Vichian Laohakosol; Suphawan Janphaisaeng

Quasi-permutation polynomials

Czechoslovak Mathematical Journal, Vol. 60 (2010), No. 2, 457–488

Persistent URL: http://dml.cz/dmlcz/140582

Czechoslovak Mathematical Journal, 60 (135) (2010), 457–488

QUASI-PERMUTATION POLYNOMIALS

Vichian Laohakosol, Bangkok, Suphawan Janphaisaeng, Phitsanulok

(Received November 25, 2008)

Abstract. A quasi-permutation polynomial is a polynomial which is a bijection from one subset of a finite field onto another with the same number of elements. This is a natural generalization of the familiar permutation polynomials. Basic properties of quasi-permutation polynomials are derived. General criteria for a quasi-permutation polynomial extending the well-known Hermite's criterion for permutation polynomials as well as a number of other criteria depending on the permuted domain and range are established. Different types of quasi-permutation polynomials and the problem of counting quasi-permutation polynomials of fixed degree are investigated.

Keywords: finite fields, permutation polynomials

MSC 2010: 11T55, 12Y05

1. Introduction

Let $\mathbb{F}_q$ denote a finite field of q elements, with q being a power of a fixed prime p. A permutation polynomial (over $\mathbb{F}_q$), abbreviated as PP, is a polynomial which is a bijection of $\mathbb{F}_q$ onto itself. The problem of finding necessary and/or sufficient conditions for permutation polynomials has been a subject of numerous investigations, see e.g. [5], [6], [8], [9], or Chapter 7 of [7]. The best known and most used criterion is due to Hermite, see e.g. Theorem 7.4 of [7], which states that $f(x) \in \mathbb{F}_q[x]$ is a PP if and only if the following two conditions hold:

(1) f has exactly one root in $\mathbb{F}_q$;

(2) for each integer t with $1 \leqslant t \leqslant q-2$ and $t \not\equiv 0 \bmod p$, the reduction of $(f(x))^t \bmod (x^q - x)$ has degree $\leqslant q-2$.

This work was supported by the Commission on Higher Education, the Thailand Research Fund RTA 51890005 and Kasetsart University Institute for Advanced Studies.

In a number of situations, it is necessary to consider not only PP but their natural generalization, here referred to as a *quasi-permutation polynomials*, abbreviated by QPP, which we now define.

Let S and T be two nonempty subsets of $\mathbb{F}_q$ with the same number of elements $s = |S| = |T|$; this terminology will be kept fixed throughout the paper. A polynomial $P(x) \in \mathbb{F}_q[x]$ is called an (S,T)-*quasi-permutation polynomial*, abbreviated by (S,T)QPP or simply QPP when both S and T are left understood, if $\{P(c);\ c \in S\} = T$. Clearly, when $S = T = \mathbb{F}_q$, $P(x)$ is the usual PP. Without imposing any structure on the sets S and T, it seems hardly possible to extract any useful information about QPP's. It is thus surprising that quite a general criterion for QPP can be derived irrespective of what the sets S and T are, and this is carried out in Section 3. Yet, most anticipated results are valid only when confined to certain structures of the sets S and T. Note also that merely imposing the structure of being a group under multiplication on either S or T already forces it to be multiplicatively invertible because each nonzero element $\alpha \in \mathbb{F}_q$ satisfies $\alpha^{q-1} = 1$. Therefore, imposing too many structures on either the set S or T, such as being a ring, would turn it into a field, which is never considered here as it is part of the PP's situation.

In the next section, basic properties of QPP are gathered. In Section 3, several general criteria for a polynomial to be a QPP are proved. In Section 4, QPP's which are linearized polynomials are investigated. In Section 5, characterizations of QPP's using the concept of characters are derived, while Section 6 deals with monomials, binomials, and other forms of QPP's are investigated. The final section deals with the problem of counting the number of QPP's of a fixed degree.

2. Basic properties

We start by investigating the representation of functions by polynomials of interest at hand. A simple interpolation technique shows immediately that any function from S to T is uniquely representable as a polynomial of degree $\leqslant s-1$.

Proposition 2.1. *If $f\colon S \to T$ is a function, where S and T are nonempty subsets of $\mathbb{F}_q$ with the same number of elements $|S| = |T| = s \leqslant q$, then there exists a polynomial $P \in \mathbb{F}_q[x]$ with $\deg P \leqslant s-1$ uniquely representing f in the sense that $P(c) = f(c)$ for all $c \in S$.*

Proof. Let $S = \{a_1, a_2, \ldots, a_s\}$ and let

$$P(x) = c_{s-1}x^{s-1} + c_{s-2}x^{s-2} + \ldots + c_1 x + c_0 \in \mathbb{F}_q[x].$$

The system of linear equations

$$c_0 + c_1 a_i + c_2 a_i^2 + \ldots + c_{s-1} a_i^{s-1} = f(a_i) \quad (i = 1, \ldots, s)$$

uniquely determines the coefficients c_i because its coefficient matrix (a_i^j) has a nonzero Vandermonde determinant. This guarantees the existence of such a polynomial. Indeed, such polynomial $P \in \mathbb{F}_q[x]$ can be obtained from the Lagrange polynomial interpolating at the points $c \in S$, see e.g. Section 2.1 in Chapter V of [4].

To prove uniqueness, assume that there is another polynomial $h \in \mathbb{F}_q[x]$ with $\deg h \leqslant s-1$ such that $h(c) = f(c)$ for all $c \in S$. Then $P - h \in \mathbb{F}_q[x]$ would be a polynomial of degree $\leqslant s-1$ which vanishes at s distinct points in a finite field, forcing $h \equiv P$. □

Remark. It is worth remarking that should we be able to obtain an injective function on S, it is always possible to compose it with a unique polynomial of degree $\leqslant s-1$ (guaranteed by Proposition 2.1) sending $f(S)$ bijectively onto T, to get an (S,T)QPP. This remark enables us generally to find QPP's over the domain S without having to worry about the set T.

The shapes of polynomials of degree $\leqslant s-1$ representing functions from S into T can be made explicit as shown in the following proposition. Recall that $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$ is a cyclic multiplicative group of order $q-1$, so we can write $\mathbb{F}_q^* = \langle \alpha \rangle$, where α is a fixed generator of $\mathbb{F}_q^*$. Each element $\beta \in \mathbb{F}_q$ can thus be written as $\beta = \alpha^i$ for some $i \in \mathbb{N} \cup \{0, -\infty\}$, with the convention that $\alpha^{-\infty} = 0$. If S is a subset of $\mathbb{F}_q$ with $|S| = s$, then we put

$$S = \{\alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_s}\} \tag{2.1}$$

for some distinct $i_1, i_2, \ldots, i_s \in \mathbb{N} \cup \{0, -\infty\}$ satisfying $i_j \not\equiv i_k \bmod (q-1)$, whenever $j \neq k$.

Proposition 2.2. *Let S and T be two nonempty subsets of $\mathbb{F}_q$ having the same number of elements $|S| = |T| = s \leqslant q$ with S written as in* (2.1). *Let*

$$W = \begin{pmatrix} 1 & \alpha^{i_1} & \ldots & (\alpha^{i_1})^{s-1} \\ 1 & \alpha^{i_2} & \ldots & (\alpha^{i_2})^{s-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{i_s} & \ldots & (\alpha^{i_s})^{s-1} \end{pmatrix}, \quad V = \det W,$$

and let $C_{k,j}$ denote the (k,j)-cofactor of W. Then

$$P(x) = a_0 + a_1 x + \ldots + a_{s-1} x^{s-1} \in \mathbb{F}_q[x]$$

is a polynomial of degree $\leqslant s-1$ *representing a function sending* S *into* T *if and only if each of its coefficients* a_j *is a* T*-linear combination of* $C_{1,j+1}/V, C_{2,j+1}/V, \ldots,$ $C_{s,j+1}/V$, *i.e.,*

$$a_j = t_1\frac{C_{1,j+1}}{V} + t_2\frac{C_{2,j+1}}{V} + \ldots + t_s\frac{C_{s,j+1}}{V} \quad (j = 0, 1, \ldots, s-1)$$

for some $t_1, \ldots, t_s \in T$.

Moreover, the number of such polynomials is equal to the number of functions from S *to* T *which is* s^s.

P r o o f. Consider

$$\begin{aligned} U &:= (f(\alpha^{i_1})\ f(\alpha^{i_2})\ f(\alpha^{i_3})\ \ldots\ f(\alpha^{i_s}))^t \\ &= (P(\alpha^{i_1})\ P(\alpha^{i_2})\ P(\alpha^{i_3})\ \ldots\ P(\alpha^{i_s}))^t \in T^s, \end{aligned}$$

where t denotes the transpose of a matrix. Then $WX = U$ where

$$X = (a_0\ a_1\ a_2\ \ldots\ a_{s-1})^t.$$

Since the matrix W has a nonzero Vandermonde determinant, the first part follows at once from Cramer's rule. Note that each function f gives rise to one vector U. Each vector U in turn gives rise to one particular set of coefficients $a_0, \ldots, a_{s-1}$, and vice versa. The second part is thus immediate. □

Next, we count the number of QPP's. Denote the set of all polynomials of degree $\leqslant q-1$ in $\mathbb{F}_q[x]$ by

$$\mathcal{P}_q := \{f \in \mathbb{F}_q[x];\ \deg f \leqslant q-1\};$$

the set of those polynomials in $\mathcal{P}_q$ which represent functions from S to T by

$$\mathcal{P}_q(S,T) := \{f \in \mathcal{P}_q;\ f\colon\ S \to T\};$$

the set of all polynomials of degree $\leqslant s-1$ in $\mathbb{F}_q[x]$ by

$$\mathcal{P}_s := \{f \in \mathbb{F}_q[x];\ \deg f \leqslant s-1\};$$

and the set of those polynomials in $\mathcal{P}_s$ which uniquely represent functions from S to T by

$$\mathcal{P}_s(S,T) := \{f \in \mathcal{P}_s;\ f\colon\ S \to T\}.$$

Further, let

$$\begin{aligned} N_q(S,T) &:= |\{f \in \mathcal{P}_q(S,T);\ f \text{ is an } (S,T)\text{QPP}\}|, \\ N_s(S,T) &:= |\{f \in \mathcal{P}_s(S,T);\ f \text{ is an } (S,T)\text{QPP}\}|. \end{aligned}$$

The next result gives information on these sets.

Proposition 2.3.

(i) *We have* $|\mathcal{P}_s(S,T)| = s^s$ *and* $N_s(S,T) = s!$.

(ii) *To each* $f \in \mathcal{P}_s(S,T)$ *there correspond exactly* q^{q-s} *polynomials in* $\mathcal{P}_q(S,T)$ *whose restriction to* S *is identical with* f *and so*

$$|\mathcal{P}_q(S,T)| = s^s \cdot q^{q-s}.$$

(iii) *To each* $f \in \mathcal{P}_s(S,T)$ *which is an* (S,T)*QPP there correspond exactly* q^{q-s} (S,T)*QPP's in* $\mathcal{P}_q(S,T)$ *whose restriction to* S *is identical with* f *and so*

$$N_q(S,T) = s! \cdot q^{q-s}.$$

P r o o f. (i) By Proposition 2.1, each function from S into T is uniquely representable as a polynomial in $\mathbb{F}_q[x]$ of degree $\leqslant s-1$ and since there are s^s such functions, we deduce that $|\mathcal{P}_s(S,T)| = s^s$. Since there are altogether $s!$ (S,T)-permutations, we have $N_s(S,T) = s!$.

(ii) Each polynomial in $\mathcal{P}_s(S,T)$ is also a function from S to T and each polynomial in $\mathcal{P}_q(S,T)$ is a function from $\mathbb{F}_q$ to $\mathbb{F}_q$ whose restriction to S is mapped into T. Since $\mathcal{P}_s(S,T) \subset \mathcal{P}_q(S,T)$, a polynomial in $\mathcal{P}_s(S,T)$ is elevated to be a polynomial in $\mathcal{P}_q(S,T)$ by assigning any of the q values in $\mathbb{F}_q$ to each of the remaining $q-s$ elements in the domain and the first assertion is immediate. The second assertion follows by using (i).

The proof of (iii) is similar to that of (ii). □

Since the number of functions: $\mathbb{F}_q \to \mathbb{F}_q$ is q^q and the number of functions: $S \to T$ is s^s, the number of functions $f\colon \mathbb{F}_q \to \mathbb{F}_q$ with $f(S) \nsubseteq T$ is $q^q - s^s q^{q-s}$ which is equal to the number of polynomials $f(x) \in \mathbb{F}_q[x]$ with $f(S) \nsubseteq T$ and $\deg f \leqslant q-1$ because any function from $\mathbb{F}_q$ into $\mathbb{F}_q$ is uniquely representable as a polynomial of degree $< q$. Moreover, if m is the number of bijective functions: $S \to T$, then the number of (S,T)QPP's of degree $\leqslant q-1$ is mq^{q-s}.

We record next, without proof, the straight-forward fact that the set of QPP's is closed under multiplication by nonzero elements of T and is closed under addition by elements of T provided the set T is so.

Proposition 2.4. *Let* $f(x) \in \mathbb{F}_q[x]$, $S,T \subseteq \mathbb{F}_q$ *with* $|S| = |T|$, $c \in T \setminus \{0\}$ *and* $b \in T$. *Assume that* $f(x)$ *is an* (S,T)*QPP.*

(i) *If* T *is closed under multiplication, then* $cf(x)$ *is an* (S,T)*QPP.*

(ii) *If* T *is closed under addition, then* $f(x)+b$ *is an* (S,T)*QPP.*

We end this section with remarks about group structure. It is well known, see e.g. Section 3 in Chapter 7 of [7], that the set $A(\mathbb{F}_q)$ of all PP's of degree $\leqslant q-1$

over $\mathbb{F}_q$ forms a group under composition and reduction modulo $x^q - x$. This group is isomorphic to S_q, the symmetric group on q letters. Also known is the fact, Theorem 7.18 of [7], that this group is generated by x^{q-2} and all linear polynomials over $\mathbb{F}_q$. In the case of QPP's, we have the following related result.

Theorem 2.5. *Let $S \subseteq \mathbb{F}_q$ and let*

$$SA(\mathbb{F}_q) := \{f(x) \in \mathbb{F}_q[x];\ f(x) \text{ is an } (S,S)\text{QPP}\} \cap A(\mathbb{F}_q).$$

Then $SA(\mathbb{F}_q)$ is a subgroup of $A(\mathbb{F}_q)$.

P r o o f. If $f, g \in SA(\mathbb{F}_q)$, then f and g are both (S,S)QPP and PP. Consequently, g^{-1} is both (S,S)QPP and PP implying that so is $f \circ g^{-1}$. □

3. 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, [1].

Theorem 3.1. *Let S and T be nonempty subsets of $\mathbb{F}_q$ containing 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 $A_k(x) := a_{s-1,k}x^{s-1} + a_{s-2,k}x^{s-2} + \ldots + a_{1,k}x + a_{0,k} \in \mathbb{F}_q[x]$. Let

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

and

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

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

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

where the empty product is taken to be 1.

P r o o f. For $k \in \mathbb{N}$ we have

$$\sum_{b\in S}(P(b))^k = \sum_{b\in S}[B_k(b)S(b) + A_k(b)] = \sum_{b\in S} A_k(b) \tag{3.1}$$

$$= a_{s-1,k}\sum_{b\in S} b^{s-1} + a_{s-2,k}\sum_{b\in S} b^{s-2} + \ldots + a_{1,k}\sum_{b\in S} b + sa_{0,k}. \tag{3.2}$$

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

$$(P(b))^k = (P(b))^{k+l(q-1)}, \tag{3.3}$$

$$(P(b))^{q-1} = (P(b))^{l(q-1)}. \tag{3.4}$$

Let

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

so that $Q(x)$ is monic and $\deg Q(x) = s$. By (3.2), (3.3) and (3.4) we have

$$\begin{aligned}
\frac{Q'(x)}{Q(x)} &= \sum_{b\in S}\frac{1}{x-P(b)} = \frac{1}{x}\sum_{b\in S}(P(b))^0 + \sum_{k=1}^{\infty}\frac{1}{x^{k+1}}\sum_{b\in S}(P(b))^k \\
&= \frac{s}{x} + \sum_{k\equiv 1 \bmod(q-1)}\frac{1}{x^{k+1}}\sum_{b\in S}P(b) \\
&\quad + \sum_{k\equiv 2 \bmod(q-1)}\frac{1}{x^{k+1}}\sum_{b\in S}(P(b))^2 \\
&\quad + \ldots + \sum_{k\equiv q-2 \bmod(q-1)}\frac{1}{x^{k+1}}\sum_{b\in S}(P(b))^{q-2} \\
&\quad + \sum_{k\equiv 0 \bmod(q-1),\, k\neq 0}\frac{1}{x^{k+1}}\sum_{b\in S}(P(b))^{q-1} \\
&= \frac{sx^{q-1} + \Big(\sum\limits_{b\in S}P(b)\Big)x^{q-2} + \ldots}{x(x^{q-1}-1)} \\
&\quad + \frac{\Big(\sum\limits_{b\in S}(P(b))^{q-2}\Big)x + \Big(\sum\limits_{b\in S}(P(b))^{q-1}\Big) - s}{x(x^{q-1}-1)} \\
&= \frac{sx^{q-1} + \Big(\sum\limits_{b\in S}A_1(b)\Big)x^{q-2} + \ldots}{x(x^{q-1}-1)} \\
&\quad + \frac{\Big(\sum\limits_{b\in S}A_{q-2}(b)\Big)x + \Big(\sum\limits_{b\in S}A_{q-1}(b)\Big) - s}{x(x^{q-1}-1)} = \frac{T(x)}{x(x^{q-1}-1)}
\end{aligned} \tag{3.5}$$

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

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

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

where $W(x) = T(x) \Big/ \prod_{\alpha \in \mathbb{F}_q \setminus T} (x-\alpha) \in \mathbb{F}_q[x]$. Since $\deg Q(x) = s$ and $Q(x)$ is monic, we have

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

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

$$\frac{U_1(x)}{U_2(x)} = \frac{T(x)}{x(x^{q-1}-1)} = \frac{Q'(x)}{Q(x)}, \tag{3.6}$$

where $U_1(x)/U_2(x)$ is in reduced form. Then $\deg U_2(x) \leqslant \deg Q(x)$. Assume that $P(x)$ is an (S,T)QPP. Then $Q(x)$ has no repeated root(s) 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 yielding $Q(x) = U_2(x)$ and $Q'(x) = U_1(x)$. Since $x(x^{q-1}-1) = \prod_{\alpha \in \mathbb{F}_q} (x-\alpha)$ and $U_2(x) = \prod_{\alpha \in T} (x-\alpha)$, by (3.6) we get

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

□

Using Theorem 3.1, we now give an example of a QPP which is not a PP.

Example. 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, we have

$$\begin{aligned}
f(x) &= 0 \cdot S(x) + A_1(x), \quad A_1(x) = x^2 + 1,\\
(f(x))^2 &= (x+1)S(x) + A_2(x), \quad A_2(x) = 2x + 1,\\
(f(x))^3 &= (x^3 + x^2 + x + 3)S(x) + A_3(x), \quad A_3(x) = 3x^2 + x + 1,\\
(f(x))^4 &= (x^5 + x^4 + 2x^3 + 4x^2 + 4x + 2)S(x) + A_4(x), \quad A_4(x) = 4x^2 - x + 1.
\end{aligned}$$

Thus, $T(x) = 3x^4 + 3x^3 + 4x - 1 = (x-3)(x-4)(3x^2 + 4x + 2)$, and so $\gcd(T(x), x(x^4-1)) = (x-3)(x-4) = \prod_{\alpha \in \mathbb{F}_5 \setminus T} (x - \alpha)$, showing, by Theorem 3.1, that $f(x)$ is a QPP.

Most of the known criteria for PP's are immediate consequences of Theorem 3.1; for instance, taking $S(x) = x^q - x$, we get:

Corollary 3.2. *Let $P(x) \in \mathbb{F}_q[x]$ and*

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

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

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

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 3.2, we obtain the classical Hermite's criterion.

Corollary 3.3. *Let $P(x)$ and $R(x)$ be defined as in Corollary* 3.2. *Then $P(x)$ is a PP if and only if the following two conditions hold:*

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

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

P r o o f. To invoke upon the result of Corollary 3.2, we need to show that the two conditions are equivalent to $R(x)$ and $x(x^{q-1} - 1)$ being 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,

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

i.e., $a_{q-1,k} = 0$ $(1 \leqslant k < q - 1)$ and $a_{q-1,q-1} = 1$, rendering (i) and (ii) true. □

In Corollary 3.3, if (i) holds but (ii) does not, then $Q(x)$ is a linearized polynomial because from (3.5) we have

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

i.e., $Q'(x) = 0$, implying that each monomial in Q has degree equal to a multiple of $p = \operatorname{char} \mathbb{F}_q$.

The main result of [1] is another consequence.

Corollary 3.4. *Let $P(x)$ and $R(x)$ be defined as in Corollary* 3.2. *Then $P(x)$ is a PP if and only if the following two conditions hold:*

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

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

P r o o f. If $P(x)$ is a PP, then (i) holds by Corollary 3.3, while (ii) holds by the definition of PP. On the other hand, assume (i) and (ii) hold. From (ii) and (3.2) we get

$$-a_{q-1,q-1} = \sum_{b\in\mathbb{F}_q} (P(b))^{q-1} = 0 + \underbrace{1+1+\ldots+1}_{(q-1)\text{times}} = -1, \tag{3.7}$$

i.e., $\deg A_{q-1}(x) = q-1$, and so $P(x)$ is a PP by Corollary 3.3. □

There is an alternative formulation similar to Theorem 3.1, whose proof, which is the same as that of Theorem 3.1, is omitted here.

Proposition 3.5. *Let $S_p(x) = \prod_{\alpha\in S} (x - P(\alpha))$. For $k \in \mathbb{N}$ put*

$$x^k = B_{k_p}(x)S_p(x) + A_{k_p}(x), \tag{3.8}$$

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

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

and

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

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

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

where the empty product is defined as 1.

Though the statements of Theorem 3.1 and Proposition 3.5 are different, the corollaries of Theorem 3.1 listed above and their counterparts derivable from Proposition 3.5 are identical because $T_p(x) = T(x)$. To see this, it is enough to verify that for each $k \in \mathbb{N}$,

$$\sum_{b\in S} A_k(b) = \sum_{b\in S} A_{k_p}(P(b)). \tag{3.9}$$

From (3.8) we have

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

from which together with (3.1) the identity (3.9) follows.

4. Linearized polynomials

Let q be a prime power and $n \in \mathbb{N}$. Recall from [7] that $L(x) \in \mathbb{F}_{q^r}[x]$, $r \in \mathbb{N}$, is called a *linearized* polynomial, or *q-polynomial*, if it is of the form

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

For such polynomials we have the following criterion for QPP.

Theorem 4.1. *Let S be an additive subgroup of $\mathbb{F}_{q^r}$, $T \subseteq \mathbb{F}_{q^r}$ with $0 \in T$ and $|S| = |T|$. 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.*

P r o o f. 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 $L(x)$ has only 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

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

□

The requirement that S is an additive group in Theorem 4.1 cannot be omitted as seen in the following example.

Example. 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 $L(x)$ 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.

The following result which is Theorem 7.9 in [7] is an immediate consequence of Theorem 4.1.

Corollary 4.2. *Every linearized polynomial in $\mathbb{F}_q[x]$ is a PP if and only if it has only the root 0 in $\mathbb{F}_q$.*

Making use of the notion of the vector space, linearized polynomials provide a large class of PP's and QPP's as shown in the next result which itself is of independent interest. Before stating the theorem, we recall some facts from linear algebra. Let S be an additive subgroup of $\mathbb{F}_{q^r}$ and $0 \in T \subseteq \mathbb{F}_{q^r}$ with $|S| = |T|$. 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 4.3. *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*

$$\alpha_i := \beta_i + \beta_i^{q^d} + \beta_i^{q^{2d}} + \ldots + \beta_i^{q^{(k-1)d}} \quad (i = 0, 1, 2, \ldots, d-1). \tag{4.1}$$

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

$$L(x) = \sum_{i=0}^{r-1} a_i x^{q^i} \in \mathbb{F}_{q^r}[x], \quad \text{with } a_t = a_i \text{ whenever } t \equiv i \bmod d. \tag{4.2}$$

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

$$A = \begin{pmatrix} a_0 & a_{d-1}^{q} & a_{d-2}^{q^2} & \dots & a_1^{q^{d-1}} \\ a_1 & a_0^{q} & a_{d-1}^{q^2} & \dots & a_2^{q^{d-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{d-1} & a_{d-2}^{q} & a_{d-3}^{q^2} & \dots & a_0^{q^{d-1}} \end{pmatrix}. \tag{4.3}$$

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

P r o o f. Write

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

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

$$\begin{aligned} \gamma_m^{q^j} &= a_0^{q^j} \beta_m^{q^j} + a_1^{q^j} \beta_m^{q^{j+1}} + \dots + a_{r-j}^{q^j} \beta_m^{q^{j+r-j}} + \dots + a_{r-1}^{q^j} \beta_m^{q^{j+r-1}} \\ &= a_{j-j}^{q^j} \beta_m^{q^j} + a_{(j+1)-j}^{q^j} \beta_m^{q^{j+1}} + \dots + a_{0-j}^{q^j} \beta_m^{q^0} + \dots + a_{(j-1)-j}^{q^j} \beta_m^{q^{j-1}} \\ &= \sum_{i=0}^{r-1} a_{i-j}^{q^j} \beta_m^{q^i}. \end{aligned} \tag{4.4}$$

Substituting into (4.2), we get

$$\begin{pmatrix} \gamma_0 & \gamma_0^{q} & \dots & \gamma_0^{q^{r-1}} \\ \gamma_1 & \gamma_1^{q} & \dots & \gamma_1^{q^{r-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_{d-1} & \gamma_{d-1}^{q} & \dots & \gamma_{d-1}^{q^{r-1}} \end{pmatrix} = \begin{pmatrix} \beta_0 & \beta_0^{q} & \dots & \beta_0^{q^{r-1}} \\ \beta_1 & \beta_1^{q} & \dots & \beta_1^{q^{r-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{d-1} & \beta_{d-1}^{q} & \dots & \beta_{d-1}^{q^{r-1}} \end{pmatrix} \begin{pmatrix} a_0 & a_{r-1}^{q} & \dots & a_1^{q^{r-1}} \\ a_1 & a_0^{q} & \dots & a_2^{q^{r-1}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{d-1} & a_{d-2}^{q} & \dots & a_d^{q^{r-1}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r-1} & a_{r-2}^{q} & \dots & a_0^{q^{r-1}} \end{pmatrix}. \tag{4.5}$$

Equating the top left hand corner, we get

$$\Delta = B_1 A_1 + B_2 A_2 + \dots + B_k A_k,$$

where

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

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

$$B_l = \begin{pmatrix} \beta_0^{q^{(l-1)d}} & \beta_0^{q^{(l-1)d+1}} & \dots & \beta_0^{q^{ld-1}} \\ \beta_1^{q^{(l-1)d}} & \beta_1^{q^{(l-1)d+1}} & \dots & \beta_1^{q^{ld-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{d-1}^{q^{(l-1)d}} & \beta_{d-1}^{q^{(l-1)d+1}} & \dots & \beta_{d-1}^{q^{ld-1}} \end{pmatrix},$$

$$A_l = \begin{pmatrix} a_{(l-1)d} & a_{(l-1)d-1}^q & \dots & a_{(l-2)d+1}^{q^{d-1}} \\ a_{(l-1)d+1} & a_{(l-1)d}^q & \dots & a_{(l-2)d+2}^{q^{d-1}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{ld-1} & a_{ld-2}^q & \dots & a_{(l-1)d}^{q^{d-1}} \end{pmatrix}.$$

Since $a_t = a_i$ if $t \equiv i \bmod d$, we have

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

Thus,

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

where, using (4.1),

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

(i) Assume that $\alpha_0, \alpha_1, \dots, \alpha_{d-1}$ are linearly independent over $\mathbb{F}_q$. By Lemma 3.51 of [7], 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 3.51 in [7].

(ii) If $\alpha_0, \alpha_1, \dots, \alpha_{d-1}$ are linearly dependent over $\mathbb{F}_q$, then Lemma 3.51 of [7] implies $\det B = 0$, and so $\det \Delta = 0$. This yields that $\gamma_0, \gamma_1, \dots, \gamma_{d-1}$ are linearly dependent over $\mathbb{F}_q$, i.e., there are $b_0, b_1, \dots, b_{d-1} \in \mathbb{F}_q$ not all zero such that

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

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

Remarks. 1. The special case where $d = r$, which forces all the matrices in (4.5) to be square, shows in particular that $L(x)$ is an (S,T)QPP if and only if

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

This special case is a generalization of Theorem 7.24 in [7].

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

Pushing the result in Theorem 4.3 (i) a little further, we get

Corollary 4.4. *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*

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

Let $L\colon S \to T$ be a linearized polynomial of the form (4.2) satisfying $a_t = a_i$ whenever $t \equiv i \bmod d$. 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 (4.3), then $L(x)$ is an (S,T)QPP.

P r o o f. By Theorem 4.1, $L(x)$ 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 when $L(\beta_0), L(\beta_1), \ldots, L(\beta_{d-1})$ are linearly independent over $\mathbb{F}_q$ whenever $\beta_0, \beta_1, \ldots, \beta_{d-1} \in S$ are linearly independent over $\mathbb{F}_q$. Theorem 4.3 then 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 4.3 do occur.

Example. In

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

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

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

Note that both S_1 and S_2 are additive subgroups of $\mathbb{F}_{2^4}$. For each $i \in \{1,2\}$, consider the linearized polynomial $L\colon\ S_i \to L(S_i)$ 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 $\beta_0 + \beta_0^{2^2} = \alpha + \alpha^4 = 1$, $\beta_1 + \beta_1^{2^2} = \alpha^2 + \alpha^8 = 1$, both of which are clearly linearly dependent over $\mathbb{F}_2$. Since $L(\beta_0) = L(\beta_1) = a_0 + a_1$, 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 $\beta_0 + \beta_0^{2^2} = 1$ and $\beta_1 + \beta_1^{2^2} = \alpha^2 + \alpha$, both of which are linearly independent over $\mathbb{F}_2$. By Theorem 4.3, $\det \begin{pmatrix} a_0 & a_1^2 \\ a_1 & a_0^2 \end{pmatrix} \neq 0$ if and only if $L(\beta_0)$ and $L(\beta_1)$ are linearly independent over $\mathbb{F}_2$.

Observe that the linearized polynomials L over $\mathbb{F}_{q^r}$ in Theorem 4.3 and Corollary 4.4 are of degree $\leqslant q^{r-1}$. As seen in Proposition 2.1, these linearized polynomials may be not the unique polynomials of degree $\leqslant s-1$ representing functions $L\colon\ S \to T$. This leads us to ask whether the unique polynomial of degree $\leqslant s-1$ representing a function equivalent to a linearized polynomial $L\colon\ S \to T$ 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 example right after.

Proposition 4.5. *Let S be an additive subgroup of $\mathbb{F}_{p^r}$ and $0 \in T \subseteq \mathbb{F}_{p^r}$ with $|S| = |T| = s \leqslant p^r$. If $L\colon\ S \to T$ is a linearized polynomial of the form*

$$L(x) = \sum_{i=0}^{r-1} a_i x^{p^i} \in \mathbb{F}_{p^r}[x], \tag{4.6}$$

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

P r o o f. By Proposition 2.1, let the unique polynomial $f\colon\ S \to T$ in $\mathbb{F}_{p^r}[x]$ with degree $\leqslant s-1$ which represents L be $f(x) = \sum\limits_{i=0}^{s-1} b_i x^i \in \mathbb{F}_{p^r}[x]$. For $y, z \in S$ and $c \in \mathbb{F}_p$, we see that

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

and

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

By Lemma 10.10 of [10], $f(x)$ is a linearized polynomial. □

Example. In

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

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

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

is the unique polynomial of degree $\leqslant 3$ representing L_S, equating the values of f and L_S over S and solving the system for the coefficients a_i we get

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

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

The requirement that S is an additive group in Proposition 4.5 cannot be dropped even when $q = p$, as shown in the following example.

Example. 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 $f(x) = a_0 + a_1x + a_2x^2 \in \mathbb{F}_{5^3}[x]$ be the unique polynomial representing L on S. Solving for the coefficients, we get $a_0 = 4\alpha/(\alpha^2 + 2\alpha + 2) \neq 0$, showing that $f(x)$ is not a linearized polynomial.

Next, we use Zhou's technique [11] to find analogues of his result for QPP's.

Theorem 4.6. *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*

$$f(x) = \sum_{k=0}^{r-1} \beta^{q^k} (\alpha_0 + \alpha^{q^k}\alpha_1 + \alpha^{2q^k}\alpha_2 + \ldots + \alpha^{(r-1)q^k}\alpha_{r-1}) x^{q^k} \in \mathbb{F}_{q^r}[x], \tag{4.7}$$

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

P r o o f. 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 $i_j \not\equiv i_k \bmod(q^r - 1)$ whenever $j \neq k$, with the convention that $\alpha^{-\infty} = 0$. Referring to Lemma 1.3 of [11], we can take an m-sequence $\{b_i\} \subseteq \mathbb{F}_q$ given by $b_i = \mathrm{Tr}(\beta\alpha^i)$ $(i \geqslant 0)$. For $i \in \{i_1, i_2, \ldots, i_s\}$, consider the numbers

$$\begin{aligned} B_i &:= \sum_{k=0}^{r-1} b_{k+i}\alpha_k = \sum_{k=0}^{r-1} \alpha_k \,\mathrm{Tr}(\beta\alpha^{k+i}) \\ &= \sum_{k=0}^{r-1} \alpha_k (\beta\alpha^{k+i} + \beta^q\alpha^{(k+i)q} + \beta^{q^2}\alpha^{(k+i)q^2} + \ldots + \beta^{q^{r-1}}\alpha^{(k+i)q^{r-1}}) \\ &= \Big(\sum_{k=0}^{r-1} \alpha_k\beta\alpha^k\Big)\alpha^i + \Big(\sum_{k=0}^{r-1} \alpha_k\beta^q\alpha^{kq}\Big)(\alpha^i)^q + \ldots \\ &\qquad + \Big(\sum_{k=0}^{r-1} \alpha_k\beta^{q^{r-1}}\alpha^{kq^{r-1}}\Big)(\alpha^i)^{q^{r-1}}. \end{aligned}$$

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

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

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

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

contradicting Lemma 1.4 of [11]. 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 the remark in Section 2, we get

Corollary 4.7. *Let S and T be subsets of $\mathbb{F}_{q^r}$ with $|S| = |T|$ and let $f(x) \in \mathbb{F}_{q^r}[x]$ be as in* (4.7).

(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 work out an example to illustrate the ideas involved.

Example. 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

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

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

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

By Theorem 4.6, $f(x)$ is an $(R, f(R))$QPP with

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

i.e., $f(x)$ is an (R,T)QPP. Take a bijective function $g\colon S \to R$ 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 2.2 and direct 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 $\leqslant 3$ representing g. By Corollary 4.7, we have that

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

is an (S,T)QPP.

Our next theorem is an analogue of Theorem 4 in [2] for QPP's.

Theorem 4.8. *Let S be an additive subgroup of $\mathbb{F}_{q^r}$ and $U = \mathbb{F}_{q^r} \setminus S^{(q^i-q^j)}$, $r > i > j \geqslant 0$, 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 each $a \in U \setminus \{0\}$.

P r o o f. For $a \in U \setminus \{0\}$ we have $0 \neq a \notin S^{(q^i-q^j)}$. Since $f(x) = x^{q^i} - ax^{q^j} = x^{q^j}(x^{q^i-q^j} - a)$, we deduce that $f(x)$ has only one root $0 \in S$ and the result follows from Theorem 4.1. □

Taking $j = 0$ in Theorem 4.8, we have

Corollary 4.9. *Let S be an additive subgroup of $\mathbb{F}_{q^r}$ and $U = \mathbb{F}_{q^r} \setminus S^{(q^i-1)}$ $(0 < i < r)$, 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 $a \in U \setminus \{0\}$.*

We illustrate its use with an example.

Example. 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 $S = \{0, \alpha, \alpha^2, \alpha^2+\alpha\} \subseteq \mathbb{F}_{2^4}$ and $U = \mathbb{F}_{2^4} \setminus S^{(2^2-2^0)} = \mathbb{F}_{2^4} \setminus S^{(3)}$. We have $S^{(3)} = \{0, 1, \alpha^3, \alpha^2+\alpha^3\}$. By Theorem 4.8, $f(x) = x^4 - ax$ is an $(S, f(S))$QPP for each $a \in U \setminus \{0\}$.

5. Criteria involving characters

Let $\langle G, * \rangle$ be a finite abelian group and F a field. A function $\chi\colon\ G \to F$ 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*, while if G is a group with respect to addition, then a character χ of G is called an *additive character*. Denote by $\hat{G}$ 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 below.

Theorem 5.1. *Let S and T be multiplicative (or additive) abelian subgroups of $\mathbb{F}_q$, and let $f(x) \in \mathbb{F}_q[x]$ be 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.

P r o o f. 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. By Theorem 5.4 of [7] we have $\sum\limits_{c\in S} \chi(f(c)) = \sum\limits_{b\in T} \chi(b) = 0$.

Conversely, assume that $\sum\limits_{c\in S} \chi(f(c)) = 0$ for all multiplicative characters $\chi \neq \chi_0$, the trivial character of S. 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 [7], by

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

showing that $f(x)$ is an (S,T)QPP. □

Specializing the result of Theorem 5.1 to quadratic characters, interesting characterizations can be derived. We start by recalling some facts about quadratic characters. Let H be a multiplicative subgroup of $\mathbb{F}_q \setminus \{0\}$, $|H| = d$. A *quadratic H-character* of $\mathbb{F}_q$ is defined as a map $\eta_H \colon \mathbb{F}_q \to \mathbb{C}$ 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 collect basic properties of quadratic characters in the following lemma.

Lemma 5.2.

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 $\eta_H(bc^{-1}) = \eta_H(bc)$.*

P r o o f. I. (i) Since H is of order d, the result follows from $(b^{d/2})^2 = b^d = 1$. (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 a quadratic character yields

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

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 $c = 0$. Assume now that 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 $\eta_H(c) = -1$. 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 next that $b \neq 0$. If $\eta_H(bc) = 1$, then $\eta_H((c^{-1})^2) = 1 = \eta_H(bc)$, and 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

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

and so

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

□

Theorem 5.3. *Let q be odd, $a \in \mathbb{F}_q$, H a 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 $\eta_H(a^2 - 1) = 1$.*

P r o o f. 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

$$(b^{d/2} + a)b = (c^{d/2} + a)c. \tag{5.1}$$

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 $(b^{d/2} + a)^{-1}$ belongs to $\mathbb{F}_q$, and (5.1) implies

$$bc^{-1} = (b^{d/2} + a)^{-1}(c^{d/2} + a). \tag{5.2}$$

If $\eta_H(b) = \eta_H(c) = 1$, then Lemma 5.2 I (ii) shows that $b^{d/2} = 1 = c^{d/2}$. Consequently, (5.2) 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 5.2 I (i) and (ii) show that $b^{d/2} = -1 = c^{d/2}$. Consequently, (5.2) 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 $\eta_H(c) = 1$. By Lemma 5.2 I (i) and (ii), we have $b^{d/2} = -1$ and $c^{d/2} = 1$. Thus,

$$\begin{aligned}
-1 &= \eta_H(b)\eta_H(c) = \eta_H(b)\eta_H(c^{-1}) \quad \text{(by Lemma 5.2 II)} \\
&= \eta_H(bc^{-1}) \quad \text{(by Lemma 5.2 III)} \\
&= \eta_H((-1 + a)^{-1}(1 + a)) \quad \text{(using (5.2))} \\
&= \eta_H((-1 + a)(1 + a)) \quad \text{(by Lemma 5.2 IV, using } a - 1 \in H = S \setminus \{0\}) \\
&= \eta_H(a^2 - 1).
\end{aligned}$$

We note 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: $a^2-1=0$, i.e., $a=\pm 1$. If $a=-1$, then $f(1)=1+a=0=f(0)$, so f is not injective 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 $b=(a+1)(a-1)^{-1}$ belongs to S. Then

$$\begin{aligned}\eta_H(b)=\eta_H((a+1)(a-1)^{-1})&=\eta_H((a+1)(a-1)) \quad \text{(by Lemma 5.2 IV)}\\ &=\eta_H(a^2-1)=-1.\end{aligned}$$

Lemmas 5.2 I (i) and I (ii) thus imply that $b^{d/2}=-1$, and so

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

showing that f is not injective on S. □

Theorem 5.3 is sharp in the sense that there are other values of a, such as $a=\pm 1$, yielding non-QPP's, as seen in the next example.

Example. For odd q, let $S=H\cup\{0\}$ where H is a multiplicative subgroup of $\mathbb{F}_q^*$ of even order d. Then $f_\pm(x)=x^{1+d/2}\pm x=x(x^{d/2}\pm 1)$ is not an $(S,f(S))$QPP. To see this, taking $a\in H$, we have $f_-(a^2)=(a^2)^{1+d/2}-a^2=0=f_-(0)$, showing that f_- is not injective. Since H is a 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, $f_+(\alpha)=\alpha((\alpha^{d/2})+1)=0=f_+(0)$, i.e., f_+ is not injective.

6. Monomials and binomials

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

Proposition 6.1. *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 6.2. *Let d be a divisor of $q-1$. Assume that S is a cyclic multiplicative subgroup of $\mathbb{F}_q^*$ with $|S| = (q-1)/d$. Then $f(x) = x^m$ is an $(S,S)QPP$ if and only if* $\gcd(m,(q-1)/d) = 1$.

P r o o f. Writing $S = \langle a\rangle$ in terms of its generator a, we have

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

□

Corollary 6.3. *Let $q = p^n$ and let d be a divisor of $q-1$. If S is a cyclic multiplicative subgroup of $\mathbb{F}_q^*$ with $|S| = (q-1)/d$, then $f(x) = x^{p^j}$ is an $(S,S)QPP$ for each $j \in \{0,1,\dots,n-1\}$.*

P r o o f. By Theorem 6.2, it suffices to verify that $\gcd(p^j,(q-1)/d) = 1$. Should $\gcd(p^j,(q-1)/d) \neq 1$, then $p \mid (p^n-1)/d$, a contradiction. □

For binomials, we have the following general results.

Theorem 6.4. A. *Let $0 \in S \subseteq \mathbb{F}_q$ and let $f(x) = x^i - ax^j$, where $i > j \geqslant 1$ and $a \in \mathbb{F}_q \setminus \{0\}$.*

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

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

(Aiii) *Let $e = \gcd(i,j)$, $i_e = i/e$, $j_e = j/e$. Assume S is closed under multiplication. Then $f(x)$ is an $(S,f(S))QPP$ if and only if* $\gcd(e,q-1) = 1$ *and $h(x) = x^{i_e} - ax^{j_e}$ is an $(S,h(S))QPP$.*

B. *Let $S \subseteq \mathbb{F}_q$, $a \in \mathbb{F}_q \setminus \{0\}$ and $i \in \mathbb{N}$. If* $\gcd(i,q-1) = 1$, *then $f(x) = x^i - a$ is an $(S,f(S))QPP$.*

P r o o f. A. (Ai) 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.

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

$$f(x) = x^i - \frac{y^i-z^i}{y^j-z^j}\,x^j = x^j\,\frac{x^{i-j}(y^j-z^j)-(y^i-z^i)}{y^j-z^j}. \tag{6.1}$$

Substituting $x = y$ and $x = z$ in (6.1), we get that $f(y) = f(z)$. Hence $f(x)$ is not an $(S,f(S))$QPP. Conversely, suppose that there are $b,c \in S$, $b \neq c$ such that

$f(b) = f(c)$. Then $b^i - ab^j = f(b) = f(c) = c^i - ac^j$, and so $b^i - c^i = a(b^j - c^j)$, implying that $a = (b^i - c^i)/(b^j - c^j) \in S_2^{(i,j)}$.

(Aiii) Clearly, $f(x) = (h \circ g)(x)$ where $h(x) = x^{i_e} - ax^{j_e}$ and $g(x) = x^e$. By Theorem 7.8 in [7], $g(x)$ is a PP of $\mathbb{F}_q$ if and only if $\gcd(e, q-1) = 1$. Since S is closed under multiplication, we conclude that $g(x)$ is an (S,S)QPP if and only if $\gcd(e, q-1) = 1$. The result follows at once from the remark in Section 2.

B. From Theorem 7.8 (ii) of [7] we know that x^i is a PP of $\mathbb{F}_q$ if and only if $\gcd(i, q-1) = 1$. □

In part A of the last theorem, if $a \notin S^{(i-j)}$, then 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. 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 final two results of this section provide examples of other forms of QPP's.

Proposition 6.5. *Let S be a nonempty subset of $\mathbb{F}_q$ closed under multiplication and let $i \in \mathbb{N}$ be 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.*

P r o o f. This is immediate from Theorem 7.8 (ii) in [7] and the remark in Section 2. □

Proposition 6.6. *Let $S, T \subseteq \mathbb{F}_q$ with $|S| = |T|$, $i \in \mathbb{N}$ with $\gcd(i, q-1) = 1$ and let u be a positive divisor of $q-1$. If $g(x) \in \mathbb{F}_q[x]$ is such that $g(x^i)$ has no nonzero root in $\mathbb{F}_q$, then $f(x) = x^i(g(x^i))^{(q-1)/i}$ is an $(S, f(S))$QPP.*

Moreover, if $h(x)$ is an $(f(S), T)$QPP, then $(h \circ f)(x) = h(x^i(g(x^i))^{(q-1)/i})$ is an (S, T)QPP.

P r o o f. From Theorem 7.10 in [7] we have that $f(x)$ is a PP of $\mathbb{F}_q$, so $f(x)$ is also an $(S, f(S))$QPP. The second part follows from the remark in Section 2. □

7. Number of QPP's of fixed degrees

Recall from Proposition 2.1 that each function from S into T is uniquely representable by a polynomial in $\mathbb{F}_q[x]$ of degree $\leqslant s-1$. Denote the set of all polynomials of degree $\leqslant s-1$ in $\mathbb{F}_q[x]$ by

$$\mathcal{P}_s := \{f \in \mathbb{F}_q[x]\colon \deg f \leqslant s-1\},$$

and the set of those polynomials in $\mathcal{P}_s$ which uniquely represent functions from S to T by

$$\mathcal{P}_s(S,T) := \{f \in \mathcal{P}_s\,;\ f\colon S \to T\}.$$

We wish to determine the number of elements in $\mathcal{P}_s(S,T)$ which are (S,T)QPP's using a technique of Das [3] which is purely computational in nature. Let $N_{S,T}(d)$ denote the number of (S,T)QPP's of exact degree $d \in \{1,2,\ldots,s-1\}$.

Theorem 7.1. *Let $S \subseteq \mathbb{F}_q$ be as described in* (2.1) *and let*

$$W := \begin{pmatrix} 1 & \alpha^{i_1} & (\alpha^{i_1})^2 & \ldots & (\alpha^{i_1})^{s-1} \\ 1 & \alpha^{i_2} & (\alpha^{i_2})^2 & \ldots & (\alpha^{i_2})^{s-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{i_s} & (\alpha^{i_s})^2 & \ldots & (\alpha^{i_s})^{s-1} \end{pmatrix}, \quad V = \det W.$$

For $b \in \mathbb{F}_q^*$, let S_b denote the system of equations (in $x_1, x_2, \ldots, x_s$)

$$\begin{aligned} C_{1,d+1}x_1 + C_{2,d+1}x_2 + \ldots + C_{s,d+1}x_s &= b, \\ C_{1,d+2}x_1 + C_{2,d+2}x_2 + \ldots + C_{s,d+2}x_s &= 0, \\ &\vdots \\ C_{1,s}x_1 + C_{2,s}x_2 + \ldots + C_{s,s}x_s &= 0, \end{aligned}$$

where $C_{i,j} = (-1)^{i+j}\det(M_{i,j})$ is the (i,j)-cofactor of W and $M_{i,j}$ is its (i,j)-minor. Then

$$N_{S,T}(d) = \sum_{b \in B\setminus\{0\}} E_b \quad \text{and} \quad N_{S,T}(d) = \sum_{b \in \mathbb{F}_q^*} E_b,$$

where

$$B = \left\{ t_1\frac{C_{1,d+1}}{V} + t_2\frac{C_{2,d+1}}{V} + \ldots + t_s\frac{C_{s,d+1}}{V}\,;\ t_1, t_2, \ldots, t_s \in T \setminus \{0\},\, t_i \neq t_j\ (i \neq j) \right\}$$

and E_b denotes the number of solutions $(x_1, x_2, \ldots, x_s) \in T^s$ of S_b with $x_i \neq x_j$ $(i \neq j)$.

P r o o f. By the description preceding (2.1), we may write $T = \{\alpha^{j_1}, \alpha^{j_2}, \ldots, \alpha^{j_s}\}$ for some $j_1, j_2, \ldots, j_s \in \mathbb{N} \cup \{0, -\infty\}$ satisfying $j_m \not\equiv j_n \bmod (q-1)$ whenever $m \neq n$, with the convention $\alpha^{-\infty} := 0$. Let

$$f(x) = \sum_{i=0}^{s-1} a_i x^i \in \mathbb{F}_q[x]$$

be the unique polynomial of degree $\leqslant s-1$ representing a function from S into T and let

$$A = (a_0 \ a_1 \ a_2 \ \ldots \ a_{s-1})^t, \quad U = (f(\alpha^{i_1}) \ f(\alpha^{i_2}) \ f(\alpha^{i_3}) \ \ldots \ f(\alpha^{i_s}))^t,$$

where t denotes the transpose of a matrix. Since the matrix W has a nonzero Vandermonde determinant, from $WA = U$ we get $A = W^{-1}U$, and so

$$\begin{aligned} &f \text{ is an (S,T)}QPP \\ &\quad \Longleftrightarrow U = P\,(\alpha^{j_1} \ \alpha^{j_2} \ \alpha^{j_3} \ \ldots \ \alpha^{j_s})^t, \text{ where } P \text{ is a permutation matrix} \\ &\quad \Longleftrightarrow A = W^{-1}P\,(\alpha^{j_1} \ \alpha^{j_2} \ \alpha^{j_3} \ \ldots \ \alpha^{j_s})^t. \end{aligned}$$

Explicitly,

(7.1)
$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{s-1} \end{pmatrix} = \prod_{1 \leqslant k < j \leqslant s} (\alpha^{i_j} - \alpha^{i_k})^{-1} \begin{pmatrix} C_{1,1} & C_{2,1} & C_{3,1} & \ldots & C_{s,1} \\ C_{1,2} & C_{2,2} & C_{3,2} & \ldots & C_{s,2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ C_{1,s} & C_{2,s} & C_{3,s} & \ldots & C_{s,s} \end{pmatrix} P \begin{pmatrix} \alpha^{j_1} \\ \alpha^{j_2} \\ \vdots \\ \alpha^{j_s} \end{pmatrix}.$$

Observe that $P\,(\alpha^{j_1} \ \alpha^{j_2} \ \alpha^{j_3} \ \ldots \ \alpha^{j_s})^t \in T^s$. From Proposition 2.2 we know that

$$a_d = t_1 \frac{C_{1,d+1}}{V} + t_2 \frac{C_{2,d+1}}{V} + \ldots + t_s \frac{C_{s,d+1}}{V}$$

for some $t_1, \ldots, t_s \in T$. If $f(x)$ is an (S,T)QPP of exact degree d, then equating the coefficients on both sides of (7.1) yields

$$a_{d+1} = a_{d+2} = \ldots = a_{s-1} = 0, \quad a_d \neq 0,$$

which is the first equality assertion. The second equality assertion follows from $E_b = 0$ for $b \in \mathbb{F}_q^* \setminus \{0\}$, which holds because of Proposition 2.2 and the definition of B. □

The proof of Theorem 7.1 enables us to find systematically all (S,T)QPP's of degree d. To do so, we first solve S_b and use the solutions to compute the coefficients from the system

$$\begin{aligned} C_{1,1}x_1 + C_{2,1}x_2 + \ldots + C_{s,1}x_s &= a_0 \det W, \\ C_{1,2}x_1 + C_{2,2}x_2 + \ldots + C_{s,2}x_s &= a_1 \det W, \\ &\vdots \\ C_{1,d+1}x_1 + C_{2,d+1}x_2 + \ldots + C_{s,d+1}x_s &= a_d \det W = b \in \mathbb{F}_q^*. \end{aligned} \tag{7.2}$$

We illustrate this remark with the following example.

Example. Let $S = \{1,2,4\}$, $T = \{2,3,4\} \subseteq \mathbb{F}_5$ and $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_5[x]$. Then

$$W = \begin{pmatrix} 1 & 1 & (1)^2 \\ 1 & 2 & (2)^2 \\ 1 & 4 & (4)^2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 4 & 1 \end{pmatrix}.$$

For $b \in \mathbb{F}_5^*$, the system S_b consists of a single equation

$$0 \neq b = C_{1,3}x_1 + C_{2,3}x_2 + C_{3,3}x_3 = 2x_1 + 2x_2 + x_3.$$

If $b = 1$, then the solutions $(x_1,x_2,x_3) \in T^3$ of S_1 with $x_i \neq x_j$ $(i \neq j)$ are $(3,4,2)$ and $(4,3,2)$. Substituting into (7.2), we get the (S,T)QPP's x^2+3x+4 and x^2+x+2.

If $b = 2$, then there is no solution $(x_1,x_2,x_3) \in T^3$ of S_2 with $x_i \neq x_j$ $(i \neq j)$.

If $b = 3$, then there is no solution $(x_1,x_2,x_3) \in T^3$ of S_3 with $x_i \neq x_j$ $(i \neq j)$.

If $b = 4$, then the solutions $(x_1,x_2,x_3) \in T^3$ of S_4 with $x_i \neq x_j$ $(i \neq j)$ are $(2,3,4)$ and $(3,2,4)$. Substituting into (7.2), we get the (S,T)QPP's $4x^2 + 4x + 4$ and $4x^2 + 2x + 2$.

Thus, there are altogether four (S,T)QPP's, namely, $x^2 + 3x + 4$, $x^2 + x + 2$, $4x^2 + 4x + 4$, $4x^2 + 2x + 2$. This is in agreement with the result of Theorem 7.1, which yields $N_{S,T}(2) = 2 + 0 + 0 + 2 = 4$.

If more information such as the value of $f(0)$ is known, the system to be solved contains more equations and the proof of Theorem 7.1 still applies. We record it here without proof. Let $N_0(d)$ denote the number of (S,T)QPP's $f \in \mathbb{F}_q[x]$ with $\deg f = d \in \{1,\ldots s-1\}$ and $f(0) = 0$, and let $N_1(d)$ denote the number of (S,T)QPP's $f \in \mathbb{F}_q[x]$ with $\deg f = d$ and $f(0) \neq 0$. For $b \in \mathbb{F}_q^*$, let $S_b^{(0)}$ denote

the system of equations

$$\begin{aligned} C_{1,1}x_1 + C_{2,1}x_2 + \ldots + C_{s,1}x_s &= 0, \\ C_{1,d+1}x_1 + C_{2,d+1}x_2 + \ldots + C_{s,d+1}x_s &= b, \\ &\vdots \\ C_{1,s}x_1 + C_{2,s}x_2 + \ldots + C_{s,s}x_s &= 0, \end{aligned}$$

and let $E_b^{(0)}$ denote the number of solutions $(x_1, x_2, \ldots, x_s) \in T^s$ of $S_b^{(0)}$ with $x_i \neq x_j$ $(i \neq j)$.

Proposition 7.2. *We have*

(i) $N_0(d) = \sum_{b \in B} E_b^{(0)}$,

(ii) $N_0(d) = \sum_{b \in \mathbb{F}_q^*} E_b^{(0)}$,

(iii) $N_1(d) = N_{S,T}(d) - N_0(d)$,

where

$$B = \left\{ t_1 \frac{C_{1,d+1}}{V} + t_2 \frac{C_{2,d+1}}{V} + \ldots + t_s \frac{C_{s,d+1}}{V}; \right. \\ \left. t_1, t_2, \ldots, t_s \in T \setminus \{0\}, t_i \neq t_j \ (i \neq j) \right\}.$$

The next example clarifies the computationally oriented aspect of Theorem 7.1 and Proposition 7.2.

Example. Let $S = \{1, 2, 4\}$, $T = \{2, 3, 4\} \subseteq \mathbb{F}_5$ and $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_5[x]$. To determine all QPP's of degree 1, we solve the system of the equations

$$\begin{aligned} 3x_1 + 0x_2 + 2x_3 &= a \neq 0, \\ 2x_1 + 2x_2 + x_3 &= 0. \end{aligned}$$

By the same process as in the previous example, this system has two solutions $(x_1, x_2, x_3) \in T^3$ such that $x_i \neq x_j$ $(i \neq j)$, namely, $(2, 4, 3)$ and $(4, 2, 3)$, so $N_{S,T}(1) = 2$. Substituting into (7.2), we obtain $f(x) = 2x$ and $f(x) = 2x + 1$ as all (S, T)QPP's of degree 1. If we add the equation $C_{1,1}x_1 + C_{2,1}x_2 + C_{3,1}x_3 = 0$ or $x_1 + 3x_2 + 2x_3 = 0$ to the same system, there is thus only one solution $(2, 4, 3)$, so $N_0(1) = 1$. Consequently, $f(x) = 2x$ is the only linear (S, T)QPP such that $f(0) = 0$. This agrees with $N_1(1) = 1 = 2 - 1 = N_{S,T}(1) - N_0(1)$.

Corollary 7.3. *We have*

$$N_{S,T}(s-1) = s! - \#(C_{1,s}x_1 + C_{2,s}x_2 + \ldots + C_{s,s}x_s = 0),$$

where # denotes the number of solutions in T^s of the corresponding equation with the restriction that $x_i \neq x_j$ $(i \neq j)$.

P r o o f. The result follows from Theorem 7.1 by observing that

$$\begin{aligned} s! = {} & |\{(x_1, x_2, \ldots, x_s) \in T^s;\ C_{1,s}x_1 + C_{2,s}x_2 + \ldots + C_{s,s}x_s \neq 0,\ x_i \neq x_j\ (i \neq j)\}| \\ & + |\{(x_1, x_2, \ldots, x_s) \in T^s;\ C_{1,s}x_1 + C_{2,s}x_2 + \ldots + C_{s,s}x_s = 0, \\ & \qquad\qquad x_i \neq x_j\ (i \neq j)\}|. \end{aligned}$$

□

Generalizing Corollary 7.3, we get

Corollary 7.4. *If $G_{S,T}(d)$ is the number of solutions in T^s of the system*

$$\begin{aligned} C_{1,d+1}x_1 + C_{2,d+1}x_2 + \ldots + C_{s,d+1}x_s &= 0, \\ C_{1,d+2}x_1 + C_{2,d+2}x_2 + \ldots + C_{s,d+2}x_s &= 0, \\ &\vdots \\ C_{1,s}x_1 + C_{2,s}x_2 + \ldots + C_{s,s}x_s &= 0 \end{aligned}$$

such that $x_i \neq x_j$ $(i \neq j)$, then

$$N_{S,T}(d) = s! - N_{S,T}(s-1) - N_{S,T}(s-2) - \ldots - N_{S,T}(d+1) - G_{S,T}(d).$$

P r o o f. Note that $G_{S,T}(s-1) = s! - N_{S,T}(s-1)$ and $N_{S,T}(s-2) + G_{S,T}(s-2) = G_{S,T}(s-1)$. By induction,

$$N_{S,T}(k) + G_{S,T}(k) = G_{S,T}(k+1) \quad (k = d, d+1, d+2, \ldots, s-2),$$

and the result follows from recursive use of this relation. □

References

[1] *L. Carlitz, J. A. Lutz*: A characterization of permutation polynomials over a finite field. Am. Math. Mon. *85* (1978), 746–748.

[2] *W. Chu, S. W. Golomb*: Circular Tuscan-k arrays from permutation binomials. J. Comb. Theory, Ser. A *97* (2002), 195–202.

[3] *P. Das*: The number of permutation polynomials of a given degree over a finite field. Finite Fields Appl. *8* (2002), 478–490.

[4] *F. R. Gantmacher*: The Theory of Matrices, Volume I. Chelsea, New York, 1977.

[5] *R. Lidl, G. L. Mullen*: When does a polynomial over a finite field permute the elements of the field? Am. Math. Mon. *95* (1988), 243–246.

[6] *R. Lidl, G. L. Mullen*: When does a polynomial over a finite field permute the elements of the field? II. Am. Math. Mon. *100* (1993), 71–74.

[7] *R. Lidl, H. Niederreiter*: Finite Fields. Addison-Wesley, Reading, 1983.

[8] *C. Small*: Permutation binomials. Int. J. Math. Math. Sci. *13* (1990), 337–342.

[9] *D. Wan, R. Lidl*: Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure. Monatsh. Math. *112* (1991), 149–163.

[10] *Z.-X. Wan*: Lectures on Finite Fields and Galois Rings. World Scientific, River Edge, 2003.

[11] *K. Zhou*: A remark on linear permutation polynomials. Finite Fields Appl. *14* (2008), 532–536.

Authors' addresses: V. Laohakosol, Kasetsart University, Bangkok 10900, Thailand, e-mail: `fscivil@ku.ac.th`; S. Janphaisaeng, Naresuan University, Phitsanulok 65000, Thailand, e-mail: `suphawanj@nu.ac.th`.