East-West J. of Mathematics: Vol. 9, No 2 (2007) pp. 161-172

A NOTE ON QUASI-PERMUTATION POLYNOMIALS

Vichian Laohakosol* and **Suphawan Janphaisaeng**†

**Department of Mathematics,*
Kasetsart University Bangkok 10900, Thailand.
email: fscivil@ku.ac.th

†*Department of Mathematics,*
Naresuan University Phitsanulok 65000, Thailand.
email: suphawanj@nu.ac.th

Abstract

A quasi-permutation polynomial is a polynomial which is a bijection from one subset of a finite field onto another subset of the same cardinality. This is a natural generalization of the familiar permutation polynomials. General discussions are made on the existence and the number of such polynomials together with examples.

1 Introduction

Let $\mathbb{F}_q$ denote the finite field of q elements. A permutation function over $\mathbb{F}_q$ is a function from $\mathbb{F}_q$ into itself which is a permutation of $\mathbb{F}_q$. Let S and T be two nonempty subsets of $\mathbb{F}_q$ with the same number of elements $s = |S| = |T|$. An (S,T)-permutation is a bijection from S onto T; this is an obvious generalization of a permutation function over $\mathbb{F}_q$. In an attempt to generalize the concept of permutation function to that of (S,T)-permutation, one immediately encounters several difficulties, one of which is illustrated in the following example.

Example. Let $S = \{1, 3, 5\}$ and $T = \{2, 4, 6\}$ be subsets of $\mathbb{F}_7 := \{0, 1, 2, 3, 4, 5, 6\}$. Consider the two relations f and g defined on $\mathbb{F}_7$ by

$$f = \{(0, 0), (0, 1), (1, 2), (2, 3), (3, 4), (4, 5), (5, 6), (6, 1)\}$$

Research supported by the Commission on Higher Education and the Thailand Research Fund through contract number RTA5180005

Key words: finite fields, permutation polynomials .

(2000) AMS Mathematics Subject Classification: 11T55, 12Y05

and

$$g = \{(0,0),(1,2),(2,3),(3,4),(4,5),(5,6),(6,1)\}.$$

Clearly, f and g are (S,T)-permutations. Yet, f is not a function from $\mathbb{F}_7$ into itself, but g is. Notice also that $f \neq g$ over $\mathbb{F}_7$, but if the domain is restricted to S, then $f = g$, i.e., f and g are the same (S,T)-permutation.

This example indicates that should one wish to study permutations over subsets of $\mathbb{F}_q$, referred to as quasi-permutations, it is more natural not to consider any general functions. An obvious candidate to consider is the polynomial function. This is also affirmatively assured by the following fact about function representation. As is well-known, see e.g. the remark after Lemma 7.1 in [4], each function from $\mathbb{F}_q$ into itself is uniquely representable as a polynomial in $\mathbb{F}_q$[x] of degree $\leq q-1$. This is also the case for functions from S into T.

Proposition 1.1. *If $f : S \to T$ is a function, where S and T are subsets of $\mathbb{F}_q$ with the same number of elements $|S| = |T| = s \leq q$, then there exists a unique polynomial $P_f \in \mathbb{F}_q[x]$ with* deg $P_f \leq s-1$ *representing f in the sense that $P_f(c) = f(c)$ for all $c \in S$.*

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

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

The system of linear equations

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

uniquely determines the coefficients c_i because its coefficient matrix $\left(a_i^j\right)$ has a vandermonde determinant. This guarantees the existence of such a polynomial P_f. To prove uniqueness, assume that there is another polynomial $h \in \mathbb{F}_q[x]$ with deg $h \leq s-1$ such that $h(c) = f(c)$ for all $c \in S$. Then $P_f - h \in \mathbb{F}_q[x]$ would be a polynomial of degree $\leq s-1$ which vanishes at s distinct points in a finite field, forcing $h \equiv P_f$. □ Proposition 1.1 tells us that each function from S to T is uniquely representable as a polynomial in $\mathbb{F}_q[x]$ of degree $\leq s-1$. There are altogether q^s polynomials of degree $\leq s-1$ over $\mathbb{F}_q$, while the number of functions from S into T is merely s^s $(\leq q^s)$. In general, without imposing any structure on the sets S and T, it is not easy to find out which polynomial does not represent such a function. The next example confirms that not all polynomials of degree $\leq s-1$ represent functions from S to T.

Example. Let $S = \{1,2,4\}$, $T = \{2,3,4\}$ be subsets of $\mathbb{F}_5 := \{0,1,2,3,4\}$. Consider the polynomial

$$P(x) = x + 4 \in \mathbb{F}_5[x]$$

of degree $1(\leq 3-1=2)$. We see that P is a function from $\mathbb{F}_5$ into $\mathbb{F}_5$ but it is not a function from S into T as $P(1)=0 \notin T$.

Our next proposition provides a necessary and sufficient condition on the polynomials of degree $\leq s-1$ to represent functions from S to T. Before doing so, we recall some elementary facts. Since ${\mathbb{F}_q}^*:= \mathbb{F}_q \setminus \{0\}$ is a cyclic group of order $q-1$, we may write ${\mathbb{F}_q}^*= \langle\alpha\rangle$, where $\alpha \in {\mathbb{F}_q}^*$ 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 $i \in \mathbb{Z}$. If S is a subset of $\mathbb{F}_q$ with $|S| = s$, then we write

$$S = \{\alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_s}\} \tag{1}$$

for some distinct $i_1, i_2, \ldots, i_s \in \mathbb{N}_0^\infty := \mathbb{N} \cup \{0, -\infty\}$ satisfying $i_j \not\equiv i_k (\bmod\, q-1)$ for $j \neq k$, where we adopt the convention that $\alpha^{-\infty} = 0$.

Proposition 1.2. *Let S and T be subsets of $\mathbb{F}_q$ with the same number of elements $|S| = |T| = s \leq q$ with S written as in* (1). *If*

$$P_f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{s-1}x^{s-1} \in \mathbb{F}_q[x]$$

is a polynomial of degree $\leq s-1$ representing a function $f:\ S \to T$, then

$$a_0 = \frac{\det(C_1(W))}{\det(W)}\ ,\ a_1 = \frac{\det(C_2(W))}{\det(W)}\ ,\ \ldots\ ,\ a_{s-1} = \frac{\det(C_s(W))}{\det(W)},$$

where

$$W = \begin{pmatrix} 1 & \alpha^{i_1} & (\alpha^{i_1})^2 & (\alpha^{i_1})^3 & \cdots & (\alpha^{i_1})^{s-1} \\ 1 & \alpha^{i_2} & (\alpha^{i_2})^2 & (\alpha^{i_2})^3 & \cdots & (\alpha^{i_2})^{s-1} \\ 1 & \alpha^{i_3} & (\alpha^{i_3})^2 & (\alpha^{i_3})^3 & \cdots & (\alpha^{i_3})^{s-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{i_s} & (\alpha^{i_s})^2 & (\alpha^{i_s})^3 & \cdots & (\alpha^{i_s})^{s-1} \end{pmatrix}$$

and for $j = 1, \ldots, s$

$$C_j(W) = \begin{pmatrix} 1 & \alpha^{i_1} & (\alpha^{i_1})^2 & \cdots & (\alpha^{i_1})^{j-2} & f(\alpha^{i_1}) & (\alpha^{i_1})^{j} & \cdots & (\alpha^{i_1})^{s-1} \\ 1 & \alpha^{i_2} & (\alpha^{i_2})^2 & \cdots & (\alpha^{i_2})^{j-2} & f(\alpha^{i_2}) & (\alpha^{i_2})^{j} & \cdots & (\alpha^{i_2})^{s-1} \\ 1 & \alpha^{i_3} & (\alpha^{i_3})^2 & \cdots & (\alpha^{i_3})^{j-2} & f(\alpha^{i_3}) & (\alpha^{i_3})^{j} & \cdots & (\alpha^{i_3})^{s-1} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{i_s} & (\alpha^{i_s})^2 & \cdots & (\alpha^{i_s})^{j-2} & f(\alpha^{i_s}) & (\alpha^{i_s})^{j} & \cdots & (\alpha^{i_s})^{s-1} \end{pmatrix}.$$

Moreover, the number of such polynomials $P_f(x)$ is equal to the number of functions from S to T which is s^s.

Proof Let

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

where t denotes the transpose of a matrix. Then $WX = U$ where $X = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{s-1} \end{pmatrix}^t$. Since the matrix W has a 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 vera, the second part is immediate. □

The following example illustrates the remarks pertaining to Propositions 1.1 and 1.2.

Example. In

$$\mathbb{F}_{3^2} \cong \mathbb{Z}_3[x]/(x^2+1) = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\},$$

where $\alpha^2 + 1 = 0$, let

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

be subsets of $\mathbb{F}_{3^2}$. Consider the function $f : S \to T$ defined by

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

To find the unique polynomial

$$P_f(x) = a_0 + a_1 x + a_2 x^2 \in \mathbb{F}_{3^2}[x]$$

of degree ≤ 2 representing f, we need to solve the system

$$\begin{aligned} 2 &= P_f(1) = a_0 + a_1 + a_2\ , \\ 2 &= P_f(\alpha+1) = a_0 + a_1(\alpha+1) + a_2(\alpha+1)^2 = a_0 + (\alpha+1)a_1 + 2\alpha a_2\ , \\ \alpha+2 &= P_f(2\alpha+1) = a_0 + a_1(2\alpha+1) + a_2(2\alpha+1)^2 = a_0 + (2\alpha+1)a_1 + \alpha a_2, \end{aligned}$$

which is equivalent to $WX = V$, where

$$W = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha+1 & 2\alpha \\ 1 & 2\alpha+1 & \alpha \end{pmatrix}, \ X = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} \text{ and } V = \begin{pmatrix} 2 \\ 2 \\ \alpha+2 \end{pmatrix}.$$

Since the matrix W has a vandermonde determinant, there is exactly one solution of this system, which is $(a_0, a_1, a_2) = (\alpha+1, \alpha+1, \alpha)$, i.e.,

$$P_f(x) = (\alpha+1) + (\alpha+1)x + \alpha x^2$$

is the unique polynomial of degree ≤ 2 representing the function f.

On the other hand, observe that the polynomial $P(x) = x^2 + 1 \in \mathbb{F}_{3^2}[x]$, of degree ≤ 2, is a function from $\mathbb{F}_{3^2}$ into $\mathbb{F}_{3^2}$ but it is not a function from S into T since $P(\alpha+1) = (\alpha+1)^2 + 1 = \alpha^2 + 2\alpha + 2 = 2\alpha + 1 \notin T$.

Another immediate consequence of Proposition 1.2 is the following result which enables us to write down explicitly those polynomials representing functions from S to T.

Corollary 1.3. *Let S and T be subsets of $\mathbb{F}_q$ with the same number of elements $|S| = |T| = s \leq q$ with S written as in* (1)*. Let*

$$W = \begin{pmatrix} 1 & \alpha^{i_1} & (\alpha^{i_1})^2 & (\alpha^{i_1})^3 & \cdots & (\alpha^{i_1})^{s-1} \\ 1 & \alpha^{i_2} & (\alpha^{i_2})^2 & (\alpha^{i_2})^3 & \cdots & (\alpha^{i_2})^{s-1} \\ 1 & \alpha^{i_3} & (\alpha^{i_3})^2 & (\alpha^{i_3})^3 & \cdots & (\alpha^{i_3})^{s-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{i_s} & (\alpha^{i_s})^2 & (\alpha^{i_s})^3 & \cdots & (\alpha^{i_s})^{s-1} \end{pmatrix}$$

be the vandermonde matrix of the elements of S, $V = \det W$ and

$$\Delta_k^{(j)} = (-1)^{k+j} \det(M_{k,j})$$

where $M_{k,j}$ denotes the (k,j)-minor of W. Then

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{s-1} x^{s-1} \in \mathbb{F}_q[x]$$

is a polynomial of degree $\leq s-1$ representing a function sending S into T if and only if each of its coefficients is a T-linear combination of $\frac{\Delta_1^{(j)}}{V}, \frac{\Delta_2^{(j)}}{V}, \dots, \frac{\Delta_s^{(j)}}{V}$, i.e.,

$$a_j = t_1 \frac{\Delta_1^{(j)}}{V} + t_2 \frac{\Delta_2^{(j)}}{V} + \cdots + t_s \frac{\Delta_s^{(j)}}{V} \quad (j = 0, 1, \dots, s-1)$$

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

We next give an example.

Example. In

$$\mathbb{F}_{3^2} \cong \mathbb{Z}_3[x]/(x^2+1) = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\},$$

where $\alpha^2 + 1 = 0$, let

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

be subsets of $\mathbb{F}_{3^2}$. Here,

$$\Delta_1^{(1)} = (-1)^{1+1}\begin{vmatrix} \alpha+2 & \alpha \\ 2\alpha+1 & \alpha \end{vmatrix} = \alpha+1,\ \Delta_2^{(1)} = (-1)^{2+1}\begin{vmatrix} 1 & 1 \\ 2\alpha+1 & \alpha \end{vmatrix} = \alpha+1,$$

$$\Delta_3^{(1)} = (-1)^{3+1}\begin{vmatrix} 1 & 1 \\ \alpha+2 & \alpha \end{vmatrix} = 1,\ \Delta_1^{(2)} = (-1)^{1+2}\begin{vmatrix} 1 & \alpha \\ 1 & \alpha \end{vmatrix} = 0,$$

$$\Delta_2^{(2)} = (-1)^{2+2}\begin{vmatrix} 1 & 1 \\ 1 & \alpha \end{vmatrix} = \alpha+2,\ \Delta_3^{(2)} = (-1)^{3+2}\begin{vmatrix} 1 & 1 \\ 1 & \alpha \end{vmatrix} = 2\alpha+1,$$

$$\Delta_1^{(3)} = (-1)^{1+3}\begin{vmatrix} 1 & \alpha+2 \\ 1 & 2\alpha+1 \end{vmatrix} = \alpha+2,\ \Delta_2^{(3)} = (-1)^{2+3}\begin{vmatrix} 1 & 1 \\ 1 & 2\alpha+1 \end{vmatrix} = \alpha,$$

$$\Delta_3^{(3)} = (-1)^{3+3}\begin{vmatrix} 1 & 1 \\ 1 & \alpha+2 \end{vmatrix} = \alpha+1,\ V = \begin{vmatrix} 1 & 1 & 1 \\ 1 & \alpha+2 & \alpha \\ 1 & 2\alpha+1 & \alpha \end{vmatrix} = 2\alpha,$$

$$\frac{\Delta_1^{(1)}}{V} = \alpha+2,\ \frac{\Delta_2^{(1)}}{V} = \alpha+2,\ \frac{\Delta_3^{(1)}}{V} = \alpha,\ \frac{\Delta_1^{(2)}}{V} = 0,\ \frac{\Delta_2^{(2)}}{V} = 2\alpha+2,$$
$$\frac{\Delta_3^{(2)}}{V} = \alpha+1,\ \frac{\Delta_1^{(3)}}{V} = 2\alpha+2,\ \frac{\Delta_2^{(3)}}{V} = 2,\ \frac{\Delta_3^{(3)}}{V} = \alpha+2.$$

By Corollary 1.3, each polynomial of degree $\leq 3-1 = 2$ representing a function from S to T is of the form

$$P(x) = a_0 + a_1x + a_2x^2,$$

where $a_0 = (\alpha+2)t_1 + (\alpha+2)t_2 + \alpha t_3, a_1 = (2\alpha+2)t_2 + (\alpha+1)t_3, a_2 = (2\alpha+2)t_1 + 2t_2 + (\alpha+2)t_3$, and conversely.

As a final remark of this section, it is worth mentioning that should we impose too strong a condition on the sets S and T such as being rings, then both become fields. This is because $a \in S\setminus\{0\} \subset \mathbb{F}_q\setminus\{0\}$ implies $1 = a^{q-1} \in S$ and so $a^{-1} = a^{q-2} \in S$. Such functions sending fields into fields are not of interest here.

2 Quasi-permutation polynomials

Recall that 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 determining PP's has been of much interest in recent years, see e.g. [2], [3] and Chapter 7 of [4]. An obvious generalization of PP is that of *quasi-permutation polynomial*, abbreviated as QPP. Let S and T be two fixed non-empty subsets of $\mathbb{F}_q$ with the same number of elements. A polynomial $P(x) \in \mathbb{F}_q[x]$ is called an (S,T)-*quasi-permutation polynomial*, abbreviated as (S,T)-QPP or simply QPP if both S

and T are left understood, if $\{P(c); c \in S\} = T$. If $S = T = \mathbb{F}_q$, then $P(x)$ is the usual PP.

Dealing with QPP's, there are cautions to be noted. First, we must deal with the difficulty that there are polynomials which are both QPP's and PP's, there are polynomials which are QPP's but not PP's, and there are polynomials which are PP's but not QPP's, as evidenced in the next two examples.

Example. Let $S = \{1, 2, 4\}$ and $T = \{2, 3, 4\}$ be subsets of $\mathbb{F}_5$. Consider

$$f(x) = 3x + 1, \quad g(x) = x^2 + x + 2, \quad h(x) = 3x + 2 \in \mathbb{F}_5[x].$$

By Theorem 7.8(i) of [4], $f(x)$ and $h(x)$ are PP's over $\mathbb{F}_5$ and, as easily shown, $f(x)$ is also an (S,T)-QPP, but $h(x)$ is not an (S,T)-QPP for $h(1) = 0 \notin T$. As for the polynomial g, from $g(1) = 4$, $g(2) = 3$, $g(4) = 2$ and $g(0) = 2 = g(4)$, we see that $g(x)$ is an (S,T)-QPP but not a PP.

A more complex example for finite fields with prime power number of elements is:

Example. In

$$\mathbb{F}_{2^3} \cong \mathbb{Z}_2[x]/(x^3 + x + 1) = \left\{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\right\},$$

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

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

be subsets of $\mathbb{F}_{2^3}$. The polynomials $P(x) = x + 1$ and $Q(x) = x \in \mathbb{F}_{2^3}[x]$ are, by Theorem 7.8 of [4], PP's over $\mathbb{F}_{2^3}$ and by direct computation $P(x)$ is also an (S,T)-QPP, but $Q(x)$ is not an (S,T)-QPP for $Q(\alpha^2 + 1) = \alpha^2 + 1 \notin T$. The polynomial

$$R(x) = (\alpha^2 + \alpha + 1)x^2 + (\alpha^2 + \alpha)x + \alpha^2 \in \mathbb{F}_{2^3}[x]$$

is an (S,T)-QPP but not a PP, because $R(\alpha) = \alpha, R(\alpha+1) = \alpha+1, R(\alpha^2+1) = \alpha^2$ and $R(0) = \alpha^2 = R(\alpha^2 + 1)$.

The second caution needed mentioning deals with the problem of counting the number of QPP's. For ordinary PP's over $\mathbb{F}_q$, it is trivial that there are altogether $q!$ PP's from a total of q^q polynomials representing all functions from $\mathbb{F}_q$ to itself. The problem of counting the number of PP's of fixed degree has also been of recent interest, see e.g. [1]. The situation is not as trivial for QPP's because there are ambiguities such as that arising from distinct polynomials over $\mathbb{F}_q$ being identical as (S,T)-polynomials, i.e., polynomials representing functions from S to T. In order to overcome some of the ambiguities, we make precise the sets of polynomials to be considered.

Definition 2.1. *Denote the set of all polynomials of degree* $\leq q-1$ *in* $\mathbb{F}_q[x]$ *by*

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

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

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

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

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

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

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

Clearly, $\mathcal{P}_s(S,T) \subseteq \mathcal{P}_q(S,T)$ and $\mathcal{P}_s \subseteq \mathcal{P}_q$. The following example shows that these inclusions can be strict.

Example. In $\mathbb{F}_3 = \{0,1,2\}$, let $S = \{1,2\}$, $T = \{0,1\}$. Direct computation shows that there are altogether 12 polynomials in $\mathcal{P}_3(S,T)$, viz.,

$$\begin{aligned}
&f_1(x) = 0,\ f_2(x) = 1,\ f_3(x) = x+2,\ f_4(x) = 2x+2,\ f_5(x) = x^2,\\
&f_6(x) = x^2+2,\ f_7(x) = x^2+x+1,\ f_8(x) = x^2+2x+1,\\
&f_9(x) = 2x^2+1,\ f_{10}(x) = 2x^2+2,\ f_{11}(x) = 2x^2+x,\ \text{and}\\
&f_{12}(x) = 2x^2+2x.
\end{aligned}$$

and there are altogether 4 polynomials in $\mathcal{P}_2(S,T)$, viz.,

$$f_1(x),\ f_2(x),\ f_3(x),\ f_4(x). \tag{2}$$

Observe that for all $a \in S$

$$f_1(a) = f_6(a) = f_9(a),\ f_2(a) = f_5(a) = f_{10}(a),$$

$$f_3(a) = f_7(a) = f_{11}(a),\ f_4(a) = f_8(a) = f_{12}(a),$$

implying that as (S,T)-polynomials

$$f_1 \equiv f_6 \equiv f_9,\ f_2 \equiv f_5 \equiv f_{10},\ f_3 \equiv f_7 \equiv f_{11},\ f_4 \equiv f_8 \equiv f_{12}, \tag{3}$$

i.e., there are essentially four distinct polynomials representing functions from S to T as displayed in (2), the elements of $\mathcal{P}_2(S,T)$.

Among polynomials in $\mathcal{P}_3(S,T)$, those (S,T)-QPP's of degree ≤ 2 are

$$f_3(x),\ f_4(x),\ f_7(x),\ f_8(x),\ f_{11}(x),\ f_{12}(x).$$

However, from (3), we know that there are essentially two distinct (S,T)-QPP's (of degree ≤ 1), namely, $f_3(x),\ f_4(x)$, with a total of 2 !=2 polynomials. This is in agreement with direct counting which yields

$$|\mathcal{P}_3| = 3^3 = 27,\ |\mathcal{P}_3(S,T)| = 2^2 \times 3 = 12,\ |\mathcal{P}_2| = 3^2 = 9,\ |\mathcal{P}_2(S,T)| = 2^2 = 4.$$

For completeness, let us find all PP's over $\mathbb{F}_3$ of degree ≤ 2. By Theorem 7.8(i) in [4], each first degree polynomial $f(x) = ax+b\ \ (a(\neq 0), b \in \mathbb{F}_3)$ is a PP, so the number of PP's with degree 1 is 6. Since $2|(3-1)$, by Corollary 7.5 in [4], there is no PP of degree 2. Hence, the number of PP's of $\mathbb{F}_3$ with degree ≤ 2 is $6 = 3!$.

This last example hints that there are relations among the number of (S,T)-QPP's in $\mathcal{P}_q(S,T)$ and the number of (S,T)-QPP's in $\mathcal{P}_s(S,T)$. To do so, let us fix some more notation.

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

Proposition 2.2. *(i) We have $|\mathcal{P}_s(S,T)| = s^s,\ N_s(S,T) = s!$.*

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

Proof (i) By Proposition 1.1, each function from S into T is uniquely representable as a polynomial in $\mathbb{F}_q[x]$ of degree $\leq s-1$ 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 using (i).

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

The next two examples provide numerical examples of the last two propositions.

Example. In $\mathbb{F}_5 = \{0,1,2,3,4\}$, let $S = \{1,2,4\}$, $T = \{2,3,4\}$. By Proposition 2.2, we have

$$|\mathcal{P}_5| = 5^5 = 3,125,\ |\mathcal{P}_5(S,T)| = 3^3 \cdot 5^2 = 675,\ N_5(S,T) = 3! \cdot 5^2 = 150,$$
$$|\mathcal{P}_3| = 5^3 = 125,\ |\mathcal{P}_3(S,T)| = 3^3 = 27,\ N_3(S,T) = 3! = 6.$$

Direct computation shows that the 27 polynomials in $\mathcal{P}_3(S,T)$ are as in Table 1.

i	$f_i(x)$		i	$f_i(x)$		i	$f_i(x)$
1	2		10	x^2+3x+4		19	$3x^2+x$
2	3		11	x^2+4x+2		20	$3x^2+2x+2$
3	4		12	$2x^2$		21	$3x^2+2x+3$
4	$2x$		13	$2x^2+1$		22	$4x^2+3$
5	$3x+1$		14	$2x^2+3x+3$		23	$4x^2+x+4$
6	x^2+3		15	$2x^2+3x+4$		24	$4x^2+2x+2$
7	x^2+x+2		16	$2x^2+4x+1$		25	$4x^2+3x+1$
8	x^2+2x		17	$3x^2$		26	$4x^2+3x+2$
9	x^2+2x+4		18	$3x^2+1$		27	$4x^2+4x+4$

Table 1: 27 polynomials in $\mathcal{P}_3(S,T)$

Among them, the six (S,T)-QPP's of degree ≤ 2 are

$$f_4(x),\ f_5(x),\ f_7(x),\ f_{10}(x),\ f_{24}(x),\ f_{27}(x).$$

Next, we find all PP's in $\mathbb{F}_5$ of degree ≤ 4. By Theorem 7.8(i) in [4], $f(x) = ax+b$; $a,b \in \mathbb{F}_5$ and $a \neq 0$, is a PP of $\mathbb{F}_5$, so the number of PP's with degree 1 is 20.

Since $2|(5-1)$ and $4|(5-1)$, by Corollary 7.5 in [4], there is no PP of $\mathbb{F}_5$ of degree 2 and degree 4. It remains to consider only the case of PP's with degree 3. Direct checking shows that there are 100 PP's $\mathbb{F}_5[x]$ of degree 3, namely,

$$x^3+d,\ x^3+x^2+2x+d,\ x^3+2x^2+3x+d,\ x^3+3x^2+3x+d,$$
$$x^3+4x^2+2x+d,\ 2x^3+d,\ 2x^3+x^2+x+d,\ 2x^3+2x^2+4x+d,$$
$$2x^3+3x^2+4x+d,\ 2x^3+4x^2+x+d,\ 3x^3+d,\ 3x^3+x^2+4x+d,$$
$$3x^3+2x^2+x+d,\ 3x^3+3x^2+x+d,\ 3x^3+4x^2+4x+d,\ 4x^3+d,$$
$$4x^3+x^2+3x+d,\ 4x^3+2x^2+2x+d,\ 4x^3+3x^2+2x+d,\ 4x^3+4x^2+3x+d$$

for all $d \in \mathbb{F}_5$. Consequently, the number of PP's of $\mathbb{F}_5$ with degree ≤ 4 is $120 = 5!$, as expected.

Example. In

$$\mathbb{F}_{2^2} \cong \mathbb{Z}_2[x]/(x^2+x+1) = \{0,1,\alpha,\alpha+1\},$$

where $\alpha^2+\alpha+1=0$, let

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

be subsets of $\mathbb{F}_{2^2}$. By Proposition 2.2, we have

$$|\mathcal{P}_4| = 4^4 = 256,\ |\mathcal{P}_4(S,T)| = 2^2 \cdot 4^2 = 64,\ N_4(S,T) = 2! \cdot 4^2 = 32,$$
$$|\mathcal{P}_2| = 4^2 = 16,\ |\mathcal{P}_2(S,T)| = 2^2 = 4,\ N_2(S,T) = 2! = 2.$$

Direct computation shows that the 64 polynomials in $\mathcal{P}_4(S,T)$ are as in Table 2.

i	$g_i(x)$		i	$g_i(x)$
1	1		33	$\alpha x^3 + 1$
2	$\alpha + 1$		34	$\alpha x^3 + \alpha + 1$
3	$(\alpha+1)x$		35	$\alpha x^3 + (\alpha+1)x$
4	$(\alpha+1)x + \alpha$		36	$\alpha x^3 + (\alpha+1)x + \alpha$
5	x^2		37	$\alpha x^3 + x^2$
6	$x^2 + \alpha$		38	$\alpha x^3 + x^2 + \alpha$
7	$x^2 + (\alpha+1)x + 1$		39	$\alpha x^3 + x^2 + (\alpha+1)x + 1$
8	$x^2 + (\alpha+1)x + \alpha + 1$		40	$\alpha x^3 + x^2 + (\alpha+1)x + \alpha + 1$
9	$\alpha x^2 + x$		41	$\alpha x^3 + \alpha x^2 + x$
10	$\alpha x^2 + x + \alpha$		42	$\alpha x^3 + \alpha x^2 + x + \alpha$
11	$\alpha x^2 + \alpha x + 1$		43	$\alpha x^3 + \alpha x^2 + \alpha x + 1$
12	$\alpha x^2 + \alpha x + \alpha + 1$		44	$\alpha x^3 + \alpha x^2 + \alpha x + \alpha + 1$
13	$(\alpha+1)x^2 + x + 1$		45	$\alpha x^3 + (\alpha+1)x^2 + x + 1$
14	$(\alpha+1)x^2 + x + \alpha + 1$		46	$\alpha x^3 + (\alpha+1)x^2 + x + \alpha + 1$
15	$(\alpha+1)x^2 + \alpha x$		47	$\alpha x^3 + (\alpha+1)x^2 + \alpha x$
16	$(\alpha+1)x^2 + \alpha x + \alpha$		48	$\alpha x^3 + (\alpha+1)x^2 + \alpha x + \alpha$
17	x^3		49	$(\alpha+1)x^3$
18	$x^3 + \alpha$		50	$(\alpha+1)x^3 + \alpha$
19	$x^3 + (\alpha+1)x + 1$		51	$(\alpha+1)x^3 + (\alpha+1)x + 1$
20	$x^3 + (\alpha+1)x + \alpha + 1$		52	$(\alpha+1)x^3 + (\alpha+1)x + \alpha + 1$
21	$x^3 + x^2 + 1$		53	$(\alpha+1)x^3 + x^2 + 1$
22	$x^3 + x^2 + \alpha + 1$		54	$(\alpha+1)x^3 + x^2 + \alpha + 1$
23	$x^3 + x^2 + (\alpha+1)x$		55	$(\alpha+1)x^3 + x^2 + (\alpha+1)x$
24	$x^3 + x^2 + (\alpha+1)x + \alpha$		56	$(\alpha+1)x^3 + x^2 + (\alpha+1)x + \alpha$
25	$x^3 + \alpha x^2 + x + 1$		57	$(\alpha+1)x^3 + \alpha x^2 + x + 1$
26	$x^3 + \alpha x^2 + x + \alpha + 1$		58	$(\alpha+1)x^3 + \alpha x^2 + x + \alpha + 1$
27	$x^3 + \alpha x^2 + \alpha x$		59	$(\alpha+1)x^3 + \alpha x^2 + \alpha x$
28	$x^3 + \alpha x^2 + \alpha x + \alpha$		60	$(\alpha+1)x^3 + \alpha x^2 + \alpha x + \alpha$
29	$x^3 + (\alpha+1)x^2 + x$		61	$(\alpha+1)x^3 + (\alpha+1)x^2 + x$
30	$x^3 + (\alpha+1)x^2 + x + \alpha$		62	$(\alpha+1)x^3 + (\alpha+1)x^2 + x + \alpha$
31	$x^3 + (\alpha+1)x^2 + \alpha x + 1$		63	$(\alpha+1)x^3 + (\alpha+1)x^2 + \alpha x + 1$
32	$x^3 + (\alpha+1)x^2 + \alpha x + \alpha + 1$		64	$(\alpha+1)x^3 + (\alpha+1)x^2 + \alpha x + \alpha + 1$

Table 2: 64 polynomials in $\mathcal{P}_4(S,T)$

Among them, the thirty-two (S,T)-QPP's of degree ≤ 3 are

$$g_3(x),\ g_4(x),\ g_5(x),\ g_6(x),\ g_{11}(x),\ g_{12}(x),\ g_{13}(x),\ g_{14}(x),$$

$$g_{19}(x),\ g_{20}(x),\ g_{21}(x),\ g_{22}(x),\ g_{27}(x),\ g_{28}(x),\ g_{29}(x),\ g_{30}(x),$$
$$g_{35}(x),\ g_{36}(x),\ g_{37}(x),\ g_{38}(x),\ g_{43}(x),\ g_{44}(x),\ g_{45}(x),\ g_{46}(x),$$
$$g_{51}(x),\ g_{52}(x),\ g_{53}(x),\ g_{54}(x),\ g_{59}(x),\ g_{60}(x),\ g_{61}(x),\ g_{62}(x)$$

and there are altogether 4 polynomials in $\mathcal{P}_2(S,T)$, viz.,

$$g_1(x),\ g_2(x),\ g_3(x),\ g_4(x).$$

Moreover, we know that there are essentially two distinct (S,T)-QPP's (of degree ≤ 1), namely, $g_3(x)$, $g_4(x)$.

For completeness, let us find all PP's in $\mathbb{F}_4$ of degree ≤ 3. By Theorem 7.8(i) in [4], $f(x) = ax + b$ $(a, b \in \mathbb{F}_5,\ a \neq 0)$ is a PP of $\mathbb{F}_4$, so the number of PP's with degree 1 is 12. Since $3|(4-1)$, by Corollary 7.5 in [4], there is no PP of degree 3. It remains to consider the case of second degree PP's. Direct checking shows that there are 12 PP's $\mathbb{F}_4[x]$ of degree 2, namely,

$$x^2 + d,\ \alpha x^2 + d,\ (\alpha + 1)x^2 + d$$

for all $d \in \mathbb{F}_4$. Consequently, the number of PP's of $\mathbb{F}_4$ with degree ≤ 3 is $24 = 4!$, as expected.

References

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

[2] R. Lidl and G.L. Mullen, *When does a polynomial over a finite field permute the elements of the field?,* Amer. Math. Monthly **95**(1988), 243-246.

[3] R. Lidl and G.L. Mullen, *When does a polynomial over a finite field permute the elements of the field?,* II, Amer. Math. Monthly **100**(1993), 71-74.

[4] R. Lidl and H. Niederreiter, “Finite Fields”, Addison-Wesley, Reading, 1983.