CHAPTER IV

CRITERIA FOR SPECIAL FORMS OF QPP'S

In this chapter, we derive some criteria for QPP's in forms of linearized polynomials, monomials, binomials and other different forms.

4.1 Linearized polynomials

In this section, we give you some necessary and sufficient conditions for QPP's in the form of linearized polynomials. Throughout this section, we let $\mathbb{F}_{q^r}$ be an extension field of $\mathbb{F}_q$ with $r \in \mathbb{N}$. Recall from [4] that $L(x) \in \mathbb{F}_{q^r}[x]$ is called a *linearized* polynomial or *q-polynomial* if it is of the form

$$L(x) = \sum_{i=0}^{m} a_i x^{q^i}.$$

For such polynomials, we have the following criterion for QPP.

Theorem 4.1.1. *Let S be an additive subgroup of $\mathbb{F}_{q^r}$, $T \subseteq \mathbb{F}_{q^r}$ with $0 \in T \subseteq \mathbb{F}_{q^r}$ and $|S| = |T| = s$. Let*

$$L(x) = \sum_{i=0}^{r-1} a_i x^{q^i} \in \mathbb{F}_{q^r}[x]$$

be a linearized polynomial sending S into T. Then $L(x)$ is an (S,T)QPP if and only if $L(x)$ has exactly one root, namely 0, in S.

Proof. Assume that $L(x)$ is an (S,T)QPP. Clearly, $L(0) = 0$ showing that $0 \in S$ is a root of $L(x)$. If $c \in S$ is a root of $L(x)$, since $L(x)$ is a bijection, we must have $c = 0$.

Conversely, assume that $L(x)$ only has the root $0 \in S$. To show that L is an (S,T)QPP, it suffices to show that L is injective on S. This is immediate from

S being an additive group and

$$0 = L(b) - L(c) = \sum_{i=0}^{r-1} a_i \left(b^{q^i} - c^{q^i} \right) = \sum_{i=0}^{r-1} a_i (b-c)^{q^i} = L(b-c).$$

□

The requirement that S is an additive group in Theorem 4.1.1 cannot be discarded as witnessed from the following example.

Example 4.1.2. Let $\mathbb{F}_9 \cong \mathbb{Z}_3[x]/(x^2+1)$, with $\alpha \in \mathbb{F}_9$ satisfying $\alpha^2 + 1 = 0$. Let $S_1 = \{0, \alpha, 2\alpha\}$ and $S_2 = \{0, \alpha+1, \alpha+2\}$ be subsets of $\mathbb{F}_9$. Clearly, S_1 is an additive subgroup of $\mathbb{F}_9$ but S_2 is not. Consider the linearized polynomial

$$L(x) = x^3 + 2x \in \mathbb{F}_9[x].$$

Since 0 is the only root of $L(x)$ in S_1, by Theorem 4.1.1, $L(x)$ is an $(S_1, L(S_1))$QPP. However, from $L(0) = 0$, $L(\alpha+1) = \alpha = L(\alpha+2)$, we see that 0 is the only root of $L(x)$ in S_2 as well, but $L(x)$ is not an $(S_2, L(S_2))$QPP.

An immediate consequence of Theorem 4.1.1 is the following result which is Theorem 2.1.5.

Corollary 4.1.3. *Every linearized polynomial in $\mathbb{F}_q[x]$ is a PP if and only if it only has the root 0 in $\mathbb{F}_q$.*

Making use of vector space notion, linearized polynomials give a large class of PP's and QPP's as shown in the next result which is of interest in its own right. Before stating the theorem, let us recall some linear algebra results. Let S be an additive subgroup of $\mathbb{F}_{q^r}$ and $0 \in T \subseteq \mathbb{F}_{q^r}$ with $|S| = |T| = s$. If $S\mathbb{F}_q \subseteq S$, then S can be viewed as a vector subspace of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$.

Theorem 4.1.4. *Let S be an additive subgroup of $\mathbb{F}_{q^r}$, $0 \in T \subseteq \mathbb{F}_{q^r}$, $|S| = |T|$. Assume that $S\mathbb{F}_q \subseteq S$ and set $d := \dim_{\mathbb{F}_q} S$, $r = kd$ $(k \in \mathbb{N})$. Let*

$\beta_0, \beta_1, \ldots, \beta_{d-1} \in S$ be linearly independent over $\mathbb{F}_q$ and put

$$\alpha_i := \beta_i + \beta_i^{q^d} + \beta_i^{q^{2d}} + \cdots + \beta_i^{q^{(k-1)d}} \quad (i = 0, 1, 2, \ldots, d-1). \tag{4.1.1}$$

Let $L : S \to T$ be a linearized polynomial of the form

$$L(x) = \sum_{i=0}^{r-1} a_i x^{q^i} \in \mathbb{F}_{q^r}[x], \text{ with } a_t = a_i \text{ whenever } t \equiv i \pmod{d}. \tag{4.1.2}$$

(i) Assume that $\alpha_0, \alpha_1, \ldots, \alpha_{d-1}$ are linearly independent over $\mathbb{F}_q$. Then $L(\beta_0), L(\beta_1), \ldots, L(\beta_{d-1})$ are linearly independent over $\mathbb{F}_q$ if and only if $\det A \neq 0$, where

$$A = \begin{pmatrix} a_0 & a_{d-1}^q & a_{d-2}^{q^2} & \cdots & a_1^{q^{d-1}} \\ a_1 & a_0^q & a_{d-1}^{q^2} & \cdots & a_2^{q^{d-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{d-1} & a_{d-2}^q & a_{d-3}^{q^2} & \cdots & a_0^{q^{d-1}} \end{pmatrix}. \tag{4.1.3}$$

(ii) If $\alpha_0, \alpha_1, \ldots, \alpha_{d-1}$ are linearly dependent over $\mathbb{F}_q$, then $L(\beta_0)$, $L(\beta_1), \ldots, L(\beta_{d-1})$ are linearly dependent over $\mathbb{F}_q$, and $L(x)$ is not an (S,T)QPP.

Proof. Write

$$\gamma_m := L(\beta_m) \quad (m = 0, 1, 2, \ldots, d-1).$$

Since $\beta_m^{q^r} = \beta_m \quad (0 \leq j \leq r-1;\ 0 \leq m \leq d-1)$, using $a_t = a_i$ if $t \equiv i \pmod{d}$, we have

$$\begin{aligned} \gamma_m^{q^j} &= a_0^{q^j} \beta_m^{q^j} + a_1^{q^j} \beta_m^{q^{j+1}} + \cdots + a_{r-j}^{q^j} \beta_m^{q^{j+r-j}} + \cdots + a_{r-1}^{q^j} \beta_m^{q^{j+r-1}} \\ &= a_{j-j}^{q^j} \beta_m^{q^j} + a_{(j+1)-j}^{q^j} \beta_m^{q^{j+1}} + \cdots + a_{0-j}^{q^j} \beta_m^{q^0} + \cdots + a_{(j-1)-j}^{q^j} \beta_m^{q^{j-1}} \\ &= \sum_{i=0}^{r-1} a_{i-j}^{q^j} \beta_m^{q^i}. \end{aligned} \tag{4.1.4}$$

Substituting into (4.1.2), we get

$$\begin{pmatrix} \gamma_0 & \gamma_0^q & \cdots & \gamma_0^{q^{r-1}} \\ \gamma_1 & \gamma_1^q & \cdots & \gamma_1^{q^{r-1}} \\ \vdots & \vdots & & \vdots \\ \gamma_{d-1} & \gamma_{d-1}^q & \cdots & \gamma_{d-1}^{q^{r-1}} \end{pmatrix} = \begin{pmatrix} \beta_0 & \beta_0^q & \cdots & \beta_0^{q^{r-1}} \\ \beta_1 & \beta_1^q & \cdots & \beta_1^{q^{r-1}} \\ \vdots & \vdots & & \vdots \\ \beta_{d-1} & \beta_{d-1}^q & \cdots & \beta_{d-1}^{q^{r-1}} \end{pmatrix} \begin{pmatrix} a_0 & a_{r-1}^q & \cdots & a_1^{q^{r-1}} \\ a_1 & a_0^q & \cdots & a_2^{q^{r-1}} \\ \vdots & \vdots & & \vdots \\ a_{d-1} & a_{d-2}^q & \cdots & a_d^{q^{r-1}} \\ \vdots & \vdots & & \vdots \\ a_{r-1} & a_{r-2}^q & \cdots & a_0^{q^{r-1}} \end{pmatrix}. \tag{4.1.5}$$

Equating the top left hand corner of (4.1.5), we get

$$\Delta = B_1A_1 + B_2A_2 + \cdots + B_kA_k$$

where

$$\Delta = \begin{pmatrix} \gamma_0 & \gamma_0^q & \cdots & \gamma_0^{q^{d-1}} \\ \gamma_1 & \gamma_1^q & \cdots & \gamma_1^{q^{d-1}} \\ \vdots & \vdots & & \vdots \\ \gamma_{d-1} & \gamma_{d-1}^q & \cdots & \gamma_{d-1}^{q^{d-1}} \end{pmatrix},$$

and for $1 \le l \le k$,

$$B_l = \begin{pmatrix} \beta_0^{q^{(l-1)d}} & \beta_0^{q^{(l-1)d+1}} & \cdots & \beta_0^{q^{ld-1}} \\ \beta_1^{q^{(l-1)d}} & \beta_1^{q^{(l-1)d+1}} & \cdots & \beta_1^{q^{ld-1}} \\ \vdots & \vdots & & \vdots \\ \beta_{d-1}^{q^{(l-1)d}} & \beta_{d-1}^{q^{(l-1)d+1}} & \cdots & \beta_{d-1}^{q^{ld-1}} \end{pmatrix}, A_l = \begin{pmatrix} a_{(l-1)d} & a_{(l-1)d-1}^q & \cdots & a_{(l-2)d+1}^{q^{d-1}} \\ a_{(l-1)d+1} & a_{(l-1)d}^q & \cdots & a_{(l-2)d+2}^{q^{d-1}} \\ \vdots & \vdots & & \vdots \\ a_{ld-1} & a_{ld-2}^q & \cdots & a_{(l-1)d}^{q^{d-1}} \end{pmatrix}.$$

Since $a_t = a_i$ if $t \equiv i \pmod{d}$, we have

$$A_l = \begin{pmatrix} a_0 & a_{d-1}^q & a_{d-2}^{q^2} & \cdots & a_1^{q^{d-1}} \\ a_1 & a_0^q & a_{d-1}^{q^2} & \cdots & a_2^{q^{d-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{d-1} & a_{d-2}^q & a_{d-3}^{q^2} & \cdots & a_0^{q^{d-1}} \end{pmatrix} = A \quad (l = 1, 2, \ldots, k).$$

Thus,

$$\Delta = (B_1 + B_2 + \cdots + B_k)A = BA,$$

where, using (4.1.1),

$$B = \begin{pmatrix} \alpha_0 & \alpha_0^q & \cdots & \alpha_0^{q^{d-1}} \\ \alpha_1 & \alpha_1^q & \cdots & \alpha_1^{q^{d-1}} \\ \vdots & \vdots & & \vdots \\ \alpha_{d-1} & \alpha_{d-1}^q & \cdots & \alpha_{d-1}^{q^{d-1}} \end{pmatrix}.$$

(i) Assume that $\alpha_0, \alpha_1, \ldots, \alpha_{d-1}$ are linearly independent over $\mathbb{F}_q$. By Lemma 2.1.10, we know that $\det B \neq 0$. Thus, $\det \Delta = 0$ if and only if $\det A = 0$ and so the assertion follows again from Lemma 2.1.10.

(ii) If $\alpha_0, \alpha_1, \ldots, \alpha_{d-1}$ are linearly dependent over $\mathbb{F}_q$, then Lemma 2.1.10 implies $\det B = 0$, and so $\det \Delta = 0$. This yields that $\gamma_0, \gamma_1, \ldots, \gamma_{d-1}$ are linearly dependent over $\mathbb{F}_q$, i.e., there are $b_0, b_1, \ldots, b_{d-1} \in \mathbb{F}_q$ not all zero such that

$$\begin{aligned} L(0) = 0 &= b_0 L(\beta_0) + b_1 L(\beta_1) + \cdots + b_{d-1} L(\beta_{d-1}) \\ &= L(b_0\beta_0 + b_1\beta_1 + \cdots + b_{d-1}\beta_{d-1}). \end{aligned}$$

If $b_0\beta_0 + b_1\beta_1 + \cdots + b_{d-1}\beta_{d-1} = 0$, since $\beta_0, \beta_1, \ldots, \beta_{d-1}$ are linearly independent over $\mathbb{F}_q$, then all $b_i = 0$, which is a contradiction. Thus, $b_0\beta_0 + b_1\beta_1 + \cdots + b_{d-1}\beta_{d-1} \neq 0$ showing that $L(x)$ is not an (S,T)QPP. □

Remarks. 1. The special case where $d = r$, which forces all matrices in (4.1.5) to be square, shows in particular that $L(x)$ is an (S,T)QPP if and only if

$$\det \begin{pmatrix} a_0 & a_{r-1}^q & a_{r-2}^{q^2} & \cdots & a_1^{q^{r-1}} \\ a_1 & a_0^q & a_{r-1}^{q^2} & \cdots & a_2^{q^{r-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{r-1} & a_{r-2}^q & a_{r-3}^{q^2} & \cdots & a_0^{q^{r-1}} \end{pmatrix} \neq 0.$$

This special case is a generalization of the above remark of Theorem 2.1.9.

2. It is trivial to see that the condition $S\mathbb{F}_q \subseteq S$ can be dropped if $q = p$.

Pushing the result in Theorem 4.1.4(i) a little further, we get:

Corollary 4.1.5. *Let S be an additive subgroup of $\mathbb{F}_{q^r}$, $0 \in T \subseteq \mathbb{F}_{q^r}$, $|S| = |T|$. Assume that $S\mathbb{F}_q \subseteq S$ and set $d := \dim_{\mathbb{F}_q} S$, $r = kd$ $(k \in \mathbb{N})$. Let $\beta_0, \beta_1, \ldots, \beta_{d-1} \in S$ be linearly independent over $\mathbb{F}_q$ and put*

$$\alpha_i := \beta_i + \beta_i^{q^d} + \beta_i^{q^{2d}} + \cdots + \beta_i^{q^{(k-1)d}} \quad (i = 0, 1, 2, \ldots, d-1).$$

Let $L : S \to T$ be a linearized polynomial of the form (4.1.2) satisfying $a_t = a_i$ whenever $t \equiv i \pmod{d}$. If $\alpha_0, \alpha_1, \ldots, \alpha_{d-1}$ are linearly independent over $\mathbb{F}_q$ and $\det A \neq 0$, where A is given by (4.1.3), then $L(x)$ is an (S,T)QPP.

Proof. By Theorem 4.1.1, $L(x)$ is an (S,T)QPP if and only if $L(x)$ has only one root $0 \in S$, that is, if and only if the linear operator on the vector space S over $\mathbb{F}_q$ induced by $L(x)$ is nonsingular. This linear operator is nonsingular precisely if $L(\beta_0), L(\beta_1), \ldots, L(\beta_{d-1})$ are linearly independent over $\mathbb{F}_q$ whenever $\beta_0, \beta_1, \ldots, \beta_{d-1} \in S$ are linearly independent over $\mathbb{F}_q$ and Theorem 4.1.4 shows that $L(\beta_0), L(\beta_1), \ldots, L(\beta_{d-1})$ are linearly independent over $\mathbb{F}_q$. □

The following example illustrates that both possibilities in Theorem 4.1.4 do actually occur.

Example 4.1.6. In

$$\mathbb{F}_{2^4} \cong \mathbb{Z}_2[x]/(x^4 + x + 1) = \left\{c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3;\ c_0, c_1, c_2, c_3 \in \mathbb{Z}_2\right\},$$

where $\alpha^4 + \alpha + 1 = 0$, let

$$S_1 = \{0, \alpha, \alpha^2, \alpha^2 + \alpha\} \subseteq \mathbb{F}_{2^4},\ S_2 = \{0, \alpha^2 + 1, \alpha^3 + 1, \alpha^2 + \alpha^3\} \subseteq \mathbb{F}_{2^4}.$$

Note that both are additive subgroups of $\mathbb{F}_{2^4}$. For each $i \in \{1, 2\}$, consider the linearized polynomial $L : S_i \to L(S_i)$ given by

$$L(x) = a_0x + a_1x^2 + a_0x^4 + a_1x^8 \in \mathbb{F}_{2^4}[x].$$

Taking $\beta_0 = \alpha, \beta_1 = \alpha^2$ both belonging to S_1 and linearly independent over $\mathbb{F}_2$, direct computation gives

$$\beta_0 + \beta_0^{2^2} = \alpha + \alpha^4 = 1, \quad \beta_1 + \beta_1^{2^2} = \alpha^2 + \alpha^8 = 1,$$

both of which are clearly linearly dependent over $\mathbb{F}_2$. Since $L(\beta_0)$ and $L(\beta_1)$ are both equal to $a_0 + a_1$, they are linearly dependent over $\mathbb{F}_2$ and so $L(x)$ is not an $(S_1, L(S_1))$QPP.

Taking $\beta_0 = \alpha^2 + 1, \beta_1 = \alpha^2 + \alpha^3$ both belonging to S_2 and linearly independent over $\mathbb{F}_2$, direct computation gives

$$\beta_0 + \beta_0^{2^2} = 1 \text{ and } \beta_1 + \beta_1^{2^2} = \alpha^2 + \alpha,$$

both of which are linearly independent over $\mathbb{F}_2$. By Theorem 4.1.4, $\det \begin{pmatrix} a_0 & a_1^2 \\ a_1 & a_0^2 \end{pmatrix} \neq 0$ if and only if $L(\beta_0), L(\beta_1)$ are linearly independent over $\mathbb{F}_2$.

Observe that the linearized polynomials L, over $\mathbb{F}_{q^r}$, in both Theorem 4.1.4 and Corollary 4.1.5 are of degree $\leq q^{r-1}$. As seen in Proposition 2.1.16, these linearized polynomials may not be those unique polynomials of degree $\leq s-1$ representing functions $L : S \to T$. This leads us to ask whether the unique polynomial of degree $\leq s-1$ representing a linearized polynomial $L : S \to T$ over $\mathbb{F}_{q^r}$ is necessarily linearized. This is so if $q = p$ as shown in the next proposition, and false otherwise as seen in the following example.

Proposition 4.1.7. *Let S be an additive subgroup of $\mathbb{F}_{p^r}$ and $T \subseteq \mathbb{F}_{p^r}$ with $0 \in T$, $|S| = |T| = s \leq p^r$. If $L : S \to T$ is a linearized polynomial of the form*

$$L(x) = \sum_{i=0}^{r-1} a_i x^{p^i} \in \mathbb{F}_{p^r}[x], \tag{4.1.6}$$

then the unique polynomial $f_L : S \to T$ in $\mathbb{F}_{p^r}[x]$ with degree $\leq s-1$ which represents L in the sense that $f_L(y) = L(y)$ $(y \in S)$ is also linearized polynomial.

Proof. Let, by Proposition 2.1.16, the unique polynomial $f_L : S \to T$ in $\mathbb{F}_{p^r}[x]$ with degree $\leq s-1$ which represents L be

$$f_L(x) = \sum_{i=0}^{s-1} b_i x^i \in \mathbb{F}_{p^r}[x].$$

For $y, z \in S$ and $c \in \mathbb{F}_p$, we see that

$$f_L(y+z) = L(y+z) = \sum_{i=0}^{r-1} a_i(y+z)^{p^i} = \sum_{i=0}^{r-1} a_i(y^{p^i}+z^{p^i}) = L(y)+L(z) = f_L(y)+f_L(z)$$

and

$$f_L(cy) = L(cy) = \sum_{i=0}^{r-1} a_i(cy)^{p^i} = c\sum_{i=0}^{r-1} a_i y^{p^i} = cL(y) = cf_L(y).$$

By Lemma 2.1.6, we conclude that $f_L(x)$ is a linearized polynomial. □

Example 4.1.8. In

$$\mathbb{F}_{4^3} = \mathbb{F}_{2^6} \cong \mathbb{Z}_2[x]/(x^6+x+1) = \{c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_5\alpha^5;\ c_i \in \mathbb{Z}_2\},$$

where $\alpha^6 + \alpha + 1 = 0$, let $S = \{0, 1, \alpha^2, \alpha^2+1\}$, $T = \{0, \alpha^3+\alpha^2+1, \alpha, \alpha^2\}$ be subsets of $\mathbb{F}_{4^3}$. Consider the linearized polynomial

$$L(x) = x + x^{16} \in \mathbb{F}_{4^3}[x]$$

whose restriction to S is a function sending S into T given by

$$L_S(x) = \begin{cases} 0 & \text{if } x = 0 \text{ or } 1, \\ \alpha^3+\alpha^2+1 & \text{if } x = \alpha^2 \text{ or } \alpha^2+1. \end{cases}$$

If

$$f_L(x) = a_0 + a_1x + a_2x^2 + a_3x^3 \in \mathbb{F}_{4^3}[x]$$

is the unique polynomial of degree ≤ 3 representing L_S, equating the values of f_L and L_S over S and solving the system for the coefficients a_i we get

$$f_L(x) = (\alpha^5+\alpha^2)x + (\alpha^5+\alpha^2)x^2,$$

which is not a linearized polynomial over $\mathbb{F}_{4^3}$, though it is a linearized polynomial over $\mathbb{F}_{2^6}$.

In addition, the requirement that S is an additive group in Proposition 4.1.7 cannot be dropped, even when $q = p$, as witnessed in the following example.

Example 4.1.9. Let $\mathbb{F}_{5^3} \cong \mathbb{Z}_5[x]/(x^3+x+1)$, with $\alpha \in \mathbb{F}_{5^3}$ satisfying $\alpha^3+\alpha+1 = 0$. Let $S = \{1, 2, \alpha\}$ and $T = \{0, 1, 3\}$ be subsets of $\mathbb{F}_{5^3}$. Clearly, S is not an additive subgroup of $\mathbb{F}_{5^3}$. Consider the linearized polynomial

$$L(x) = x + x^5 + x^{5^2} \in \mathbb{F}_{5^3}[x].$$

Then L is a function from S into T since $L(1) = 3$, $L(2) = 1$, and $L(\alpha) = 0$. Let $f_L(x) = a_0 + a_1x + a_2x^2 \in \mathbb{F}_{5^3}[x]$ be the unique polynomial representing L on S. Solving for the coefficients, we get

$$a_0 = \frac{4\alpha}{\alpha^2 + 2\alpha + 2} \neq 0,$$

showing that $f_L(x)$ is not a linearized polynomial.

Next, we use Zhou's technique, [10], to find analogues of his result for QPP's.

Theorem 4.1.10. *Let $S \subseteq \mathbb{F}_{q^r}$, $|S| = s$, α a primitive element in $\mathbb{F}_{q^r}$, $\{\alpha_0, \alpha_1, \ldots, \alpha_{r-1}\}$ a basis of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$ and $\beta \in \mathbb{F}_{q^r} \setminus \{0\}$. If*

$$f(x) = \sum_{k=0}^{r-1} \beta^{q^k} \left(\alpha_0 + \alpha^{q^k}\alpha_1 + \alpha^{2q^k}\alpha_2 + \cdots + \alpha^{(r-1)q^k}\alpha_{r-1}\right) x^{q^k} \in \mathbb{F}_{q^r}[x], \quad (4.1.7)$$

then $f(x)$ is an $(S, f(S))$ QPP.

Proof. Since α is a primitive element of $\mathbb{F}_{q^r}$, we can write

$$S = \{\alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_s}\},$$

where $i_1, i_2, \ldots, i_s \in \mathbb{N} \cup \{0, -\infty\}$ are such that $i_j \not\equiv i_k \pmod{q^r-1}$ whenever $j \neq k$, with the convention that $\alpha^{-\infty} = 0$ and the corresponding congruence relation is interpreted as $-\infty \not\equiv i_k \pmod{q^r-1}$ for all $i_k \in \mathbb{N} \cup \{0\}$. By Lemma 2.1.14, we can

take an m-sequence $a = \{a_i\}$, $a_i \in \mathbb{F}_q$ given by $a_i = Tr(\beta\alpha^i)$ $(i \geq 0)$. Consider, for $i \in \{i_1, i_2, \ldots, i_s\}$, the numbers

$$\begin{aligned} B_i &:= \sum_{k=0}^{r-1} a_{k+i}\alpha_k = \sum_{k=0}^{r-1} \alpha_k Tr(\beta\alpha^{k+i}) \\ &= \sum_{k=0}^{r-1} \alpha_k(\beta\alpha^{k+i} + \beta^q\alpha^{(k+i)q} + \beta^{q^2}\alpha^{(k+i)q^2} + \cdots + \beta^{q^{r-1}}\alpha^{(k+i)q^{r-1}}) \\ &= \left(\sum_{k=0}^{r-1} \alpha_k\beta\alpha^k\right)\alpha^i + \left(\sum_{k=0}^{r-1} \alpha_k\beta^q\alpha^{kq}\right)(\alpha^i)^q + \cdots + \left(\sum_{k=0}^{r-1} \alpha_k\beta^{q^{r-1}}\alpha^{kq^{r-1}}\right)(\alpha^i)^{q^{r-1}}. \end{aligned}$$

The B_i's are distinct. For otherwise, there are $u, v \in \{1, 2, \ldots, s\}$ such that $u \neq v$ but

$$\sum_{k=0}^{r-1} a_{k+i_u}\alpha_k = B_{i_u} = B_{i_v} = \sum_{k=0}^{r-1} a_{k+i_v}\alpha_k.$$

Since $\{\alpha_0, \alpha_1, \ldots, \alpha_{r-1}\}$ is a basis of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$, this yields

$$a_{k+i_u} = a_{k+i_v} \quad (k = 0, 1, 2, \ldots, r-1),$$

which contradicts Lemma 2.1.15. Hence, $|\{B_i\ ;\ i = i_1, i_2, \ldots, i_s\}| = s$. Since $B_i = f(\alpha^i)$ $(i = i_1, i_2, \ldots, i_s)$, we conclude that $f(x) \in \mathbb{F}_{q^r}[x]$ is an $(S, f(S))$QPP. □

Using Remark 2.1.18, we get

Corollary 4.1.11. *Let S and T be subsets of $\mathbb{F}_{q^r}$ with $|S| = |T| = s$ and let $f(x) \in \mathbb{F}_{q^r}[x]$ be as in (4.1.7).*

(i) If $P(x) \in \mathbb{F}_{q^r}[x]$ is a bijection from $f(S)$ to T, then $(P \circ f)$ is an (S,T)QPP.

(ii) If $Q(x) \in \mathbb{F}_{q^r}[x]$ is a bijection from S to $R \subseteq \mathbb{F}_{q^r}$ and $f(R) = T$, then $(f \circ Q)$ is an (S,T)QPP.

We next give an example.

Example 4.1.12. In

$$\mathbb{F}_{2^3} \cong \mathbb{Z}_2[x]/(x^3 + x + 1) = \{c_0 + c_1\alpha + c_2\alpha^2;\ c_i \in \mathbb{Z}_2\},$$

where $\alpha^3+\alpha+1=0$, let

$$S=\{\alpha,\alpha^2,\alpha^2+\alpha,\alpha^2+\alpha+1\},\ T=\{\alpha,\alpha+1,\alpha^2+\alpha,\alpha^2+1\}$$

be subsets of $\mathbb{F}_{2^3}$. Clearly, α is a primitive element in $\mathbb{F}_{2^3}$ and $\{1,\alpha,\alpha^2\}$ is a basis of $\mathbb{F}_{2^3}$ over $\mathbb{F}_2$. Choose $\beta=\alpha+1\in\mathbb{F}_{2^3}^*$. Let $R=\{1,\alpha,\alpha+1,\alpha^2+1\}\subseteq\mathbb{F}_{2^3}$. Consider the linearized polynomial

$$\begin{aligned}f(x)&=\sum_{k=0}^{2}(\alpha+1)^{2^k}\left(1+\alpha^{2^k}\alpha+\alpha^{2\cdot 2^k}\alpha^2\right)x^{2^k}\\&=(\alpha^2+1)x+(\alpha^2+\alpha)x^2+(\alpha^2+\alpha)x^4\in\mathbb{F}_{2^3}[x].\end{aligned}$$

By Proposition 4.1.10, $f(x)$ is an $(R,f(R))$QPP, with

$$f(1)=\alpha^2+1,\ f(\alpha)=\alpha^2+\alpha,\ f(\alpha+1)=\alpha+1,\ f(\alpha^2+1)=\alpha,$$

i.e., $f(x)$ is an (R,T)QPP. Take a bijective function $g:S\to R$ given by

$$g(x)=\begin{cases}1 & \text{if } x=\alpha^2+\alpha+1,\\ \alpha & \text{if } x=\alpha^2+\alpha,\\ \alpha+1 & \text{if } x=\alpha^2,\\ \alpha^2+1 & \text{if } x=\alpha.\end{cases}$$

By Proposition 2.1.19 and directly computation,

$$P_g(x)=\alpha+x+x^2+(\alpha^2+\alpha)x^3\in\mathbb{F}_{2^3}[x]$$

is the unique polynomial of degree ≤ 3 representing g. By Corollary 4.1.11, we have

$$\begin{aligned}(f\circ P_g)(x)&=(\alpha^2+\alpha)+(\alpha^2+1)x+(\alpha+1)x^2+(\alpha+1)x^3+(\alpha^2+\alpha+1)x^6\\&\quad+(\alpha^2+\alpha)x^8+(\alpha^2+1)x^{12}\\&\equiv(\alpha^2+\alpha)+(\alpha+1)x+(\alpha+1)x^2+(\alpha+1)x^3+(\alpha^2+1)x^5\\&\quad+(\alpha^2+\alpha+1)x^6\pmod{x^{2^3}-x}\end{aligned}$$

is an (S,T)QPP.

Our next theorem is an analogue of Theorem 2.1.8 for QPP's.

Theorem 4.1.13. *Let S be a nonempty additive subgroup of $\mathbb{F}_{q^r}$ and $U = \mathbb{F}_{q^r} - S^{(q^i-q^j)}$, $i > j \geq 0$, where*

$$S^{(q^i-q^j)} = \{\beta^{q^i-q^j}; \beta \in S \setminus \{0\}\}.$$

Then

$$f(x) = x^{q^i} - ax^{q^j}$$

is an $(S, f(S))$QPP for all $a \in U \setminus \{0\}$.

Proof. For $a \in U \setminus \{0\}$, we have $0 \neq a \notin S^{(q^i-q^j)}$. Since

$$f(x) = x^{q^i} - ax^{q^j} = x^{q^j}(x^{q^i-q^j} - a),$$

$f(x)$ has only one root 0 in S and the result follows from Theorem 4.1.1. □

Corollary 4.1.14. *Let $0 < i < r$ be an integer, S a nonempty additive subgroup of $\mathbb{F}_{q^r}$ and $U = \mathbb{F}_{q^r} - S^{(q^i-1)}$, where $S^{(q^i-1)} = \{\beta^{q^i-1}; \beta \in S \setminus \{0\}\}$. Then $f(x) = x^{q^i} - ax$ is an $(S, f(S))$QPP for all $a \in U \setminus \{0\}$.*

Proof. It follows immediately from Theorem 4.1.13 by using $j = 0$. □

Example 4.1.15. In

$$\mathbb{F}_{2^4} \cong \mathbb{Z}_2[x]/(x^4 + x + 1) = \{c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3;\ c_i \in \mathbb{Z}_2\},$$

where $\alpha^4 + \alpha + 1 = 0$, let $S = \{0, \alpha, \alpha^2, \alpha^2 + \alpha\}$ be a subset of $\mathbb{F}_{2^4}$ and $U = \mathbb{F}_{2^4} - S^{(2^2-2^0)} = \mathbb{F}_{2^4} - S^{(3)}$. We have $S^{(3)} = \{0, 1, \alpha^3, \alpha^2 + \alpha^3\}$. By Theorem 4.1.13, $f(x) = x^4 - ax$ is an $(S, f(S))$QPP for each $a \in U \setminus \{0\}$.

4.2 Monomials and binomials

Regarding monomials and binomials, the following proposition is basic and its easy proof is omitted.

Proposition 4.2.1. *Let $S \subseteq \mathbb{F}_q$.*

(i) $f(x) = x$ is an (S, S)QPP.

(ii) If S is closed under multiplication, then $f(x) = ax$ is an (S, S)QPP for each $a \in S \setminus \{0\}$.

(iii) If S is closed under addition, then $f(x) = x + b$ is an (S, S)QPP for each $b \in S$.

(iv) Every linear polynomial $f(x) = ax+b \in \mathbb{F}_q[x]$ $(a \neq 0)$ is an $(S, f(S))$QPP.

Concerning monomials, the following criterion is useful.

Theorem 4.2.2. *Let d be a divisor of $q-1$. Assume that S is a cyclic multiplicative subgroup of $\mathbb{F}_q^*$ with $|S| = \frac{q-1}{d}$. Then $f(x) = x^m$ is an (S, S)QPP if and only if* $\gcd\left(m, \frac{q-1}{d}\right) = 1$.

Proof. Writing $S = \langle a \rangle$ in terms of its generator α, we have

$$\begin{aligned} \gcd\left(m, \frac{q-1}{d}\right) = 1 &\iff \langle a^m \rangle \text{ is a cyclic subgroup of } \mathbb{F}_q \setminus \{0\} \text{ of order } \frac{q-1}{d} \\ &\iff \langle a^m \rangle = \langle a \rangle = S \\ &\iff f(x) = x^m \text{ is an } (S, S)\text{QPP}. \end{aligned}$$

□

Corollary 4.2.3. *Let $q = p^n$ and let d be a divisor $q-1$. Assume that S is a cyclic multiplicative subgroup of $\mathbb{F}_q^*$ with $|S| = \frac{q-1}{d}$. Then for each $j \in \{0, 1, \ldots, n-1\}$, $f(x) = x^{p^j}$ is an (S, S)QPP.*

Proof. By Theorem 4.2.2, it suffices to verify that $\gcd\left(p^j, \frac{q-1}{d}\right) = 1$. Should $\gcd\left(p^j, \frac{q-1}{d}\right) \neq 1$, then $p \mid \frac{p^n-1}{d}$, a contradiction. □

For binomials, we have the following general results.

Theorem 4.2.4. *Let $0 \in S \subseteq \mathbb{F}_q$ and let $f(x) = x^i - ax^j$, where $i > j \geq 1$ and $a \in \mathbb{F}_q \setminus \{0\}$.*

(i) If $a \in S^{(i-j)} := \{\alpha^{i-j}; \alpha \in S\}$, then $f(x)$ is not an $(S, f(S))QPP$.

(ii) $f(x)$ is an $(S, f(S))QPP$ if and only if $a \notin \left\{\frac{y^i-z^i}{y^j-z^j}; y, z \in S, y \neq z\right\} =: S_2^{(i,j)}$.

(iii) Let $e = \gcd(i, j)$, $i' = i/e$, $j' = j/e$. If S is closed under multiplication, then $f(x)$ is an $(S, f(S))QPP$ if and only if $\gcd(e, q-1) = 1$ and $h(x) = x^{i'} - ax^{j'}$ is an $(S, h(S))QPP$.

Proof. (i) Let $\beta \in S \setminus \{0\}$ be such that $a = \beta^{i-j}$. Thus

$$f(\beta) = \beta^j(\beta^{i-j} - a) = 0 = f(0),$$

showing that f is not injective on S.

(ii) Assume that $a \in S_2^{(i,j)}$, i.e. $a = \frac{y^i-z^i}{y^j-z^j}$ for some $y, z \in S$, $y \neq z$. Then

$$f(x) = x^i - \left(\frac{y^i - z^i}{y^j - z^j}\right)x^j = x^j\left(\frac{x^{i-j}(y^j - z^j) - (y^i - z^i)}{y^j - z^j}\right). \tag{4.2.1}$$

Substituting $x = y$ and $x = z$ in (4.2.1), we get that $f(y) = f(z)$. Hence $f(x)$ is not an $(S, f(S))$QPP. Conversely, suppose that there exist $b, c \in S$, $b \neq c$ such that $f(b) = f(c)$. Then

$$b^i - ab^j = f(b) = f(c) = c^i - ac^j,$$

so $b^i - c^i = a(b^j - c^j)$ implies that $a = \frac{b^i-c^i}{b^j-c^j}$ which is in $S_2^{(i,j)}$.

(iii) We have $f(x) = (h \circ g)(x)$ where $h(x) = x^{i'} - ax^{j'}$ and $g(x) = x^e$. By Theorem 2.1.4(ii), $g(x)$ is a PP of $\mathbb{F}_q$ if and only if $\gcd(e, q-1) = 1$. Since S is closed

under multiplication, then $g(x)$ is an (S,S)QPP if and only if $\gcd(e, q-1) = 1$. Using Remark 2.1.18, the proof is completed. □

When $a \notin S^{(i-j)}$, there are polynomials $f(x) = x^i - ax^j$ which are $(S, f(S))$QPP as well as those which are not, as shown in the following example.

Example 4.2.5. In

$$\mathbb{F}_{3^2} \cong \mathbb{Z}_3[x]/(x^2+1) = \{c_0 + c_1\alpha;\ c_i \in \mathbb{Z}_3\},$$

where $\alpha^2 + 1 = 0$, let $S_1 = \{0, 2, \alpha+1\}$ and $S_2 = \{0, 2, \alpha+2\}$ be subsets of $\mathbb{F}_{3^2}$. Consider the binomial

$$f(x) = x^3 - x^2 \in \mathbb{F}_{3^2}[x].$$

Clearly, $1 \notin S_1^{(3-2)}$ and $1 \notin S_2^{(3-2)}$. Since $f(0) = 0, f(2) = 1 = f(\alpha+1)$ and $f(\alpha+2) = \alpha+2$, we see that $f(x) = x^3 - x^2$ is not an $(S_1, f(S_1))$QPP but it is an $(S_2, f(S_2))$QPP.

The next proposition is obtained immediately from Theorem 2.1.4(ii).

Proposition 4.2.6. *Let $i \in \mathbb{N}$, $a \in \mathbb{F}_q$ and $S \subseteq \mathbb{F}_q$. If $\gcd(i, q-1) = 1$, then $f(x) = x^i - a$ is an $(S, f(S))$QPP.*

4.3 Other forms

Next, by using Remark 2.1.18 about compositing functions, we derive other forms of QPP's.

Proposition 4.3.1. *Let S be a nonempty subset of $\mathbb{F}_q$ with closed under multiplication and $i \in \mathbb{N}$ such that $\gcd(i, q-1) = 1$. If $g(x) \in \mathbb{F}_q[x]$ is an $(S, g(S))$QPP, then $f(x) = g(x^i)$ is an $(S, f(S))$QPP.*

Proof. It follows from Theorem 2.1.4(ii) and Remark 2.1.18. □

Proposition 4.3.2. *Let $S, T \subset \mathbb{F}_q$ with $|S| = |T|$, $i \in \mathbb{N}$ such that $\gcd(i, q-1) = 1$ and u a positive divisor of $q-1$. Let $g(x) \in \mathbb{F}_q[x]$ be such that $g(x^i)$ has no nonzero root in $\mathbb{F}_q$. Then $f(x) = x^i \left(g(x^i)\right)^{(q-1)/i}$ is an $(S, f(S))QPP$. And if $h(x)$ is an $(f(S), T))QPP$, then $(h \circ f)(x) = h\left(x^i \left(g(x^i)\right)^{(q-1)/i}\right)$ is an $(S, T)QPP$.*

Proof. From Theorem 2.1.11, we get that $f(x)$ is a PP of $\mathbb{F}_q$, so $f(x)$ is also an $(S, f(S))$QPP. The second part holds from Remark 2.1.18. □