a non-square;

(ii) *For Families 4) to 5) in Theorem 1 we only have partial results:*

- 4) if  $P_3(x, y)$ ,  $\varepsilon \in \mathbb{F}_q^* \setminus \{-1\}$  is planar over  $\mathbb{F}_q^2$ , then  $\frac{k}{\gcd(k, \ell)}$  is odd and  $1 + \varepsilon^{-1} \in \mathbb{F}_q^*$  is a non-square. Moreover, if  $k \mid \ell$ , then this condition on  $\varepsilon$  is also sufficient for  $P_3(x, y)$  to be planar;
- 5) if  $k \mid \ell$ , then  $X^{Q+q} + \varepsilon X^{Q+1}$ ,  $\varepsilon \in \mathbb{F}_{q^2}^* \setminus \mu_{q+1}$  is planar over  $\mathbb{F}_{q^2}$  if and only if  $q \geq 5$  and  $1 - \varepsilon^{(-1)^{1+\ell/k}(q+1)}$  is a square in  $\mathbb{F}_q^*$ .

Finally, when  $k \mid \ell$ , it turns out planar functions  $f_{\underline{c}}(X)$  are all linear equivalent to  $X^2$ . Here we also describe the result in terms of the coefficients  $c_i$ 's.

**Theorem 3.** Let  $p$  be an odd prime,  $k$  and  $\ell$  positive integers such that  $k \mid \ell$ ,  $q = p^k$  and  $Q = p^\ell$ . For any  $\underline{c} = (c_0, c_1, c_2, c_3) \in \mathbb{F}_{q^2}^4$ , define

$$e = \begin{cases} c_1^{q+1} - c_2^{q+1} & (\frac{\ell}{k} \text{ is odd}) \\ c_3^{q+1} - c_0^{q+1} & (\frac{\ell}{k} \text{ is even}) \end{cases}$$

and

$$\theta = \begin{cases} c_1(c_0^q + c_3^q) - c_2^q(c_0 + c_3) & (\frac{\ell}{k} \text{ is odd}) \\ c_3(c_1^q + c_2^q) - c_0^q(c_1 + c_2) & (\frac{\ell}{k} \text{ is even}). \end{cases}$$

Then  $f_{\underline{c}}(X)$  given in (2) is planar over  $\mathbb{F}_{q^2}$  if and only if  $e^2 - \theta^{q+1}$  is a square in  $\mathbb{F}_q^*$ , and in this case  $f_{\underline{c}}(X)$  is linear equivalent to  $X^2$ .

### C. Discussions

In Theorem 1, since  $f_{\underline{c}}(X)$  is a Dembowski-Ostrom (DO for short) polynomial, when  $f_{\underline{c}}(X)$  is planar, the CCZ-equivalence, EA-equivalence and linear equivalence all coincide with each other [5]. Since planar functions in odd characteristic are natural analogue of APN functions in characteristic two, Theorem 1 can be considered as both complementing and parallel to [20, Theorem 1.1], which gave a complete classification of APN functions from the class of  $f_{\underline{c}}(X)$  for even  $q$  (by using the language of  $(Q, Q)$ -biprojective functions).

In Theorem 2, when  $k \nmid \ell$ , planar functions from Families 1)–3) are all known:  $X^{Q+1}$  and  $X^{Q+q}$  resemble the Albert family [2], and  $P_2(x, y)$  is a subclass of the Zhou-Pott family [35]. As for Families 4) and 5) when  $k \nmid \ell$ , we did experiments by **MAGMA** for some small values of  $p, k$  and  $\ell$  but it seems no such planar functions exist regardless of the choice of  $\varepsilon$ . It may be an interesting question to investigate

whether or not there are planar functions from Families 4) and 5) of Theorem 1 when  $k \nmid \ell$ . We leave this as an open problem.

Next, we explain the method we use in proving Theorems 1–3. The polynomial  $f_{\underline{c}}(X)$  can be written as  $f_{\underline{c}}(X) = X^{Q+1}A(X^{q-1})$  where

$$A(X) = c_0X^{Q+1} + c_1X^Q + c_2X + c_3.$$

Define

$$B(X) = c_3^qX^{Q+1} + c_2^qX^Q + c_1^qX + c_0^q, \quad g(X) = B(X)/A(X).$$

It was well-known that when  $q$  is even, permutation properties of  $f_{\underline{c}}(X)$  are closely related to those of the accompanying rational function  $g(X)$  defined over  $\mu_{q+1}$ . Encompassing this idea, many techniques were developed to study this  $g(X)$  over  $\mu_{q+1}$  in the literature, most of the techniques were elementary but quite complex and involved a lot of computation. In a recent paper [17], Ding and Zieve provided a new way of studying  $g(X)$ : they employed advanced tools such as the Hurwitz genus formula from arithmetic geometry to study geometric properties of  $g(X)$  (i.e. the type of branch points and ramification indices) from which permutation properties of  $f_{\underline{c}}(X)$  follow in some natural way. This powerful technique allowed them to resolve eight conjectures and open problems from the literature concerning  $f_{\underline{c}}(X)$  for  $q$  even and to cover most of the previous results. In proving Theorem 1–3, we adopt their ideas to study  $f_{\underline{c}}(X)$  for odd  $q$ . We do a careful analysis of geometric properties of  $g(X)$  for odd  $q$  and give a classification. While the ideas and techniques are similar to that of [17], the study  $g(X)$  is more complex in this paper. It turns out that the linear equivalence result comes naturally from this study of  $g(X)$ , from which planar functions in  $f_{\underline{c}}(X)$  can also be identified. We comment that this idea was already hinted in [17] (see [17, Theorem 1.2]), though the authors may not be aware of it at the time.

It seems possible that the classification results of [20] can be obtained in this way. It might be interesting to see if Theorem 1 can be obtained by adopting the approach of  $(Q, Q)$ -biprojective polynomials utilised in [20] for odd characteristic.

The paper is organized as follows. In Section II we introduce some universal notations and recall some background results that are needed for our proofs. In Section III we give detailed geometric properties of the rational function  $g(X)$  under consideration and in Section IV we classify  $g(X)$  in terms of linear equivalence. In Section V we derive the list of linear equivalence classes of  $f_{\underline{c}}(X)$  under the classification

of  $g(X)$ . Then in Section VI we prove Theorems 1–3. Finally in Section VII we conclude our paper and provide some open problems.

## II. PRELIMINARIES

Throughout this paper, we adopt the following notation:

- for any finite set  $S$ ,  $\#S$  is the cardinality of  $S$ ;
- for any field  $K$ ,  $K^* = K \setminus \{0\}$ ,  $\mathbb{P}^1(K) = K \cup \{\infty\}$  is set of  $K$ -rational points in  $\mathbb{P}^1$ , and  $\overline{K}$  is an algebraic closure of  $K$ ;
- $p$  is an (odd) prime,  $k$  is a positive integer,  $q = p^k$ ,  $\mathbb{F}_q$  is the finite field of order  $q$ ;
- for any positive integer  $d$ ,  $\mu_d$  is the set of  $d$ -th roots of unity in  $\overline{\mathbb{F}_q}$ ;
- for any  $c \in \mathbb{F}_{q^2}$ ,  $\bar{c} = c^q$ ;

### A. Self-conjugate reciprocal polynomials

Let  $D(X) \in \mathbb{F}_{q^2}[X]$ . Denote by  $D^{(q)}(X)$  the polynomial in  $\mathbb{F}_{q^2}[X]$  formed by taking  $q$ -th powers (or conjugates) on all the coefficients of  $D(X)$ . The *conjugate reciprocal* of  $D(X)$  is defined as

$$\widehat{D}(X) := X^{\deg D} D^{(q)}(1/X).$$

To be more precise, if  $D(X) = \sum_{i=0}^r a_i X^i$  with  $a_i \in \mathbb{F}_{q^2}$  for all  $i$  and  $a_r \neq 0$  where  $r > 0$ , then  $D^{(q)}(X) = \sum_{i=0}^r \bar{a}_i X^i$  and  $\widehat{D}(X) = \sum_{i=0}^r \bar{a}_{r-i} X^i$ . Note that if  $D(0) = a_0 = 0$ , then  $\deg \widehat{D} < r = \deg D$ . Otherwise if  $D(0) \neq 0$  then we have  $\deg \widehat{D} = \deg D$ .

A nonzero polynomial  $D(X) \in \mathbb{F}_{q^2}[X]$  is called *self-conjugate reciprocal* (SCR for short) if  $\widehat{D}(X) = \alpha D(X)$  for some  $\alpha \in \mathbb{F}_{q^2}^*$ . In particular this implies  $D(0) \neq 0$ .

The following about conjugate reciprocals and SCR polynomials are immediate from the above definitions:

**Lemma 4.** *All of the following hold:*

- if  $D(X) \in \mathbb{F}_{q^2}[X]$  is SCR then  $\widehat{D}(X)/D(X) \in \mu_{q+1}$ ;
- if  $D(X) \in \mathbb{F}_{q^2}[X]$  is nonzero and  $\alpha \in \overline{\mathbb{F}_q}^*$ , then the multiplicity of  $\alpha$  as a root of  $D(X)$  equals the multiplicity of  $\alpha^{-q}$  as a root of  $\widehat{D}(X)$ ;
- $D(X) \in \mathbb{F}_{q^2}[X]$  is SCR if and only if the multiset of roots of  $D(X)$  is preserved by the function  $\alpha \mapsto \alpha^{-q}$ . In particular, if  $\deg D = 1$  then it is SCR if and only if its unique root is in  $\mu_{q+1}$ ;

- if  $\alpha \in \mathbb{F}_{q^2}^*$  and  $\beta \in \mathbb{F}_q$  then  $\alpha X^2 + \beta X + \bar{\alpha}$  is SCR.

There are simple conditions describing the nature of the roots of a degree-2 SCR polynomial, but the situation is quite different for  $p = 2$  and for  $p \geq 3$  being odd. Here we focus on the case  $p \geq 3$ . Interested readers may refer to [17, Lemma 2.4] for the case  $p = 2$ .

**Lemma 5.** *Assume  $p$  is odd and  $D(X) = \alpha X^2 + \beta X + \bar{\alpha}$  with  $\alpha \in \mathbb{F}_{q^2}$  and  $\beta \in \mathbb{F}_q$  not both zero. Define  $\Delta(D) := \beta^2 - 4\alpha\bar{\alpha}$ . Then the following hold:*

- 1)  $D(X)$  has a multiple root (which must be in  $\mu_{q+1}$ ) if and only if  $\Delta(D) = 0$ ;
- 2)  $D(X)$  has two distinct roots in  $\mu_{q+1}$  if and only if  $\Delta(D)$  is a non-square in  $\mathbb{F}_q^*$ ;
- 3)  $D(X)$  has no roots in  $\mu_{q+1}$  if and only if  $\Delta(D)$  is a square in  $\mathbb{F}_q^*$ .

This result is quite elementary, since we cannot find it in the literature, for the sake of completeness, we provide a proof here.

*Proof.* If  $\alpha = 0$  and  $\beta \neq 0$ , then  $D(X) = \beta X$  is a degree-one polynomial, with a unique root 0, which is not in  $\mu_{q+1}$ . We also have  $\Delta(D) = \beta^2$  being a square in  $\mathbb{F}_q^*$ . So 3) applies to this case.

Hence from now on we assume  $\alpha \neq 0$ . By Lemma 4,  $D(X)$  is a degree-2 SCR polynomial. It is clear that  $D$  has a multiple root if and only if  $\Delta(D) = 0$ , and by Lemma 4, since its multiset of roots is preserved by the function  $\gamma \mapsto \gamma^{-q}$ , this multiple root must satisfy  $\gamma = \gamma^{-q}$ , that is,  $\gamma \in \mu_{q+1}$ .

Now suppose  $\Delta(D) \neq 0$ . Then  $D(X)$  has two distinct roots  $\gamma, \delta$ . Note that  $\gamma\delta = \frac{\bar{\alpha}}{\alpha} \in \mu_{q+1}$ , so either both  $\gamma, \delta$  are in  $\mu_{q+1}$ , or none of them are in  $\mu_{q+1}$ . Noting that  $\Delta(D) \in \mathbb{F}_q^*$ , there is an  $\theta \in \mathbb{F}_{q^2}^*$  such that  $\theta^2 = \Delta(D)$ . Easy to see that we have either  $\bar{\theta} = \theta$  or  $-\theta$ , according to whether  $\theta \in \mathbb{F}_q^*$  or not. We may take  $\gamma = -\frac{\beta+\theta}{2\alpha}$ . We see that  $\gamma \in \mu_{q+1}$  if and only if  $\gamma^{q+1} = 1$ , that is,

$$\left(\frac{\beta+\theta}{2\alpha}\right) \left(\frac{\beta+\bar{\theta}}{2\bar{\alpha}}\right) = 1.$$

This can be further simplified as

$$\beta^2 + \beta(\theta + \bar{\theta}) + \theta\bar{\theta} = 4\alpha\bar{\alpha},$$

and again

$$\beta(\theta + \bar{\theta}) + \theta\bar{\theta} + \theta^2 = 0.$$

Taking  $\bar{\theta} = \varepsilon\theta$  where  $\varepsilon \in \{\pm 1\}$  we have

$$\theta(1 + \varepsilon)(\beta + \theta) = 0.$$

Since  $\theta \neq 0$  and  $\beta + \theta \neq 0$  as  $\gamma \neq 0$ , this implies that  $\varepsilon = -1$ , that is  $\theta \notin \mathbb{F}_q^*$ . Hence we conclude that in this case  $\gamma, \delta \in \mu_{q+1}$  if and only if  $\theta \notin \mathbb{F}_q^*$ . This completes the proof of Lemma 5.  $\square$

### B. Rational Functions

Let  $K$  be a field and  $G(X) = N(X)/D(X)$  be a rational function in  $K$  where  $N, D \in K[X]$  and  $D$  is nonzero. Let  $C(X) = \gcd(N(X), D(X))$ , the monic greatest common divisor of  $N(X)$  and  $D(X)$  in  $K[X]$ . We write  $N(X) = C(X)N_0(X)$ ,  $D(X) = C(X)D_0(X)$  with  $N_0, D_0 \in K[X]$ , so that  $\gcd(N_0(X), D_0(X)) = 1$ . We identify  $G(X)$  with  $G_0(X) = N_0(X)/D_0(X)$  and view  $G(X)$  as the function  $\mathbb{P}^1(K) \rightarrow \mathbb{P}^1(K)$  defined by  $\alpha \mapsto G_0(\alpha)$ , so  $G(X)$  is also well-defined at elements  $\alpha \in K$  even if  $N(\alpha) = D(\alpha) = 0$ . We refer to  $N_0$  and  $D_0$  as the numerator and denominator of  $G$  respectively, and define the degree of  $G$  as  $\deg G = \max\{\deg N_0, \deg D_0\}$  if  $G(X) \neq 0$ .  $G$  is called *separable* if the field extension  $K(x)/K(G(x))$  is a separable extension of function fields where  $x$  is transcendental over  $K$ . In fact,  $G$  is separable if and only if  $G'(X) \neq 0$  if and only if  $G \notin K(X^p)$  where  $p = \text{char}(K)$  [18, Lemma 2.2].

We say non-constant  $F, G \in K(X)$  are *linearly equivalent over  $K$*  (or  *$K$ -linearly equivalent* for short) if there are degree-one  $\rho, \sigma \in K(X)$  such that  $G = \rho \circ F \circ \sigma$ .

The following are results about degree-one rational functions over  $\mathbb{F}_{q^2}$  satisfying certain properties [17], [36]. These are very useful when we study geometric properties of the accompanying function  $g_{\underline{c}}(X)$ .

**Lemma 6.** *A degree-one  $\rho(X) \in \mathbb{F}_{q^2}(X)$  permutes  $\mu_{q+1}$  if and only if  $\rho(X) = (\bar{\beta}X + \bar{\alpha})/(\alpha X + \beta)$  for some  $\alpha, \beta \in \mathbb{F}_{q^2}$  with  $\alpha\bar{\alpha} \neq \beta\bar{\beta}$ .*

**Lemma 7.** *A degree-one  $\rho(X) \in \mathbb{F}_{q^2}(X)$  maps  $\mu_{q+1}$  onto  $\mathbb{P}^1(\mathbb{F}_q)$  if and only if  $\rho(X) = (\delta X + \gamma\bar{\delta})/(X + \gamma)$  for some  $\gamma \in \mu_{q+1}$  and  $\delta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ .*

Given  $D(X) \in \mathbb{F}_{q^2}[X]$  and  $r \geq 0$ , define  $G_0(X) := X^r D(X)^{q-1}$ . It is easy to see that  $G_0(\mu_{q+1}) \subset \mu_{q+1} \cup \{0\}$ . Moreover,  $G_0(\mu_{q+1}) \subset \mu_{q+1}$  if and only if  $0 \notin D(\mu_{q+1})$ , and under this situation  $G_0$  induces the same function as the rational function  $G(X) := X^r D^{(q)}(1/X)/D(X)$  on  $\mu_{q+1}$ . While  $G(X)$  is usually defined over  $\mathbb{F}_{q^2}$ , it can be transformed into a rational function defined over  $\mathbb{F}_q$  as follows:

**Lemma 8.** [17, Lemma 2.11] Let  $G(X) = X^r D^{(q)}(1/X)/D(X)$  for some  $D(X) \in \mathbb{F}_{q^2}[X]$  and  $r \geq 0$ . Let  $\rho, \sigma \in \mathbb{F}_{q^2}(X)$  be any degree-one rational functions mapping  $\mu_{q+1}$  onto  $\mathbb{P}^1(\mathbb{F}_q)$ , and define

$$h = \rho \circ g \circ \sigma^{-1}.$$

Then we have  $h(X) \in \mathbb{F}_q(X)$ .

### C. Branch points and ramification

Here we introduce the concepts of branch points and ramification, which are the main tools to describe the geometric properties of the accompanying rational function  $g_{\mathbb{C}}(X)$  later on.

For a non-constant rational function  $G(X) \in \overline{\mathbb{F}}_q(X)$ , write  $G(X) = N(X)/D(X)$  where  $N(X), D(X) \in \overline{\mathbb{F}}_q[X]$  with  $\gcd(N(X), D(X)) = 1$ . For any  $\alpha \in \overline{\mathbb{F}}_q$ , define  $H_\alpha(X) \in \overline{\mathbb{F}}_q[X]$  as

$$H_\alpha(X) := \begin{cases} N(X) - G(\alpha)D(X) & (G(\alpha) \in \overline{\mathbb{F}}_q), \\ D(X) & (G(\alpha) = \infty). \end{cases}$$

It is clear that  $H_\alpha(\alpha) = 0$  for all  $\alpha \in \overline{\mathbb{F}}_q$ . The *ramification index*  $e_G(\alpha)$  of  $\alpha$  is then its multiplicity as a root of  $H_\alpha(X)$ . The ramification index of  $\infty$  is defined as  $e_G(\infty) := e_{G_1}(0)$ , where  $G_1(X) := G(\frac{1}{X})$ . Given any  $\beta \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$ , the *ramification multiset*  $E_G(\beta)$  of  $G(X)$  over  $\beta$  is the multiset of ramification indices  $e_G(\alpha)$  for any  $\alpha \in G^{-1}(\beta)$ , that is,  $E_G(\beta) := [e_G(\alpha) : \alpha \in G^{-1}(\beta)]$ . In particular, the elements in  $E_G(\beta)$  are positive integers whose sum is  $\deg G$ . We call  $\alpha \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$  a *ramification point* (or *critical point*) of  $G(X)$  if  $e_G(\alpha) > 1$ , and its corresponding image  $G(\alpha)$  a *branch point* (or *critical value*) of  $G$ . Hence a point  $\beta \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$  is a branch point of  $G$  if and only if  $E_G(\beta) \neq [1^{\deg G}]$ , where  $[m^n]$  denotes the multiset consisting of  $n$  copies of  $m$ , or equivalently,  $\sharp G^{-1}(\beta) < \deg G$ .

One most important result regarding ramification is known as the Hurwitz genus formula (see [30, Corollary 3.5.6]), which applying to the field extension  $\overline{\mathbb{F}}_q(x)/\overline{\mathbb{F}}_q(G(x))$  for transcendental  $x$  over  $\overline{\mathbb{F}}_q$  yields the following result used in our proof:

**Lemma 9.** Let  $G(X) \in \overline{\mathbb{F}}_q(X)$  be a rational function of degree  $n$ . Then

$$2n - 2 \geq \sum_{\alpha \in \mathbb{P}^1(\overline{\mathbb{F}}_q)} (e_G(\alpha) - 1)$$

with equality holds if and only if  $\text{char}(\overline{\mathbb{F}}_q) \nmid e_G(\alpha)$  for all  $\alpha \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$ .

#### D. Linear equivalence, EA-equivalence and CCZ-equivalence

Linear equivalence, EA-equivalence and CCZ-equivalence are equivalence relations of functions over the finite field  $\mathbb{F}_{p^n}$  under which planar (or PN) and APN properties are invariant. Due to these equivalence relations, one PN (or APN) function can generate a huge class of PN (resp. APN) functions. While the notion of these equivalence relations was introduced in 2006 in [4], the ideas behind this notion appeared much earlier [9], [27]. Let us first recall some definitions:

**Definition 1.** A function  $F : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$  is called

- linear if  $F(\alpha + \beta) = F(\alpha) + F(\beta)$  for any  $\alpha, \beta \in \mathbb{F}_{p^n}$ ;
- affine if  $F$  is a sum of a linear function and a constant;
- affine permutation (or linear permutation) if  $F$  is both affine (resp. linear) and a permutation on  $\mathbb{F}_{p^n}$ .
- Dembowski-Ostrom polynomial (DO polynomial) if

$$F(X) = \sum_{0 \leq k, j < n} a_{k,j} X^{p^k + p^j}, \quad a_{ij} \in \mathbb{F}_{p^n}.$$

In particular,  $F$  is affine if and only if  $F(X) = b + \sum_{j=0}^{n-1} a_j X^{p^j}$  where  $a_j, b \in \mathbb{F}_{p^n}$  for any  $j$ .

**Definition 2.** Two functions  $F$  and  $F'$  from  $\mathbb{F}_{p^n}$  to itself are called:

- affine equivalent (or linear equivalent) if  $F' = A_1 \circ F \circ A_2$ , where the mappings  $A_1, A_2$  are affine (resp. linear) permutations of  $\mathbb{F}_{p^n}$ ;
- extended affine equivalent (EA-equivalent) if  $F' = A_1 \circ F \circ A_2 + A$ , where the mappings  $A, A_1, A_2$  are affine, and where  $A_1, A_2$  are permutations of  $\mathbb{F}_{p^n}$ ;
- Carlet-Charpin-Zinoviev equivalent (CCZ-equivalent) if for some affine permutation  $\mathcal{L}$  of  $\mathbb{F}_{p^n}^2$  the image of the graph of  $F$  is the graph of  $F'$ , that is,  $\mathcal{L}(G_F) = G_{F'}$ , where

$$G_F = \{(x, F(x)) : x \in \mathbb{F}_{p^n}\}, \quad G_{F'} = \{(x, F'(x)) : x \in \mathbb{F}_{p^n}\}.$$

It is obvious that linear equivalence is a particular case of affine equivalence, and affine equivalence is a particular case of EA-equivalence. It was known that EA-equivalence is a particular case of CCZ-equivalence and every permutation is CCZ-equivalence to its inverse [9]. CCZ-equivalence is more general than EA-equivalence but there are particular cases of functions for which CCZ-equivalence can be reduced to EA-equivalence. For instance, CCZ-equivalence coincides with linear equivalence for DO

planar functions [5], [6]. Since the quadrinomial  $f_{\underline{c}}(X)$  (2) is a DO polynomial, we only consider linear equivalence in this paper. For simplicity, if two such polynomials  $f_1$  and  $f_2$  are linear equivalent, we call them *equivalent* to each other.

**Definition 3.** Two functions  $F$  and  $F'$  from  $\mathbb{F}_{p^n}$  to itself are called multiplicatively equivalent if there are  $\alpha, \beta \in \mathbb{F}_{p^n}^*$  and a positive integer  $k$  with  $\gcd(k, p^n - 1) = 1$  such that

$$f_1(X) \equiv \alpha f_2(\beta X^k) \pmod{X^{p^n} - X}.$$

It is easy to see that if  $f_1$  and  $f_2$  are multiplicative equivalent with  $n$  being a power of  $p$  (including the case  $n = 1$ ), then  $f_1$  and  $f_2$  are also linear equivalent.

### III. GEOMETRIC PROPERTIES OF $g(X)$

For any  $\underline{c} = (c_0, c_1, c_2, c_3) \in \mathbb{F}_{q^2}^4$ , define

$$A(X) = A_{\underline{c}}(X) := c_0 X^{Q+1} + c_1 X^Q + c_2 X + c_3. \quad (4)$$

The quadrinomial  $f_{\underline{c}}(X)$  given in (2) can be written as  $f_{\underline{c}}(X) = X^{Q+1} A(X^{q-1})$ .

Let us assume that  $\underline{c} \neq \underline{0}$ . Denote

$$B(X) = B_{\underline{c}}(X) := \bar{c}_3 X^{Q+1} + \bar{c}_2 X^Q + \bar{c}_1 X + \bar{c}_0, \quad (5)$$

$$g(X) = g_{\underline{c}}(X) := B_{\underline{c}}(X)/A_{\underline{c}}(X). \quad (6)$$

Here we use the notation  $\bar{c} := c^q$  for any  $c \in \mathbb{F}_{q^2}$ .

When  $q$  is even, geometric properties of  $g_{\underline{c}}(X)$  were given in [17] in order to study when  $f_{\underline{c}}(X)$  is a permutation on  $\mathbb{F}_{q^2}$ . In this Section, we refine and extend this work to give detailed geometric properties of  $g_{\underline{c}}(X)$  for all  $q$  while focusing on the case that  $q$  is odd. This will be useful when we classify  $g_{\underline{c}}(X)$

in the next Section. To describe the result, let us define a few parameters

$$\begin{cases} e_1 & := c_0\bar{c}_0 - c_1\bar{c}_1 - c_2\bar{c}_2 + c_3\bar{c}_3, \\ e_2 & := -c_0\bar{c}_0 - c_1\bar{c}_1 + c_2\bar{c}_2 + c_3\bar{c}_3, \\ e_3 & := -c_0\bar{c}_0 + c_1\bar{c}_1 - c_2\bar{c}_2 + c_3\bar{c}_3, \\ \theta_2 & := \bar{c}_2c_3 - \bar{c}_0c_1, \\ \theta_3 & := \bar{c}_1c_3 - \bar{c}_0c_2, \\ \theta_1^2 & := e_2^2 - 4\theta_2\theta_3, \end{cases} \quad (7)$$

and three polynomials

$$\begin{cases} W(X) & := (c_1c_2 - c_0c_3)X^2 + e_1X + (\bar{c}_1\bar{c}_2 - \bar{c}_0\bar{c}_3), \\ U(X) & := \bar{\theta}_2X^2 + e_2X + \theta_2, \\ V(X) & := \bar{\theta}_3^{1/Q}X^2 + e_3^{1/Q}X + \theta_3^{1/Q}. \end{cases} \quad (8)$$

Here for simplicity, we drop the subscript  $\underline{c}$  in the notation when there is no ambiguity. It is easy to see that  $e_1, e_2, e_3, \theta_1^2 \in \mathbb{F}_q$ ,  $\theta_1, \theta_2, \theta_3 \in \mathbb{F}_{q^2}$  and  $W(X), U(X), V(X) \in \mathbb{F}_{q^2}[X]$  are SCR polynomials.

We first state some properties that relate the three polynomials  $U(X), V(X)$  and  $W(X)$  in (8) with  $A(X)$  and  $B(X)$  given in (4) and (5) respectively:

**Lemma 10.** *Assume  $\underline{c} \neq \underline{0}$  and  $q$  is odd. Denote  $C(X) = \gcd(A(X), B(X))$ , the greatest monic common divisor of  $A(X)$  and  $B(X)$ .*

- 1) *If  $U(X)$  and  $V(X)$  are not both zero, then  $C(X) \mid \gcd(U(X), V(X))$  and  $C(X)$  is either  $X$  or a monic SCR polynomial of degree at most two;*
- 2) *Assume none of  $U(X), V(X)$  or  $W(X)$  is the zero polynomial. Denote  $\Gamma = \Gamma_{\underline{c}}$  the union of the set of roots of  $V(X)$  and the set with  $(2 - \deg V)$  copies of  $\infty$  (this set is either empty if  $\deg V = 2$ , or  $\{\infty\}$  if  $\deg V = 1$ ); denote  $\Lambda = \Lambda_{\underline{c}}$  the union of the set of roots of  $W(X)$  and the set with  $(2 - \deg W)$  copies of  $\infty$ .*
  - a)  *$\#\Gamma = \#\Lambda \in \{1, 2\}$ , and the cardinality is 1 if and only if  $\theta_1 = 0$ ;*
  - b) *Either both  $\Gamma, \Lambda \subset \mu_{q+1}$ , or both sets are of the form  $\{\alpha, \bar{\alpha}^{-1}\}$  for some  $\alpha \in \mathbb{F}_{q^2} \setminus \mu_{q+1}$ ;*
  - c)  *$\Gamma$  is the complete set of ramification points of  $g$ , and any branch point of  $g$  is in  $\Lambda$ ;*
  - d) *Assume  $C(X) = 1$ . Then  $\Lambda$  gives the complete set of branch points of  $g$ . Moreover, the  $g$ -ramification multiset of any  $\lambda \in \Lambda$  is either  $[Q + 1]$  or  $[1, Q]$ .*

We remark when  $q$  is even, all the above statements of Lemma 10 remain true except 2(c) in the special case that  $Q = 2$  and  $C(X) \neq 1$  and  $\deg g = 1$ , in such as case  $\Gamma = \emptyset$  since  $g$  has no ramification or branch points.

*Proof.* Here we borrow ideas from the proof of [17, Theorem 3.1] and treat the case that  $q$  is odd.

For any polynomial of the form  $P(X) := \alpha X^2 + \beta X + \gamma$  with  $\alpha, \beta, \gamma \in \mathbb{F}_{q^2}$ , define

$$\Delta(P) := \beta^2 - 4\alpha\gamma.$$

Thus if  $\deg(P) = 2$  then  $\Delta(P)$  is the discriminant of  $P(X)$ . Recall from [17] that  $U(X), V(X)$  and  $W(X)$  stated in (8) satisfy the following identities:

$$U(X) = (\bar{c}_3 X + \bar{c}_2)A(X) - (c_0 X + c_1)B(X); \quad (9)$$

$$V(X)^Q = A(X)B'(X) - A'(X)B(X); \quad (10)$$

$$\Delta(W) = \Delta(U) = \Delta(V)^Q = \theta_1^2; \quad (11)$$

$$U(X)V(X)^Q = W(g(X))A(X)^2. \quad (12)$$

It is immediate from (9) and (10) that  $C(X) \mid U(X)$  and  $C(X) \mid V(X)^Q$ . Moreover, the second part of Statement 1 easily follows from the fact that each of  $U(X)$  and  $V(X)$  is either a constant times  $X$  or a degree-two SCR polynomial and the assumption that they are not both zero. Now assume  $C(X) \nmid V(X)$ . This implies  $C(X)$  is not square-free. In particular it must be the square of a linear SCR polynomial. Hence  $U(X)$  is a constant multiple of  $C(X)$ , which implies  $\theta_1 = 0$ . Then Equation (11) implies  $\Delta(V) = 0$ , and  $C(X) \mid V(X)^Q$  implies that the unique root of  $C(X)$  is a root of  $V(X)$ , so  $V(X)$  is also a constant multiple  $C(X)$ , a contradiction. Hence we have  $C(X) \mid \gcd(U(X), V(X))$ .

Statements 2(a) and 2(b) follow from Equation (11), Lemmas 4 and 5 in Section II. In addition, the right hand side of (10) is simply  $A(X)^2 g'(X)$ . Hence we see that any ramification point of  $g$  in  $\overline{\mathbb{F}}_q$  must be in  $\Gamma$ . On the other hand, writing  $A(X) = A_0(X)C(X)$  and  $B(X) = B_0(X)C(X)$  for  $A_0, B_0 \in \mathbb{F}_{q^2}[X]$ , so that  $\gcd(A_0(X), B_0(X)) = 1$ . Then (12) can be rewritten as

$$U(X)V(X)^Q = W(g(X))A_0(X)^2 C(X)^2. \quad (13)$$

Here we note that  $W(g(X))A_0(X)^2 = W\left(\frac{B_0(X)}{A_0(X)}\right) A_0(X)^2$  is a polynomial in  $\mathbb{F}_{q^2}$ .

Denote  $\Gamma_1 := \Gamma \setminus \{\infty\}$ . If  $\theta_1 = 0$ , then  $U(X) = \bar{\theta}_2(X - \alpha)^2$ ,  $V(X) = \bar{\theta}_3^{1/Q}(X - \gamma)^2$  and  $W(X) =$

$c(X - \lambda)^2$  for some  $c \in \mathbb{F}_{q^2}^*$  and  $\alpha, \gamma, \lambda \in \mu_{q+1}$ . We have  $\Gamma_1 = \{\gamma\}$  and  $\Lambda = \{\lambda\}$ . Putting these into (13) and taking square root on both sides, we have

$$(X - \alpha)(X - \gamma)^Q = \tilde{c}(B_0(X) - \lambda A_0(X))C(X)$$

for some  $\tilde{c} \in \mathbb{F}_{q^2}^*$ .

Here  $C(X) = 1$  if  $\alpha \neq \gamma$ , otherwise  $C(X) = (X - \gamma)^i$  for some  $i \leq 2$ . Upon dividing both sides by  $C(X)$ , it is easy to see that  $\gamma$  is a multiple root of the LHS (the factor  $X - \gamma$  appears with exponent at least  $Q - 1 \geq 2$ ). Hence it is also so in the RHS, which is precisely equivalent to saying that  $\gamma \in \Gamma_1$  is a ramification point of  $g(X)$ , and its image is a branch point of  $g$ , that is,  $\lambda \in \Lambda$ .

Now assume  $\theta_1 \neq 0$ . Then  $\#\Gamma = \#\Lambda = 2$  and  $U(X), V(X)$  and  $W(X)$  are square-free. Writing  $U(X) = U_0(X)C(X)$  and  $V(X) = V_0(X)C(X)$ , and upon dividing both sides of (13) by  $C(X)^2$ , we obtain

$$U_0(X)V_0(X)^Q C(X)^{Q-1} = W(g(X))A_0(X)^2.$$

Now any  $\gamma \in \Gamma_1$  is a root of either  $V_0(X)$  or  $C(X)$ . Since  $Q \geq 3$ ,  $X - \gamma$  appears as a factor with exponent at least two in LHS. Hence  $\gamma$  is a multiple root of LHS and hence also a root of RHS. This clearly implies  $\gamma$  is a ramification point of  $g(X)$ , whose image  $g(\gamma)$  is either a root of  $W(X)$  or  $\infty$ , and is hence a branch point of  $g$ . Note that  $g(\gamma) = \infty$  if and only if  $\gamma$  is a root of  $A_0(X)$ , whence this may happen only if  $\deg W = 1$ . In either case, we see that the branch point  $g(\gamma) \in \Lambda$ .

To complete the proof of Statement 2(c), we need to show that  $\infty$  is a ramification point of  $g$  if and only if  $\deg V = 1$ . This can be proved as follows:  $\infty$  is a ramification point of  $g$  if and only if  $0$  is a ramification point of  $g(1/X) = g_{\underline{c}'}(X)$  where  $\underline{c}' = (c_3, c_2, c_1, c_0)$ . It is easy to verify that  $V_{\underline{c}'}(X) = -V^{(q)}(X)$  and  $W_{\underline{c}'}(X) = W(X)$ . Hence  $0$  is a ramification point of  $g_{\underline{c}'}$  if and only if  $0$  is a root of  $V^{(q)}$  if and only if  $0$  is a root of  $V$ , which is equivalent to  $\deg V = 1$ . In this case, the branch point  $g(\infty) = g_{\underline{c}'}(0)$  is in  $\Lambda_{\underline{c}'} = \Lambda$ .

Finally, assume  $C(X) = 1$ . Then  $\deg g = \max\{\deg A, \deg B\}$ . Note that the latter is not  $Q + 1$  if and only if  $c_0 = c_3 = 0$ , whence in this case  $C(X) \neq 1$ . Hence  $\deg g = Q + 1$ . By (12), for any ramification point  $\gamma \in \Gamma$ ,  $e_g(\gamma)$  is either  $Q + 1$  or  $Q$  according to whether it is a root of  $U(X)$  or not. This implies that the  $g$ -ramification multiset of the corresponding branch point  $g(\gamma) \in \Lambda$  is  $[Q + 1]$  or  $[1, Q]$ . Hence each branch point corresponds to exactly one ramification point. By Statements 2(a) and (c), then  $g(\Gamma) = \Lambda$ ,

so  $\Lambda$  gives the complete set of branch points of  $g$ . □

Armed with Lemma 10, we can give more detailed information about geometric properties of  $g_{\underline{c}}(X)$ . We remark that Lemma 11 are still true when  $p = 2$ , though we focus on the case that  $q$  is odd.

**Lemma 11.** *Assume  $\underline{c} \neq \underline{0}$  and  $q$  is odd. Then we have*

- 1)  $g(X)$  is constant if and only if  $U(X)$  and  $V(X)$  are both zero;
- 2)  $g(X)$  is non-constant and  $A(X)$  has a root in  $\mu_{q+1}$  if and only if at least one of  $U(X), V(X)$  is a nonzero polynomial with roots in  $\mu_{q+1}$  and  $\deg g \neq Q + 1$ ;
- 3)  $g(X)$  is non-constant and  $A(X)$  has no roots in  $\mu_{q+1}$  if and only if one of the following is true:
  - a)  $g(X)$  is  $\overline{\mathbb{F}}_q$ -linearly equivalent to  $X^n$  where  $n \in \{Q + 1, Q - 1\}$ ; this occurs if and only if  $U(X)/V(X) \in \mathbb{F}_{q^2}^*$ ; or
  - b)  $g(X)$  has at least one branch point in  $\mathbb{P}^1(\overline{\mathbb{F}}_q)$  with ramification multiset  $[1, Q]$ .

*Proof.* For 1), if  $g(X)$  is constant, then there is  $\lambda \in \mathbb{F}_{q^2}^*$  such that  $\bar{c}_3 = \lambda c_0, \bar{c}_2 = \lambda c_1, \bar{c}_1 = \lambda c_2$  and  $\bar{c}_0 = \lambda c_3$ . Putting into the formulas in (7) implies  $e_2 = e_3 = \theta_2 = \theta_3 = 0$ . Hence  $U(X)$  and  $V(X)$  are both zero; Next assume that both  $U(X)$  and  $V(X)$  are zero. By using (9), we see that  $g(X) = \frac{\bar{c}_3 X + \bar{c}_2}{c_0 X + c_1}$ , so  $\deg g \leq 1$ . By using (10), we see that  $A(X)B'(X) - A'(X)B(X) = 0$ , so  $g(X)$  is non-separable. This shows that  $g(X)$  is constant. So we have proved 1) of Lemma 11.

For 2), let us first assume that  $g(X)$  is non-constant and  $A(X)$  has a root  $\alpha$  in  $\mu_{q+1}$ . Then at least one of  $U(X)$  and  $V(X)$  is nonzero. Note that the multiset of roots of  $B(X)$  in  $\overline{\mathbb{F}}_q^*$  is the same as the multiset of  $(-q)$ -th powers of roots of  $A(X)$  in  $\overline{\mathbb{F}}_q^*$ . Hence  $\alpha = \alpha^{-q}$  is also a root of  $B(X)$ , which implies  $C(X) = \gcd(A(X), B(X))$  has a root in  $\mu_{q+1}$ . On the other hand, if  $C(X)$  has a root in  $\mu_{q+1}$ , then obviously so does  $A(X)$ . Hence to prove Statement 2), it suffices to show that  $C(X)$  has a root in  $\mu_{q+1}$  if and only if any nonzero member among  $U(X), V(X)$  have roots in  $\mu_{q+1}$  and  $\deg g \neq Q + 1$ . This follows from Statement 1 of Lemma 10 by simply noting that whenever  $U(X)$  (resp.  $V(X)$ ) is nonzero, then either all its roots are in  $\mu_{q+1}$  or none of the roots are, and also that  $\deg g \neq Q + 1$  if and only if  $C(X) \neq 1$ . This proves 2) of Lemma 11.

As for 3), let us assume that  $g(X)$  is non-constant, and  $A(X)$  has no roots in  $\mu_{q+1}$ . We first know by 1) of Lemma 11 that at least one of  $U(X)$  and  $V(X)$  is nonzero.

If  $U(X) = 0$  and  $V(X) \neq 0$ , then  $\theta_1 = 0$ . By (13),  $\Delta(V) = 0$ . By Lemma 5,  $V(X)$  has a multiple root in  $\mu_{q+1}$ . Moreover,  $U(X) = 0$  implies that  $\deg g \leq 1 < Q + 1$  and so  $A(X)$  has a root in  $\mu_{q+1}$  by

Statement 2) of Lemma 11.

If  $V(X) = 0$  and  $U(X) \neq 0$ , then  $\Delta(V) = 0$ . By (13),  $\theta_1 = 0$ . By Lemma 5,  $U(X)$  has a multiple root in  $\mu_{q+1}$ . Moreover,  $V(X) = 0$  implies that  $g$  is non-separable, so that  $\deg g \neq Q + 1$ . Hence  $A(X)$  has a root in  $\mu_{q+1}$  by Statement 2) of Lemma 11.

From now on we assume both  $U(X)$  and  $V(X)$  are nonzero, so that  $\max\{\deg U, \deg V\} \leq 2$ , and so  $\deg C \leq 2$  by Statement 1 of Lemma 10. If  $\deg g = Q + 1$  then  $C(X) = 1$  and Statement 2) of Lemma 11 implies  $A(X)$  has no roots in  $\mu_{q+1}$ . Moreover, by Statement 2) of Lemma 10, there are one or two branch points of  $g$ , each with ramification multiset  $[Q + 1]$  or  $[1, Q]$ . If at least one has ramification multiset  $[1, Q]$  then we are done. Now assume all branch points of  $g$  have ramification multiset  $[Q + 1]$ . In particular  $p \nmid e_g(\alpha)$  for all  $\alpha \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$ . By the Hurwitz genus formula (Lemma 9), we see that there must be exactly two such branch points. Both have a unique  $g$ -preimage in  $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ . Hence  $g(X)$  is  $\overline{\mathbb{F}}_q$ -linearly equivalent to  $X^{Q+1}$ .

Finally assume  $\deg g \neq Q + 1$ , so that  $C(X) \neq 1$ . By Statement 2) of Lemma 11, then  $V(X)$  (and  $U(X)$ ) has no roots in  $\mu_{q+1}$ . Hence the set  $\Gamma$  as defined in Lemma 10 is of the form  $\{\alpha, \bar{\alpha}^{-1}\}$  for some  $\alpha \in \mathbb{F}_{q^2} \setminus \mu_{q+1}$ . This could happen only if  $C(X)$  is a nonzero constant multiple of  $V(X)$  (and hence also  $U(X)$ ). If  $C(X) = X$ , then  $c_0 = c_3 = 0$  while at least one of  $c_1$  or  $c_2$  is nonzero, so  $\max\{\deg A, \deg B\} = Q$ . If  $\deg C = 2$ , then at least one of  $c_0$  or  $c_3$  is nonzero, so  $\max\{\deg A, \deg B\} = Q + 1$ . In either case we have  $\deg g = Q - 1$ . Putting these into (13) and dividing both sides by  $C(X)^2$  we have

$$V(X)^{Q-1} = \tilde{c} W(g(X)) A_0(X)^2$$

for some constant  $\tilde{c} \in \mathbb{F}_{q^2}^*$ .

This immediately implies that  $e_g(\gamma) = Q - 1 = \deg g$  for all  $\gamma \in \Gamma$ . Since  $Q \geq 3$ ,  $g$  has two branch points with unique preimages in  $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ , and thereby is  $\overline{\mathbb{F}}_q$ -linearly equivalent to  $X^{Q-1}$ . This proves 3) a) and b) of Lemma 11.

Finally, if  $g(X)$  is  $\overline{\mathbb{F}}_q$ -linearly equivalent to  $X^{Q+1}$ , then  $C(X) = 1$ , by counting multiplicity of the term  $X - \gamma$  for all  $\gamma \in \Gamma$  on both sides of (13), we see that  $U(X)/V(X) \in \mathbb{F}_{q^2}$ ; if  $g(X)$  is  $\overline{\mathbb{F}}_q$ -linearly equivalent to  $X^{Q-1}$ , then  $\deg C = 2$ , we also have  $U(X)/V(X) \in \mathbb{F}_{q^2}^*$ . If  $U(X)/V(X) \notin \mathbb{F}_{q^2}^*$ , clearly  $g(X)$  is not  $\overline{\mathbb{F}}_q$ -linearly equivalent to  $X^n$  for  $n \in \{Q + 1, Q - 1\}$ . Now the proof of Lemma 11 is complete.  $\square$

#### IV. CLASSIFICATION OF $g(X)$

We will see in later sections that Cases 1) and 2) of Lemma 11 do not yield planar functions, which are the main interest of this paper. So we examine  $g(X)$  further according to Case 3) of Lemma 11. We first consider Case 3) a).

**Lemma 12.** *Let  $\underline{c} \neq \underline{0}$ . Assume that  $A(X)$  has no roots in  $\mu_{q+1}$  and  $g(X)$  is  $\overline{\mathbb{F}}_q$ -linearly equivalent to  $X^n$  where  $n \in \{Q+1, Q-1\}$ . Then one of the following holds:*

- 1)  $g(X) = \rho^{-1} \circ X^{Q+1} \circ \sigma$  for some degree-one  $\rho, \sigma \in \mathbb{F}_{q^2}(X)$  both of which map  $\mu_{q+1}$  onto  $\mathbb{P}^1(\mathbb{F}_q)$ ;
- 2)  $g(X) = \rho^{-1} \circ X^{Q+1} \circ \sigma$  for some degree-one  $\rho, \sigma \in \mathbb{F}_{q^2}(X)$  both of which permute  $\mu_{q+1}$ ;
- 3)  $g(X) = \rho^{-1} \circ X^{Q-1} \circ \sigma$  for some degree-one  $\rho, \sigma \in \mathbb{F}_{q^2}(X)$  both of which permute  $\mu_{q+1}$ , and there exists  $\alpha \in \mathbb{F}_{q^2} \setminus \mu_{q+1}$  such that  $\sigma(\{\alpha, \bar{\alpha}^{-1}\}) = \{0, \infty\}$  and  $\gcd(A(X), B(X))$  is a constant multiple of  $(\bar{\alpha}X - 1)(X - \alpha)$ .

The proof of Theorem 12 was essentially given by following and combining the proofs of [17, Lemma 5.1 and Proposition 5.3], though in their proofs some extra assumptions were made on some other parameters to fit their purpose. For the convenience of readers, we provide a detailed proof here.

*Proof of Lemma 12.* Let  $\Gamma$  and  $\Lambda$  be defined as in Lemma 10.

First, we know that  $g(X)$  has 2 branch points in  $\mathbb{P}^1(\mathbb{F}_q)$ , so that  $\#\Gamma = \#\Lambda = 2$ . We first assume  $\Gamma \subset \mu_{q+1}$ . Then we also have  $\Lambda \subset \mu_{q+1}$ . Since  $A(X)$  has no roots in  $\mu_{q+1}$ ,  $n = \deg g = Q+1$  by Lemma 11. Let  $\Gamma = \{\alpha_1, \alpha_2\}$  and  $\Lambda = \{\beta_1, \beta_2\}$ . Since each point in  $\Gamma$  is the unique  $g$ -preimage of a point in  $\Lambda$ , we may assume  $g(\alpha_1) = \beta_1$  and  $g(\alpha_2) = \beta_2$ . Now define

$$\sigma(X) := \frac{\gamma(X - \alpha_2)}{X - \alpha_1}$$

and

$$\tilde{\rho}(X) := \frac{\delta(X - \beta_2)}{X - \beta_1},$$

where  $\gamma, \delta \in \mathbb{F}_{q^2}^*$  such that  $\bar{\gamma}/\gamma = \alpha_2/\alpha_1$  and  $\bar{\delta}/\delta = \beta_2/\beta_1$  respectively. Then we have

$$\sigma(X) = \frac{\gamma X - \alpha_1 \bar{\gamma}}{X - \alpha_1}$$

and

$$\tilde{\rho}(X) = \frac{\delta X - \beta_1 \bar{\delta}}{X - \beta_1}$$

respectively, that is,  $\sigma(\mu_{q+1}) = \tilde{\rho}(\mu_{q+1}) = \mathbb{P}^1(\mathbb{F}_q)$  by Lemma 7. In addition,  $\sigma(\alpha_1) = \infty = \tilde{\rho}(\beta_1)$  and  $\sigma(\alpha_2) = 0 = \tilde{\rho}(\beta_2)$ . This implies that the function  $h(X) := \tilde{\rho} \circ g \circ \sigma^{-1}(X)$  maps  $\mathbb{P}^1(\mathbb{F}_q)$  into  $\mathbb{P}^1(\mathbb{F}_q)$ , and 0 and  $\infty$  are the unique  $h$ -preimages of 0 and  $\infty$  respectively. In addition,  $\deg h = \deg g = Q + 1$ . Together with Lemma 8, we conclude that  $h(X) = \varepsilon X^{Q+1}$  for some  $\varepsilon \in \mathbb{F}_q^*$ . Finally, we have  $g(X) = \tilde{\rho}^{-1} \circ h \circ \sigma(X) = \rho^{-1} \circ X^{Q+1} \circ \sigma(X)$ , where  $\rho(X) := \varepsilon^{-1} \tilde{\rho}(X) \in \mathbb{F}_{q^2}(X)$  is of degree-one and maps  $\mu_{q+1}$  onto  $\mathbb{P}^1(\mathbb{F}_q)$ . This proves 1) of Lemma 12.

Next we assume  $\Gamma \cap \mu_{q+1} = \emptyset$ . By Statement 2(b) of Lemma 10, we have  $\Gamma = \{\alpha, \bar{\alpha}^{-1}\}$  and  $\Lambda = \{\beta, \bar{\beta}^{-1}\}$  for some  $\alpha, \beta \in \mathbb{P}^1(\mathbb{F}_{q^2}) \setminus \mu_{q+1}$ . Again each point in  $\Gamma$  is the unique  $g$ -preimage of a point in  $\Lambda$ , so we may assume that  $g(\alpha) = \beta$  and  $g(\bar{\alpha}^{-1}) = \bar{\beta}^{-1}$ . Now define  $\sigma(X) = -\frac{\bar{\alpha}X-1}{X-\alpha}$  if  $\alpha \in \mathbb{F}_{q^2} \setminus \mu_{q+1}$  and  $\sigma(X) = X$  if  $\alpha = \infty$ . Similarly, define  $\tilde{\rho}(X) = -\frac{\bar{\beta}X-1}{X-\beta}$  if  $\beta \in \mathbb{F}_{q^2} \setminus \mu_{q+1}$  and  $\tilde{\rho}(X) = X$  if  $\beta = \infty$ . In all these cases  $\sigma, \tilde{\rho}$  both permute  $\mu_{q+1}$ . In addition,  $\sigma(\alpha) = \infty = \tilde{\rho}(\beta)$  and  $\sigma(\bar{\alpha}^{-1}) = 0 = \tilde{\rho}(\bar{\beta}^{-1})$ . Combining these we conclude that the function  $h(X) := \tilde{\rho} \circ g \circ \sigma^{-1}(X)$  maps  $\mu_{q+1}$  into  $\mu_{q+1}$ , and 0 and  $\infty$  are the unique  $h$ -preimages of 0 and  $\infty$  respectively. Hence  $h(X) = \varepsilon X^n$  for some  $\varepsilon \in \overline{\mathbb{F}}_q^*$ , where  $n := \deg g$ . Since  $h(\mu_{q+1}) \subset \mu_{q+1}$ , we must have  $\varepsilon \in \mu_{q+1}$ . This implies that  $g(X) = \tilde{\rho}^{-1} \circ h \circ \sigma(X) = \rho^{-1} \circ X^n \circ \sigma(X)$ , where  $\rho(X) := \varepsilon^{-1} \tilde{\rho}(X) \in \mathbb{F}_{q^2}(X)$  is of degree-one and permutes  $\mu_{q+1}$ . In addition, by Lemma 11,  $n = Q + 1$  or  $Q - 1$  according to whether  $C(X) = 1$  or not. The case  $C(X) = 1$  corresponds to 2) of Lemma 12. If  $C(X) \neq 1$ , then  $n = Q - 1$ , we also know that  $C(X)$  is a constant multiple of  $V(X)$ . If  $\deg V = 1$ , then  $C(X) = X = -(\bar{\alpha}X - 1)(X - \alpha)$  with  $\alpha = 0$ , and  $\sigma(\{0, \infty\}) = \{0, \infty\}$ . Otherwise  $C(X) = (X - \alpha)(X - \bar{\alpha}^{-1}) = \bar{\alpha}^{-1}(\bar{\alpha}X - 1)(X - \alpha)$ . This proves 3) of Lemma 12. Now the proof of Lemma 12 is complete.  $\square$

Next we consider  $g(X)$  in Case 3) b) of Lemma 11.

**Lemma 13.** *Let  $\underline{c} \neq \underline{0}$ . Assume  $g(X)$  has at least one branch point with ramification multiset  $[1, Q]$ .*

*Then either one of the following holds:*

- 1)  $g(X) = \rho^{-1} \circ \frac{X^{Q+1}}{X+1} \circ \sigma$  for some degree-one  $\rho, \sigma \in \mathbb{F}_{q^2}(X)$  both of which map  $\mu_{q+1}$  to  $\mathbb{P}^1(\mathbb{F}_q)$ ;
- 2)  $g(X) = \rho^{-1} \circ \frac{X^Q}{X^{Q+1} + \varepsilon} \circ \sigma$  for some degree-one  $\rho, \sigma \in \mathbb{F}_{q^2}(X)$  both of which map  $\mu_{q+1}$  to  $\mathbb{P}^1(\mathbb{F}_q)$ ,  
and  $\varepsilon \in \mathbb{F}_q^*$ ;
- 3)  $g(X) = \rho^{-1} \circ \frac{X^Q(X-1)}{X+\varepsilon} \circ \sigma$  for some degree-one  $\rho, \sigma \in \mathbb{F}_{q^2}(X)$  both of which map  $\mu_{q+1}$  to  $\mathbb{P}^1(\mathbb{F}_q)$ ,  
and  $\varepsilon \in \mathbb{F}_q^* \setminus \{-1\}$ ;
- 4)  $g(X) = \rho^{-1} \circ \frac{X^Q(\varepsilon X+1)}{X+\varepsilon} \circ \sigma$  for some degree-one  $\rho, \sigma \in \mathbb{F}_{q^2}(X)$  both of which permute  $\mu_{q+1}$ , and

$$\varepsilon \in \mathbb{F}_{q^2}^* \setminus \mu_{q+1}.$$

*Proof.* Since  $\deg g = Q + 1$ , from Lemma 11, we see that  $C(X) = 1$ ,  $A(X)$  has no roots in  $\mu_{q+1}$ ,  $U(X)$  and  $V(X)$  are both nonzero,  $U(X)/V(X) \notin \mathbb{F}_{q^2}^*$ , and  $g(X)$  is not  $\overline{\mathbb{F}}_q$ -linearly equivalent to a monomial.

We first consider the case where  $\gcd(U, V) \neq 1$ . Since  $U(X)/V(X) \notin \mathbb{F}_{q^2}^*$ , we must have  $\deg U = \deg V = 2$ . In addition,  $U(X)$  and  $V(X)$  only have one common root, say  $\alpha$ . If  $\alpha$  is not in  $\mu_{q+1}$ , then  $\alpha^{-q}$  will also be a common root of  $U(X)$  and  $V(X)$  since they are SCR polynomials, a contradiction. Hence  $\alpha \in \mu_{q+1}$ . It cannot be a multiple root either. Hence  $\theta_1 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$  by Lemma 5, which in turn implies that  $U(X), V(X)$  and  $W(X)$  all have two distinct roots in  $\mu_{q+1}$  by (11). Let  $\beta_1$  and  $\beta_2$  be the other roots of  $U(X)$  and  $V(X)$  respectively. In addition, let  $\Lambda = \{\gamma_1, \gamma_2\}$  be the set of roots of  $W$ . Using Equation (13), we see that  $\alpha$  has multiplicity  $Q + 1$  as a ramification point of  $g$ , while  $\beta_2$  has multiplicity  $Q$ . Lemma 10 implies that  $\alpha$  is the unique  $g$ -preimage of some element in  $\Lambda$ . Let us assume that this root is  $\gamma_2$ . Then  $\gamma_1$  is the unique branch point with  $g$ -ramification multiset  $[1, Q]$ . In fact Equation (13) implies that  $g(\beta_1) = \gamma_1 = g(\beta_2)$ . Define

$$\tilde{\sigma}(X) := \frac{\delta_1(X - \alpha)}{X - \beta_2}$$

and

$$\tilde{\rho}(X) := \frac{\delta_2(X - \gamma_2)}{X - \gamma_1},$$

where  $\delta_1, \delta_2 \in \mathbb{F}_{q^2}^*$  such that  $\bar{\delta}_1/\delta_1 = \alpha/\beta_2$  and  $\bar{\delta}_2/\delta_2 = \gamma_2/\gamma_1$  respectively. By Lemma 7,  $\tilde{\sigma}, \tilde{\rho}$  both map  $\mu_{q+1}$  onto  $\mathbb{P}^1(\mathbb{F}_q)$ . In addition,  $\tilde{\sigma}(\beta_2) = \infty = \tilde{\rho}(\gamma_1)$  and  $\tilde{\sigma}(\alpha) = 0 = \tilde{\rho}(\gamma_2)$ . Combining these results, we find that the rational function  $h(X) := \tilde{\rho} \circ g \circ \tilde{\sigma}^{-1}(X)$  has degree  $Q + 1$  and maps  $\mathbb{P}^1(\mathbb{F}_q)$  into  $\mathbb{P}^1(\mathbb{F}_q)$ , and 0 is the unique  $h$ -preimage of 0, and  $\infty$  is another branch point of  $h$ , with  $\infty$  as an  $h$ -preimage of multiplicity  $Q$ . Together with Lemma 8, we conclude that  $h(X) = \frac{\lambda X^{Q+1}}{X + \varepsilon}$  for some  $\lambda, \varepsilon \in \mathbb{F}_q^*$ . This implies  $g(X) = \tilde{\rho}^{-1} \circ h \circ \tilde{\sigma}(X) = \rho^{-1} \circ \frac{X^{Q+1}}{X + \varepsilon} \circ \sigma(X)$ , where  $\sigma(X) := \varepsilon^{-1} \tilde{\sigma}(X)$  and  $\rho(X) := \lambda^{-1} \varepsilon^{-Q} \tilde{\rho}(X)$  are both of degree-one in  $\mathbb{F}_{q^2}(X)$  and map  $\mu_{q+1}$  onto  $\mathbb{P}^1(\mathbb{F}_q)$ . This proves 1) of Lemma 13.

From now on we assume  $\gcd(U, V) = 1$ . We first assume  $U(X)$  has a root in  $\mu_{q+1}$ . If this is the unique root of  $U$ , then  $\theta_1 = 0$  by Lemma 5, and  $V(X)$  and  $W(X)$  both have a unique multiple root in  $\mu_{q+1}$  by Equation (11) too. Let us denote by  $\alpha_1, \alpha_2$  and  $\beta$  the unique roots of  $U(X), V(X)$  and  $W(X)$  respectively. Since  $\gcd(U, V) = 1$ ,  $\alpha_1 \neq \alpha_2$ . Since  $W$  has only one root, by Lemma 10, we must have  $g(\alpha_1) = \beta = g(\alpha_2)$ , and  $\beta$  is the unique branch point of  $g$ , whose ramification multiset is  $[1, Q]$ . Now

define

$$\sigma(X) := \frac{\gamma(X - \alpha_1)}{X - \alpha_2}$$

and

$$\tilde{\rho}(X) := \frac{X - \beta}{\delta X - \beta\bar{\delta}},$$

where  $\gamma, \delta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ , with  $\bar{\gamma}/\gamma = \alpha_2/\alpha_1$ . Then both  $\sigma$  and  $\tilde{\rho}$  map  $\mu_{q+1}$  onto  $\mathbb{P}^1(\mathbb{F}_q)$ . In addition,  $\sigma(\alpha_1) = \infty$  and  $\sigma(\alpha_2) = 0 = \tilde{\rho}(\beta)$ . Combining these we find that the rational function  $h(X) := \tilde{\rho} \circ g \circ \sigma^{-1}(X)$  has degree  $Q + 1$  and maps  $\mathbb{P}^1(\mathbb{F}_q)$  into  $\mathbb{P}^1(\mathbb{F}_q)$ , 0 is the unique branch point of  $h$ , with 0 and  $\infty$  as its  $h$ -preimages of multiplicity  $Q$  and 1 respectively. By Lemma 8,  $h(X) \in \mathbb{F}_q(X)$ . Hence  $h(X) = \frac{X^Q}{D(X)}$  for some  $D(X) \in \mathbb{F}_q[X]$  of degree  $Q+1$  with  $D(0) \neq 0$ . Since  $g(X) = \frac{B(X)}{A(X)}$ , we must have  $D(X) = A_{\underline{c}_0}(X)$  for some  $\underline{c}_0 = (c_{00}, c_{01}, c_{02}, c_{03}) \in \mathbb{F}_q^4$ , with  $c_{00}c_{03} \neq 0$ . Then  $D(X)^2 h'(X) = -X^Q(c_{00}X^Q + c_{02})$ . Since 0 is the unique critical point of  $h$ , we must have  $c_{02} = 0$ . Hence  $h(X) = \frac{X^Q}{c_{00}X^{Q+1} + c_{01}X^Q + c_{03}}$ . This implies  $g(X) = \tilde{\rho}^{-1} \circ h \circ \sigma(X) = \rho^{-1} \circ \frac{X^Q}{X^{Q+1} + \varepsilon} \circ \sigma(X)$ , where  $\rho(X) = (c_{00}\tilde{\rho}(X))/(1 - c_{01}\tilde{\rho}(X))$  and  $\varepsilon = c_{03}/c_{00} \in \mathbb{F}_q^*$ , so  $\rho(\mu_{q+1}) = \mathbb{P}^1(\mathbb{F}_q)$ . This proves 2) of Lemma 13.

Now we assume  $U$  has two distinct roots in  $\mu_{q+1}$ . By Lemma 5, this implies  $\theta_1 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ , and  $V(X), W(X)$  have two distinct roots in  $\mu_{q+1}$  too by Equation (11). Denote by  $\Sigma = \{\alpha_1, \alpha_2\}, \Gamma = \{\beta_1, \beta_2\}$  and  $\Lambda = \{\gamma_1, \gamma_2\}$  the set of roots of  $U(X), V(X)$  and  $W(X)$  respectively. Since  $\gcd(U, V) = 1$ , we have  $\Sigma \cap \Gamma = \emptyset$ . By Lemma 10,  $\Gamma$  is the set of ramification points of  $g$ , each of which has multiplicity  $Q$ . In addition, we may assume  $g(\alpha_i) = \gamma_i = g(\beta_i)$  for  $i = 1, 2$ . Then both elements of  $\Lambda$  have  $g$ -ramification multiset  $[1, Q]$ . Now define

$$\tilde{\sigma}(X) := \frac{\delta_1(X - \beta_2)}{X - \beta_1}$$

and

$$\tilde{\rho}(X) := \frac{\delta_2(X - \gamma_2)}{X - \gamma_1},$$

where  $\delta_1, \delta_2 \in \mathbb{F}_{q^2}^*$  such that  $\bar{\delta}_1/\delta_1 = \beta_2/\beta_1$  and  $\bar{\delta}_2/\delta_2 = \gamma_2/\gamma_1$  respectively. Then  $\tilde{\sigma}, \tilde{\rho}$  both map  $\mu_{q+1}$  onto  $\mathbb{P}^1(\mathbb{F}_q)$ . In addition,  $\tilde{\sigma}(\beta_1) = \infty = \tilde{\rho}(\gamma_1)$  and  $\tilde{\sigma}(\beta_2) = 0 = \tilde{\rho}(\gamma_2)$ . Combining these we find that the rational function  $h(X) := \tilde{\rho} \circ g \circ \tilde{\sigma}^{-1}(X)$  has degree  $Q + 1$ , maps  $\mathbb{P}^1(\mathbb{F}_q)$  into  $\mathbb{P}^1(\mathbb{F}_q)$ , 0 and  $\infty$  are the branch points of  $h$ , as  $h$ -preimages of 0 and  $\infty$  of multiplicity  $Q$  respectively. Together with Lemma 8, we have  $h(X) = \frac{\lambda X^Q(X + \varepsilon_1)}{X + \varepsilon_2}$  for some  $\lambda, \varepsilon_1, \varepsilon_2 \in \mathbb{F}_q^*$ , with  $\varepsilon_1 \neq \varepsilon_2$ . This implies that  $g(X) = \tilde{\rho}^{-1} \circ h \circ \tilde{\sigma}(X) = \rho^{-1} \circ \frac{X^Q(X-1)}{X + \varepsilon} \circ \sigma(X)$ , where  $\sigma(X) := -\varepsilon_1^{-1}\tilde{\sigma}(X)$  and  $\rho(X) := -\lambda^{-1}\varepsilon_1^{-Q}\tilde{\rho}(X)$

are both of degree-one in  $\mathbb{F}_{q^2}(X)$  and map  $\mu_{q+1}$  onto  $\mathbb{P}^1(\mathbb{F}_q)$ , and  $\varepsilon = -\varepsilon_2/\varepsilon_1 \in \mathbb{F}_q^* \setminus \{-1\}$ . This proves 3) of Lemma 13.

Finally we assume  $U$  has no roots in  $\mu_{q+1}$ . By Lemma 5, this implies  $\theta_1 \in \mathbb{F}_q^*$ , and  $V(X), W(X)$  both have no roots in  $\mu_{q+1}$  by Equation (11). If  $\deg U = 1$ , define  $\Sigma = \{0, \infty\}$ . If  $\deg U = 2$ , define  $\Sigma$  as the set of roots of  $U(X)$ , which is of the form  $\{\alpha, \bar{\alpha}^{-1}\}$  for some  $\alpha \in \mathbb{F}_{q^2}^* \setminus \mu_{q+1}$ . To combine these two cases, let us simply write  $\Sigma = \{\alpha, \bar{\alpha}^{-1}\}$  where  $\alpha \in \mathbb{P}^1(\mathbb{F}_{q^2}) \setminus \mu_{q+1}$ . Assume  $\Gamma = \{\beta, \bar{\beta}^{-1}\}$  and  $\Lambda = \{\gamma, \bar{\gamma}^{-1}\}$  as defined in Lemma 10 respectively, where  $\beta, \gamma \in \mathbb{P}^1(\mathbb{F}_{q^2}) \setminus \mu_{q+1}$ . Since  $\gcd(U, V) = 1$ , we have  $\Sigma \cap \Gamma = \emptyset$ . Hence by Lemma 10,  $\Gamma$  is the set of ramification points of  $g$ , each of which has multiplicity  $Q$ . In addition, we may assume  $g(\alpha) = \gamma = g(\beta)$ . Since  $g(\bar{X}^{-1}) = \overline{g(X)}^{-1}$ , we automatically have  $g(\bar{\alpha}^{-1}) = \bar{\gamma}^{-1} = g(\bar{\beta}^{-1})$ . Then both elements of  $\Lambda$  have  $g$ -ramification multiset  $[1, Q]$ . Now define  $\sigma(X) := -\frac{\bar{\beta}X-1}{X-\bar{\beta}}$  if  $\beta \in \mathbb{F}_{q^2} \setminus \mu_{q+1}$  and  $\sigma(X) := X$  if  $\beta = \infty$ . Similarly, define  $\tilde{\rho}(X) = -\frac{\bar{\gamma}X-1}{X-\bar{\gamma}}$  if  $\gamma \in \mathbb{F}_{q^2} \setminus \mu_{q+1}$  and  $\tilde{\rho}(X) = X$  if  $\gamma = \infty$ . In all these cases  $\sigma, \tilde{\rho}$  both permute  $\mu_{q+1}$ . In addition,  $\sigma(\beta) = \infty = \tilde{\rho}(\gamma)$  and  $\sigma(\bar{\beta}^{-1}) = 0 = \tilde{\rho}(\bar{\gamma}^{-1})$ . Combining these we find that the rational function  $h(X) := \tilde{\rho} \circ g \circ \sigma^{-1}(X) \in \mathbb{F}_{q^2}(X)$  has degree  $Q+1$ , maps  $\mu_{q+1}$  into  $\mu_{q+1}$ ,  $0$  and  $\infty$  are the branch points of  $h$ , as  $h$ -preimages of  $0$  and  $\infty$  of multiplicity  $Q$  respectively. Hence  $h(X) = X^Q h_1(X)$  for some degree-one  $h_1(X) \in \mathbb{F}_{q^2}(X)$  such that  $h_1(0), h_1(\infty) \notin \{0, \infty\}$ . Since both  $h(X)$  and  $X^Q$  map  $\mu_{q+1}$  to  $\mu_{q+1}$ , so is  $h_1(X)$ . Therefore  $h_1(X)$  permutes  $\mu_{q+1}$  and by Lemma 6 it must be of the form  $\frac{\bar{\varepsilon}_2 X + \bar{\varepsilon}_1}{\varepsilon_1 X + \varepsilon_2}$  for some  $\varepsilon_1, \varepsilon_2 \in \mathbb{F}_{q^2}^*$ , such that  $\varepsilon_1 \bar{\varepsilon}_1 \neq \varepsilon_2 \bar{\varepsilon}_2$ . This implies  $g(X) = \tilde{\rho}^{-1} \circ h \circ \sigma(X) = \rho^{-1} \circ \frac{X^Q(\bar{\varepsilon}X+1)}{X+\varepsilon} \circ \sigma(X)$ , where  $\rho(X) := \frac{\varepsilon_1}{\bar{\varepsilon}_1} \tilde{\rho}(X) \in \mathbb{F}_{q^2}(X)$  is of degree-one and permutes  $\mu_{q+1}$ , and  $\varepsilon = \frac{\varepsilon_2}{\varepsilon_1} \in \mathbb{F}_{q^2}^* \setminus \mu_{q+1}$ . This proves 4) of Lemma 13. Now the proof of Lemma 13 is complete.  $\square$

The proofs of Lemma 12 and 13 actually provided detailed conditions as to which family that  $g(X)$  belongs. We record the results here for future references.

**Proposition 14.** *Let  $\underline{c} \neq \underline{0}$ . Assume that  $g(X)$  is non-constant and  $A(X)$  has no roots in  $\mu_{q+1}$ . Then both  $U(X)$  and  $V(X)$  are nonzero.*

(i) *If  $U(X)/V(X) \in \mathbb{F}_{q^2}^*$  is constant, then*

- (1)  $\Gamma \subset \mu_{q+1} \iff g(X)$  belongs to Family 1) of Lemma 12;
- (2)  $\Gamma \cap \mu_{q+1} = \emptyset, C(X) = 1 \iff g(X)$  belongs to Family 2) of Lemma 12;
- (3)  $\Gamma \cap \mu_{q+1} = \emptyset, C(X) \neq 1 \iff g(X)$  belongs to Family 3) of Lemma 12;

(ii) *If  $U(X)/V(X)$  is non-constant, then*

- (1)  $\gcd(U(X), V(X)) \neq 1 \iff g(X)$  belongs to Family 1) of Lemma 13;
- (2)  $\gcd(U(X), V(X)) = 1, U(X)$  has a unique root in  $\mu_{q+1} \iff g(X)$  belongs to Family 2) of Lemma 13;
- (3)  $\gcd(U(X), V(X)) = 1, U(X)$  has two distinct roots in  $\mu_{q+1} \iff g(X)$  belongs to Family 3) of Lemma 13;
- (4)  $\gcd(U(X), V(X)) = 1, U(X)$  has no roots in  $\mu_{q+1} \iff g(X)$  belongs to Family 4) of Lemma 13.

## V. LINEAR EQUIVALENCE CLASSES OF $f(X)$

In this section we turn Lemmas 12 and 13 about the classification of  $g(X)$  into linear equivalence classes of  $f(X)$ .

**Lemma 15.** *We use notation from Section III. For  $\underline{c} \neq \underline{0}$ , suppose  $\deg g = Q + 1$ .*

- 1) *If  $g(X) = \rho^{-1} \circ \frac{A_{\underline{c}_1}(X)}{A_{\underline{c}_0}(X)} \circ \sigma$  for some degree-one  $\rho, \sigma \in \mathbb{F}_{q^2}(X)$  both of which map  $\mu_{q+1}$  to  $\mathbb{P}^1(\mathbb{F}_q)$  and some  $\underline{c}_0, \underline{c}_1 \in \mathbb{F}_q^4$ , then  $f(X)$  is linear equivalent to the  $(Q, Q)$ -biprojective function  $P : \mathbb{F}_q^2 \rightarrow \mathbb{F}_q^2$  defined by*

$$P(x, y) = (y^{Q+1}A_{\underline{c}_1}(x/y), y^{Q+1}A_{\underline{c}_0}(x/y)).$$

- 2) *If  $g = \rho^{-1} \circ g_{\underline{c}_0}(X) \circ \sigma$  for some degree-one  $\rho, \sigma \in \mathbb{F}_{q^2}(X)$  both of which permute  $\mu_{q+1}$  and some  $\underline{c}_0 \in \mathbb{F}_{q^2}^4$ , then  $f(X)$  is linear equivalent to  $f_{\underline{c}_0}(X)$ .*

*Proof.* 1). Since  $\rho, \sigma$  map  $\mu_{q+1}$  to  $\mathbb{P}^1(\mathbb{F}_q)$ , there exist  $\alpha, \beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$  and  $\gamma, \delta \in \mu_{q+1}$  such that

$$\sigma(X) = \frac{\alpha X + \gamma \bar{\alpha}}{X + \gamma}$$

and

$$\rho(X) = \frac{\beta X + \delta \bar{\beta}}{X + \delta}.$$

Clearly

$$\rho^{-1}(X) = -\frac{\delta(X - \bar{\beta})}{X - \beta}.$$

We may expand the expression  $g(X) = \rho^{-1} \circ \frac{A_{\underline{e}_1}(X)}{A_{\underline{e}_0}(X)} \circ \sigma$  and obtain

$$\begin{aligned} g(X) &= -\frac{\delta(X - \bar{\beta})}{X - \beta} \circ \frac{A_{\underline{e}_1}(X)}{A_{\underline{e}_0}(X)} \circ \frac{\alpha X + \gamma \bar{\alpha}}{X + \gamma} \\ &= -\frac{\delta \left[ A_{\underline{e}_1} \left( \frac{\alpha X + \gamma \bar{\alpha}}{X + \gamma} \right) - \bar{\beta} A_{\underline{e}_0} \left( \frac{\alpha X + \gamma \bar{\alpha}}{X + \gamma} \right) \right]}{A_{\underline{e}_1} \left( \frac{\alpha X + \gamma \bar{\alpha}}{X + \gamma} \right) - \beta A_{\underline{e}_0} \left( \frac{\alpha X + \gamma \bar{\alpha}}{X + \gamma} \right)}. \end{aligned}$$

Multiplying  $(X + \gamma)^{Q+1}$  on both the numerator and denominator of the right side, we obtain

$$g(X) = -\frac{\delta \gamma^{Q+1} X^{Q+1} D^{(q)}(1/X)}{D(X)}, \quad (14)$$

where

$$D(X) := (X + \gamma)^{Q+1} \left[ A_{\underline{e}_1} \left( \frac{\alpha X + \gamma \bar{\alpha}}{X + \gamma} \right) - \beta A_{\underline{e}_0} \left( \frac{\alpha X + \gamma \bar{\alpha}}{X + \gamma} \right) \right].$$

Since  $A_{\underline{e}_1}(X), A_{\underline{e}_0}(X) \in \mathbb{F}_q[X]$ , we have  $D(X) \in \mathbb{F}_{q^2}[X]$ .

Comparing (14) with the expression  $g(X) = \frac{B(X)}{A(X)}$  and using the condition  $\deg g = Q + 1$ , we shall have

$$\begin{aligned} \max \{ \deg B, \deg A \} &= \max \{ \deg X^{Q+1} D^{(q)}(1/X), \deg D \} = Q + 1, \\ \gcd(B(X), A(X)) &= \gcd(X^{Q+1} D^{(q)}(1/X), D(X)) = 1. \end{aligned}$$

This implies that

$$A(X) = \lambda D(X),$$

for some  $\lambda \in \mathbb{F}_{q^2}^*$ . Now using

$$f(X) = X^{Q+1} A(X^{q-1}) = X^{Q+1} A(\bar{X}/X),$$

we obtain

$$f(X) = \lambda (\bar{X} + \gamma X)^{Q+1} \left[ A_{\underline{e}_1} \left( \frac{\alpha \bar{X} + \gamma \bar{\alpha} X}{\bar{X} + \gamma X} \right) - \beta A_{\underline{e}_0} \left( \frac{\alpha \bar{X} + \gamma \bar{\alpha} X}{\bar{X} + \gamma X} \right) \right].$$

The above expression of  $f(X)$  can be further simplified. Writing  $\gamma = \bar{\varepsilon}/\varepsilon$  for some  $\varepsilon \in \mathbb{F}_{q^2}^*$ , and letting

$$\begin{cases} x &= \varepsilon \alpha \bar{X} + \bar{\varepsilon} \bar{\alpha} X, \\ y &= \varepsilon \bar{X} + \bar{\varepsilon} X, \end{cases} \quad (15)$$

clearly  $x, y \in \mathbb{F}_q$  for any  $X \in \mathbb{F}_{q^2}$ , we can write  $f(X)$  as

$$f(X) = \frac{\lambda}{\varepsilon^{Q+1}} y^{Q+1} \left[ A_{\varepsilon_1} \left( \frac{x}{y} \right) - \beta A_{\varepsilon_0} \left( \frac{x}{y} \right) \right] = L_1 \circ P \circ L_2(X),$$

where

$$L_1(x, y) = \frac{\lambda}{\varepsilon^{Q+1}} (x - \beta y) : \mathbb{F}_q^2 \rightarrow \mathbb{F}_{q^2}$$

and

$$L_2(X) = (x, y) = (\varepsilon \alpha \bar{X} + \bar{\varepsilon} \bar{\alpha} X, \varepsilon \bar{X} + \bar{\varepsilon} X) : \mathbb{F}_{q^2} \rightarrow \mathbb{F}_q^2.$$

Clearly  $L_1$  and  $L_2$  are linear functions. They are also permutation:  $L_1$  is bijective since  $\lambda \varepsilon \neq 0$  and  $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ ;  $L_2$  is bijective since

$$\det \begin{bmatrix} \varepsilon \alpha & \bar{\varepsilon} \bar{\alpha} \\ \varepsilon & \bar{\varepsilon} \end{bmatrix} = \varepsilon \bar{\varepsilon} (\alpha - \bar{\alpha}) \neq 0.$$

Therefore  $f$  is linear equivalent to  $P$  over  $\mathbb{F}_{q^2}$ .

2). Since  $\rho, \sigma$  permute  $\mu_{q+1}$ , there exist  $\alpha_i, \beta_i \in \mathbb{F}_{q^2}$  for  $i = 1, 2$  such that  $\alpha_1 \bar{\alpha}_1 \neq \alpha_2 \bar{\alpha}_2, \beta_1 \bar{\beta}_1 \neq \beta_2 \bar{\beta}_2$ ,

$$\sigma(X) = \frac{\bar{\alpha}_2 X + \bar{\alpha}_1}{\alpha_1 X + \alpha_2}, \quad \rho(X) = \frac{\bar{\beta}_2 X + \bar{\beta}_1}{\beta_1 X + \beta_2}.$$

As  $g_{\varepsilon_0}(X) = \frac{B_{\varepsilon_0}(X)}{A_{\varepsilon_0}(X)}$  and  $g(X) = \rho^{-1} \circ g_{\varepsilon_0}(X) \circ \sigma$ , we have

$$\begin{aligned} g(X) &= -\frac{\beta_2 X - \bar{\beta}_1}{\beta_1 X - \bar{\beta}_2} \circ \frac{B_{\varepsilon_0}(X)}{A_{\varepsilon_0}(X)} \circ \frac{\bar{\alpha}_2 X + \bar{\alpha}_1}{\alpha_1 X + \alpha_2} \\ &= -\frac{\beta_2 B_{\varepsilon_0} \left( \frac{\bar{\alpha}_2 X + \bar{\alpha}_1}{\alpha_1 X + \alpha_2} \right) - \bar{\beta}_1 A_{\varepsilon_0} \left( \frac{\bar{\alpha}_2 X + \bar{\alpha}_1}{\alpha_1 X + \alpha_2} \right)}{\beta_1 B_{\varepsilon_0} \left( \frac{\bar{\alpha}_2 X + \bar{\alpha}_1}{\alpha_1 X + \alpha_2} \right) - \bar{\beta}_2 A_{\varepsilon_0} \left( \frac{\bar{\alpha}_2 X + \bar{\alpha}_1}{\alpha_1 X + \alpha_2} \right)}. \end{aligned}$$

Similarly we can obtain

$$g(X) = \frac{X^{Q+1} D^{(g)}(1/X)}{D(X)},$$

where

$$D(X) := (\alpha_1 X + \alpha_2)^{Q+1} \left[ \beta_1 B_{\varepsilon_0} \left( \frac{\bar{\alpha}_2 X + \bar{\alpha}_1}{\alpha_1 X + \alpha_2} \right) - \bar{\beta}_2 A_{\varepsilon_0} \left( \frac{\bar{\alpha}_2 X + \bar{\alpha}_1}{\alpha_1 X + \alpha_2} \right) \right] \in \mathbb{F}_{q^2}[X].$$

Also using similar argument as in 1), and noting that  $\deg g = Q + 1$ , we have  $A(X) = \gamma D(X)$  for some

$\gamma \in \mathbb{F}_q^*$ . This further implies that

$$\begin{aligned} f(X) &= \gamma(\alpha_1 \bar{X} + \alpha_2 X)^{Q+1} \left[ \beta_1 B_{\underline{c}_0} \left( \frac{\bar{\alpha}_2 \bar{X} + \bar{\alpha}_1 X}{\alpha_1 \bar{X} + \alpha_2 X} \right) - \bar{\beta}_2 A_{\underline{c}_0} \left( \frac{\bar{\alpha}_2 \bar{X} + \bar{\alpha}_1 X}{\alpha_1 \bar{X} + \alpha_2 X} \right) \right] \\ &= L_1 \circ f_{\underline{c}_0}(X) \circ L_2, \end{aligned}$$

where  $L_1, L_2$  are given by

$$L_1(X) = \gamma(\beta_1 \bar{X} - \bar{\beta}_2 X), \quad L_2(X) = \alpha_1 \bar{X} + \alpha_2 X.$$

The maps  $L_1, L_2 : \mathbb{F}_{q^2} \rightarrow \mathbb{F}_{q^2}$  are linear permutations because  $\alpha_1 \bar{\alpha}_1 \neq \alpha_2 \bar{\alpha}_2$  and

$$(\gamma \beta_1)(\overline{\gamma \beta_1}) = \gamma^2 \beta_1 \bar{\beta}_1 \neq \gamma^2 \beta_2 \bar{\beta}_2 = (-\gamma \bar{\beta}_2)(-\overline{\gamma \bar{\beta}_2}).$$

Hence  $f(X)$  is linear equivalent to  $f_{\underline{c}_0}(X)$  over  $\mathbb{F}_{q^2}$ . This completes the proof of Lemma 15.  $\square$

Assuming that  $g(X)$  is non-constant and  $A(X)$  has no roots in  $\mu_{q+1}$ , we can list and prove all the possible linear equivalence classes of  $f(X)$  as follows.

**Theorem 16.** *If  $g(X)$  is non-constant and  $A(X)$  has no roots in  $\mu_{q+1}$ , then  $f(X)$  is linear equivalent to one of the following functions:*

- 1)  $P_0(x, y) = (x^{Q+1}, y^{Q+1}) : \mathbb{F}_q^2 \rightarrow \mathbb{F}_q^2$ ;
- 2)  $f_0(X) = X^{Q+1}$ ;
- 3)  $f_1(X) = X^{Q+q}$ ;
- 4)  $P_1(x, y) = (x^{Q+1}, xy^Q + y^{Q+1}) : \mathbb{F}_q^2 \rightarrow \mathbb{F}_q^2$ ;
- 5)  $P_2(x, y) = (x^Q y, x^{Q+1} + \varepsilon y^{Q+1}) : \mathbb{F}_q^2 \rightarrow \mathbb{F}_q^2$  for some  $\varepsilon \in \mathbb{F}_q^*$ ;
- 6)  $P_3(x, y) = (x^{Q+1} - x^Q y, xy^Q + \varepsilon y^{Q+1}) : \mathbb{F}_q^2 \rightarrow \mathbb{F}_q^2$  for some  $\varepsilon \in \mathbb{F}_q^* \setminus \{-1\}$ ;
- 7)  $f_2(X) = X^{Q+q} + \varepsilon X^{Q+1}$  for some  $\varepsilon \in \mathbb{F}_{q^2}^* \setminus \mu_{q+1}$ .

*Proof.* By 3) of Lemma 11, we know that  $g(X)$  must be in one of the families in Lemmas 12 or 13.

We first look at cases when  $g(X)$  is in Family 1) of Lemma 12 or Families 1) to 3) of Lemma 13. In all these four families  $\deg g = Q + 1$  and  $g(X)$  is of the form  $\rho^{-1} \circ \frac{A_{\underline{c}_1}(X)}{A_{\underline{c}_0}(X)} \circ \sigma$  for some  $\underline{c}_0, \underline{c}_1 \in \mathbb{F}_q^4$  and degree-one  $\rho, \sigma \in \mathbb{F}_{q^2}(X)$  both of which map  $\mu_{q+1}$  to  $\mathbb{P}^1(\mathbb{F}_q)$ . Hence 1) of Lemma 15 applies, and  $f(X)$  is linearly equivalent to functions listed in 1), 4), 5) and 6) of Theorem 16 respectively.

Now consider the case when  $g(X)$  is in Family 2) of Lemma 12 or Family 4) of Lemma 13. In both

families  $\deg g = Q + 1$  and  $g(X)$  is of the form  $\rho^{-1} \circ g_{\underline{c}_0}(X) \circ \sigma$  for some degree-one  $\rho, \sigma \in \mathbb{F}_{q^2}(X)$  both of which permute  $\mu_{q+1}$ , and  $\underline{c}_0 = (0, 0, 0, 1)$  and  $(0, 0, 1, \varepsilon)$  respectively. Hence 2) of Lemma 15 applies, and  $f(X)$  is linearly equivalent to functions listed in 2) and 7) of Theorem 16 respectively.

It remains to investigate the case when  $g(X)$  is in Family 3) of Lemma 12. Here  $\deg g = Q - 1$ , so we cannot apply Lemma 15 directly. Instead, we can find the linear equivalence of  $f(X)$  directly, as in the proofs of Lemma 15. Writing  $\sigma, \rho$  explicitly as

$$\sigma(X) = \frac{\bar{\alpha}_2 X + \bar{\alpha}_1}{\alpha_1 X + \alpha_2}, \quad \rho(X) = \frac{\bar{\beta}_2 X + \bar{\beta}_1}{\beta_1 X + \beta_2},$$

where  $\alpha_i, \beta_i \in \mathbb{F}_{q^2}$  for  $i = 1, 2$  such that  $\alpha_1 \bar{\alpha}_1 \neq \alpha_2 \bar{\alpha}_2, \beta_1 \bar{\beta}_1 \neq \beta_2 \bar{\beta}_2$ , we have

$$\begin{aligned} g(X) &= \rho^{-1} \circ X^{Q-1} \circ \sigma = -\frac{\beta_2 X - \bar{\beta}_1}{\beta_1 X - \bar{\beta}_2} \circ X^{Q-1} \circ \frac{\bar{\alpha}_2 X + \bar{\alpha}_1}{\alpha_1 X + \alpha_2} \\ &= -\frac{\beta_2(\bar{\alpha}_2 X + \bar{\alpha}_1)^{Q-1} - \bar{\beta}_1(\alpha_1 X + \alpha_2)^{Q-1}}{\beta_1(\bar{\alpha}_2 X + \bar{\alpha}_1)^{Q-1} - \bar{\beta}_2(\alpha_1 X + \alpha_2)^{Q-1}}. \end{aligned}$$

This can be further written as

$$g(X) = \frac{X^{Q+1} D^{(q)}(1/X)}{D(X)}, \tag{16}$$

where

$$D(X) := (\alpha_1 X + \alpha_2)(\bar{\alpha}_2 X + \bar{\alpha}_1) [\beta_1(\bar{\alpha}_2 X + \bar{\alpha}_1)^{Q-1} - \bar{\beta}_2(\alpha_1 X + \alpha_2)^{Q-1}].$$

Again by using  $g(X) = \frac{B(X)}{A(X)}$  and  $\deg g = Q - 1$ , we conclude that  $A(X) = \gamma D(X)$  for some  $\gamma \in \mathbb{F}_q^*$ .

Now from  $f(X) = X^{Q+1} A(\bar{X}/X)$ , we have

$$\begin{aligned} f(X) &= \gamma(\alpha_1 \bar{X} + \alpha_2 X)(\bar{\alpha}_2 \bar{X} + \bar{\alpha}_1 X) [\beta_1(\bar{\alpha}_2 \bar{X} + \bar{\alpha}_1 X)^{Q-1} - \bar{\beta}_2(\alpha_1 \bar{X} + \alpha_2 X)^{Q-1}] \\ &= \gamma[\beta_1(\alpha_1 \bar{X} + \alpha_2 X)(\bar{\alpha}_2 \bar{X} + \bar{\alpha}_1 X)^Q - \bar{\beta}_2(\alpha_1 \bar{X} + \alpha_2 X)^Q(\bar{\alpha}_2 \bar{X} + \bar{\alpha}_1 X)] \\ &= L_1 \circ X^Q \bar{X} \circ L_2(X), \end{aligned}$$

where

$$L_1(X) = \gamma(\beta_1 \bar{X} - \bar{\beta}_2 X)$$

and

$$L_2(X) = \alpha_1 \bar{X} + \alpha_2 X.$$

Since  $\alpha_1\bar{\alpha}_1 \neq \alpha_2\bar{\alpha}_2$  and

$$(\gamma\beta_1)(\overline{\gamma\beta_1}) = \gamma^2\beta_1\bar{\beta}_1 \neq \gamma^2\beta_2\bar{\beta}_2 = (-\gamma\bar{\beta}_2)(\overline{-\gamma\bar{\beta}_2}),$$

the maps  $L_1, L_2 : \mathbb{F}_{q^2} \rightarrow \mathbb{F}_{q^2}$  are linear permutations, and hence  $f(X)$  is linear equivalent to  $X^Q\bar{X}$ , that is, the function in 3) of Theorem 16. Now the proof of Theorem 16 is complete. □

We remark here that all results in this section work for  $p = 2$  as well. Moreover, this classification also provides an alternative proof to the main result in [20] that all permutation quadrinomials  $f_{\underline{c}}(X)$  given in the form of (2) are linear equivalent to Gold or “doubly-Gold” functions.

## VI. PROOFS OF THEOREMS 1–3

We are now in a position to prove Theorems 1–3. Let us first define two-to-one functions.

**Definition 4.** *Given finite sets  $R$  and  $S$ , a map  $F : R \rightarrow S$  is said to be **two-to-one** (or 2-to-1 for short) if one of the following holds:*

- 1) *if  $\#R$  is even, then for any  $s \in S$ ,  $\#F^{-1}(s) \in \{0, 2\}$ ;*
- 2) *if  $\#R$  is odd, then there is a unique  $s_0 \in S$  such that  $\#F^{-1}(s_0) = 1$ , and for any  $s \in S \setminus \{s_0\}$ ,  $\#F^{-1}(s) \in \{0, 2\}$ .*

The following result was known.

**Theorem 17.** [12, Theorem 1.1] *Let  $\mathbb{F}_q$  be a finite field of odd order  $q$  and  $f(x)$  be a DO polynomial over  $\mathbb{F}_q$ . The following statements are equivalent:*

- (i)  *$f(x)$  is planar;*
- (ii)  *$f(x)$  is a two-to-one map,  $f(0) = 0$  and  $f(x) \neq 0$  for any  $x \in \mathbb{F}_q^*$ .*

Note that the quadrinomial  $f_{\underline{c}}(X)$  is a DO polynomial. To make sure that Theorem 17 applies, we need to show that if  $f$  is 2-to-1, then 0 is the only  $f$ -preimage of 0 in  $\mathbb{F}_{q^2}$ . This is a partial consequence of the following lemma.

**Lemma 18.** *Let  $p$  be odd and  $\underline{c} \neq \underline{0}$ . If  $f(X)$  is 2-to-1 over  $\mathbb{F}_{q^2}$ , then  $g(X)$  is non-constant and  $A(X)$  has no roots in  $\mu_{q+1}$ .*

*Proof.* Obviously  $f(0) = 0$ . Now suppose  $A(\alpha) = 0$  for some  $\alpha \in \mu_{q+1}$ . Then for any  $x \in \mathbb{F}_{q^2}^*$  such that  $x^{q-1} = \alpha$ , the number of such  $x$  is exactly  $q - 1$ , we have

$$f(x) = x^{Q+1}A(x^{q-1}) = x^{Q+1}A(\alpha) = 0,$$

so  $\#f^{-1}(0) \geq (q - 1) + 1 = q \geq 3$ , so  $f$  can not be 2-to-1 over  $\mathbb{F}_{q^2}$ .

Next suppose  $g(X) = \frac{B(X)}{A(X)} = \lambda$  is a constant  $\lambda \in \mathbb{F}_{q^2}^*$ . For any fixed  $\alpha \in \mu_{q+1}$  and any  $x \in \mathbb{F}_{q^2}^*$  such that  $x^{q-1} = \alpha$ , we have

$$f(x)^{q-1} = x^{(q-1)(Q+1)}A(x^{q-1})^{q-1} = \alpha^{Q+1}A(\alpha)^{q-1}.$$

Noting that since  $\alpha \in \mu_{q+1}$ , the right hand side can be written as

$$\alpha^{Q+1}A(\alpha)^{q-1} = \alpha^{Q+1} \frac{A(\alpha)^q}{A(\alpha)} = \frac{B(\alpha)}{A(\alpha)} = \lambda,$$

that is (since  $\alpha \in \mu_{q+1}$  is arbitrary),

$$f(x)^{q-1} = \lambda, \quad \forall x \in \mathbb{F}_{q^2}^*.$$

Noting that  $f(x)$  takes at most  $q - 1$  distinct values and  $x$  varies in the set  $\mathbb{F}_{q^2}^*$  which has cardinality  $q^2 - 1$ , there is one value  $y \in \mathbb{F}_{q^2}^*$  with  $y^{q-1} = \lambda$  such that  $\#f^{-1}(y) \geq \frac{q^2-1}{q-1} = q + 1 \geq 4$ , so  $f$  is not 2-to-1 over  $\mathbb{F}_{q^2}^*$ .  $\square$

Now we can give a proof of Theorems 1 and 2. For simplicity, we prove them together here.

#### A. Proof of Theorems 1 and 2

For  $\underline{c} \neq \underline{0}$ , if  $f(X)$  is planar, Lemma 18 ensures that  $g(X)$  is nonconstant and  $A(X)$  has no roots in  $\mu_{q+1}$ , then by Theorem 16, we know that  $f(X)$  must be in one of the linear equivalence classes 1)–7). Note that 2-to-1 and planar properties are preserved under linear equivalence. Therefore it suffices to check the functions listed in Theorem 16 to see whether or not they are planar (the number labels correspond to the family numbers in Theorem 16).

**Case 1.**  $P_0(x, y)$ : since  $Q + 1$  is even, it is easy to see that  $P_0(\pm 1, \pm 1) = (1, 1)$ , that is,  $\#P_0^{-1}((1, 1)) \geq 4$ , so  $P_0$  can never be 2-to-1.

**Case 2.**  $f_0(X) = X^{Q+1}$ :  $f_0$  is 2-to-1 on  $\mathbb{F}_{q^2}$  if and only if  $\gcd(Q + 1, q^2 - 1) = 2$ , which holds if and only if  $\frac{\ell}{\gcd(k, \ell)}$  is even, since  $q = p^k$ ,  $Q = p^\ell$  and  $p$  is odd.

**Case 3).**  $f_1(X) = X^{Q+q}$ :  $f_1$  is 2-to-1 one  $\mathbb{F}_{q^2}$  if and only if  $\gcd(Q+q, q^2-1) = 2$ . It is easy to check that this is equivalent to  $\frac{k\ell}{\gcd(k,\ell)^2}$  is odd.

**Case 4).**  $P_1(x, y)$ : since  $Q+1$  is even, 1 and  $-1$  are two distinct solutions of  $x^{Q+1} = 1$  in  $\mathbb{F}_q^*$ . At the same time,  $xy^Q + y^{Q+1} = 0$  has two solutions  $y = 0, -x$  for each fixed nonzero  $x$ . Hence all the four points  $(1, 0), (-1, 0), (1, -1)$  and  $(-1, 1)$  are  $P_1$ -preimages of  $(1, 0)$  in  $\mathbb{F}_q^2$ . Therefore  $P_1$  cannot be 2-to-1.

**Case 5).**  $P_2(x, y)$ : suppose  $P_2(x, y)$  is 2-to-1 on  $\mathbb{F}_q^2$ . Since  $x^{Q+1} = 1$  has  $d = \gcd(Q+1, q-1) \geq 2$  solutions  $x \in \mathbb{F}_q^*$ , say  $x_1, \dots, x_d$ , and obviously  $P_2(x_i, 0) = (0, 1)$  for any  $i$ , so  $d = 2$ , that is,  $\frac{k}{\gcd(k,\ell)}$  is odd. Moreover, if  $\varepsilon \in \mathbb{F}_q^*$  is a square, then the equation  $\varepsilon y^{Q+1} = 1$  has two solutions  $y_1, y_2 \in \mathbb{F}_q^*$ , and we have  $P_2(\pm 1, 0) = P_2(0, y_1) = P_2(0, y_2) = (0, 1)$ , so  $P_2(x, y)$  cannot be 2-to-1 on  $\mathbb{F}_q^2$ . So if  $P_2(x, y)$  is 2-to-1 on  $\mathbb{F}_q^2$  then  $\frac{k}{\gcd(k,\ell)}$  is odd and  $\varepsilon \in \mathbb{F}_q^*$  is a non-square.

From now on we assume  $\frac{k}{\gcd(k,\ell)}$  is odd and  $\varepsilon \in \mathbb{F}_q^*$  is a non-square. Then  $\gcd(Q+1, q-1) = 2$ . It is easy to see that  $\sharp P_2^{-1}((0, b)) = 2$  for any  $b \in \mathbb{F}_q^*$ . Next, for any  $\alpha \in \mathbb{F}_q^*$  and  $\beta \in \mathbb{F}_q$ , we consider  $(x, y) \in \mathbb{F}_q^2$  such that

$$x^Q y = \alpha, \quad x^{Q+1} + \varepsilon y^{Q+1} = \beta. \quad (17)$$

Since  $\alpha \neq 0$ , we have  $x, y \neq 0$ , and the above equations are equivalent to  $y = \alpha x^{-Q}$  and

$$\varepsilon \alpha^{Q+1} (x^{-Q-1})^{Q+1} - \beta x^{-Q-1} + 1 = 0. \quad (18)$$

So the number of solutions  $(x, y) \in \mathbb{F}_q^2$  to Equations (17) is the same as the number of solutions  $x \in \mathbb{F}_q$  to Equation (18). We claim that this number is always 0 or 2 for any  $\alpha \in \mathbb{F}_q^*$  and any  $\beta \in \mathbb{F}_q$ , so that  $P_2(x, y)$  is 2-to-1 on  $\mathbb{F}_q^2$ .

First consider the case  $\beta = 0$ : If  $q \equiv 1 \pmod{4}$ , then  $-\varepsilon \in \mathbb{F}_q^*$  is a non-square, so Equation (18) is not solvable for  $x \in \mathbb{F}_q$ ; if  $q \equiv 3 \pmod{4}$ , then  $-\varepsilon \in \mathbb{F}_q^*$  is a square, Equation (18) is solvable, and the number of roots  $x \in \mathbb{F}_q$  is  $\gcd((Q+1)^2, q-1) = 2$ . So the claim is prove in this case.

Next consider the case  $\beta \neq 0$ : Let  $z = x^{-Q-1}$ , then we have

$$\varepsilon \alpha^{Q+1} z^{Q+1} - \beta z + 1 = 0. \quad (19)$$

Using the substitution  $z = -[\beta(\varepsilon\alpha^{Q+1})^{-1}]^{1/Q}z_1$ , we obtain

$$z_1^{Q+1} + z_1 + [\varepsilon(\alpha/\beta)^{Q+1}]^{1/Q} = 0. \quad (20)$$

Note that  $a := [\varepsilon(\alpha/\beta)^{Q+1}]^{1/Q}$  is a non-square in  $\mathbb{F}_q^*$ . By [22, Theorems 8–9 and Lemma 5], (20) has at most 2 solutions for  $z_1$  in  $\mathbb{F}_q^*$ , and if (20) does have solutions in  $\mathbb{F}_q^*$ , then they are precisely the roots, say  $x_1, x_2$  of the quadratic polynomial  $H(x) = F(a)x^2 + G(a)x + aF(a)^Q$ , where  $F, G$  are specified polynomials with coefficients in  $\mathbb{F}_q$  such that  $F(a) \neq 0$ . Note that  $x_1 \cdot x_2 = aF(a)^{Q-1}$ , which is a non-square in  $\mathbb{F}_q^*$ . Hence either  $x_1, x_2 \notin \mathbb{F}_q^*$ , i.e.,  $H(x)$  has no roots in  $\mathbb{F}_q^*$ , which implies that (20) and hence (18) has no roots in  $\mathbb{F}_q^*$ , or one of the roots of  $H(x)$  is a square in  $\mathbb{F}_q^*$  and the other is a non-square in  $\mathbb{F}_q^*$ . Say  $x_1$  is a square and  $x_2$  is a non-square in  $\mathbb{F}_q^*$ . For these  $x_1, x_2$ , the total number of solutions of  $x \in \mathbb{F}_q$  such that  $x^{-Q-1} = -[\beta(\varepsilon\alpha^{Q+1})^{-1}]^{1/Q}x_1$  or  $-[\beta(\varepsilon\alpha^{Q+1})^{-1}]^{1/Q}x_2$  is still 2. So in this case Equation (18) still has either 0 or 2 solutions in  $\mathbb{F}_q$ . Now the claim is proved, so  $P_2(x, y)$  is 2-to-1.

**Case 6).**  $P_3(x, y)$ : First, noting that for any  $x, y \in \mathbb{F}_q^*$ ,

$$P_3 : (x, 0) \mapsto (x^{Q+1}, 0), \quad (0, y) \mapsto (0, \varepsilon y^{Q+1}), \quad (y, y) \mapsto (0, (1 + \varepsilon)y^{Q+1}),$$

by using similar argument for  $P_2(x, y)$ , we see that if  $P_3(x, y)$  is 2-to-1 on  $\mathbb{F}_q^2$ , then  $\frac{k}{\gcd(k, \ell)}$  is odd and  $\varepsilon^{-1}(1 + \varepsilon) = 1 + \varepsilon^{-1} \in \mathbb{F}_q^*$  is a non-square.

From now on we assume  $1 + \varepsilon^{-1}$  is a non-square in  $\mathbb{F}_q^*$  and  $\frac{k}{\gcd(k, \ell)}$  is odd. Under this general condition we are unable to conclude anything. So we assume that  $k \mid \ell$ . Then  $x^Q = x$  for any  $x \in \mathbb{F}_q$ . We claim that in this case  $P_3(x, y) = (x^2 - xy, xy + \varepsilon y^2)$  is 2-to-1 on  $\mathbb{F}_q^2$ , that is, the number of  $(x, y) \in \mathbb{F}_q^2$  such that

$$x^2 - xy = \alpha, \quad xy + \varepsilon y^2 = \beta \quad (21)$$

is either 0 or 2 for any  $(\alpha, \beta) \in \mathbb{F}_q^2 \setminus \{(0, 0)\}$ . The proof is as follows.

Consider  $(\alpha, \beta) \in \mathbb{F}_q^2$  with  $\alpha \neq 0$ . Then  $x(x - y) = \alpha$  implies  $x \neq 0$ , and  $y = x - \alpha x^{-1}$ . Hence  $y(x + \varepsilon y) = \beta$  becomes  $(x - \alpha x^{-1})[(1 + \varepsilon)x - \alpha \varepsilon x^{-1}] = \beta$ , or equivalently,

$$(1 + \varepsilon)x^4 - (\alpha + 2\alpha\varepsilon + \beta)x^2 + \alpha^2\varepsilon = 0. \quad (22)$$

Let  $z = x^2$ , then we have

$$(1 + \varepsilon)z^2 - (\alpha + 2\alpha\varepsilon + \beta)z + \alpha^2\varepsilon = 0. \quad (23)$$

The product of the two roots of (23) is  $\frac{\alpha^2\varepsilon}{1+\varepsilon} = \alpha^2(1 + \varepsilon^{-1})^{-1}$  is a non-square in  $\mathbb{F}_q^*$ . Hence at most one of them makes the equation  $x^2 = z$  solvable in  $\mathbb{F}_q$  for  $x$  (and if so then there are 2 solutions), which in turn gives 2 solutions to the equation (22). Each such solution gives one corresponding value of  $y$ . Hence  $(\alpha, \beta)$  has 0 or 2  $P_3$ -preimages in  $\mathbb{F}_q^2$  for each choice of  $\alpha \in \mathbb{F}_q^*$  and  $\beta \in \mathbb{F}_q$ . If  $\alpha = 0$  but  $\beta \neq 0$ , the result is obvious. Combining all possible cases, we see that  $P_3$  is 2-to-1 if and only if  $1 + \varepsilon^{-1}$  is a non-square in  $\mathbb{F}_q^*$ .

**Case 7).** For  $f_2(X) = X^{Q+q} + \varepsilon X^{Q+1}$  for some  $\varepsilon \in \mathbb{F}_{q^2}^* \setminus \mu_{q+1}$ : Under the genral condition we are not able to conclude anything except that  $\gcd(Q + 1, q - 1) = 2$ , that is,  $\frac{k}{\gcd(k, \ell)}$  is odd.

Let us assume that  $k \mid \ell$ . We consider first that  $\frac{\ell}{k}$  is even. Then for any  $x \in \mathbb{F}_{q^2}$ , we have  $f_2(x) = x\bar{x} + \varepsilon x^2$ . We will use this expression to find conditions on  $\varepsilon \in \mathbb{F}_{q^2}^* \setminus \mu_{q+1}$  such that  $f_2$  is planar on  $\mathbb{F}_{q^2}$ .

$f_2$  is planar if and only if for any  $a \in \mathbb{F}_{q^2}^*$  and any  $b \in \mathbb{F}_{q^2}$ , the equation  $f(x + a) - f(x) = b$  always has a unique root  $x \in \mathbb{F}_{q^2}$ . Replacing  $x$  by  $ax$ , and dividing  $a^Q\bar{a}$  on both sides, we obtain for any  $a \in \mathbb{F}_{q^2}^*$  and any  $b \in \mathbb{F}_{q^2}$ , the equation

$$x + \bar{x} + \frac{2\varepsilon a}{a}x = \frac{b}{a^Q\bar{a}} - 1 - \frac{\varepsilon a}{a} \quad (24)$$

always have a unique solution  $x \in \mathbb{F}_{q^2}$ . The left hand side of (24) is linear in  $x$ , so this is equivalent to the statement that for any  $a \in \mathbb{F}_{q^2}^*$ ,  $x = 0$  is the only solution of the equation

$$x + \bar{x} + \frac{2\varepsilon a}{a}x = 0 \quad (25)$$

in  $\mathbb{F}_{q^2}$ , so, for any  $a \in \mathbb{F}_{q^2}^*$  and any  $x \in \mathbb{F}_{q^2}^*$ , we have  $x + \bar{x} + \frac{2\varepsilon a}{a}x \neq 0$ , that is,

$$2\varepsilon \frac{a}{a} \neq \frac{-x - \bar{x}}{x} = -1 - \frac{\bar{x}}{x}.$$

As  $x$  runs over  $\mathbb{F}_{q^2}^*$ ,  $z := \frac{\bar{x}}{x}$  runs over  $\mu_{q+1}$ . Since  $a \in \mathbb{F}_{q^2}^*$  is also arbitrary here, we need to have

$$2\varepsilon\bar{2\varepsilon} = 4\varepsilon\bar{\varepsilon} \neq (1 + z)(1 + \bar{z}) = (1 + z)(1 + z^{-1}), \quad \forall z \in \mu_{q+1},$$

or equivalently, the equation

$$4\varepsilon\bar{\varepsilon} = (1 + z)(1 + z^{-1})$$

has no roots in  $\mu_{q+1}$ . This is equivalent to that

$$z^2 + (2 - 4\varepsilon\bar{\varepsilon})z + 1 = 0 \quad (26)$$

has no roots in  $\mu_{q+1}$ . By Lemma 5, this is equivalent to that

$$\Delta = (2 - 4\varepsilon\bar{\varepsilon})^2 - 4 = (4\varepsilon\bar{\varepsilon})^2 (1 - (\varepsilon\bar{\varepsilon})^{-1})$$

is a square in  $\mathbb{F}_q^*$ , that is,  $1 - (\varepsilon\bar{\varepsilon})^{-1} \in \mathbb{F}_q^*$  is a square. This proves the case  $\frac{\ell}{k}$  is even.

If  $\frac{\ell}{k}$  is odd, noting that in this case  $f_2(x) = \bar{x}^2 + \varepsilon x\bar{x}$  for any  $x \in \mathbb{F}_{q^2}$  and  $\bar{x}^2 + \varepsilon x\bar{x} = \varepsilon(\overline{x\bar{x} + \bar{\varepsilon}^{-1}x^2})$ , by using the result for  $\frac{\ell}{k}$  being even, we conclude that in this case  $f_2$  is planar if and only if  $1 - \varepsilon\bar{\varepsilon} \in \mathbb{F}_q^*$  is a square. This proves the case  $\frac{\ell}{k}$  is odd. Now we have proved Theorems 1 and 2.  $\square$

### B. Proof of Theorem 3

Now we assume  $k \mid \ell$ . This implies that  $Q = p^\ell = q^{\ell/k}$ . Then  $X^Q$  induces the same function on  $\mathbb{F}_{q^2}$  as  $\bar{X}$  or  $X$  according to whether  $\frac{\ell}{k}$  is odd or even. Therefore  $f_{\underline{c}}(X)$  induces the same function on  $\mathbb{F}_{q^2}$  as

$$F_{\underline{c}}(X) := \begin{cases} c_2\bar{X}^2 + (c_0 + c_3)X\bar{X} + c_1X^2 & (\frac{\ell}{k} \text{ is odd}) \\ c_0\bar{X}^2 + (c_1 + c_2)X\bar{X} + c_3X^2 & (\frac{\ell}{k} \text{ is even}). \end{cases} \quad (27)$$

This leads us to study a simpler form of polynomials, namely  $\tilde{f}(X) = \tilde{f}_{\underline{a}}(X) = a_0\bar{X}^2 + a_1X\bar{X} + a_2X^2 \in \mathbb{F}_{q^2}[X]$  for  $\underline{a} = (a_0, a_1, a_2) \in \mathbb{F}_{q^2}^3$ . We see that  $\tilde{f}(X) = X^2\tilde{A}(X^{q-1})$  where  $\tilde{A}(X) = \tilde{A}_{\underline{a}}(X) = a_0X^2 + a_1X + a_2$ .

We first introduce some notations. For  $\underline{a} = (a_0, a_1, a_2) \in \mathbb{F}_{q^2}^3$ , define

$$\begin{aligned} \tilde{B}(X) &= \tilde{B}_{\underline{a}}(X) := \bar{a}_2X^2 + \bar{a}_1X + \bar{a}_0 = X^2\tilde{A}^{(q)}(1/X), \\ \tilde{G}(X) &= \tilde{G}_{\underline{a}}(X) := \frac{\tilde{B}(X)}{\tilde{A}(X)}, \\ \tilde{e} &= \tilde{e}(\underline{a}) := a_2\bar{a}_2 - a_0\bar{a}_0, \end{aligned} \quad (28)$$

$$\tilde{\theta} = \tilde{\theta}(\underline{a}) := \bar{a}_1a_2 - \bar{a}_0a_1. \quad (29)$$

Then we have the following result, and Theorem 3 follows immediately by the relation (27).

**Lemma 19.** *Let  $\underline{a} = (a_0, a_1, a_2) \in \mathbb{F}_{q^2}^3$ . Then  $\tilde{f}(X) = \tilde{f}_{\underline{a}}(X) = a_0\bar{X}^2 + a_1X\bar{X} + a_2X^2 \in \mathbb{F}_{q^2}[X]$  is 2-to-1 over  $\mathbb{F}_{q^2}$  if and only if  $\tilde{e}^2 - \tilde{\theta}^{q+1}$  is a square in  $\mathbb{F}_q^*$ . Moreover, in this case  $\tilde{f}(X)$  is equivalent to  $X^2$ .*

*Proof of Lemma 19.* Since  $\gcd(2, q-1) = 2$ , as similar to Lemma 18, we see that  $\tilde{A}(X)$  has no roots in  $\mu_{q+1}$  and  $\tilde{G}(X)$  is non-constant on  $\mu_{q+1}$ . Since  $\deg \tilde{G} \leq 2$ , we actually must have  $\deg \tilde{G} = 2$ , that is,  $\gcd(\tilde{A}(X), \tilde{B}(X)) = 1$ . In particular, no points have ramification index divisible by  $p = \text{char}(\overline{\mathbb{F}}_q)$ . By Hurwitz genus formula (Lemma 9),  $\tilde{G}$  must have exactly two branch points in  $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ , each having a unique preimage in  $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ . Hence in particular  $\tilde{G}$  is  $\overline{\mathbb{F}}_q$ -linearly equivalent to  $X^2$ .

Define  $\tilde{V}(X) := \tilde{B}'(X)\tilde{A}(X) - \tilde{B}(X)\tilde{A}'(X)$ . It is easy to see that

$$\tilde{V}(X) = \tilde{\theta}^q X^2 + 2\tilde{\epsilon}X + \tilde{\theta},$$

where  $\tilde{\theta}$  and  $\tilde{\epsilon}$  are given in (29) and (28) respectively. The ramification points of  $\tilde{G}$  are the roots of  $\tilde{V}$  in  $\overline{\mathbb{F}}_q$  (and  $\infty$  if  $\deg \tilde{V} = 1$ ). Since  $\tilde{G}$  is separable, we have  $\tilde{V}(X) \neq 0$ , that is, at least one of  $\tilde{\epsilon}$  and  $\tilde{\theta}$  is nonzero. Moreover,  $\tilde{G}$  has two distinct ramification points. Hence  $\tilde{\Delta} := \frac{1}{4}\Delta(\tilde{V}) = \tilde{\epsilon}^2 - \tilde{\theta}^{q+1} \neq 0$ . Furthermore, by Lemma 5,  $\tilde{V}$  has no roots in  $\mu_{q+1}$  if and only if  $\tilde{\Delta}$  is a square in  $\mathbb{F}_q^*$ .

We first assume  $\tilde{\Delta}$  is a non-square in  $\mathbb{F}_q$ , so both ramification points of  $\tilde{G}$  are in  $\mu_{q+1}$ . Following the proof of Lemma 12 in Section III, we see that  $\tilde{G}(X) = \rho^{-1} \circ X^2 \circ \sigma$  for some degree-one  $\rho, \sigma \in \mathbb{F}_{q^2}[X]$  mapping  $\mu_{q+1}$  onto  $\mathbb{P}^1(\mathbb{F}_q)$ . Following the proof of Lemma 15 in Section V, we see that  $\tilde{f}(X)$  is equivalent to  $(x, y) \mapsto (x^2, y^2) : \mathbb{F}_q^2 \rightarrow \mathbb{F}_q^2$ . This map is not 2-to-1 since the four distinct points  $(1, 1), (-1, 1), (1, -1), (-1, -1) \in \mathbb{F}_q^2$  are all mapped to the same point  $(1, 1) \in \mathbb{F}_q^2$ .

Now we assume  $\tilde{\Delta}$  is a square in  $\mathbb{F}_q^*$ , so neither ramification points of  $\tilde{G}$  are in  $\mu_{q+1}$ . Following the proof of Lemma 12 in Section III, we see that  $\tilde{G}(X) = \rho^{-1} \circ X^2 \circ \sigma$  for some degree-one  $\rho, \sigma \in \mathbb{F}_{q^2}[X]$  permuting  $\mu_{q+1}$ . Following the proof of Lemma 15 in Section V, we see that  $\tilde{f}(X)$  is equivalent to  $X^2$ , which is indeed 2-to-1 and hence planar. This completes the proof of Lemma 19, and also the proof of Theorem 3.  $\square$

## VII. CONCLUSION

In this paper, we listed all possible equivalence classes of planar functions from a class of quadrinomials. This supplements the classification result of APN functions [20] from this class of quadrinomials in characteristic 2. We adopted a ‘‘geometric method’’ developed by Ding and Zieve [17] in odd characteristic to study this problem, and the linear equivalence result followed naturally from this method. It may be interesting to see if other results can be obtained in this way. The following question is on our mind when writing this paper:

Is it true that the condition  $k \mid \ell$  is necessary for polynomials in Families 4 or 5 in Theorem 1 to be planar? If the answer is positive, then it implies that the quadrinomials of the form (2) do not yield new planar functions (up to CCZ-equivalence).

## REFERENCES

- [1] K. Abdukhalikov, “Symplectic spreads, planar functions, and mutually unbiased bases,” *J. Algebr. Comb.* **41** (2015), no. 4, 1055–1077.
- [2] A. Albert, “On nonassociative division algebras,” *Trans. Amer. Math. Soc.* **72** (1952), 292–309.
- [3] C. Blondeau and K. Nyberg, “Perfect nonlinear functions and cryptography,” *Finite Fields Appl.* **32** (2015), 120–147.
- [4] L. Budaghyan, C. Carlet and A. Pott, “New classes of almost bent and almost perfect nonlinear functions,” *IEEE Trans. Inform. Theory* **52** (2006), 1141–1152.
- [5] L. Budaghyan and T. Hellesest, “New perfect nonlinear multinomials over  $\mathbb{F}_{p^{2k}}$  for any odd prime  $p$ ,” *Proc. of Internat. Conference on Sequences and Their Applications—SETA '08*, Lecture Notes in Comput. Sci., Vol. 5203, Springer-Verlag, Berlin, 2008, pp. 401–414.
- [6] L. Budaghyan and T. Hellesest, “New commutative semifields defined by new PN multinomials,” *Cryptogr. Commun.* **3** (2011), no. 1, 1–16.
- [7] C. Carlet, “Open questions on nonlinearity and on APN functions,” in *Proc. Int. Workshop Arithmetic Finite Fields*. Gebze, Turkey: Springer, 2014, pp. 83–107.
- [8] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*, Cambridge University Press, 2021.
- [9] C. Carlet, P. Charpin and V. Zinoviev, “Codes, bent functions and permutations suitable for DES-like cryptosystems,” *Des. Codes Cryptogr.* **15** (1998), 125–156.
- [10] C. Carlet, C. Ding and J. Yuan, “Linear codes from perfect nonlinear mappings and their secret sharing schemes,” *IEEE Trans. Inform. Theory* **51** (2005), 2089–2102.
- [11] R. Chen, S. Mesnager, “Characterizations of a class of planar functions over finite fields,” *Finite Field Appl.* **95** (2024), Paper No. 102382, 23 pp.
- [12] Y. Q. Chen and J. Polhill, “Paley type group schemes and planar Dembowski-Ostrom polynomials,” *Discrete Math.* **311** (2011), 1349–1364.
- [13] R.S. Coulter and M. Henderson, “Commutative presemifields and semifields,” *Adv. Math.* **217** (2008), no. 1, 282–304.
- [14] P. Dembowski and T. Ostrom, “Planes of order  $n$  with collineation groups of order  $n^2$ ,” *Math. Z.* **103** (1968), 239–258.
- [15] C. Ding and C. Tang, *Designs from linear codes*, second ed., World Scientific, Singapore, 2022.
- [16] C. Ding and J. Yin, “Signal sets from functions with optimum nonlinearity,” *IEEE Trans. Commun.* **55** (2007), no. 5, 936–940.
- [17] Z. Ding and M. E. Zieve, “Determination of a Class of Permutation Quadrinomials,” *P. Lon. Math. Soc.* **127** (2023), no. 2, 221–260.
- [18] Z. Ding and M. E. Zieve, “Low-degree permutation rational functions over finite fields,” *Acta Arith.* **202** (2022), 253–280.
- [19] F. Göloğlu, “Classification of fractional projective permutations over finite fields,” *Finite Fields Appl.* **81** (2022), Paper No. 102027, 50 pp.
- [20] F. Göloğlu, “Classification of  $(q, q)$ -biprojective APN functions,” *IEEE Trans. Inform. Theory* **69** (2023), no. 3, 1988–1999.
- [21] A. Haukenes, *Classification and computational search for planar functions in characteristic 3*, Master thesis, Dept. Informatics, Univ. Bergen, 2022, via <https://bora.uib.no/bora-xmlui/handle/11250/3001135>
- [22] K. H. Kim, J. Choe and S. Mesnager, “Solving  $X^{q+1} + X + a = 0$  over finite fields,” *Finite Fields Appl.* **70** (2021), Paper No. 101797, 16 pp.

- [23] K. H. Kim, S. Mesnager, C. H. Kim and M. Jo, “Completely characterizing a class of permutation quadrinomials,” *Finite Fields Appl.* **87** (2023), Paper No. 102155, 27 pp.
- [24] K. Li, C. Li, T. Helleseth, and L. Qu, “A complete characterization of the APN property of a class of quadrinomials,” *IEEE Trans. Inform. Theory* **67** (2021), no. 11, 7535–7549.
- [25] N. Li, M. Xiong and X. Zeng, “On Permutation Quadrinomials and 4-Uniform BCT,” *IEEE Trans. Inform. Theory* **67** (2021), no. 7, 4845–4855.
- [26] K. Nyberg, “Perfect nonlinear S-boxes,” *Advances in Cryptography – EUROCRYPT ’91*, Lect. Notes Comput. Sc. **547** (1992), 378–386.
- [27] K. Nyberg, “Differentially uniform mappings for cryptography,” *Advances in Cryptography–EUROCRYPT ’93*, Lect. Notes Comput. Sc., **765** (1994), Springer-Verlag, Berlin, 55–64.
- [28] A. Pott, “Almost perfect and planar functions,” *Des. Codes Cryptogr.* **78** (2016), no. 1, 41–195.
- [29] C. Shi, J. Peng, H. Kan and L. Zheng, “On CCZ-equivalence between the Bracken-Tan-Tan function and power functions,” *Finite Fields Appl.* **93** (2024), Paper No. 102340, 19 pp.
- [30] H. Stichtenoth, *Algebraic Function Fields and Codes*, 2nd Ed. Berlin, Germany: Graduate Text in Mathematics **254**, Springer-Verlag, 2009.
- [31] Z. Tu, X. Liu and X. Zeng, “A revisit to a class of permutation quadrinomials,” *Finite Fields Appl.* **59** (2019), 57–85.
- [32] G. Weng, W. Qiu, Z. Wang and Q. Xiang, “Pseudo-Paley graphs and skew Hadamard difference sets from presemifields,” *Des. Codes Cryptogr.* **44** (2007), 49–62.
- [33] Y. Wu, L. Wang, N. Li, X. Zeng and X. Tang, “On the boomerang uniformity of a class of permutation quadrinomials over finite fields,” *Discrete Math.* **345** (2022), Paper No. 113000, 14 pp.
- [34] J. Yuan, C. Carlet and C. Ding, “The weight distribution of a class of linear codes from perfect nonlinear functions,” *IEEE Trans. Inform. Theory* **52** (2006), no. 2, 712–717.
- [35] Y. Zhou and A. Pott, “A new family of semifields with 2 parameters,” *Adv. Math.* **234** (2013), 43–60.
- [36] M. E. Zieve, “Permutation polynomials on  $\mathbb{F}_q$  induced from Rédei function bijections on subgroups of  $\mathbb{F}_q^*$ ,” *Monatsh. Math.*, to appear. arXiv:1310.0776v2, 7 Oct 2013.