Two Properties of Pseudo-Polynomials over a Galois Field

Rattiya Meesa\textsuperscript{1,a}, Vichian Laohakosol\textsuperscript{2,b}, Tuangrat Chaichana\textsuperscript{1,c} and Boonrod Yuttanan\textsuperscript{3,d}

\textsuperscript{1} Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok 10330, Thailand
\textsuperscript{2} Department of Mathematics, Faculty of Science, Kasetsart University, Bangkok 10900, Thailand
\textsuperscript{3} Algebra and Applications Research Unit, Department of Mathematics and Statistics, Faculty of Science, Prince of Songkla University, Songkhla 90112, Thailand

E-mail: \textsuperscript{a}rattiya3328@gmail.com, \textsuperscript{b}fscivil@ku.ac.th, \textsuperscript{c}tuangrat.c@chula.ac.th and \textsuperscript{d}boonrod.y@psu.ac.th

Abstract. Let $\mathcal{F}$ be the completion, with respect to the degree valuation, of the field of rational functions $\mathbb{F}_q(x)$ over $\mathbb{F}_q$, the Galois (finite) field of $q$ elements. A function $f : \mathcal{F} \to \mathcal{F}$ is integer-valued if $f(\mathbb{F}_q[x]) \subseteq \mathbb{F}_q[x]$. An integer-valued function $f$ is called a pseudo-polynomial if $f(M + K) \equiv f(M) \pmod{K}$ for all $M \in \mathbb{F}_q[x]$ and $K \in \mathbb{F}_q[x] \setminus \{0\}$. Based on an interpolation series introduced by Carlitz in 1935, explicit shapes of pseudo-polynomials are established. Using an asymptotic characterization of polynomials, it is also proved that the set of all pseudo-polynomials is an integral domain but not a unique factorization domain.

1. Introduction

In the classical case, an integer-valued function is a real-valued function that sends the set $\mathbb{N}_0$ of non-negative rational integers to the set $\mathbb{Z}$ of rational integers. An integer-valued function $f(t)$ satisfying $f(t + m) \equiv f(t) \pmod{m}$ for all $t \in \mathbb{N}_0$ and all $m \in \mathbb{N}$ is called pseudo-polynomial. In [1] and [2], de Bruijn and Hall showed that if $f(t)$ is an integer-valued function, then it is a pseudo-polynomial if and only if it can be expressed as an interpolation series

$$f(t) = c_0 + \sum_{i=0}^{\infty} s_i c_i \left(\begin{array}{c} t \\ i \end{array}\right)$$

where $c_i \in \mathbb{Z}$, $s_i = \text{lcm}(1, 2, \ldots, i)$ and $\left(\begin{array}{c} t \\ i \end{array}\right) = \frac{t(t-1)(t-2)\cdots(t-i+1)}{i!}$. This representation enables to refer to the set $\{s_i t^i\}$ as a basis for the set of pseudo-polynomials. Hall also showed, using asymptotic argument, that the set of pseudo-polynomials is an integral domain but it is not a unique factorization domain.

In the case of positive characteristic $p$, let $\mathbb{F}_q(x)$ be the ring of polynomials over a finite field $\mathbb{F}_q$ where $q$ is a power of $p$, and let $\mathbb{F}_q(x)$ denote the quotient field of $\mathbb{F}_q(x)$. The
degree valuation $| \cdot |$ over $\mathbb{F}_q(x)$ is defined by

$$|0| = 0 \text{ and } \left| \frac{f(x)}{g(x)} \right| = q^d f(x)^{-\deg g(x)} \quad \text{for } f(x), g(x) \in \mathbb{F}_q(x) \setminus \{0\}.$$ 

Let $\mathcal{F}$ be the completion of $\mathbb{F}_q(x)$ with respect to this valuation. A function $f : \mathcal{F} \to \mathcal{F}$ is called an integer-valued function (over $\mathbb{F}_q[x]$) if $f(\mathbb{F}_q[x]) \subset \mathbb{F}_q[x]$, and it is a pseudo-polynomial (over $\mathbb{F}_q[x]$) if it also satisfies $f(M + K) \equiv f(M) \pmod{K}$ for all $M \in \mathbb{F}_q[x]$ and $K \in \mathbb{F}_q[x] \setminus \{0\}$.

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

$$\mathcal{P} = \{ f : \mathbb{F}_q[x] \to \mathbb{F}_q[x] \mid f(M + K) \equiv f(M) \pmod{K} \text{ for all } M \in \mathbb{F}_q[x] \text{ and } K \in \mathbb{F}_q[x] \setminus \{0\} \}.$$

In [3], Carlitz introduced a set of polynomials, which play a role analogous to the binomial expansions, by

$$\psi_0(t) = t \quad \text{and} \quad \psi_k(t) = \prod_{\deg M < k} (t - M) \quad \text{for } k \in \mathbb{N}$$

where the product extends over all polynomials $M$ in $\mathbb{F}_q[x]$ (including 0) of degree less than $k$. The polynomials $\psi_k(t)$ can also be expressed in the form

$$\psi_k(t) = \sum_{j=0}^{k} (-1)^{k-j} \left[ \begin{array}{c} k \\ j \end{array} \right] t^j$$

where $\left[ \begin{array}{c} k \\ j \end{array} \right] = \frac{F_k}{F_j L_{k-j}}$, $F_k = \langle k \rangle (k-1)^q \cdots (1)^q^{-1}$, $L_k = \langle k \rangle (k-1) \cdots (1)$, $F_0 = 1$, $L_0 = 1$ and $\langle r \rangle = x^r - x$. As mentioned in [3], $\psi_k(x^q) = \psi_k(M) = F_k$ for each monic polynomial $M$ of degree $k$, $F_k$ is the product of all monic polynomials in $\mathbb{F}_q[x]$ of degree $k$, and $L_k$ is the lcm of all polynomials in $\mathbb{F}_q[x]$ of degree $k$.

The polynomials $\psi_k(t)$ are special cases of the polynomials $G_k(t)$ defined as follows:

Let $G_0(t) = 1$. For $k > 1$, if its $q$-adic expansion is $k = \alpha_0 + \alpha_1 q + \cdots + \alpha_{d(k)} q^{d(k)}$, where $d(k)$ is referred to as its upper $q$-index, then define

$$G_k(t) = \psi_0^{\alpha_0}(t) \psi_1^{\alpha_1}(t) \cdots \psi_d^{\alpha_d}(t) \quad \text{and} \quad \deg G_k = \alpha_0 \deg \psi_0 + \cdots + \alpha_d \deg \psi_d = k.$$

It is also convenient to define

$$G'_k(t) = \prod_{i=0}^{d(k)} G'_{\alpha_i q^i}(t), \quad G'_{\alpha_i q^i}(t) = \begin{cases} \psi_0^{\alpha_i}(t) & \text{for } 0 \leq \alpha_i < q - 1 \\ \psi_1^{\alpha_i}(t) - F_i^{\alpha_i} & \text{for } \alpha_i = q - 1 \end{cases}$$

and

$$g_k = F_0^{\alpha_0}(t) F_1^{\alpha_1}(t) \cdots F_d^{\alpha_d}(t).$$

Remark that for $0 \leq i < 2q$, we have $d(i) = 0$ or 1 and $i = \alpha_0 + \alpha_1 q$ with $\alpha_1 = 0$ if $d(i) = 0$ and $\alpha_1 = 1$ if $d(i) = 1$. In this case, we see that $L_{d(i)} = F_0$ or $\langle 1 \rangle = F_1$ which are identical with the corresponding $g_i = F_0^{\alpha_0} = F_0$ or $F_0^{\alpha_0} F_1^{\alpha_1} = F_1$.

By using the above notation of Carlitz, Laohakosol and Kongsakorn [4] gave the conditions for elements in $\mathbb{F}_q(x)[t]$ and their higher derivatives to be integer-valued functions.

In [5], Wagner studied linear pseudo-polynomials over $\mathbb{F}_q[x]$. In this case, the congruence condition reduces to $f(K) \equiv 0 \pmod{K}$ for all $K \in \mathbb{F}_q[x] \setminus \{0\}$. In his proof,
Wagner made use of an interpolation series for linear pseudo-polynomial, analogous to that of de Bruijn [1] and Hall [2], but expressed instead in terms of Carlitz polynomials \( \psi_k(t) \), namely,
\[
f(t) = \sum_{i=0}^{\infty} L_i A_i \frac{\psi_i(t)}{F_i}
\]
where \( A_i \in \mathbb{F}_q[x] \). This shows that the set \( \{ L_i \psi_i(t)/F_i \} \) forms a basis for the set of linear pseudo-polynomials over \( \mathbb{F}_q[x] \). In addition, Wagner proved that the non-commutative ring of linear pseudo-polynomials over \( \mathbb{F}_q[x] \) (with respect to addition and composition) has no zero divisor, and he also considered integer-valued polynomials in \( \mathbb{F}_q(x)[t] \) whose divided differences remain integer-valued.

In this paper, we first derive interpolation series for \( \mathcal{I} \) and \( \mathcal{P} \), and use them to determine a basis for general pseudo-polynomials over \( \mathbb{F}_q[x] \) extending the linear case of Wagner and in the last part we prove that \( \mathcal{P} \) is an integral domain but not a unique factorization domain.

2. Results

Our results are distributed into two parts. The first part deals with explicit interpolation series for elements of \( \mathcal{I} \) and \( \mathcal{P} \). The second part contains the proof that \( \mathcal{P} \) is an integral domain but not a unique factorization domain.

2.1. Interpolation series for \( \mathcal{I} \) and \( \mathcal{P} \)

We begin with interpolation series for \( \mathcal{I} \).

Theorem 1. Let \( f : \mathcal{F} \rightarrow \mathcal{F} \). If \( f(t) \in \mathcal{I} \), then it is uniquely representable as an interpolation series of the form \( \sum_{i=0}^{\infty} A_i G_i(t)/g_i \), where \( A_i \in \mathbb{F}_q[x] \). This representation is well-defined because the sum \( \sum_{i=0}^{\infty} A_i G_i(M)/g_i \) reduces to a finite sum as \( G_i(M) = 0 \) whenever \( d(i) > \deg M \), for each \( M \in \mathbb{F}_q[x] \), and the representation is interpreted as yielding the same value of \( f(M) \) on both sides.

Proof. Assume that \( f(t) \) is an integer-valued function. We will show that for \( n \in \mathbb{N} \), there exists a unique polynomial \( P_n^f(t) \in \mathbb{F}_q(x)[t] \) of degree \( q^n - 1 \), such that \( P_n^f(M) = f(M) \) for all polynomials \( M \in \mathbb{F}_q[x] \) of degree less than or equal to \( n - 1 \). For a polynomial \( P_n(t) = c_0 + c_1 t + \cdots + c_{q^n-1} t^{q^n-1} \), let \( M_1, M_2, \ldots, M_{q^n-1} \in \mathbb{F}_q[x] \setminus \{0\} \) be all the distinct polynomials of degree less than or equal to \( n - 1 \). Set \( c_0 := f(0) \). 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,
\[
\begin{align*}
f(0) &= c_0 \\
f(M_1) &= c_0 + c_1 M_1 + \cdots + c_{q^n-1} M_1^{q^n-1} \\
& \vdots \\
f(M_{q^n-1}) &= c_0 + c_1 M_{q^n-1} + \cdots + c_{q^n-1} M_{q^n-1}^{q^n-1},
\end{align*}
\]
i.e.,
\[
\begin{bmatrix}
M_1 & M_1^2 & M_1^3 & \cdots & M_1^{q^n-1} \\
M_2 & M_2^2 & M_2^3 & \cdots & M_2^{q^n-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
M_{q^n-1} & M_{q^n-1}^2 & M_{q^n-1}^3 & \cdots & M_{q^n-1}^{q^n-1}
\end{bmatrix}
\begin{bmatrix}
c_1 \\
c_2 \\
\vdots \\
c_{q^n-1}
\end{bmatrix}
= \begin{bmatrix}
f(M_1) - f(0) \\
f(M_2) - f(0) \\
\vdots \\
f(M_{q^n-1}) - f(0)
\end{bmatrix}.
\]
Clearly, the determinant of coefficient matrix is equal to \(M_1 M_2 \cdots M_{q^n - 1} \prod_{1 \leq i < j \leq q^n - 1} (M_i - M_j) \neq 0\), showing that the system is uniquely solvable; we denote this particular polynomial by \(P_n^{(f)}(t)\). Invoking upon Theorem 2 of [6], this polynomial can also be uniquely expressed as

\[
P_n^{(f)}(t) = \sum_{i=0}^{q^n - 1} B_i G_i(t),
\]

where

\[
B_i = (-1)^{m_i} \frac{L_{m_i}}{F_{m_i}} \sum_{\deg M < m_i} G_{q^{m_i - 1 - i}(M)} P_n^{(f)}(M)
\]

with \(m_i = d(i) + 1\), \(d(i)\) being the upper \(q\)-index of \(i\). For each \(0 \leq i \leq q^n - 1\), note that \(d(i) \leq n - 1\). Since \(f(M) = P_n^{(f)}(M)\) for all \(M\) of degree \(< m_i\), it follows that

\[
B_i = (-1)^{m_i} \frac{L_{m_i}}{F_{m_i}} \sum_{\deg M < m_i} G_{q^{m_i - 1 - i}(M)} f(M),
\]

or

\[
g_i B_i = (-1)^{m_i} \sum_{\deg M < m_i} G_{q^{m_i - 1 - i}(M)} \frac{f(M)}{g_{q^{m_i - 1 - i}}} \]

and so

\[
P_n^{(f)}(t) = \sum_{i=0}^{q^n - 1} A_i G_i(t), \quad A_i = (-1)^{m_i} \sum_{\deg M < m_i} G_{q^{m_i - 1 - i}(M)} \frac{f(M)}{g_{q^{m_i - 1 - i}}}
\]

By Lemma 2 of [6], \(G_{q^{m_i - 1 - i}(M)}/g_{q^{m_i - 1 - i}} \in \mathbb{F}_q[x]\) implying that \(A_i \in \mathbb{F}_q[x]\).

With the above preparation, we proceed now to derive our interpolation series. Consider

\[
P_n^{(f)}(t) = \sum_{i=0}^{q^n - 1} A_i \frac{G_i(t)}{g_i} \quad \text{and} \quad P_{n+1}^{(f)}(t) = \sum_{i=0}^{q^{n+1} - 1} A_i' \frac{G_i(t)}{g_i}
\]

where \(A\) and \(A'\) are defined as above. For \(0 \leq i \leq q^n - 1\), we have \(m_i = d(i) + 1 \leq n\). So for each \(M \in \mathbb{F}_q[x]\) with \(\deg M < m_i \leq n\), we have \(P_n^{(f)}(M) = f(M) = P_{n+1}^{(f)}(M)\). Thus,

\[
A_i = (-1)^{m_i} \frac{L_{m_i}}{F_{m_i}} \sum_{\deg M < m_i} G_{q^{m_i - 1 - i}(M)} P_n^{(f)}(M)
\]

\[
= (-1)^{m_i} \frac{L_{m_i}}{F_{m_i}} \sum_{\deg M < m_i} G_{q^{m_i - 1 - i}(M)} f(M)
\]

\[
= (-1)^{m_i} \frac{L_{m_i}}{F_{m_i}} \sum_{\deg M < m_i} G_{q^{m_i - 1 - i}(M)} P_{n+1}^{(f)}(M)
\]

\[
= A_i'.
\]

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

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

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

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

**Theorem 2.** A function $f : \mathcal{F} \to \mathcal{F}$ is a pseudo-polynomial over $\mathbb{F}_q[x]$ if and only if it is representable as an interpolation series of the form $\sum_{i=0}^{\infty} B_i L_d(i) G_i(t)/g_i$, where $B_i \in \mathbb{F}_q[x]$ and $d(i)$ denotes the upper $q$-index of $i$.

**Proof.** From the proof of Theorem 1, we know that the unique polynomial of degree $\leq q^n - 1$ which takes the same values as $f$ over the set of all polynomials $M \in \mathbb{F}_q[x]$ with $\deg M < n$ is $P(t) = \sum_{r=0}^{n-1} A_r G_r(t)/g_i$, where for $r \in \mathbb{N}$ with $q^r > i$, we have $A_r = (-1)^r \sum_{\deg N < r} G_{q^r - 1 - i}(N) f(N)/g_{q^r - 1 - i}$. Moreover, if $f$ is a pseudo-polynomial, then

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

for all $M \in \mathbb{F}_q[x]$, $K \in \mathbb{F}_q[x] \setminus \{0\}$ and $\deg M, \deg K < n$. By Theorem 3.1 of [7], this holds if and only if $P$ and its first order difference are integer-valued and this is the case if and only if each $A_i \in \mathbb{F}_q[x]$ is divisible by $L_{d(i)}$. Since the degree bound, $n$, is arbitrary, the congruence relation holds for all $M \in \mathbb{F}_q[x]$, $K \in \mathbb{F}_q[x] \setminus \{0\}$ and the desired result follows. □

2.2. Factorization in $\mathcal{P}$

We begin by recalling the following definitions,

**Definition 1.** An element $u(t) \in \mathcal{P}$ is called a unit if there is $v(t) \in \mathcal{P}$ such that $u(t)v(t) = 1$ for all $t \in \mathbb{F}_q[x]$.

**Definition 2.** A non-unit element $f \in \mathcal{P} \setminus \{0\}$ is called an irreducible element in $\mathcal{P}$ if $f = gh$ for some $g, h \in \mathcal{P}$, then either $g$ or $h$ is a unit.

**Definition 3.** Denote by $\mathcal{U(\mathcal{P})}$ the set of all units in $\mathcal{P}$.

Now, we produce the properties of $\mathcal{U(\mathcal{P})}$ as follows.

**Lemma 1.** We have $\mathcal{U(\mathcal{P})} = \mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$.

**Proof.** Let $c \in \mathbb{F}_q^*$. Clearly, the constant function $f(t) = c$ is a unit in $\mathcal{P}$ (its inverse being $g(t) = 1/c$), showing that $\mathbb{F}_q^* \subseteq \mathcal{U(\mathcal{P})}$. Conversely, let $f(t) = \sum_{i=0}^{\infty} B_i L_d(i) G_i(t)/g_i$ be a unit in $\mathcal{P}$. Then there exists $g(t) \in \mathcal{P}$ such that $g(t)f(t) = 1$. Substituting for $t$ by any $M \in \mathbb{F}_q[x]$, we arrive at $g(M) = 1/f(M) \in \mathbb{F}_q[x]$. This implies that $f(\mathbb{F}_q[x]) \subseteq \mathbb{F}_q^*$. To show that $f(t) \in \mathbb{F}_q^*$, it suffices to show that $f(N) = B_0$ for any $N \in \mathbb{F}_q[x]$. We have

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

If $N \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$, using $f(\mathbb{F}_q[x]) \subseteq \mathbb{F}_q^*$, the relation (*) show 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 $\mathcal{U(\mathcal{P})} \subseteq \mathbb{F}_q^*$. □
By Lemma 1, it is easy to see that for each \( E \in \mathbb{F}_q[x] \), the elements \( t - E \) and \( x \) are irreducible in \( \mathcal{P} \).

**Theorem 3.** The set \( \mathcal{P} \) is an integral domain.

**Proof.** The fact that \( \mathcal{P} \) is a ring with respect to addition and multiplication is easily checked. There remains to check that it has no zero divisors. Assume that \( f \) and \( g \in \mathcal{P} \setminus \{0\} \). 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 elements in \( \mathcal{P} \) such that \( P_1 \nmid K_1, P_2 \nmid K_2 \). 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.,

\[
M_2 + h_2 P_2 = M_1 + h_1 P_1
\]

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

\[
f(M_1 + h_1 P_1) \equiv f(M_1) \equiv K_1 \pmod{h_1 P_1}, \quad g(M_2 + h_2 P_2) \equiv g(M_2) \equiv K_2 \pmod{h_2 P_2},
\]

indicating that both \( f(M_1 + h_1 P_1) \) and \( g(M_2 + h_2 P_2) \) are not zero. We have

\[
(f \cdot g)(M_1 + h_1 P_1) = f(M_1 + h_1 P_1) \cdot g(M_1 + h_1 P_1) = f(M_1 + h_1 P_1) \cdot g(M_2 + h_2 P_2) \neq 0.
\]

If \( M_1 = M_2 \), then

\[
(f \cdot g)(M_1) = f(M_1)g(M_1) = f(M_1)g(M_2) = K_1 K_2 \neq 0.
\]

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

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

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

**Proof.** If \( A_i = 0 \) for \( i \geq 2q \), then the interpolation series reduces to

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

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

**Lemma 3.** Let \( f(t) \in \mathcal{P} \) and \( m \in \mathbb{N} \). If \( f(t) \) is of order \( x^{m \deg t} \), i.e., if there exists \( c > 0 \), \( N \in \mathbb{N} \) such that

\[
|f(M)| \leq cq^{m \deg M} \quad \text{for all } M \in \mathbb{F}_q[x] \text{ with } \deg M \geq N,
\]

briefly written as \( f(t) = O(x^{m \deg t}) \), 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 [6, Theorem 3], we have

\[
A_n = (-1)^{d(n)+1} \frac{L_{d(n)+1}}{F_{d(n)+1}} \sum_{K=d(n)+1}^{d(n)+1} G'_{q^{d(n)+1}-1-n(K)} f(K).
\]

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

\[
j = \gamma_0 + \gamma_1 q + \gamma_2 q^2 + \cdots + \gamma_d q^d(j)
\]
where $0 \leq \gamma_k \leq q - 1$ and $\gamma_{d(j)} \neq 0$. Since $q^{d(j)+1} - 1 = (q - 1)(q^{d(j)} + q^{d(j)-1} + \cdots + 1)$,

\[
q^{d(j)+1} - j - 1 = (q - 1)(q^{d(j)} + q^{d(j)-1} + \cdots + 1) - j
\]

\[
= (q - 1)\left(q^{d(j)} + q^{d(j)-1} + \cdots + 1\right) - (\gamma_0 + \gamma_1 q + \cdots + \gamma_{d(j)} q^{d(j)})
\]

\[
= \beta_0 + \beta_1 q + \cdots + \beta_{d(j)} q^{d(j)}\text{ where } \beta_k = (q - 1) - \gamma_k.
\]

For a monic polynomial $K$ of degree $d(j) + 1$, we have

\[
G'_{q^{d(j)+1} - 1} (K) = \prod_{k=0}^{d(j)} G'_{\beta_k} (K) = \prod_{k=0}^{d(j)} \psi_{\beta_k} (K) \prod_{k=0}^{d(j)} \{\psi_k^{q-1} (K) - F_k^{q-1}\}.
\]

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

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

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

\[
\deg G'_{q^{d(j)+1} - 1} (K) = \deg \prod_{k=0}^{d(j)} \psi_{\beta_k} (K)
\]

\[
= (d(j) + 1)(\beta_0 + \beta_1 q + \cdots + \beta_{d(j)} q^{d(j)})
\]

\[
= (d(j) + 1)(q^{d(j)+1} - j - 1).
\]

Thus,

\[
\deg A_j \leq \deg L_{d(j)+1} - \deg F_{d(j)+1} + \deg G'_{q^{d(j)+1} - 1} (K) + \deg f (K)
\]

\[
< (q + q^2 + \cdots + q^{d(j)+1}) - (d(j) + 1)q^{d(j)+1} + (d(j) + 1)(q^{d(j)+1} - j - 1) + c' + m(d(j) + 1) \text{ (for some } c', c < q^{c'})
\]

\[
< 2q^{d(j)+1} - (j + 1)(d(j) + 1) + c' + m(d(j) + 1)
\]

\[
< 2q^{d(j)+1} - q^{d(j)}(2q) + c' + (m - 1)(d(j) + 1) \text{ (since } j \geq q^{d(j)} \text{ and } d(j) + 1 > 2q)
\]

\[
= c' + (m - 1)(d(j) + 1).
\]

Consequently, for sufficiently large $k$, we have $\deg A_k < c' + (m - 1)(d(k) + 1)$ for some $c' > 0$. Since $f \in \mathcal{P}$, we know then that $L_{d(k)} | A_k$. Therefore, $\deg L_{d(k)} \leq \deg A_k$ or $A_k = 0$. If some $A_k \neq 0$, then for $k$ sufficiently large, we get

\[
q^{d(k)} < q^1 + q^2 + \cdots + q^{d(k)} = \deg L_{d(k)} \leq \deg A_k < c' + (m - 1)(d(k) + 1),
\]

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

**Lemma 4.** Let $f \in \mathcal{P}$. If $f(t) \in \mathbb{F}_q (x)[t]$ and if there exist $g, h \in \mathcal{P}$ such that $f(t) = g(t)h(t)$ for all $t \in \mathbb{F}_q [x]$, then $g(t)$ and $h(t)$ are $\mathbb{F}_q (x)[t]$.

**Proof.** Write $f(t) = a_0 t^n + a_{n-1} t^{n-1} + \cdots + a_0$. Let $M \in \mathbb{F}_q [x]$. Then, $|f(M)| \leq A q^{n \deg M}$, where $A = \max \{|a_0|, |a_1|, \ldots , |a_n|\}$. If $g(t)$ is not a polynomial, Lemma 3 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 $|g(M_j)| > A q^{n \deg M_j} = A q^{n_j}$, and so

\[
A q^{n_j} \geq |f(M_j)| = |g(M_j)||h(M_j)| > A q^{n_j},
\]

which is contradiction. \hfill \Box
Theorem 4. $\mathcal{P}$ is not a unique factorization domain.

Proof. Let us first treat the case $q = 2$. Consider $g(t) := \psi_2(t)/x$. By Theorem 2, $g(t)$ has an interpolation of the form $g(t) = A_4G_4/g_4$, where $A_4 = F_2/x$, and so $g(t) \in \mathcal{P}$. Since $g(t) = \frac{1}{2} \prod_{\deg E < 2} (t - E)$, 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 by Lemma 4, each factor would be a polynomial over $\mathbb{F}_q(x)$ having degree less than $2q$, with one of its factors having leading coefficient in $\mathbb{F}_q(x) \setminus \mathbb{F}_q[x]$, which is impossible by Lemma 2. Thus, $g(t)$ is irreducible in $\mathcal{P}$. We have $\psi_2(t) \in \mathcal{P}$ and

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

where $x$, $g(t)$ and $t - E$ are irreducible in $\mathcal{P}$. This implies 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 $g(t) := \psi_1^2(t)/x$. 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. \qed

References
[1] De Bruijn N G 1955 Indag. Math. 17 363–7
[2] Hall R R 1971 Mathematika 18 71–7
[3] Carlitz L 1935 Duke Math. J. 1 137–68
[4] Laohakosol L and Kongsakorn K 1999 Bull. Malays. Math. Sci. Soc. 22 45–52
[5] Wagner C G 1974 Arch. Math. 25 45–52
[6] Carlitz L 1940 Duke Math. J. 6 486–504
[7] Wagner C G 1976 Arch. Math. 27 495–501