CHAPTER III
MAIN RESULTS

In this chapter, we begin with the definitions of integer-valued functions and general pseudo-polynomials over $\mathbb{F}_q[x]$ which are analogous to Hall's and de Bruijn's by reducing the linear condition of Wagner's results. Then Wagner's interpolation series that representing linear pseudo-polynomial is generalized to general pseudo-polynomial over $\mathbb{F}_q[x]$. Section 3.2 provides some algebraic structures for $\mathcal{P}$. The difference and higher order differences of integer-valued functions are studied in the last section.

3.1 Interpolation series for integer-valued polynomials and pseudo-polynomials over $\mathbb{F}_q[x]$

Definition 3.1. *An* ***integer-valued function over*** $\mathbb{F}_q[x]$ *is a function from the set* $\mathbb{F}_q[x]$ *to* $\mathbb{F}_q[x]$.

Definition 3.2. *A* ***pseudo-polynomial over*** $\mathbb{F}_q[x]$ *is an integer-valued function over* $\mathbb{F}_q[x]$ *and satisfies*

$$f(M+K) \equiv f(M) \pmod{K}$$

for all $M \in \mathbb{F}_q[x]$ *and all* $K \in \mathbb{F}_q[x]\backslash\{0\}$.

Throughout denote the set of all integer-valued functions over $\mathbb{F}_q[x]$ by IVF, and denote the set of all pseudo-polynomials over $\mathbb{F}_q[x]$ by $\mathcal{P}$.

Example 3.3.

1. The set of all constant functions $\mathbb{F}_q$ and the set of all polynomial functions $(\mathbb{F}_q[x])[t]$ are subset of $\mathcal{P}$.

2. Let $A \in \mathbb{F}_q\left(\left(\frac{1}{x}\right)\right)$. Write $A = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0 + \frac{a_{-1}}{x} + \cdots$, where $a_i \in \mathbb{F}_q$. Define

$$[A] := a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0.$$

A function $f : \mathbb{F}_q[x] \to \mathbb{F}_q[x]$ defined by

$$f(t) = [At]$$

is an integer-valued function over $\mathbb{F}_q[x]$.

To find the explicit shapes for the elements in IVF and $\mathcal{P}$, we need the following identities.

Lemma 3.4. *Let $k \in \mathbb{N}$. For $0 \le i \le q^k - 1$, we have*

$$g_{q^k-1-i} \cdot g_i = g_{q^k-1} = \frac{F_k}{L_k}.$$

Proof. Let $i \in \mathbb{N}_0$ with $0 \le i \le q^k - 1$. Clearly, $g_{q^k-1} \cdot g_0 = g_{q^k-1}$ so we assume that $i \ge 1$. It can be expressed with respect to base q as

$$i = \alpha_0 + \alpha_1 q + \alpha_2 q^2 + \cdots + \alpha_{d(i)} q^{d(i)}.$$

where $\alpha_{d(i)} \ne 0$ and $0 \le \alpha_j < q$ for all j. Since $i \le q^k - 1$, $d(i) \le k - 1$. If $d(i) < k - 1$, set $\alpha_{d(i)+1}, \alpha_{d(i)+2}, \ldots, \alpha_{k-1} = 0$. So we have

$$i = \alpha_0 + \alpha_1 q + \alpha_2 q^2 + \cdots + \alpha_{k-1} q^{k-1}.$$

where $0 \le \alpha_j < q$ for all j. Since $q^k - 1 = (q-1)(q^{k-1} + q^{k-2} + \cdots + 1)$, we have by Definition 2.9, that

$$\begin{aligned} g_{q^k-1} &= F_1^{q-1}F_2^{q-1}\cdots F_{k-1}^{q-1} \\ &= (F_1^{q-1-\alpha_1}F_2^{q-1-\alpha_2}\cdots F_{k-1}^{q-1-\alpha_{k-1}})\cdot(F_1^{\alpha_1}F_2^{\alpha_2}\cdots F_{k-1}^{\alpha_{k-1}}) \\ &= g_{q^k-1-i}\cdot g_i. \end{aligned}$$

Next, we will show that $g_{q^k-1}=\dfrac{F_k}{L_k}$. By applying Definition 2.6, this yields

$$\begin{aligned} \frac{F_k}{L_k} &= \frac{[k][k-1]^q[k-2]^{q^2}\cdots[1]^{q^{k-1}}}{[k][k-1][k-2]\cdots[1]} \\ &= [k-1]^{q-1}[k-2]^{q^2-1}\cdots[1]^{q^{k-1}-1} \\ &= \left([k-1][k-2]^{q+1}\cdots[1]^{q^{k-2}+q^{k-3}+\cdots+1}\right)^{q-1} \\ &= \left\{\left([k-1][k-2]^q\cdots[1]^{q^{k-2}}\right)\left([k-2][k-3]^q\cdots[1]^{q^{k-3}}\right)\cdots([2][1]^q)([1])\right\}^{q-1} \\ &= (F_{k-1}F_{k-2}\cdots F_2F_1)^{q-1} \\ &= F_{k-1}^{q-1}F_{k-2}^{q-1}\cdots F_2^{q-1}F_1^{q-1} \\ &= g_{q^k-1}. \end{aligned}$$

This completes the proof. □

Theorem 3.5. *Let $f(t)\in IVF$. Then it is uniquely representable as an interpolation series of the form*

$$f(t)=\sum_{i=0}^{\infty}A_i\frac{G_i(t)}{g_i},$$

where $A_i\in\mathbb{F}_q[x]$.

Remark This representation is well-defined for $t\in\mathbb{F}_q[x]$ because for each $M\in\mathbb{F}_q[x]$ with $d(i)>\deg M$, we have $\psi_{d(i)}(M)=0$. By the Definition 2.9,

$$G_i(M)=0.$$

So the sum $\sum_{i=0}^{\infty}A_i\dfrac{G_i(M)}{g_i}$ reduces to a finite sum and **the representation is interpreted as yielding the same value of $f(M)$ on both sides.**

Proof of Theorem 3.5. Assume that $f(t)$ is an integer-valued function. We first show that for $n \in \mathbb{N}$, there exists a unique polynomial $P_n^{(f)}(t) \in \mathbb{F}_q(x)[t]$ of degree less than or equal to $q^n - 1$, such that $P_n^{(f)}(M) = f(M)$ for all polynomials $M \in \mathbb{F}_q[x]$ of degree less than or equal to $n - 1$.

Let $n \in \mathbb{N}$. Set $c_0 := f(0)$ and let $P_n(t) := c_0 + c_1 t + \cdots + c_{q^n-1}t^{q^n-1}$. We show that all c_i's are uniquely determined. Let $M_1, M_2, \ldots, M_{q^n-1} \in \mathbb{F}_q[x]\setminus\{0\}$ be all distinct polynomials of degree less than or equal to $n - 1$. To fulfill the requirement that $P_n(M_i) = f(M_i)$ for all i, it suffices to show that the following system of equations is solvable for the coefficients c_i's.

$$\begin{aligned} f(0) &= c_0, \\ f(M_1) &= c_0 + c_1 M_1 + \cdots + c_{q^n-1} M_1^{q^n-1}, \\ &\vdots \\ f(M_{q^n-1}) &= c_0 + c_1 M_{q^n-1} + \cdots + c_{q^n-1} M_{q^n-1}^{q^n-1}. \end{aligned}$$

Rewriting the previous system to the matrix form, we have

$$\begin{bmatrix} M_1 & M_1^2 & M_1^3 & \ldots & M_1^{q^n-1} \\ M_2 & M_2^2 & M_2^3 & \ldots & M_2^{q^n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ M_{q^n-1} & M_{q^n-1}^2 & M_{q^n-1}^3 & \ldots & M_{q^n-1}^{q^n-1} \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_{q^n-1} \end{bmatrix} = \begin{bmatrix} f(M_1) - f(0) \\ f(M_2) - f(0) \\ \vdots \\ f(M_{q^n-1}) - f(0) \end{bmatrix}.$$

We have

$$\det C := \det \begin{bmatrix} M_1 & M_1^2 & M_1^3 & \ldots & M_1^{q^n-1} \\ M_2 & M_2^2 & M_2^3 & \ldots & M_2^{q^n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ M_{q^n-1} & M_{q^n-1}^2 & M_{q^n-1}^3 & \ldots & M_{q^n-1}^{q^n-1} \end{bmatrix}$$

$$= (M_1 M_2 \cdots M_{q^n-1}) \det \begin{bmatrix} 1 & M_1 & M_1^2 & \dots & M_1^{q^n-2} \\ 1 & M_2 & M_2^2 & \dots & M_2^{q^n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & M_{q^n-1} & M_{q^n-1}^2 & \dots & M_{q^n-1}^{q^n-2} \end{bmatrix}$$

$$= M_1 M_2 \cdots M_{q^n-1} \prod_{1 \le i < j \le q^n - 1} (M_i - M_j).$$

Since $\mathbb{F}_q[x]$ is an integral domain and $M_i - M_j \neq 0$ for $i \neq j$, $\det C \neq 0$. This shows that the system is solvable and has a unique solution. Now we have the unique polynomial $P_n^{(f)}(t)$ as required.

Invoking upon Theorem 2.13, this polynomial can also be uniquely expressed as

$$P_n^{(f)}(t) = \sum_{i=0}^{q^n-1} C_i G_i(t).$$

We have $i < q^{d(i)+1}$ where $d(i)$ is the upper q-index of i. Then, with $m_i = d(i) + 1$,

$$C_i = (-1)^{m_i} \frac{L_{m_i}}{F_{m_i}} \sum_{\deg M < m_i} G'_{q^{m_i}-1-i}(M) P_n^{(f)}(M).$$

For each $0 \le i \le q^n - 1$, we observe that $d(i) \le n - 1$. Therefore $m_i = d(i) + 1 \le n$. Moreover, from the first part of the proof, $f(M) = P_n^{(f)}(M)$ for all M of degree less than n. It follows that

$$C_i = (-1)^{m_i} \frac{L_{m_i}}{F_{m_i}} \sum_{\deg M < m_i} G'_{q^{m_i}-1-i}(M) f(M).$$

Then

$$g_i C_i = (-1)^{m_i} \frac{L_{m_i}}{F_{m_i}} g_i \sum_{\deg M < m_i} G'_{q^{m_i}-1-i}(M) f(M).$$

By Lemma 3.4 and the fact that $i \le q^{d(i)} - 1 < q^{d(i)+1} = q^{m_i}$, we have $\frac{L_{m_i}}{F_{m_i}} g_i = \frac{1}{g_{q^{m_i}-1-i}}$. So,

$$g_i C_i = (-1)^{m_i} \sum_{\deg M < m_i} \frac{G'_{q^{m_i}-1-i}(M)}{g_{q^{m_i}-1-i}} f(M).$$

Therefore,

$$P_n^{(f)}(t) = \sum_{i=0}^{q^n-1} A_i \frac{G_i(t)}{g_i},$$

where

$$A_i = (-1)^{m_i} \sum_{\deg M < m_i} \frac{G'_{q^{m_i}-1-i}(M)}{g_{q^{m_i}-1-i}} f(M).$$

By Theorem 2.12, $\dfrac{G'_{q^{m_i}-1-i}(M)}{g_{q^{m_i}-1-i}} \in \mathbb{F}_q[x]$ implies that $A_i \in \mathbb{F}_q[x]$.

With the above preparation, we proceed now to derive our interpolation series. To this end, consider

$$P_n^{(f)}(t) = \sum_{i=0}^{q^n-1} A_i \frac{G_i(t)}{g_i}$$

and

$$P_{n+1}^{(f)}(t) = \sum_{i=0}^{q^{n+1}-1} A'_i \frac{G_i(t)}{g_i},$$

where the coefficients A_i's and A'_i's are defined as above. For $0 \le i \le q^n - 1$, we have $m_i = d(i) + 1 \le n$. So for each $M \in \mathbb{F}_q[x]$ with $\deg M < m_i \le n$, we have

$$P_n^{(f)}(M) = f(M) = P_{n+1}^{(f)}(M).$$

Thus,

$$\begin{aligned} A_i &= (-1)^{m_i} \frac{L_{m_i}}{F_{m_i}} \sum_{\deg M < m_i} G'_{q^{m_i}-1-i}(M) P_n^{(f)}(M) \\ &= (-1)^{m_i} \frac{L_{m_i}}{F_{m_i}} \sum_{\deg M < m_i} G'_{q^{m_i}-1-i}(M) f(M) \\ &= (-1)^{m_i} \frac{L_{m_i}}{F_{m_i}} \sum_{\deg M < m_i} G'_{q^{m_i}-1-i}(M) P_{n+1}^{(f)}(M) \\ &= A'_i. \end{aligned}$$

This implies that

$$\sum_{i=0}^{q^{n+1}-1} A'_i \frac{G_i(t)}{g_i} = P_n^{(f)}(t) + \sum_{i=q^n}^{q^{n+1}-1} A'_i \frac{G_i(t)}{g_i}.$$

Since $G_i(M) = 0$ for all i with $d(i) > \deg M$, for $M \in \mathbb{F}_q[x]$ of degree $n-1$, we have

$$\begin{aligned}\sum_{i=0}^{\infty} A_i \frac{G_i(M)}{g_i} &= \sum_{i=0}^{q^n-1} A_i \frac{G_i(M)}{g_i} + \sum_{i=q^n}^{\infty} A_i \frac{G_i(M)}{g_i} \\ &= \sum_{i=0}^{q^n-1} A_i \frac{G_i(M)}{g_i} + 0 \\ &= f(M),\end{aligned}$$

showing that the function $f(t)$ can be represented by the stated interpolation series. □

Modifying the preceding proof, we next derive interpolation series for pseudo-polynomials.

Theorem 3.6. *Let $f(t) \in IVF$. Then $f(t) \in \mathcal{P}$ if and only if it is representable as an interpolation series of the form*

$$\sum_{i=0}^{\infty} B_i L_{d(i)} \frac{G_i(t)}{g_i},$$

where $B_i \in \mathbb{F}_q[x]$ and $d(i)$ denotes the upper q-index of i.

Proof. From the proof of Theorem 3.5, for all $n \in \mathbb{N}_0$, the unique polynomial of degree $\leq q^n - 1$ which takes the same values as $f(t)$ over the set of all polynomials $M \in \mathbb{F}_q[x]$ with $\deg M < n$ is

$$P_n^{(f)}(t) = \sum_{i=0}^{q^n-1} A_i \frac{G_i(t)}{g_i},$$

and for $r \in \mathbb{N}$ with $q^r > i$, we have

$$A_i = (-1)^r \sum_{\deg N < r} \frac{G'_{q^r-1-i}(N) f(N)}{g_{q^r-1-i}}.$$

Moreover, $f(t)$ is a pseudo-polynomial, if and only if

$$P_n^{(f)}(M+K) = f(M+K) \equiv f(M) = P_n^{(f)}(M) \pmod{K}$$

for all $M, K \in \mathbb{F}_q[x], K \neq 0$ and $\deg M, \deg K < n$ for all $n \in \mathbb{N}_0$. By Theorem 2.18,

$$\begin{aligned} P_n^{(f)}(t) \in \mathcal{P} \text{ for all } n \in \mathbb{N}_0 \quad &\Leftrightarrow P_n^{(f)}(t) \in I_0 \cap I_1 = \bar{I}_1 \text{ for all } n \in \mathbb{N}_0 \\ &\Leftrightarrow L_{d(i)} \mid A_i \text{ for all } i \leq n \text{ and } n \in \mathbb{N}_0. \end{aligned}$$

Hence, the desired result follows. □

3.2 Some Algebraic Structures of $\mathcal{P}$

It is known that IVF is a commutative ring under addition and multiplication of functions. The identity under addition is $0(t)$ defined by $0(t) = 0 \in \mathbb{F}_q$ for all $t \in \mathbb{F}_q[x]$ and the identity under multiplication is $1(t)$ defined by $1(t) = 1 \in \mathbb{F}_q$ for all $t \in \mathbb{F}_q[x]$. The inverse under addition of $f(t) \in IVF$ is $(-f)(t) := -f(t)$ for all $t \in \mathbb{F}_q[x]$.

Theorem 3.7. *$\mathcal{P}$ is a subring of IVF.*

Proof. Note that $\mathcal{P} \subset IVF$ and $0(t), 1(t) \in \mathcal{P}$. To show that $\mathcal{P}$ is a subring of IVF, it suffices to show that $f(t) - g(t), f(t)g(t) \in \mathcal{P}$ for all $f(t), g(t) \in \mathcal{P}$. Let $f(t), g(t) \in \mathcal{P}$. Then

$$(f-g)(M+K) = f(M+K) - g(M+K) \equiv f(M) - g(M) = (f-g)(M) \pmod{K}$$

and

$$(f \cdot g)(M+K) = f(M+K) \cdot g(M+K) \equiv f(M) \cdot g(M) = (f \cdot g)(M) \pmod{K}$$

for all $M \in \mathbb{F}_q[x]$ and $K \in \mathbb{F}_q[x] \backslash \{0\}$. This completes the proof. □

We define units in $\mathcal{P}$ in the usual way.

Definition 3.8. *An element $u(t) \in \mathcal{P}$ is called a **unit** if there is $v(t) \in \mathcal{P}$ such that $u(t)v(t) = 1(t)$.*

Denote by $\mathcal{U}(\mathcal{P})$ be the set of all units in $\mathcal{P}$.

Lemma 3.9. *We have* $\quad \mathcal{U}(\mathcal{P}) = \mathbb{F}_q^* := \mathbb{F}_q \backslash \{0\}$.

Proof. Let $c \in \mathbb{F}_q^*$. Since $\mathbb{F}_q^*$ is a multiplicative group, there exists $c' \in \mathbb{F}_q^*$ such that $c'c = 1$. This shows that $\mathbb{F}_q^* \subseteq \mathcal{U}(\mathcal{P})$.

Conversely, let

$$f(t) = \sum_{i=0}^{\infty} B_i L_{d(i)} \frac{G_i(t)}{g_i}$$

be a unit in $\mathcal{P}$. Then there exists $g(t) \in \mathcal{P}$ such that

$$g(t)f(t) = 1(t).$$

Substituting for t by any $M \in \mathbb{F}_q[x]$, we arrive at

$$g(M) = (f(M))^{-1}, \text{ the inverse of } f(M) \text{ in } \mathbb{F}_q[x].$$

This implies that $f(\mathbb{F}_q[x]) \subseteq \mathbb{F}_q^*$. Moreover, $B_0 = f(0) \in \mathbb{F}_q^*$. To show that $f(t) \in \mathbb{F}_q^*$, it suffices to show that $f(N) = B_0$ for any $N \in \mathbb{F}_q[x] \backslash \{0\}$. We have

$$f(N) = f(0 + N) \equiv f(0) = B_0 \pmod{N}. \tag{$*$}$$

If $N \in \mathbb{F}_q[x] \backslash \mathbb{F}_q$, using $f(\mathbb{F}_q[x]) \subseteq \mathbb{F}_q^*$, the relation $(*)$ shows that $f(N) = B_0$. If $N \in \mathbb{F}_q^*$, since

$$f(N) \equiv f(N + x) \pmod{x}$$

and $f(N + x) = B_0$ by the previous case, we conclude again that $f(N) = B_0$. This can hold for all $M \in \mathbb{F}_q[x]$ only when $f(t)$ is a constant function with value in $\mathbb{F}_q^*$, showing then that $\mathcal{U}(\mathcal{P}) \subseteq \mathbb{F}_q^*$. □

Definition 3.10. *A non-unit element $f(t) \in \mathcal{P}\backslash\{0(t)\}$ is called an* ***irreducible element*** *in $\mathcal{P}$ if whenever $f(t) = g(t)h(t)$ for some $g(t), h(t) \in \mathcal{P}$, then either $g(t)$ or $h(t)$ is a unit.*

Theorem 3.11. *The set $\mathcal{P}$ is an integral domain.*

Proof. By Theorem 3.7, we have $\mathcal{P}$ is a commutative ring under addition and multiplication. There remains to check that it has no zero divisors. Assume that $f(t)$ and $g(t) \in \mathcal{P}\backslash\{0(t)\}$. Then there are $M_1, M_2 \in \mathbb{F}_q[x]$ such that

$$f(M_1) = K_1 \neq 0$$

and

$$g(M_2) = K_2 \neq 0.$$

Let P_1 and P_2 be two distinct irreducible polynomials in $\mathbb{F}_q[x]$ such that

$$P_1 \nmid K_1 \quad \text{and} \quad P_2 \nmid K_2.$$

Since $\gcd(P_1, P_2) = 1$, there are $A, B \in \mathbb{F}_q[x]$ such that

$$AP_1 - BP_2 = 1.$$

If $M_1 \neq M_2$, then

$$(M_2 - M_1)AP_1 - (M_2 - M_1)BP_2 = M_2 - M_1,$$

i.e.,

$$M_2 + h_2P_2 = M_1 + h_1P_1,$$

where $h_1 = (M_2 - M_1)A \neq 0$ and $h_2 = (M_2 - M_1)B \neq 0$. Then

$$f(M_1 + h_1P_1) \equiv f(M_1) \equiv K_1 \pmod{h_1P_1}$$

and

$$g(M_2 + h_2P_2) \equiv g(M_2) \equiv K_2 \pmod{h_2P_2}.$$

Since $P_1 \nmid K_1$ and $P_2 \nmid K_2$, these indicate that both $f(M_1+h_1P_1)$ and $g(M_2+h_2P_2)$ are not zero. We have

$$\begin{aligned}(f \cdot g)(M_1 + h_1P_1) &= f(M_1 + h_1P_1) \cdot g(M_1 + h_1P_1)\\ &= f(M_1 + h_1P_1) \cdot g(M_2 + h_2P_2)\\ &\neq 0.\end{aligned}$$

If $M_1 = M_2$, then

$$\begin{aligned}(f \cdot g)(M_1) &= f(M_1)g(M_1)\\ &= f(M_1)g(M_2)\\ &= K_1K_2\\ &\neq 0.\end{aligned}$$

The two possibilities show that $(f \cdot g)(t)$ is not a zero map, and so $\mathcal{P}$ has no zero divisor. □

To show that $\mathcal{P}$ is not a unique factorization domain, we need three more lemmas.

Lemma 3.12. *Let $f(t) \in \mathcal{P}$ with the expansion in Theorem 3.6. If $B_i = 0$ for all $i \geq 2q$, then $f(t) \in \mathbb{F}_q[x][t]$.*

Proof. If $B_i = 0$ for $i \geq 2q$, then the interpolation series reduces to

$$f(t) = \sum_{i=0}^{2q-1} B_i L_{d(i)} \frac{G_i(t)}{g_i}.$$

By Remark 2.10, we have that $g_i = L_{d(i)}$ for $0 \leq i \leq 2q - 1$, and so $f(t) \in (\mathbb{F}_q[x])[t]$. □

Definition 3.13. *Let $f(t), g(t) \in IVF$. Then $f(t) = O(g(t))$ if and only if there exist a positive real number c and a positive integer N such that*

$$|f(M)| \leq c|g(M)| \quad \textit{for all } M \in \mathbb{F}_q[x] \textit{ with } \deg M \geq N.$$

Lemma 3.14. *Let $f(t) \in \mathcal{P}$ and $m \in \mathbb{N}$. If $f(t) = O(x^{m \deg t})$, then $f(t) \in \mathbb{F}_q(x)[t]$.*

Proof. From the hypothesis, there exist $c > 0$ and $N \in \mathbb{N}$ such that $|f(M)| \leq cq^{m \deg M}$ for all $M \in \mathbb{F}_q[x]$, with $\deg M \geq N$. Since $q^{d(n)+1} > n$, by Theorem 2.14, we have

$$A_n = (-1)^{d(n)+1} \frac{L_{d(n)+1}}{F_{d(n)+1}} \sum_{\substack{\deg K = d(n)+1 \\ K \text{ is monic}}} G'_{q^{d(n)+1}-1-n}(K) f(K).$$

We show now that $A_n = O(x^{(m-1)(d(n)+1)})$. Let $N' = \max\{N, 2q\}$, and choose j so that $d(j) \geq N'$. Write

$$j = \gamma_0 + \gamma_1 q + \gamma_2 q^2 + \cdots + \gamma_{d(j)} q^{d(j)},$$

where $0 \leq \gamma_k \leq q - 1$, $\gamma_{d(j)} \neq 0$. Then,

$$\begin{aligned} q^{d(j)+1} - j - 1 &= (q-1)(q^{d(j)} + q^{d(j)-1} + \cdots + 1) - j \\ &= (q-1)(q^{d(j)} + q^{d(j)-1} + \cdots + 1) - (\gamma_0 + \gamma_1 q + \cdots + \gamma_{d(j)} q^{d(j)}) \\ &= \beta_0 + \beta_1 q + \cdots + \beta_{d(j)} q^{d(j)}, \text{ where } \beta_k = (q-1) - \gamma_k. \end{aligned}$$

Therefore $d(q^{d(j)+1} - 1) = d(j)$ and so, for a monic polynomial K of degree $d(j)+1$, we have

$$\begin{aligned} G'_{q^{d(j)+1}-1-j}(K) &= \prod_{k=0}^{d(j)} G'_{\beta_k q^k}(K) \\ &= \prod_{\substack{k=0 \\ \beta_k \neq q-1}}^{d(j)} G'_{\beta_k q^k}(K) \prod_{\substack{k=0 \\ \beta_k = q-1}}^{d(j)} G'_{\beta_k q^k}(K) \end{aligned}$$

$$= \prod_{\substack{k=0 \\ \beta_k \neq q-1}}^{d(j)} \psi_k^{\beta_k}(K) \prod_{\substack{k=0 \\ \beta_k = q-1}}^{d(j)} \{\psi_k^{q-1}(K) - F_k^{q-1}\}.$$

For $0 \leq k \leq d(j)$, we have

$$\deg F_k = kq^k \quad \text{and} \quad \deg \psi_k(K) = \deg \prod_{deg E<k} (K - E) = q^k(d(j) + 1).$$

Since $d(j) + 1 > k$. we see that

$$\deg\{\psi_k^{q-1}(K) - F_k^{q-1}\} = \deg \psi_k^{q-1}(K).$$

and so

$$\begin{aligned} \deg G'_{q^{d(j)+1}-1-j}(K) &= \deg \prod_{k=0}^{d(j)} \psi_k^{\beta_k}(K) \\ &= (d(j) + 1)(\beta_0 + \beta_1 q^1 + \cdots + \beta_{d(j)} q^{d(j)}) \\ &= (d(j) + 1)(q^{d(j)+1} - j - 1). \end{aligned}$$

Thus,

$$\begin{aligned} \deg A_j &\leq \deg L_{d(j)+1} - \deg F_{d(j)+1} + \deg G'_{q^{d(j)+1}-1-j}(K) + \deg f(K) \\ &< (q + q^2 + \cdots + q^{d(j)+1}) - (d(j) + 1)q^{d(j)+1} + (d(j) + 1)(q^{d(j)+1} - j - 1) \\ &\quad + c' + m(d(j) + 1) \qquad \text{(for some } c' \text{ such that } c < q^{c'}) \\ &< 2q^{d(j)+1} - (j + 1)(d(j) + 1) + c' + m(d(j) + 1) \\ &< 2q^{d(j)+1} - q^{d(j)}(2q) + c' + (m - 1)(d(j) + 1) \qquad \text{(since } j \geq q^{d(j)} \text{ and } d(j) + 1 > 2q) \\ &= c' + (m - 1)(d(j) + 1). \end{aligned}$$

Consequently, for sufficiently large k, we have $|A_k| < C|x^{(m-1)(d(k)+1)}|$ for some

$C > 0$. Since $f \in \mathcal{P}$, we know then that $L_{d(k)} \mid A_k$. Therefore,

$$\deg L_{d(k)} \leq \deg A_k \quad \text{or} \quad A_k = 0.$$

If some $A_k \neq 0$, then for k sufficiently large, we get

$$\begin{aligned} q^{d(k)} &< q^1 + q^2 + \cdots + q^{d(k)} \\ &= \deg L_{d(k)} \\ &\leq \deg A_k \\ &< c' + (m-1)(d(k)+1), \end{aligned}$$

which is a contradiction. and so $A_k = 0$, i.e.. $f(t)$ is a polynomial over $\mathbb{F}_q(x)$. □

Lemma 3.15. *Let $f(t) \in \mathcal{P}$. If $f(t) \in \mathbb{F}_q(x)[t]$ and if there exist $g(t), h(t) \in \mathcal{P}$ such that*

$$f(t) = g(t)h(t)$$

for all $t \in \mathbb{F}_q[x]$, then $g(t), h(t) \in \mathbb{F}_q(x)[t]$.

Proof. Write $f(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_0$. Let $M \in \mathbb{F}_q[x]$. Then,

$$|f(M)| \leq Aq^{n \deg M},$$

where $A = \max\{|a_0|, |a_1|, \ldots, |a_n|\}$. If $g(t)$ is not a polynomial, Lemma 3.14 yields $g(t) \neq O(x^{n \deg t})$, which in turn implies that there exists an increasing sequence $\{n_j\}$ with $\deg M_j = n_j$ such that

$$|g(M_j)| > Aq^{n \deg M_j} = Aq^{n \cdot n_j},$$

and so

$$Aq^{n\, n_j} \geq |f(M_j)| = |g(M_j)||h(M_j)| > Aq^{n\, n_j},$$

which is a contradiction. □

In particular, Lemma 3.15 holds for linear pseudo-polynomials over $\mathbb{F}_q[x]$. The following corollaries provide alternative proofs for this linear case independently from previous lemmas. Let $\mathcal{L}$ be the set of all linear pseudo-polynomials over $\mathbb{F}_q[x]$.

Corollary 3.16. *If $f(t) \in \mathcal{L}$ and $f(x^n) = O(x^{q^n})$, then $f(t) \in \mathbb{F}_q(x)[t]$.*

Proof. Assume that $f(t) \in \mathcal{L}$ and $f(x^n) = O(x^{q^n})$. Then there exists $c > 0$ and $N \in \mathbb{N}$ such that $|f(x^n)| \leq cq^{q^n}$ for all $n > N$. Since $f(t) \in \mathcal{L}$, for each $n \in \mathbb{N}$

$$f(x^n) = \frac{A_0\psi_0(x^n)}{F_0} + \frac{A_1\psi_1(x^n)}{F_1} + \frac{A_2\psi_2(x^n)}{F_2} + \ldots + A_n.$$

So

$$A_n = \frac{\det\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & f(x^0) \\ \frac{\psi_0(x^1)}{F_0} & 1 & 0 & \cdots & 0 & f(x^1) \\ \frac{\psi_0(x^2)}{F_0} & \frac{\psi_1(x^2)}{F_1} & 1 & \cdots & 0 & f(x^2) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{\psi_0(x^{n-1})}{F_0} & \frac{\psi_1(x^{n-1})}{F_1} & \frac{\psi_2(x^{n-1})}{F_2} & \cdots & 1 & f(x^{n-1}) \\ \frac{\psi_0(x^n)}{F_0} & \frac{\psi_1(x^n)}{F_1} & \frac{\psi_2(x^n)}{F_2} & \cdots & \frac{\psi_{n-1}(x^n)}{F_{n-1}} & f(x^n) \end{bmatrix}}{\det\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ \frac{\psi_0(x^1)}{F_0} & 1 & 0 & \cdots & 0 & 0 \\ \frac{\psi_0(x^2)}{F_0} & \frac{\psi_1(x^2)}{F_1} & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{\psi_0(x^{n-1})}{F_0} & \frac{\psi_1(x^{n-1})}{F_1} & \frac{\psi_2(x^{n-1})}{F_2} & \cdots & 1 & 0 \\ \frac{\psi_0(x^n)}{F_0} & \frac{\psi_1(x^n)}{F_1} & \frac{\psi_2(x^n)}{F_2} & \cdots & \frac{\psi_{n-1}(x^n)}{F_{n-1}} & 1 \end{bmatrix}}.$$

Since the matrix in the denominator of A_n is lower triangular, its determinant is

1. Thus

$$A_n = f(x^n) - f(x^{n-1})\frac{\psi_{n-1}(x^n)}{F_{n-1}} + f(x^{n-2})D_{n-2,n} - f(x^{n-3})D_{n-3,n} + \dots$$
$$+ (-1)^{n+2} f(x^0) D_{0,n},$$

where $D_{i,j}$ is the determinant of the matrix in numerator of A_n which cut row $(i+1)^{\text{th}}$ and column $(j+1)^{\text{th}}$ for all $0 \le i, j \le n$. We have

$$\begin{aligned}
|D_{0,n}| &\le |\frac{\psi_0(x^1)}{F_0}\frac{\psi_1(x^2)}{F_1}\frac{\psi_2(x^3)}{F_2}\cdots\frac{\psi_{n-1}(x^n)}{F_{n-1}}| &&= q^{q^1+q^2+q^3+\dots q^{n-1}},\\
|D_{1,n}| &\le |\frac{\psi_1(x^2)}{F_1}\frac{\psi_2(x^3)}{F_2}\frac{\psi_3(x^4)}{F_3}\cdots\frac{\psi_{n-1}(x^n)}{F_{n-1}}| &&= q^{q^1+q^2+q^3+\dots q^{n-1}},\\
|D_{2,n}| &\le |\frac{\psi_2(x^3)}{F_2}\frac{\psi_3(x^4)}{F_3}\frac{\psi_4(x^5)}{F_4}\cdots\frac{\psi_{n-1}(x^n)}{F_{n-1}}| &&= q^{q^2+q^3+q^4+\dots q^{n-1}},\\
|D_{3,n}| &\le |\frac{\psi_3(x^4)}{F_3}\frac{\psi_4(x^5)}{F_4}\frac{\psi_5(x^6)}{F_5}\cdots\frac{\psi_{n-1}(x^n)}{F_{n-1}}| &&= q^{q^3+q^4+q^5+\dots q^{n-1}},\\
&\vdots &&\vdots\\
|D_{n-1,n}| &\le |\frac{\psi_{n-1}(x^n)}{F_{n-1}}| &&= q^{q^{n-1}}.\\
|D_{n,n}| &\le |1| &&= q^0.
\end{aligned}$$

Next we will claim that $A_n = O(x^{q^n})$. Let $n \ge N$. For each $N \le m \le n-1$,

$$|D_{m,n}||f(x^m)| \le q^{q^m+q^{m+1}+\dots+q^{n-1}}cq^{q^m} \le cq^{q^n}.$$

Since $|D_{n,n}||f(x^n)| \le cq^{q^n}$, it follows that $|D_{m,n}||f(x^m)| \le cq^{q^n}$ for all $N \le m \le n$. Let $q^r := \max\{|f(x^0)|, |f(x^1)|, |f(x^2)|, \dots, |f(x^{N-1})|\}$. Then

$$\begin{aligned}
|A_n| &\le \max\{\max_{0\le i\le N-1}\{|D_{i,n}|q^r\}, cq^{q^n}\}\\
&= \max\{|D_{0,n}|q^r, cq^{q^n}\}\\
&= \max\{q^{q^1+q^2+\dots+q^{n-1}}q^r, cq^{q^n}\}\\
&\le \max\{q^{q^1+q^2+\dots+q^{n-1}}\max\{q^r, c\}, q^{q^n}\max\{q^r, c\}\}\\
&= q^{q^n}\max\{q^r, c\}.
\end{aligned}$$

Hence $A_n = O(x^{q^n})$, as required. Since $A_n = O(x^{q^n})$, there exists $c > 0$ and for sufficiently large $K \in \mathbb{N}$,

$$\deg A_k \le q^k + c,$$

for all $k > K$. Since $f(t) \in \mathcal{L}$, $L_k \mid A_k$ for all k. That is

$$\deg L_k \leq \deg A_k \quad \text{or} \quad A_k = 0.$$

Note that

$$\deg L_k = q^1 + q^2 + \cdots + q^k.$$

So $A_k = 0$ for sufficiently large $k > K$. Hence $f(t)$ is a polynomial. ☐

Corollary 3.17. *Let $f(t) \in \mathcal{L}$. If $f(t) \in \mathbb{F}_q(x)[t]$ and if there exist $g(t), h(t) \in \mathcal{L}$ such that*

$$f(t) = g(t)h(t)$$

for all $t \in \mathbb{F}_q[x]$, then $g(t), h(t) \in \mathbb{F}_q(x)[t]$.

Proof. Assume that $f(t) = a_m t^{q^m} + a_{m-1} t^{q^{m-1}} + \cdots + a_0 t$. So

$$|f(x^n)| \leq M q^{nq^m}$$

where

$$M = \max\{|a_0|, |a_1|, \ldots, |a_m|\}.$$

Assume by a contradiction that $g(t)$ is not a polynomial function in $\mathcal{P}$. We have

$$g(x^n) \neq O(x^{q^n}).$$

So there exists an increasing sequence $\{n_j\}$ such that $|g(x^{n_j})| > M q^{q^{n_j}}$ for all $j \in \mathbb{N}$. Therefore, for a sufficiently large j, we have

$$\begin{aligned} M q^{n_j q^m} &\geq |f(x^{n_j})| \\ &= |g(x^{n_j})||h(x^{n_j})| \\ &> M q^{q^{n_j}}. \end{aligned}$$

which is a contradiction. ☐

Example 3.18. Let E be a polynomial over $\mathbb{F}_q[x]$. By Theorem 3.6, the polynomial $t - E$ is a pseudo-polynomial ($A_0 = -E$, $A_1 = 1$ and $A_i = 0$ for all $i > 1$). If $t - E$ is reducible over $\mathcal{P}$,

$$t - E = f(t)g(t)$$

for some non-unit elements $f(t), g(t) \in \mathcal{P}$. By Lemma 3.15, $f(t)$ and $g(t)$ are polynomials over $\mathbb{F}_q(x)$ with an indeterminate t. Thus $\deg f(t), \deg g(t) \leq 1$. By Lemma 3.12, $f(t)$ and $g(t)$ are polynomials over $\mathbb{F}_q[x]$. That is $f(t)$ or $g(t) \in \mathbb{F}_q[x]$. Without loss of generality, we may assume that $f(t) \in \mathbb{F}_q[x]$.

- If $f(t) \in \mathbb{F}_q$, by Lemma 3.9 $f(t)$ is a unit in $\mathcal{P}$, a contradiction.
- If $f(t) \in \mathbb{F}_q[x]\backslash\mathbb{F}_q$, then

$$g(t) = \frac{t - E}{f(t)} \quad \in \mathbb{F}_q[x][t].$$

Thus $g(t) \in \mathbb{F}_q$. By Lemma 3.9, it is a unit in $\mathcal{P}$, a contradiction.

So, for each $E \in \mathbb{F}_q[x]$, $t - E$ is irreducible in $\mathcal{P}$. Similarly, we can prove that $f(t) = x$ is irreducible in $\mathcal{P}$.

By Lemma 3.6, Lemma 3.14 and Lemma 3.15, we have the conclusion for the factorization in $\mathcal{P}$ as follows.

Theorem 3.19. *$\mathcal{P}$ is not a unique factorization domain.*

Proof. Let us first treat the case $q = 2$. Consider

$$g(t) := \frac{\psi_2(t)}{x}.$$

By Theorem 3.6, $g(t)$ has an interpolation of the form

$$g(t) = \frac{A_4 G_4}{g_4},$$

where $A_1 = F_2/x$, and so $g(t) \in \mathcal{P}$. Since

$$g(t) = \frac{1}{x} \prod_{\deg E<2} (t - E),$$

we see that $g(t) \in \mathbb{F}_q(x)[t]$ with degree $q^2 = 4 = 2q$. If $g(t)$ could be factored in $\mathbb{F}_q(x)[t] \cap \mathcal{P}$, then each factor in $\mathbb{F}_q(x)[t]$ would have degree less than $2q$, with one of its factors having leading coefficient in $\mathbb{F}_q(x)\backslash\mathbb{F}_q[x]$, which is impossible by Lemma 3.12. Thus, $g(t)$ is irreducible in $\mathcal{P}$. Since $\psi_2(t) \in \mathcal{P}$ and

$$xg(t) = \psi_2(t) = \prod_{\deg E<2} (t - E).$$

where x, $g(t)$ and $t - E$ are irreducible in $\mathcal{P}$, we deduce that $\psi_2(t)$ can be factored as a product of irreducible elements in more than one way.

As for the case $q > 2$, consider

$$g(t) := \frac{\psi_1^2(t)}{x}.$$

Proceeding in the same manner as above, we deduce that $g(t) \in \mathbb{F}_q(x)[t] \cap \mathcal{P}$ and $g(t)$ is irreducible over $\mathcal{P}$. From $\psi_1^2(t) \in \mathcal{P}$ and

$$xg(t) = \psi_1^2(t) = \prod_{\deg E<2} (t - E)^2,$$

where x. $g(t)$ and $t - E$ are irreducible in $\mathcal{P}$, we arrive at the fact that $\psi_1^2(t)$ can be factored as a product of irreducible elements in more than one ways. □

3.3 Difference and Higher Order Differences

In this section, a generalization of differences for polynomials introduced by Wagner [7] is investigated.

Definition 3.20. *Let $f : \mathbb{F}_q[x] \to \mathbb{F}_q[x]$. For each $M \in \mathbb{F}_q[x]\backslash\{0\}$, the* ***difference***

for a function *$f(t)$ is defined by*

$$\Delta_M f(t) = \frac{f(t+M) - f(t)}{M},$$

for all $t \in \mathbb{F}_q[x]$ and for let $r > 0$ and $M_1, M_2, \ldots, M_r \in \mathbb{F}_q[x]\backslash\{0\}$. We define the r^{th} ***difference of function*** *$f(t)$ inductively by*

$$\Delta_{M_1,M_2,\ldots,M_r} f(t) = \Delta_{M_r}(\Delta_{M_1,M_2,\ldots,M_{r-1}} f(t)),$$

for all $t \in \mathbb{F}_q[x]$.

We define the sets of $\mathcal{P}_r$ for positive integer r as follows.

Definition 3.21. *For any positive integer r, we define*

$$\mathcal{I}_0 = \Big\{ f : \mathbb{F}_q[x] \to \mathbb{F}_q[x] \Big\},$$
$$\mathcal{I}_r = \Big\{ f(t) \in \mathcal{I}_0 \;\Big|\; \Delta_{M_1,M_2,\ldots,M_r} f(t) \in \mathcal{I}_0 \text{ for all } M_1, M_2, \ldots, M_r \in \mathbb{F}_q[x]\backslash\{0\} \Big\},$$
$$\mathcal{P}_r = \mathcal{I}_1 \cap \mathcal{I}_2 \cap \cdots \cap \mathcal{I}_r.$$

We remark that the set of all pseudo-polynomials $\mathcal{P}$ is $\mathcal{P}_1$ and the set of all integer-valued functions IVF is $\mathcal{I}_0$. To find the explicit shape of an element in $\mathcal{P}_r$ for $r \geq 1$, it is convenient to define

$$R_j^{(r)} = \operatorname{lcm}\Big\{ L_{e(i_1)}, L_{e(i_2)}, \ldots, L_{e(i_r)} \;\Big|\; i_1, i_2, \ldots, i_r > 0, i_1 + i_2 + \cdots + i_r \leq j \text{ and } \frac{j!}{i_1! i_2! \cdots i_r! (j - i_1 - i_2 - \cdots - i_r)!} \text{ is prime to } p \Big\},$$

for all $r \leq j$. Then we have

Theorem 3.22. *Let $f(t) \in \mathcal{P}_0$. We have that $f(t) \in \mathcal{P}_r$ if and only if it is representable as an interpolation series of the form*

$$\sum_{i=0}^{\infty} B_i \bar{R}_i^{(r)} \frac{G_i}{g_i}.$$

where $\bar{R}_i^{(r)} = lcm\left\{R_j^{(1)}, R_j^{(2)}, \ldots, R_j^{(r)}\right\}$.

Proof. From the proof of Theorem 3.5, for all $n \in \mathbb{N}_0$, the unique polynomial of degree $\leq q^n - 1$ which takes the same values as $f(t)$ over the set of all polynomials $M \in \mathbb{F}_q[x]$ with $\deg M < n$ is

$$P_n^{(f)}(t) = \sum_{i=0}^{q^n-1} A_i \frac{G_i(t)}{g_i},$$

and where for $r \in \mathbb{N}$ with $q^r > i$, we have

$$A_i = (-1)^r \sum_{\deg N < r} \frac{G'_{q^r-1-i}(N) f(N)}{g_{q^r-1-i}}.$$

Moreover, $f(t) \in \mathcal{P}_r = \mathcal{I}_1 \cap \mathcal{I}_2 \cap \cdots \cap \mathcal{I}_r$ if and only if

$$\Delta_{M_1, M_2, \ldots, M_j} f(t) \in \mathcal{I}_0$$

for all $M_1, M_2, \ldots, M_j \in \mathbb{F}_q[x] \backslash \{0\}$ and for $j \leq r$. This holds if and only if

$$\Delta_{M_1, M_2, \ldots, M_j} P_n^{(f)}(t) \in I_0$$

for all $M_1, M_2, \ldots, M_j \in \mathbb{F}_q[x] \backslash \{0\}$ and for $j \leq r$, that is,

$$P_n^{(f)}(t) \in I_0 \cap I_1 \cap \cdots \cap I_r = \bar{I}_r$$

for all $n \in \mathbb{N}_0$. By Theorem 2.19

$$\begin{aligned} P_n^{(f)}(t) \in \bar{I}_r \text{ for all } n \in \mathbb{N}_0 &\Leftrightarrow R_i^{(1)} \mid A_i,\ R_i^{(2)} \mid A_i,\ \ldots, R_i^{(r)} \mid A_i \ \text{ for all } i \leq n \text{ and } \\ &\quad\; n \in \mathbb{N}_0 \\ &\Leftrightarrow \bar{R}_i^{(r)} \mid A_i \ \text{ for all } i \leq n \text{ and } n \in \mathbb{N}_0. \end{aligned}$$

This proves the results. □