CHAPTER III

GENERAL CRITERIA AND CRITERIA INVOLVING CHARACTERS

There are two sections in this chapter. In the first section, general criteria for QPP's are derived while in the second section, characterizations of QPP's via characters along the same line as those of PP's are investigated.

3.1 General criteria

We start this section by establishing a very general necessary and sufficient condition for QPP; its proof is inspired by the work of Carlitz and Lutz [12].

Theorem 3.1.1. *Let S and T be nonempty subsets of $\mathbb{F}_q$ with the same number of elements, s, and $S(x) = \prod_{\alpha \in S}(x - \alpha)$. For $P(x) \in \mathbb{F}_q[x]$ and $k \in \mathbb{N}$, put*

$$(P(x))^k = B_k(x)S(x) + A_k(x),$$

where $B_k(x)$ and $A_k(x) := a_{s-1,k}x^{s-1} + a_{s-2,k}x^{s-2} + \cdots + a_{1,k}x + a_{0,k} \in \mathbb{F}_q[x]$. Let

$$V_j = \sum_{b \in S} b^j \quad (j = 0, 1, \ldots, s-1)$$

and

$$\begin{aligned} T(x) = {} & sx^{q-1} + x^{q-2}(a_{s-1,1}V_{s-1} + a_{s-2,1}V_{s-2} + \cdots + a_{0,1}V_0) \\ & + x^{q-3}(a_{s-1,2}V_{s-1} + a_{s-2,2}V_{s-2} + \cdots + a_{0,2}V_0) + \cdots \\ & + x(a_{s-1,q-2}V_{s-1} + a_{s-2,q-2}V_{s-2} + \cdots + a_{0,q-2}V_0) \\ & + (a_{s-1,q-1}V_{s-1} + a_{s-2,q-1}V_{s-2} + \cdots + a_{0,q-1}V_0 - s). \end{aligned}$$

Then $P(x)$ is an (S,T) QPP if and only if

$$\gcd\left(T(x), x(x^{q-1} - 1)\right) = \prod_{\alpha \in \mathbb{F}_q \setminus T} (x - \alpha),$$

where the empty product is taken to be 1.

Proof. For $k \in \mathbb{N}$, we have

$$\sum_{b\in S}(P(b))^k = \sum_{b\in\ S}[B_k(b)S(b) + A_k(b)] = \sum_{b\in S} A_k(b) \tag{3.1.1}$$

$$= a_{s-1,k}\sum_{b\in\ S} b^{s-1} + a_{s-2,k}\sum_{b\in\ S} b^{s-2} + \cdots + a_{1,k}\sum_{b\in S} b + sa_{0,k} \tag{3.1.2}$$

For $b \in S \subset \mathbb{F}_q$, k, $l \in \mathbb{N}$, it is evident that

$$(P(b))^k = (P(b))^{k+l(q-1)} \tag{3.1.3}$$

$$(P(b))^{q-1} = (P(b))^{l(q-1)}. \tag{3.1.4}$$

Let

$$Q(x) = \prod_{b\in S}(x - P(b)),$$

so that $Q(x)$ is monic and deg $Q(x) = s$. By (3.1.2), (3.1.3) and (3.1.4), we have

$$\frac{Q'(x)}{Q(x)} = \sum_{b\in\ S}\frac{1}{x - P(b)} = \frac{1}{x}\sum_{b\in S}(P(b))^0 + \sum_{k=1}^{\infty}\frac{1}{x^{k+1}}\sum_{b\in S}(P(b))^k$$

$$= \frac{s}{x} + \sum_{k\ \equiv\ 1\ (\mathrm{mod}\ q-1)}\frac{1}{x^{k+1}}\sum_{b\in S}P(b) + \sum_{k\ \equiv\ 2\ (\mathrm{mod}\ q-1)}\frac{1}{x^{k+1}}\sum_{b\in\ S}(P(b))^2$$

$$+ \cdots + \sum_{k\ \equiv\ q-2\ (\mathrm{mod}\ q-1)}\frac{1}{x^{k+1}}\sum_{b\in\ S}(P(b))^{q-2} + \sum_{k\ \equiv\ 0\ (\mathrm{mod}\ q-1),\ k\neq 0}\frac{1}{x^{k+1}}\sum_{b\in S}(P(b))^{q-1}$$

$$= \frac{sx^{q-1} + \left(\sum_{b\in\ S}P(b)\right)x^{q-2} + \cdots + \left(\sum_{b\in\ S}(P(b))^{q-2}\right)x + \left(\sum_{b\in S}(P(b))^{q-1}\right) - s}{x(x^{q-1}-1)}$$

$$= \frac{sx^{q-1} + \left(\sum_{b\in\ S}A_1(b)\right)x^{q-2} + \cdots + \left(\sum_{b\in\ S}A_{q-2}(b)\right)x + \left(\sum_{b\in S}A_{q-1}(b)\right) - s}{x(x^{q-1}-1)}$$

$$= \frac{T(x)}{x(x^{q-1}-1)} \tag{3.1.5}$$

where $T(x)$ is of the form as stated in the statement of the theorem.

Assume that $\gcd\left(T(x), x(x^{q-1}-1)\right) = \prod_{\alpha\in\mathbb{F}_q\setminus T}(x-\alpha)$. Then

$$\frac{Q'(x)}{Q(x)} = \frac{V(x)}{\prod_{\beta\in T}(x-\beta)},$$

where $V(x) = \frac{T(x)}{\prod_{\alpha\in\ \mathbb{F}_q\setminus T}(x-\alpha)} \in \mathbb{F}_q[x]$. Since deg $Q(x) = s$ and $Q(x)$ is monic, then

$$Q(x) = \prod_{\beta\in T}(x-\beta).$$

Consequently,

$$\prod_{b\in S}(x-P(b)) = Q(x) = \prod_{\beta\in T}(x-\beta),$$

implying that $\{P(b);\ b\in\ S\} = \{\beta;\ \beta\in T\}$, i.e. $P(x)$ is an (S,T)QPP.

Let

$$\frac{U(x)}{W(x)} = \frac{T(x)}{x(x^{q-1}-1)} = \frac{Q'(x)}{Q(x)}, \tag{3.1.6}$$

where $U(x)/W(x)$ is in reduced form. Then $\deg W(x) \le \deg Q(x)$.

Assume that $P(x)$ is an (S,T)QPP. Then $Q(x)$ has not a repeated root and $Q(x) = \prod_{b\in S}(x-P(b)) = \prod_{\alpha\in T}(x-\alpha)$. Thus $Q'(x)/Q(x)$ is in reduced form. Hence, $Q(x) = W(x)$ and $Q'(x) = U(x)$. Since $x(x^{q-1}-1) = \prod_{\alpha\in\mathbb{F}_q}(x-\alpha)$ and $W(x) = \prod_{\alpha\in T}(x-\alpha)$, by (3.1.6), we get $\gcd\left(T(x), x(x^{q-1}-1)\right) = \prod_{\alpha\in\ \mathbb{F}_q\setminus T}(x-\alpha)$.

□

Using Theorem 3.1.1, an example of a QPP which is not a PP is given in the next example.

Example 3.1.2. Let $f(x) = x^2+1 \in \mathbb{F}_5[x]$. Since $f(2) = 0 = f(3)$, $f(x)$ is not a PP. Take $S = \{0,2,4\}$, $T = \{0,1,2\}$. Then

$$S(x) = \prod_{\alpha\in S}(x-\alpha) = x(x-2)(x-4) = x^3 - x^2 + 3x.$$

Using the notation of Theorem 3.1.1, we have

$$f(x) = 0\cdot S(x) + A_1(x),\ A_1(x) = x^2+1$$

$$(f(x))^2 = (x+1)\cdot S(x) + A_2(x),\ A_2(x) = 2x+1$$

$$(f(x))^3 = (x^3+x^2+x+3)\cdot S(x) + A_3(x),\ A_3(x) = 3x^2+x+1$$

$$(f(x))^4 = (x^5+x^4+2x^3+4x^2+4x+2)\cdot S(x) + A_4(x),\ A_4(x) = 4x^2-x+1.$$

Thus, $T(x) = 3x^4+3x^3+4x-1 = (x-3)(x-4)(3x^2+4x+2)$, and so $\gcd\left(T(x), x(x^4-1)\right) = (x-3)(x-4) = \prod_{\alpha\in\mathbb{F}_5\setminus T}(x-\alpha)$, showing, by Theorem 3.1.1 that $f(x)$ is a QPP.

Most known criteria for PP's are immediate consequences of Theorem 3.1.1. Taking $S(x) = x^q - x$, we get the following results.

Corollary 3.1.3. *Let $P(x)$ be a polynomial with coefficients in $\mathbb{F}_q$, $k \in \mathbb{N}$ and*

$$(P(x))^k = B_k(x)(x^q - x) + A_k(x),$$

where $A_k(x) = a_{q-1,k}x^{q-1} + a_{q-2,k}x^{q-2} + \cdots + a_{1,k}x + a_{0,k} \in \mathbb{F}_q[x]$. Let

$$R(x) = -a_{q-1,1}x^{q-2} - a_{q-1,2}x^{q-3} - \cdots - a_{q-1,q-2}x - a_{q-1,q-1}.$$

Then $P(x)$ is a PP if and only if $R(x)$ and $x(x^{q-1} - 1)$ are relatively prime.

Specializing the reduction polynomials in Corollary 3.1.3, we obtain the classical Hermite's criterion.

Corollary 3.1.4. *Let $P(x)$ and $R(x)$ be defined as Corollary 3.1.3. Then $P(x)$ is a PP if and only if the following two conditions hold:*

(i) $\deg A_k(x) < q - 1 \quad (1 \leq k < q - 1)$,

(ii) $\deg A_{q-1}(x) = q - 1$.

Proof. To invoke upon the result of Corollary 3.1.3, we need show that the two conditions are equivalent to $R(x)$ and $x(x^{q-1} - 1)$ are relatively prime.

If (i) and (ii) hold, then $R(x) = -a_{q-1,q-1} \neq 0$, so $R(x)$ and $x(x^{q-1} - 1)$ are relatively prime.

On the other hand, since $Q(x) = x(x^{q-1} - 1)$, we have $Q'(x) = -1$. Thus,

$$-a_{q-1,1}x^{q-2} - a_{q-1,2}x^{q-3} - \cdots - a_{q-1,q-1} = R(x) = Q'(x) = -1.$$

Hence, $a_{q-1,k} = 0$ for all $1 \leq k < q - 1$ and $a_{q-1,q-1} = 1$, i.e. (i) and (ii) hold. □

In Corollary 3.1.4, if (i) holds but (ii) does not, then $Q(x)$ is a linearized polynomial because from (3.1.5),

$$\frac{Q'(x)}{Q(x)} = \frac{-a_{q-1,1}x^{q-2} - a_{q-1,2}x^{q-3} - \cdots - a_{q-1,q-1}}{x(x^{q-1}-1)} = 0,$$

we get $Q'(x) = 0$ implying that each monomial in Q has degree equal to multiple of char $\mathbb{F}_q$.

Another consequence is the main result of [12].

Corollary 3.1.5. *Let $P(x)$ and $R(x)$ be defined as Corollary 3.1.3. Then $P(x)$ is a PP if and only if the following two conditions hold:*

(i) $\deg A_k(x) < q-1 \quad (1 \le k < q-1)$,

(ii) the equation $P(x) = 0$ has exactly one solution in $\mathbb{F}_q$.

Proof. If $P(x)$ is a permutation polynomial, then (i) holds by Corollary 3.1.4, while (ii) holds by the definition of permutation polynomial.

On the other hand, assume that (i) and (ii) hold. From (ii) and (3.1.2), we get

$$-a_{q-1,q-1} = \sum_{b\in\mathbb{F}_q}(P(b))^{q-1} = 0 + \underbrace{1+1+\ldots+1}_{q-1 \text{ times}} = -1, \tag{3.1.7}$$

i.e., $\deg A_{q-1}(x) = q-1$. By Corollary 3.1.4, $P(x)$ is a PP. □

There is an alternative formulation similar to Theorem 3.1.1, whose proof, which is the same that of Theorem 3.1.1, is omitted here.

Proposition 3.1.6. *Let $S_p(x) = \prod_{\alpha\in S}(x - P(\alpha))$. For $k \in \mathbb{N}$, put*

$$x^k = B_{k_p}(x)S_p(x) + A_{k_p}(x), \tag{3.1.8}$$

where $B_{k_p}(x)$, $A_{k_p}(x) := c_{s-1,k}x^{s-1} + c_{s-2,k}x^{s-2} + \cdots + c_{1,k}x + c_{0,k} \in \mathbb{F}_q[x]$. Let

$$W_j = \sum_{b\in\ S}(P(b))^j \quad (j = 0, 1, \ldots, s-1)$$

and

$$\begin{aligned} T_p(x) = & sx^{q-1} + x^{q-2}(c_{s-1,1}W_{s-1} + c_{s-2,1}W_{s-2} + \cdots + c_{0,1}W_0) \\ & + x^{q-3}(c_{s-1,2}W_{s-1} + c_{s-2,2}W_{s-2} + \cdots + c_{0,2}W_0) + \cdots \\ & + x(c_{s-1,q-2}W_{s-1} + c_{s-2,q-2}W_{s-2} + \cdots + c_{0,q-2}W_0) \\ & + (c_{s-1,q-1}W_{s-1} + c_{s-2,q-1}W_{s-2} + \cdots + c_{0,q-1}W_0 - s). \end{aligned}$$

Then $P(x)$ is an (S,T)QPP if and only if

$$\gcd\left(T_p(x), x(x^{q-1}-1)\right) = \prod_{\alpha \in \mathbb{F}_q \setminus T} (x-\alpha),$$

where the empty product is defined as 1.

Though the statements of Theorem 3.1.1 and Proposition 3.1.6 are different, the corollaries of Theorem 3.1.1 listed above and their counterparts derivable from Proposition 3.1.6 are identical because $T_p(x) = T(x)$. To see this, it is enough to show that for each $k \in \mathbb{N}$,

$$\sum_{b \in S} A_k(b) = \sum_{b \in S} A_{k_p}(P(b)). \tag{3.1.9}$$

From (3.1.8), we have

$$\begin{aligned} \sum_{b \in S} (P(b))^k &= \sum_{b \in S} \left\{ B_{k_p}(P(b)) S_p(P(b)) + A_{k_p}(P(b)) \right\} \\ &= \sum_{b \in S} \left\{ B_{k_p}(P(b)) \prod_{\alpha \in S} (P(b) - P(\alpha)) + A_{k_p}(P(b)) \right\} = \sum_{b \in S} A_{k_p}(P(b)), \end{aligned}$$

from which together with (3.1.1), the identity (3.1.9) follows.

3.2 Criteria involving characters

In this section, we use the concept of characters to determine QPP's. Before doing so, we give the definition of character.

Definition 3.2.1. Let $\langle G, * \rangle$ be a finite abelian group and F a field. A function $\chi : G \to F$ is called a *character* if it is a homomorphism of G into the multiplicative group F^* of nonzero elements of F, i.e. a mapping from G into F^* such that $\chi(g_1 * g_2) = \chi(g_1)\chi(g_2)$ for all $g_1, g_2 \in G$. If $\chi(g) = 1$ for all $g \in G$, then χ is said to be *trivial*. All other characters of G are called *nontrivial*. If G is a group with respect to multiplication, then a character χ of G is called a *multiplicative character* and if G is a group with respect to addition, then a character χ of G is called an *additive character*. Denote by $\hat{G}$ is the set of characters of G; it is an abelian group under the multiplication of characters, i.e., $\chi_1(h)\chi_2(h) = \chi_1\chi_2(h)$ for all $h \in G$.

Some criteria for QPP's based on the use of characters of abelian subgroups of $\mathbb{F}_q$ are given next.

Theorem 3.2.2. *Let S and T be multiplicative (or additive) subgroups of $\mathbb{F}_q$, and $f(x) \in \mathbb{F}_q[x]$ sending S onto T. Then $f(x)$ is an (S,T)QPP if and only if*

$$\sum_{c \in S} \chi(f(c)) = 0$$

for each nontrivial character χ of S.

Proof. We give only a proof for multiplicative S; the other case is similar. Assume that $f(x)$ is an (S,T)QPP. We may assume without loss of generality that both S and T have the same set of characters. Let χ be a nontrivial character of both S and T. Then by Theorem 2.1.13,

$$\sum_{c \in S} \chi(f(c)) = \sum_{b \in T} \chi(b) = 0.$$

Conversely, assume that $\sum_{c \in S} \chi(f(c)) = 0$ for all multiplicative characters $\chi \neq \chi_0$, the trivial character of S. Then for fixed $a \in T = f(S)$, the number N of

solutions of $f(x) = a$ in S is given, see e.g. equation (5.5) p. 189 of [4], by

$$N = \frac{1}{|S|}\sum_{c\in S}\sum_{\chi\in\hat{S}}\chi(f(c))\overline{\chi(a)} = \frac{1}{|S|}\left(\sum_{c\in S}\chi_0(f(c))\overline{\chi_0(a)} + \sum_{\chi\neq\chi_0}\sum_{c\in S}\chi(f(c))\overline{\chi(a)}\right)$$
$$= \frac{1}{|S|}\left(\sum_{c\in S}1\cdot 1 + \sum_{\chi\neq\chi_0}\overline{\chi(a)}\sum_{c\in S}\chi(f(c))\right) = \frac{1}{|S|}\left(|S| + \sum_{\chi\neq\chi_0}\overline{\chi(a)}\cdot 0\right) = 1.$$

Hence, $f(x)$ is an (S,T)QPP. □

Specializing the result of Theorem 3.2.2 to quadratic characters, interesting characterizations can be derived. We start by recalling some facts about quadratic characters. Let H be a nonempty multiplicative subgroup of $\mathbb{F}_q \setminus \{0\}$, $|H| = d$. A *quadratic H-character* of $\mathbb{F}_q$ is defined as a map $\eta_H : \mathbb{F}_q \to \mathbb{C}$ satisfying, for each $c \in \mathbb{F}_q$,

$$\eta_H(c) = \begin{cases} 0 & \text{if } c = 0, \\ 1 & \text{if } c = b^2 \text{ for some } b \in H, \\ -1 & \text{otherwise.} \end{cases}$$

We gather basic properties of quadratic characters in the following lemma.

Lemma 3.2.3. *I. If $b \in H$, then*

(i) either $b^{d/2} = 1$ or -1;

(ii) $\eta_H(b) = 1$ if and only if $b^{d/2} = 1$.

II. If $c \in \mathbb{F}_q \setminus \{0\}$, then $\eta_H(c) = \eta_H(c^{-1})$.

III. Let $b, c \in \mathbb{F}_q$. Then $\eta_H(bc) = \eta_H(b)\eta_H(c)$ holds only when $b = 0$, or $c = 0$, or $\eta_H(b) \neq \eta_H(c)$, or $\eta_H(b) = \eta_H(c) = 1$.

IV. If $b \in \mathbb{F}_q$ and $c \in H$, then $\eta_H(bc^{-1}) = \eta_H(bc)$.

Proof. I. (i) Since H is of order d, from $(b^{d/2})^2 = b^d = 1$, the result follows.

(ii) Since H is a subgroup of the multiplicative group $\mathbb{F}_q \setminus \{0\}$, H is cyclic, i.e.,

$H = \langle \alpha \rangle$ for some $\alpha \in H$. We first verify that $b^{1/2} \in H$ if and only if $b = \alpha^{2i}$ for some $i \in \mathbb{N} \cup \{0\}$. If $b = \alpha^{2i}$ for some $i \in \mathbb{N} \cup \{0\}$, then $b^{1/2} = \alpha^i \in H$. If $b^{1/2} \in H$, then $b^{1/2} = \alpha^i$ for some $i \in \mathbb{N} \cup \{0\}$, and so $b = \alpha^{2i}$. Now the definition of quadratic character yields

$$\eta_H(b) = 1 \Leftrightarrow b = h^2 \text{ (for some } h \in H) \Leftrightarrow b^{1/2} \in H$$
$$\Leftrightarrow b = \alpha^{2i} \text{ for some } i \in \mathbb{N} \cup \{0\} \Leftrightarrow b^{d/2} = (\alpha^{2i})^{d/2} = (\alpha^i)^d = 1.$$

II. We have

$$\eta_H(c) = 1 \Leftrightarrow c = h^2 \ (h \in H) \Leftrightarrow c^{-1} = (h^{-1})^2 \Leftrightarrow \eta_H(c^{-1}) = 1.$$

III. The result holds trivially when $b = 0$ or $c = 0$. For the rest of the proof assume both b and c are nonzero. If $\eta_H(b) = \eta_H(c) = 1$, then $b = u^2$ and $c = v^2$ for some $u, v \in H$, and so $bc = (uv)^2$ showing that $\eta_H(bc) = 1 = \eta_H(b)\eta_H(c)$.

If $\eta_H(b) \neq \eta_H(c)$, say $\eta_H(b) = 1$, $\eta_H(c) = -1$, then $b = u^2$ for some $u \in H$ and $c \neq v^2$ for all $v \in H$. Suppose that $(bc)^{1/2} \in H$. Then $bc = w^2$ for some $w \in H$, and so $c = w^2 b^{-1} = (wu^{-1})^2$, which contradicts with $\eta_H(c) = -1$. Thus $(bc)^{1/2} \notin H$ and so $\eta_H(bc) = -1 = \eta_H(b)\eta_H(c)$.

IV. As a preliminary result, we show that $\eta_H(bc(c^{-1})^2) = \eta_H(bc)$. If $b = 0$, then $\eta_H(bc(c^{-1})^2) = \eta_H(bc^{-1}) = 0 = \eta_H(bc)$.

Assume $b \neq 0$. If $\eta_H(bc) = 1$, then $\eta_H((c^{-1})^2) = 1 = \eta_H(bc)$, so by part III,

$$\eta_H(bc(c^{-1})^2) = \eta_H(bc)\eta_H((c^{-1})^2) = \eta_H(bc) \cdot 1 = \eta_H(bc).$$

If $\eta_H(bc) = -1$, then by part III,

$$\eta_H(bc(c^{-1})^2) = \eta_H(bc)\eta_H((c^{-1})^2) = \eta_H(bc) \cdot 1 = \eta_H(bc).$$

Using the preliminary result, we have

$$\eta_H(bc^{-1}) = \eta_H(bcc^{-1}c^{-1}) = \eta_H(bc(c^{-1})^2) = \eta_H(bc).$$

□

Theorem 3.2.4. *Let q be odd, $a \in \mathbb{F}_q$, H a nonempty multiplicative subgroup of $\mathbb{F}_q \setminus \{0\}$ of even order d, and $S = H \cup \{0\}$.*

(i) If $a - 1 \in H = S \setminus \{0\}$ and $\eta_H(a^2 - 1) = 1$, then $f(x) = x^{1+d/2} + ax$ is an $(S, f(S))QPP$.

(ii) If $a + 1 \in S$ and $a - 1 \in H = S \setminus \{0\}$, then $f(x) = x^{1+d/2} + ax$ is an $(S, f(S))QPP$ if and only if $\eta_H(a^2 - 1) = 1$.

Proof. Let $f(x) = x^{1+d/2} + ax$. We proceed to prove the assertion (ii) as the assertion (i) will be deduced along the way. Assuming $a + 1 \in S$ and $a - 1 \in H = S \setminus \{0\}$, it suffices to show that

$$\eta_H(a^2 - 1) \neq 1 \iff f \text{ is not injective on } S.$$

Assume that f is not injective on S. Then there are $b, c \in S, b \neq c$ such that $f(b) = f(c)$. We consider two possible cases.

Case 1. $c = 0$ or $b = 0$. Without loss of generality assume $c = 0$. Then $b \in H$. Thus

$$(b^{d/2} + a)b = b^{d/2+1} + ab = f(b) = f(c) = 0,$$

implying that $b^{d/2} + a = 0$. Consequently,

$$\eta_H(a^2 - 1) = \eta_H(b^d - 1) = \eta_H(0) = 0 \neq 1.$$

Case 2. $b \neq 0$ and $c \neq 0$. From

$$b^{d/2+1} + ab = f(b) = f(c) = c^{d/2+1} + ac$$

we deduce that

$$(b^{d/2} + a)b = (c^{d/2} + a)c. \tag{3.2.1}$$

If $b^{d/2} + a = 0$, then the same reasoning as in Case 1 yields the result. If $b^{d/2} + a \neq 0$, then its inverse $(b^{d/2} + a)^{-1} \in \mathbb{F}_q$, and (3.2.1) implies

$$bc^{-1} = (b^{d/2} + a)^{-1}(c^{d/2} + a). \tag{3.2.2}$$

If $\eta_H(b) = \eta_H(c) = 1$, then Lemma 3.2.3 I (ii) shows that $b^{d/2} = 1 = c^{d/2}$. Consequently, (3.2.2) yields $bc^{-1} = (1+a)^{-1}(1+a) = 1$, i.e., $b = c$, which is a contradiction.

If $\eta_H(b) = \eta_H(c) = -1$, then Lemma 3.2.3 I show that $b^{d/2} = -1 = c^{d/2}$. Consequently, (3.2.2) yields $bc^{-1} = (-1+a)^{-1}(-1+a) = 1$, i.e., $b = c$, again a contradiction.

Thus, $\eta_H(b) \neq \eta_H(c)$. We assume, without loss of generality, that $\eta_H(b) = -1$ and $\eta_H(c) = 1$. Then by Lemma 3.2.3 I, $b^{d/2} = -1$ and $c^{d/2} = 1$. Thus

$$\begin{aligned}
-1 = \eta_H(b)\eta_H(c) &= \eta_H(b)\eta_H(c^{-1}) \quad \text{(by Lemma 3.2.3 II)} \\
&= \eta_H(bc^{-1}) \qquad\qquad \text{(by Lemma 3.2.3 III)} \\
&= \eta_H((-1+a)^{-1}(1+a)) \qquad \text{(using also (3.2.2))} \\
&= \eta_H((-1+a)(1+a)) \qquad \text{(by Lemma 3.2.3 IV, using } a-1 \in H = S \setminus \{0\}) \\
&= \eta_H(a^2-1).
\end{aligned}$$

We note in passing that at this point the assertion (i) holds.

Conversely, if $\eta_H(a^2-1) \neq 1$, then $a^2 - 1 = 0$ or $\eta_H(a^2-1) = -1$. There are two possible cases.

Case 1. $a^2 - 1 = 0$. Then $a = \pm 1$. If $a = -1$, then $f(1) = 1 + a = 0 = f(0)$, so f is not one-to-one on S. If $a = 1$, then $0 = a - 1 \in H = S \setminus \{0\}$, which is a contradiction.

Case 2. $\eta_H(a^2-1) = -1$. By hypothesis, the element $b = (a+1)(a-1)^{-1} \in S$. Then

$$\begin{aligned}
\eta_H(b) = \eta_H((a+1)(a-1)^{-1}) &= \eta_H((a+1)(a-1)) \quad \text{(by Lemma 3.2.3 IV)} \\
&= \eta_H(a^2-1) = -1.
\end{aligned}$$

Lemmas 3.2.3 I thus imply that $b^{d/2} = -1$. Thus

$$f(b) = b^{d/2+1} + ab = (b^{d/2} + a)b = (-1 + a)b = a + 1 = f(1),$$

showing that f is not injective on S. □

Theorem 3.2.4 is sharp in the sense that there are other values of a, such as $a = \pm 1$, yielding non-QPP's as in the next example.

Example 3.2.5. For odd q, let $S = H \cup \{0\}$ where H is a nonempty multiplicative subgroup of $\mathbb{F}_q^*$ of even order d. Then

$$f_{\pm}(x) = x^{1+d/2} \pm x = x(x^{d/2} \pm x)$$

is not an $(S, f(S))$QPP.

To see this, taking $a \in H$, we have

$$f_{-}(a^2) = \left(a^2\right)^{1+d/2} - a^2 = 0 = f_{-}(0),$$

showing that f_{-} is not injective. Since H is a nonempty multiplicative subgroup of $\mathbb{F}_q^*$ of even order d, we have $H = \langle \alpha \rangle$ for some $\alpha \in \mathbb{F}_q^*$ with $\alpha^d = 1$ and $\alpha^{d/2} = -1$. Now,

$$f_{+}(\alpha) = \alpha\left((\alpha^{d/2}) + 1\right) = 0 = f_{+}(0),$$

i.e., f_{+} is not injective.