CHAPTER II

PRELIMINARIES

We start this chapter by collecting definitions, notations, and some useful results that will be used in the later chapters. Details and proofs can be found in Lidl and Niederreiter [4], Chu [8], Wan [9] and Zhou [10]. Throughout this thesis, the following symbols will be standard:

$\mathbb{N}$ the set of all natural numbers,

$\mathbb{Z}$ the set of all whole numbers,

$\mathbb{F}_q$ a finite field with q elements where q is a power of the prime p,

$\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$.

Definition 2.1.1. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial* (over $\mathbb{F}_q$), abbreviated as PP, if it is a bijection of $\mathbb{F}_q$ onto itself.

Theorem 2.1.2. [4, 7.4] *The polynomial $f(x) \in \mathbb{F}_q[x]$ is a PP if and only if the following two conditions hold:*

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

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

Corollary 2.1.3. [4, 7.5] *If $d > 1$ is a divisor of $q-1$, then there is no PP of $\mathbb{F}_q$ of degree d.*

Theorem 2.1.4. [4, 7.8] *(i) Every linear polynomial $\in \mathbb{F}_q[x]$ is a PP over $\mathbb{F}_q$.*
(ii) The monomial x^n is a PP over $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$.

Theorem 2.1.5. [4, 7.9] *The p-polynomial (linearized polynomial over $\mathbb{F}_q$)*

$$L(x) = \sum_{i=0}^{m} a_i x^{p^i} \in \mathbb{F}_q[x]$$

is a PP over $\mathbb{F}_q$ if and only if $L(x)$ only has the root 0 in $\mathbb{F}_q$.

Lemma 2.1.6. [9, 10.10] *Let $l(x)$ be a linearized polynomial over $\mathbb{F}_q$ and $\mathbb{F}_q$ be of characteristic p, then*

$$l(x+y) = l(x) + l(y),\ \forall x, y \in \mathbb{F}_q$$

and

$$l(cx) = cl(x),\ \forall x \in \mathbb{F}_q, c \in \mathbb{F}_p.$$

Conversely, if $l(x) \in \mathbb{F}_q[x]$ be such that both of the above two conditions hold, then $l(x)$ is a linearized polynomial over $\mathbb{F}_q$.

Definition 2.1.7. [8, *p.* 197] Let S be a subset of $\mathbb{F}_q$. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a *set complete mapping* associated with the set S of $\mathbb{F}_q$ if $f(x) + ax$ is a PP over $\mathbb{F}_q$ for all $a \in S$.

Theorem 2.1.8. [8, 4] *Let $\mathbb{F}_q$ be the finite field with $q = p^r$. Let $0 < s < r$ be an integer, and $d = \gcd(p^s - 1, p^r - 1) = p^{\gcd(s,r)} - 1$. Then $f(x) = x^{p^s}$ is a set complete mapping for $-S$ with $S = \mathbb{F}_q - \mathbb{F}_q^d$. The size of the set S is $1 + \frac{d-1}{d}(q-1)$.*

Let $\mathbb{F}_{q^r}$ be an extension of $\mathbb{F}_q$ with $r \in \mathbb{N}$ and consider linearized polynomials $L(x)$ of the form

$$L(x) = \sum_{i=0}^{r-1} \alpha_i x^{q^i} \in \mathbb{F}_{q^r}[x]. \tag{2.1.1}$$

Then $L(x)$ is a PP over $\mathbb{F}_{q^r}$ if and only if $\det(A) \neq 0$, where the $r \times r$ matrix A is given by

$$\begin{pmatrix} \alpha_0 & \alpha_{r-1}^{q} & \alpha_{r-2}^{q^2} & \cdots & \alpha_1^{q^{r-1}} \\ \alpha_1 & \alpha_0^{q} & \alpha_{r-1}^{q^2} & \cdots & \alpha_2^{q^{r-1}} \\ \alpha_2 & \alpha_1^{q} & \alpha_0^{q^2} & \cdots & \alpha_3^{q^{r-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ \alpha_{r-1} & \alpha_{r-2}^{q} & \alpha_{r-3}^{q^2} & \cdots & \alpha_0^{q^{r-1}} \end{pmatrix}.$$

The set of $L(x)$ in (2.1.1) that are PP's over $\mathbb{F}_{q^r}$ constitutes a group under the operation of composition modulo $x^{q^r} - x$. This group is known as the *Betti-Mathieu group.*

Theorem 2.1.9. [4, 7.27] *The Betti-Mathieu group is isomorphic to the general linear group $GL(r, \mathbb{F}_q)$ of nonsingular $r \times r$ matrices over $\mathbb{F}_q$ under matrix multiplication.*

Lemma 2.1.10. [4, 3.51] *Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be elements of $\mathbb{F}_{q^r}$. Then*

$$\begin{pmatrix} \gamma_1 & \gamma_1^q & \cdots & \gamma_0^{q^{n-1}} \\ \gamma_2 & \gamma_2^q & \cdots & \gamma_1^{q^{n-1}} \\ \vdots & \vdots & & \vdots \\ \gamma_n & \gamma_n^q & \cdots & \gamma_n^{q^{n-1}} \end{pmatrix} = \alpha_1 \prod_{j=1}^{n-1} \prod_{c_1,\ldots,c_j \in \mathbb{F}_q} \left(\alpha_{j+1} - \sum_{k=1}^{j} c_k \alpha_k \right),$$

and so the determinant is not zero if and only if $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ are linearly independent over $\mathbb{F}_q$.

Theorem 2.1.11. [4, 7.10] *Let $i \in \mathbb{N}$ with $\gcd(i, q-1) = 1$ and let u be a positive divisor of $q-1$. Let $g \in \mathbb{F}_q[x]$ be such that $g(x^u)$ has no nonzero root in $\mathbb{F}_q$. Then $f(x) = x^i(g(x^s))^{(q-1)/s}$ is a PP over $\mathbb{F}_q$.*

Theorem 2.1.12. [4, 7.18] *Let S_q be the symmetric group on q letters. For $q > 2$, S_q is generated by x^{q-2} and all linear polynomials over $\mathbb{F}_q$.*

Theorem 2.1.13. [4, 5.4] *If χ is a nontrivial character of the finite abelian group G, then*

$$\sum_{g \in G} \chi(g) = 0.$$

If $g \in G$ with $g \neq 1_G$, then

$$\sum_{g \in \hat{G}} \chi(g) = 0,$$

where $\hat{G}$ is the set of characters of G; it is an abelian group under the multiplication of characters, i.e., $\chi_1(h)\chi_2(h) = \chi_1\chi_2(h)$ for all $h \in G$.

Lemma 2.1.14. [10, 1.3] *Let a be a sequence over $\mathbb{F}_q$. Then a is an m-sequence with period q^r-1 if and only if the elements of a can be represented by $a_i = Tr(\beta\alpha^i)$, $i \geq 0$, $\beta \in \mathbb{F}_{q^r} \setminus \{0\}$ where α is a primitive element in $\mathbb{F}_{q^r}$.*

Lemma 2.1.15. [10, 1.4] *Let a be an m-sequence, then in every period of a, each nonzero r-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_r) \in \mathbb{F}_q^r$ occurs exactly once.*

Next, we give basic properties about function representation and QPP's with some examples. First, we investigate 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 $\leq s-1$.

Proposition 2.1.16. *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

$$P_f(x) = c_{s-1}x^{s-1} + c_{s-2}x^{s-2} + \cdots + c_1x + c_0 \in \mathbb{F}_q[x].$$

The system of linear equations

$$c_0 + c_1a_i + c_2a_i^2 + \cdots + c_{s-1}a_i^{s-1} = f(a_i) \quad (i = 1, \ldots, s),$$

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 2.1.16 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 2.1.17. 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 $P(1)=0 \notin T$.

Remark 2.1.18. *It is noteworthy to remark that should we be able to obtain an injective function on S, it is always possible to composite it with a unique polynomial of degree $\leq s-1$, guaranteed by Proposition 2.1.16, sending $f(S)$ bijectively onto T, resulting in an (S,T)QPP. This remark enables us at times to find QPP's over the domain S without having to worry about the set T.*

The explicit shape of those polynomials of degree $\leq s-1$ representing functions from S into T is given in the following Proposition. Since $\mathbb{F}_q^*$ is a cyclic multiplicative 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 $i \in \mathbb{N} \cup \{0, -\infty\}$ with the convention that $\alpha^{-\infty} = 0$. If S is a subset of $\mathbb{F}_q$ with $|S| = s$, then we write

$$S = \{\alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_s}\} \tag{2.1.2}$$

for some distinct $i_1, i_2, \ldots, i_s \in \mathbb{N} \cup \{0, -\infty\}$ satisfying $i_j \not\equiv i_k \pmod{q-1}$ whenever

$j \neq k$ with the convention that $\alpha^{-\infty} = 0$ and the corresponding congruence relation is interpreted as $-\infty \not\equiv i_k \pmod{q-1}$ for all $i_k \in \mathbb{N} \cup \{0\}$.

Proposition 2.1.19. *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 (2.1.2). Let*

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

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

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

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

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

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

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. Consider

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

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 versa, the second part is immediate. □

We next give an example.

Example 2.1.20. 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 Proposition 2.1.19, each polynomial of degree $\leq 3 - 1 = 2$ representing a function from S to T is of the form

$$P(x) = a_0 + a_1 x + a_2 x^2,$$

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.

Next, we derive basic properties about QPP's. Dealing with QPP's, there are two 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 2.1.21. 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 2.1.4, $f(x)$ 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 2.1.22. 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 2.1.4, 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. The problem of counting the number of PP's of fixed degree has also been of recent interest, see e.g. [11]. In contrast to the case of PP's, there are other difficulties such as those about the number of QPP's. In order to be systematic, let us 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

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

Further, let

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

The next result gives information on these sets.

Proposition 2.1.23. *(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 2.1.16, 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 example provides a numerical example of the last proposition.

Example 2.1.24. Let $S = \{1,2,4\}$, $T = \{2,3,4\}$ be subsets of $\mathbb{F}_5 := \{0,1,2,3,4\}$. By Proposition 2.1.23, 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 this table.

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	$4x^2+4x+4$

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 2.1.4, $f(x)=ax+b$; $a,b\in\mathbb{F}_5$ 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 2.1.3, there is no PP of $\mathbb{F}_5$ such that 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.

Since the number of functions from $\mathbb{F}_q$ into $\mathbb{F}_q$ is q^q and the number of functions from S into T is s^s, the number of functions f from $\mathbb{F}_q$ 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 $\deg f \leq q-1$ 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 from S onto T, then the number of (S,T)QPP's of degree $\leq q-1$ is mq^{q-s}.

The set of QPP's is closed under multiplication by nonzero elements of T and closed under addition by elements of T provided the set T is correspondingly so. We omit its straightforward proof.

Proposition 2.1.25. *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 chapter with some remarks about group structure. It is well-known that the set of all PP's of degree $< q$ over $\mathbb{F}_q$, denoted here by $A(\mathbb{F}_q)$, forms a group under composition and reduction modulo $x^q - x$. This group is isomorphic to the symmetric group on q letters, S_q. Also known is the fact, Theorem 2.1.12, 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 a related result.

Theorem 2.1.26. *Let $S \subseteq \mathbb{F}_q$ and*

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

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

Proof. 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 $f \circ g^{-1}$ is also. □