Turkish Journal of Mathematics

Volume 45 | Number 3 Article 24

1-1-2021

Integer-valued polynomials satisfying the Lucas property

RATTIYA MEESA

VICHIAN LAOHAKOSOL

TUANGRAT CHAICHANA

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2021) 45: 1459 – 1478

doi:10.3906/mat-2102-104

Integer-valued polynomials satisfying the Lucas property

Rattiya MEESA[1,*], **Vichian LAOHAKOSOL**[2], **Tuangrat CHAICHANA**[1]
[1]Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok, Thailand
[2]Department of Mathematics, Faculty of Science, Kasetsart University, Bangkok, Thailand

Received: 23.02.2021 • **Accepted/Published Online:** 26.04.2021 • **Final Version:** 20.05.2021

Abstract: The classical theorem of Lucas states that the binomial polynomials, which form a basis for integer-valued polynomials, satisfy a congruence relation related to their integer parameters. We consider here three problems connected with this result in the setting of discrete valued structures. The first problem asks for the shapes of Lagrange-type interpolation polynomials which constitute a basis for integer-valued polynomials and satisfy the Lucas property; the result so obtained extends a 2001 result of Boulanger and Chabert. For the second problem, we show that the Carlitz polynomials, which form a basis for integer-valued polynomials in a function field, satisfy the Lucas property, and derive criteria guaranteeing that Carlitz-like polynomials, which constitute a basis for integer-valued polynomials, enjoy the Lucas property. The third problem is to find conditions on general polynomials which form a basis for integer-valued polynomials ensuring that they satisfy the Lucas property.

Key words: Integer-valued polynomial, Lucas property, discrete valuation domain with finite residue field

1. Introduction

Let D be an integral domain with quotient field K. An integer-valued polynomial over D is a polynomial over K that maps D to itself. Denote the set of all integer-valued polynomials over D by

$$\mathrm{Int}(D) = \{f(t) \in K[t] \mid f(D) \subseteq D\};$$

the set $\mathrm{Int}(D)$ is a subring of $K[t]$ containing $D[t]$ and is also a D-module ([3, Chapter I.1], [9]). In the classical case where $D = \mathbb{Z}$, the $\mathbb{Z}$-module $\mathrm{Int}(\mathbb{Z})$ is free with a regular basis, [3, Proposition I.1.1]. One best known regular basis is the set of binomial polynomials $\left\{\binom{t}{n}\right\}_{n\geq 0}$ defined by

$$\binom{t}{0} = 1, \quad \binom{t}{n} = \frac{t(t-1)\cdots(t-n+1)}{n!} \quad (n \geq 1).$$

Let $p \in \mathbb{Z}$ be a prime, and let $k, n \in \mathbb{N}$ whose base p-representations are

$$k = k_0 + k_1 p + \cdots + k_s p^s, \quad n = n_0 + n_1 p + \cdots + n_s p^s \quad (0 \leq k_i, n_i < p).$$

The classical theorem of Lucas, [7], states that

$$\binom{k}{n} \equiv \binom{k_0}{n_0}\binom{k_1}{n_1}\cdots\binom{k_s}{n_s} \pmod{p}. \tag{1.1}$$

*Correspondence: rattiya3328@gmail.com
2010 *AMS Mathematics Subject Classification:* 13F20

There is a simple, short proof of this theorem in [7] where some information on the number and conditions for binomial coefficients to be divisible by p is also obtained. Recently, Boulanger and Chabert [2] generalized Lucas's theorem from $\mathbb{Z}$ to a discrete valuation domain with a finite residue field. We now briefly describe their work.

Throughout this paper, let V be a discrete valuation domain with valuation ν and a finite residue field, and let K be its quotient field. Let $\mathfrak{m} = (T)$ be the maximal ideal of V generated by T, and let q be the cardinality of the residue field $V/\mathfrak{m}$. Denote the set of representatives of $V/\mathfrak{m}$ by

$$U = \{u_0 = 0, u_1, \ldots, u_{q-1}\},$$

so that each element $A \in V$ can be uniquely represented as a base T-representation [8, Chapter 4] (or power series in T over U) of the form

$$\sum_{i=0}^{\infty} A_i T^i \in U[[T]].$$

Recall that the valuation $\nu(A)$ of $A \in V\{0\}$ is a positive integer, indeed it is the largest integer n such that $A \in \mathfrak{m}^n$; in a similar manner, denote by $\nu_q(\ell)$ the largest power of q that divides $\ell \in \mathbb{N}$.

Let $\{B_n(t)\}_{n\geq 0}$ be a sequence of polynomials forming a basis for the V-module $\mathrm{Int}(V)$. We say that the sequence $\{B_n(t)\}$ satisfies the Lucas property modulo $\mathfrak{m}$ if it enjoys the following property: for $n \in \mathbb{N}_0 := \mathbb{N}\cup\{0\}$ with base q-representation

$$n = n_0 + n_1 q + \cdots + n_{d(n)} q^{d(n)} \quad (0 \leq n_i < q,\ n_{d(n)} \neq 0 \text{ if } n \in \mathbb{N}), \tag{1.2}$$

and for $A \in V$ with base T-representation

$$A = A_0 + A_1 T + \cdots + A_j T^j + \cdots \in U[[T]],$$

the congruence relation

$$B_n(A) \equiv B_{n_0}(A_0) B_{n_1}(A_1) \cdots B_{n_{d(n)}}(A_{d(n)}) \pmod{\mathfrak{m}} \tag{1.3}$$

holds.

If the polynomials $\{B_n(t)\}$ are constructed as Lagrange-type interpolation polynomials in the manner similar to that in [2], i.e. there is a sequence $\{w_n\}_{n\geq 0}$ of distinct elements in V such that

$$B_0(t) = 1, \qquad B_n(t) = \frac{(t-w_0)(t-w_1)\cdots(t-w_{n-1})}{(w_n-w_0)(w_n-w_1)\cdots(w_n-w_{n-1})} \quad (n \geq 1), \tag{1.4}$$

our first problem is to determine the sequence $\{w_n\}$ which characterizes the Lucas property of the basis $\{B_n(t)\}$. This is carried out in Section 2 and will give an extension to a result of Boulanger and Chabert [2].

For our second problem, we work in $\mathbb{F}_q(x)$, the field of rational functions over the finite field $\mathbb{F}_q$ of q elements, equipped with the x-adic valuation whose discrete valuation domain is V, and whose maximal ideal is $\mathfrak{m} = (x) := xV$. In [4–6], Carlitz introduced the following set of polynomials over $\mathbb{F}_q[x]$, referred to as Carlitz polynomials,

$$\psi_0(t) = t,\ \psi_k(t) = \prod_{\deg M < k} (t - M) \quad (k \in \mathbb{N}), \tag{1.5}$$

where the product extends over all polynomials $M \in \mathbb{F}_q[x]$ of degree $< k$, including the zero polynomial. Carlitz defined the following elements in $\mathbb{F}_q[x]$ which play the role analogous to the factorials in $\mathbb{Z}$,

$$F_0 = 1, \quad F_k = \langle k \rangle \langle k-1 \rangle^q \cdots \langle 1 \rangle^{q^{k-1}} \quad (k \geq 1),$$

where $\langle k \rangle := x^{q^k} - x$. Since $\psi_k(x^k) = \psi_k(M) = F_k$ for each monic polynomial M of degree k, we have, [4], F_k is the product of all monic polynomial in $\mathbb{F}_q[x]$ of degree k. The polynomials $\psi_k(t)$ form a basis for the so-called linear polynomials over $\mathbb{F}_q[x]$, while a basis for general polynomials over $\mathbb{F}_q[x]$ is given by the polynomials $G_k(t)$ defined by

$$G_0(t) = 1, \quad G_k(t) = \psi_0^{k_0}(t)\psi_1^{k_1}(t) \cdots \psi_{d(k)}^{k_{d(k)}}(t) \quad (k \geq 1), \tag{1.6}$$

where $k = k_0 + k_1 q + \cdots + k_{d(k)} q^{d(k)}$ is its base q-representation. Correspondingly, the factorial-like elements generalizing the F_k's are defined by

$$g_0 = 1, \quad g_k = F_0^{k_0} F_1^{k_1} \cdots F_{d(k)}^{k_{d(k)}} \quad (k \geq 1). \tag{1.7}$$

Carlitz proved that $\{G_n(t)/g_n\}$ is a basis of the $\mathbb{F}_q[x]$-module $\mathrm{Int}(\mathbb{F}_q[x])$. Since the shape of this basis is different from the one in (1.4), the first part of our second problem is to show that $\{G_n(t)/g_n\}$ satisfies the Lucas property. This first part naturally leads us to the second part of asking for criterion rendering the validity of the Lucas property of the sequences generalizing those of Carlitz polynomials.

Our third and final problem is an amalgamation of the previous two. We ask for conditions on general polynomials forming a basis for $\mathrm{Int}(V)$ which guarantee that they satisfy the Lucas property.

2. The first problem

Adopting the same notation as in Section 1, let $\{w_n\}$ be a sequence in V whose associated polynomials are $B_n(t)$ as in (1.4). The sequence $\{w_n\}$ is called a g-IVP (generating integer-valued polynomial) sequence if its associated polynomial sequence $\{B_n(t)\}$ is a basis for $\mathrm{Int}(V)$. It is to be noted that the notion of g-IVP sequence defined here is essentially equivalent to that of $\mathfrak{m}$-ordering sequence first introduced and studied by Bhargava in [1].

To determine those g-IVP sequences whose associated polynomials satisfy the Lucas property, we need to introduce some new notion. A sequence $\{a_n\}_{n\geq 0} \subseteq V$ is said to be a very well distributed and well ordered (VWDWO) if for all $\ell, m \in \mathbb{N}_0$, the sequence elements satisfy

$$\nu(a_\ell - a_m) = \nu_q(\ell - m).$$

We recall the following result from [3, Remarks II.2.2].

Lemma 2.1 *A sequence $\{a_n\} \subseteq V$ is VWDWO if and only if for all $s \in \mathbb{N}_0$, any choice of q^s consecutive terms provides a complete set of residues modulo $\mathfrak{m}^s$ in V.*

Any g-IVP sequence $\{w_n\}$ which satisfies the VWDWO property is characterized by the next two theorems.

Theorem 2.2 *If $\{w_n\}$ is a g-IVP sequence with $w_0 = 0$, then $w_1, \ldots, w_{q-1}$ are units, each of which belongs to a distinct class in $V/\mathfrak{m}$.*

Moreover, the first q elements of $\{w_n\}$ can be chosen to be all the elements of the set of representatives U of $V/\mathfrak{m}$, i.e. $\{w_0 = 0, w_1, \ldots, w_{q-1}\} = U$.

Proof Let $\{B_n(t)\}$ be the polynomial sequence associated with $\{w_n\}$. To show that w_1 is a unit in V, consider $B_1(t) = \frac{t-w_0}{w_1-w_0} = \frac{t}{w_1}$. Since $B_1(t)$ is integer-valued, we have $B_1(1) = 1/w_1 \in V$, so w_1 is a unit in V, and we are done in the case $q = 2$.

If $q > 2$, we proceed by induction, assuming that $w_1, \ldots, w_k$ $(1 \leq k < q-1)$, are units belonging to different residue classes in $V/\mathfrak{m}$, so that $\nu(w_i - w_j) = 0$ $(1 \leq i < j \leq k)$. Consider

$$B_{k+1}(t) = \frac{t(t-w_1)\cdots(t-w_k)}{w_{k+1}(w_{k+1}-w_1)\cdots(w_{k+1}-w_k)}.$$

Since $k+1 \leq q-1 < |V/\mathfrak{m}|$, there exists a unit $A \in V \setminus \{0\}$ belonging to a class in $V/\mathfrak{m}$ different from those of $w_0, w_1, \ldots, w_k$, and so $\nu(A - w_i) = 0$ $(0 \leq i \leq k)$. Since

$$B_{k+1}(A) = \frac{A(A-w_1)\cdots(A-w_k)}{w_{k+1}(w_{k+1}-w_1)\cdots(w_{k+1}-w_k)} \in V$$

(i.e. $\nu(B_{k+1}(A)) \geq 0$) and $\nu(A(A-w_1)\cdots(A-w_k)) = 0$, we have

$$\nu(w_{k+1}(w_{k+1}-w_1)\cdots(w_{k+1}-w_k)) \leq 0.$$

As $w_{k+1}(w_{k+1}-w_1)\cdots(w_{k+1}-w_k) \in V \setminus \{0\}$, this forces

$$\nu(w_{k+1}(w_{k+1}-w_1)\cdots(w_{k+1}-w_k)) = 0.$$

Because $w_i \in V$, we deduce that $\nu(w_{k+1}) = \nu(w_{k+1}-w_1) = \cdots = \nu(w_{k+1}-w_k) = 0$, which shows w_{k+1} is a unit in V belonging to a class different from $w_1, \ldots, w_k$ in $V/\mathfrak{m}$, and the induction is complete. The second assertion follows immediately from the first. □

The next technical lemma provides more precise information about a congruence property of the polynomials $B_n(t)$.

Lemma 2.3 *Let $\{w_n\}$ be a g-IVP sequence whose associated polynomial sequence is $\{B_n(t)\}$. Let the subset of the first q elements of $\{w_n\}$ be $\{w_0 = 0, w_1, \ldots, w_{q-1}\} = U$, and denote any other element by*

$$w_n = a_0^{(n)} + a_1^{(n)}T + \cdots + a_j^{(n)}T^j + \cdots \quad (a_j^{(n)} \in U,\ n \geq q) \tag{2.1}$$

(this representation is also applicable for $n = 0, 1, \ldots, q-1$). Let

$$A = A_0 + A_1T + \cdots + A_jT^j + \cdots \in V. \tag{2.2}$$

For a fixed $m \in \mathbb{N}_0$, if the condition on the digit values

$$a_0^{(n)} = w_{n_0},\ a_1^{(n)} = w_{n_1},\ \ldots,\ a_m^{(n)} = w_{n_m} \tag{2.3}$$

holds for all $n \in \mathbb{N}_0$ *whose base* q*-representation is* (1.2)*, then for each* $k \in \{0, 1, \ldots, q-2\}$*, we have*

$$B_{(k+1)q^{m+1}}(A) \equiv \prod_{s=0}^{k} \frac{A_{m+1} - a_{m+1}^{(sq^{m+1}+r_s)}}{a_{m+1}^{((k+1)q^{m+1})} - a_{m+1}^{(sq^{m+1})}} \pmod{\mathfrak{m}},$$

where the integers $r_s \in \{0, 1, \ldots, q^{m+1}-1\}$ *are uniquely determined and satisfy the relation*

$$w_{r_s} \equiv A_0 + A_1 T + \cdots + A_m T^m \pmod{\mathfrak{m}^{m+1}}.$$

Proof Assume that $a_0^{(n)} = w_{n_0}$, $a_1^{(n)} = w_{n_1}$, $\ldots$, $a_m^{(n)} = w_{n_m}$. For $0 \le k \le q-2$, replacing A and w_i by the expressions in (2.2), respectively, (2.1), we write

$$B_{(k+1)q^{m+1}}(A) = \prod_{s=0}^{k} \Omega_s, \quad \text{where} \quad \Omega_s := \prod_{i=sq^{m+1}}^{(s+1)q^{m+1}-1} \frac{A - w_i}{w_{(k+1)q^{m+1}} - w_i} = \frac{\Lambda_1(s)}{\Lambda_2(s)}.$$

The numerator of Ω_s is

$$\begin{aligned}\Lambda_1(s) &= \prod_{i=sq^{m+1}}^{(s+1)q^{m+1}-1} ((A_0 + \cdots + A_m T^m) - (a_0^{(i)} + \cdots + a_m^{(i)} T^m)) + (A_{m+1} - a_{m+1}^{(i)}) T^{m+1} + \ldots \\ &= \prod_{\substack{N \in U[T] \\ \deg N \le m}} (A_0 + \cdots + A_m T^m - N) + \Sigma_0 \cdot \Pi_0 + (\text{terms with powers of } T \ge 2m+2), \end{aligned} \tag{2.4}$$

where

$$\Sigma_0 := \sum_{i=sq^{m+1}}^{(s+1)q^{m+1}-1} (A_{m+1} - a_{m+1}^{(i)}) T^{m+1},$$

$$\Pi_0 := \prod_{\substack{M \in U[T] \\ \deg M \le m \\ M \ne a_0^{(i)} + \cdots + a_m^{(i)} T^m}} (A_0 + \cdots + A_m T^m - M)$$

Since N and M run through all elements in $U[T]$ (including 0) of degree $\le m$ and $M \ne a_0^{(i)} + \cdots + a_m^{(i)} T^m$, in the right-hand expression of (2.4) the first term vanishes, while the second term reduces to

$$(A_{m+1} - a_{m+1}^{(r_s)}) T^{m+1} \prod_{\substack{M \in U[T],\, \deg M \le m \\ M \ne A_0 + \cdots + A_m T^m}} (A_0 + \cdots + A_m T^m - M),$$

for some uniquely determined $r_s \in \{sq^{m+1}, \ldots, (s+1)q^{m+1} - 1\}$ satisfying

$$a_i^{(r_s)} = A_i \quad (0 \le i \le m). \tag{2.5}$$

Thus,

$$\Lambda_1(s) =(A_{m+1} - a_{m+1}^{(r_s)})T^{m+1} \prod_{\substack{\deg M\le m\\ M\neq A_0+\cdots+A_mT^m}} (A_0 + \cdots + A_mT^m - M)$$
$$+ (\text{terms with powers of } T \geq 2m + 2). \tag{2.6}$$

Note that the denominator $\Lambda_2(s)$ of Ω_s takes exactly the same form as Λ_1 but with the coefficients A_i of A being replaced by the coefficients $a_i^{((s+1)q^{m+1})}$ of $w_{(s+1)q^{m+1}}$, and so in an expression similar to the right-hand side of (2.6) for $\Lambda_2(s)$, the first term of expansion vanishes and the second term reduces to

$$(a_{m+1}^{((s+1)q^{m+1})} - a_{m+1}^{(r'_s)})T^{m+1} \prod_{\substack{M'\in U[T],\ \deg M'\le m\\ M'\neq a_0^{((s+1)q^{m+1})}+\cdots+a_m^{((s+1)q^{m+1})}T^m}} (a_0^{((s+1)q^{m+1})} + \cdots + a_m^{((s+1)q^{m+1})}T^m - M'),$$

for some uniquely determined $r'_s \in \{sq^{m+1}, \ldots, (s + 1)q^{m+1} - 1\}$ satisfying

$$a_i^{(r'_s)} = a_i^{((s+1)q^{m+1})} \quad (0 \leq i \leq m). \tag{2.7}$$

By the assumption (2.3), we have

$$a_0^{((s+1)q^{m+1})} = a_1^{((s+1)q^{m+1})} = \cdots = a_m^{((s+1)q^{m+1})} = w_0 = 0$$

and

$$a_0^{(sq^{m+1})} = a_1^{(sq^{m+1})} = \cdots = a_m^{(sq^{m+1})} = w_0 = 0,$$

so (2.7) shows that $r'_s = sq^{m+1}$, and the second term of Λ_2 becomes

$$(a_{m+1}^{((s+1)q^{m+1})} - a_{m+1}^{(sq^{m+1})})T^{m+1} \prod_{\substack{\deg M'\le m\\ M'\neq 0}} (0 - M').$$

Thus,

$$\Lambda_2(s) = (a_{m+1}^{((s+1)q^{m+1})} - a_{m+1}^{(sq^{m+1})})T^{m+1} \prod_{\substack{\deg M'\le m\\ M'\neq 0}} (0 - M') + (\text{terms with powers of } T \geq 2m + 2). \tag{2.8}$$

We claim now that $\prod_{s=0}^{k} \Lambda_2(s) \neq 0$, i.e. the denominator of $B_{(k+1)q^{m+1}}(A)$ does not vanish. To verify this, observe that since $k + 1 \leq q - 1$, choosing A_{m+1} in such a way that $\prod_{s=0}^{k} \left(A_{m+1} - a_{m+1}^{(r_s)}\right) \neq 0$ yields the nonvanishing of the numerator of $B_{(k+1)q^{m+1}}(A)$, i.e. $\prod_{s=0}^{k} \Lambda_1(s) \neq 0$. This together with the fact that $B_{(k+1)q^{m+1}}(A)$ is integer-valued, i.e. $\in V$, shows that its denominator $\prod_{s=0}^{k} \Lambda_2(s)$ does not vanish.

Since both the sets

$$\{A_0 + A_1T + \cdots + A_mT^m - M \mid M \in U[T], \deg M \leq m,\ M \neq A_0 + A_1T + \cdots + A_mT^m\}$$

and

$$\{-M' \mid M' \in U[T], \deg M' \leq m \text{ and } M' \neq 0\}$$

are identical with the set of all nonzero residue classes modulo $\mathfrak{m}^{m+1}$, we have

$$\prod_{\substack{\deg M \leq m \\ M \neq A_0+\cdots+A_mT^m}} (A_0 + \cdots + A_mT^m - M) \equiv \prod_{\substack{\deg M' \leq m \\ M' \neq 0}} (0 - M') \pmod{\mathfrak{m}^{m+1}}. \tag{2.9}$$

By (2.6), (2.8) and (2.9), we get

$$B_{(k+1)q^{m+1}}(A) = \prod_{s=0}^{k} \frac{\Lambda_1(s)}{\Lambda_2(s)} \equiv \prod_{s=0}^{k} \frac{(A_{m+1} - a_{m+1}^{(r_s)})}{(a_{m+1}^{((s+1)q^{m+1})} - a_{m+1}^{(sq^{m+1})})} \pmod{\mathfrak{m}},$$

for some $sq^{m+1} \leq r_s \leq (s+1)q^{m+1} - 1$ and by (2.1) and (2.5), we get $a_i^{(r_s)} = A_i \quad (0 \leq i \leq m)$, i.e.

$$w_{r_s} \equiv A_0 + A_1T + \cdots + A_mT^m \pmod{\mathfrak{m}^{m+1}},$$

as required. □

The explicit shape of a g-IVP sequence $\{w_n\}$ which is VWDWO and satisfies the Lucas property is obtained in the following theorem.

Theorem 2.4 *Let $\{w_n\} := \{w_0 = 0, w_1, w_2, \ldots\}$ be a g-IVP sequence whose associated w-polynomial sequence is $\{B_n(t)\}_{n\geq 0}$. Assume that*

1. *the sequence $\{B_n(t)\}$ satisfies the Lucas property modulo $\mathfrak{m}$*
2. *the sequence $\{w_n\}$ is a VWDWO sequence.*

Then the sequence $\{w_n\}$ is uniquely determined in the sense that for each n written with respect to the base q-representation (1.2), we have

$$w_n = w_{n_0} + w_{n_1}T + \cdots + w_{n_{d(n)}}T^{d(n)}. \tag{2.10}$$

(Since the sequence $\{w_n\}$ mentioned above depends on the choice of $w_1, \ldots, w_{q-1}$ and on the choice of T, its asserted uniqueness is implicitly subject to this dependence.)

Proof Since $\{w_n\}$ is a g-IVP sequence with $w_0 = 0$, by Theorem 2.2, we can take its first q elements to be those of U, i.e.

$$\{w_0 = 0, w_1, \ldots, w_{q-1}\} = U. \tag{2.11}$$

Using the notation as set out in (2.1) of Lemma 2.3, the set (2.11) shows that

$$a_0^{(0)}(= 0),\ a_0^{(1)},\ \cdots,\ a_0^{(q-1)} \in U, \tag{2.12}$$

$$a_i^{(0)} = a_i^{(1)} = \cdots = a_i^{(q-1)} = 0 \quad (i \geq 1). \tag{2.13}$$

We prove the theorem by establishing (2.10) component-wise that $a_j^{(n)} = w_{n_j}$.

As the first step, we show that

$$a_0^{(n)} = w_{n_0} \quad \text{for all } n \in \mathbb{N}_0. \tag{2.14}$$

This clearly holds for $n \in \{0, 1, \ldots, q-1\}$ because of (2.12). Since $\{w_n\}$ is a VWDWO sequence, by Lemma 2.1, any q consecutive terms in the sequence form a complete set of residues modulo $\mathfrak{m}$. Thus, for $0 \le i \le q-1$, we get

$$w_{q+i} \equiv w_i \pmod{\mathfrak{m}} \qquad (0 \le i \le q-1),$$

and so

$$a_0^{(q+i)} \equiv w_i \pmod{\mathfrak{m}};$$

proceeding inductively, we have

$$w_{jq+i} \equiv w_{(j-1)q+i} \equiv \cdots \equiv w_{q+i} \equiv w_i \pmod{\mathfrak{m}} \qquad (j \in \mathbb{N}). \tag{2.15}$$

Using the notation (1.2), we deduce from (2.15) for $n \ge 0$ that

$$a_0^{(n)} \equiv w_n \equiv w_{n_0} \pmod{\mathfrak{m}}.$$

Being elements of U shows then that (2.14) is fulfilled.

As our second (general) step, for $e \in \mathbb{N}_0$, we show that

$$a_{e+1}^{(n)} = w_{n_{e+1}} \quad \text{for all } n \in \mathbb{N}_0. \tag{2.16}$$

We prove this using two induction processes. We proceed by induction on e, assuming that

$$a_0^{(n)} = w_{n_0},\ a_1^{(n)} = w_{n_1}, \cdots,\ a_e^{(n)} = w_{n_e}; \tag{2.17}$$

with the case $e = 0$ being just verified above. Taking any $A = A_0 + A_1 T + \cdots \in V$, using Lemma 2.3 with $m = e, k = 0$ and (2.13), we have

$$B_{q^{e+1}}(A) \equiv \frac{A_{e+1} - a_{e+1}^{(r_0)}}{a_{e+1}^{(q^{e+1})} - a_{e+1}^{(0)}} = \frac{A_{e+1} - a_{e+1}^{(r_0)}}{a_{e+1}^{(q^{e+1})}} \pmod{\mathfrak{m}}, \tag{2.18}$$

for some $r_0 \in \{0, 1, \ldots, q^{e+1} - 1\}$ satisfying $w_{r_0} \equiv A_0 + \cdots + A_e T^e \pmod{\mathfrak{m}^{e+1}}$.
If $a_{e+1}^{(r_0)} \neq 0$, then $a_{e+1}^{(r_0)} = w_\ell$ for some $\ell \in \{1, 2, \ldots, q-1\}$. Putting $A_{e+1} = w_\ell$, we get

$$B_{q^{e+1}}(A) \equiv 0 \pmod{\mathfrak{m}}. \tag{2.19}$$

On the other hand, since $B_{q^{e+1}}(A)$ satisfies the Lucas property, we get

$$B_{q^{e+1}}(A) \equiv B_1(A_{e+1}) = \frac{A_{e+1} - w_0}{w_1 - w_0} = \frac{w_\ell}{w_1} \neq 0 \pmod{\mathfrak{m}},$$

contradicting (2.19). Thus, $a_{e+1}^{(r_0)} = 0 = w_0$; this being true for any such r_0 implies then that

$$a_{e+1}^{(n)} = 0 = w_{n_{e+1}} \quad (0 \le n \le q^{e+1} - 1). \tag{2.20}$$

Next, using Lemma 2.3 with $k=1, m=e$, we have

$$B_{2q^{e+1}}(A) \equiv \alpha_0 \cdot \alpha_1 \pmod{\mathfrak{m}},$$

where

$$\alpha_0 := \frac{A_{e+1} - a_{e+1}^{(r_0)}}{a_{e+1}^{(2q^{e+1})} - a_{e+1}^{(0)}},\ \alpha_1 := \frac{A_{e+1} - a_{e+1}^{(q^{e+1}+r_1)}}{a_{e+1}^{(2q^{e+1})} - a_{e+1}^{(q^{e+1})}} \tag{2.21}$$

for some $0 \le r_i \le q^{e+1}-1 \quad (i \in \{0,1\})$ satisfying

$$w_{r_i} \equiv A_0 + \cdots + A_e T^e \pmod{\mathfrak{m}^{e+1}} \tag{2.22}$$

Using (2.13) and (2.20), we see that $\alpha_0 = \frac{A_{e+1}}{a_{e+1}^{(2q^{e+1})}}$. We turn now to α_1. Since $\{w_n\}$ is a VWDWO sequence, the set $\{w_0 = 0, w_1, \ldots, w_{q^{e+2}-1}\}$ constitutes a residue class modulo $\mathfrak{m}^{e+2}$. Thus, from (2.20), for larger n in the next range, i.e. for $q^{e+1} \le n \le q^{e+2}-1$ we must have $a_{e+1}^{(n)} \neq w_0\ (=0)$; in particular, $a_{e+1}^{(q^{e+1}+r_1)} \neq w_0$. If $a_{e+1}^{(q^{e+1}+r_1)} \neq w_1$, then $a_{e+1}^{(q^{e+1}+r_1)} = w_\ell$ for some $\ell \in \{2,3,\ldots,q-1\}$. Putting $A_{e+1} = w_\ell$ in (2.21), we have

$$\alpha_1 = 0. \tag{2.23}$$

However, the Lucas property implies that

$$\alpha_0 \cdot \alpha_1 \equiv B_{2q^{e+1}}(A) \equiv B_2(A_{e+1}) = \frac{A_{e+1}(A_{e+1}-w_1)}{w_2(w_2-w_1)} \equiv \frac{w_\ell(w_\ell - w_1)}{w_2(w_2-w_1)} \neq 0 \pmod{\mathfrak{m}},$$

contradicting (2.23), and so $a_{e+1}^{(q^{e+1}+r_1)} = w_1$. Since r_1 satisfies (2.22) and the elements $A_0,\ A_1,\ \ldots,\ A_e$ can take any values in U, the "for some" restriction on r_1 can be removed, and so

$$a_{e+1}^{(n)} = w_1 = w_{n_{e+1}} \quad (q^{e+1} \le n \le 2q^{e+1}-1). \tag{2.24}$$

From the VWDWO property modulo $\mathfrak{m}^{e+2}$, because of (2.20) and (2.24), the residues w_0 and w_1 have already been exhausted by those $a_{e+1}^{(n)}$ with $n \in \{0,1,\ldots,2q^{e+1}-1\}$. Thus, for larger n in the next range, we have

$$a_{e+1}^{n} \notin \{w_0, w_1\} \quad \text{for all } n \in \{2q^{e+1},\ 2q^{e+1}+1,\ \ldots,\ q^{e+2}-1\}. \tag{2.25}$$

We pause here to remark that the ongoing proof of (2.16) for $q=2$ is now complete from (2.20), (2.24) and the VWDWO property, while for $q=3$, since there are three residue classes, the proof of (2.16) is also complete from (2.20), (2.24), (2.25) and the VWDWO property. This leaves us to consider henceforth only the case $q>3$. We now proceed by induction on $h = 1,2,\ldots,q-3$ to show that

$$a_{e+1}^{(n)} = w_{n_{e+1}} \quad \text{for all } n \in \{(h+1)q^{e+1}, \ldots,\ (h+2)q^{e+1}-1\}.$$

The induction hypothesis asserts that for each $0 \le s \le q^{e+1}-1$, we have

$$a_{e+1}^{(s)} = w_0,\ a_{e+1}^{(q^{e+1}+s)} = w_1,\ \ldots,\ a_{e+1}^{(hq^{e+1}+s)} = w_h \quad \text{and} \quad a_{e+1}^{((h+1)q^{e+1})} \notin \{w_0, \ldots, w_h\};$$

this hypothesis holds when $h = 1$ as already shown in (2.20), (2.24) and (2.25). Applying Lemma 2.3 with $k = h+1, m = e$, we get

$$B_{(h+2)q^{e+1}}(A) \equiv \prod_{s=0}^{h+1} \alpha_s \pmod{\mathfrak{m}}, \quad \alpha_s := \frac{A_{e+1} - a_{e+1}^{(sq^{e+1}+r_s)}}{a_{e+1}^{((h+2)q^{e+1})} - a_{e+1}^{(sq^{e+1})}}$$

for some $r_s \in \{0, 1, \ldots, q^{e+1}-1\}$ satisfying $w_{r_s} \equiv A_0 + \cdots + A_e T^e \pmod{\mathfrak{m}^{e+1}}$. Using the induction hypothesis, we get

$$\alpha_s = \frac{A_{e+1} - w_s}{a_1^{(h+2)q^{e+1}} - w_s} \quad (0 \le s \le h).$$

Turning now to α_{h+1}, by arguments similar to those leading to (2.24), we deduce that $a_{e+1}^{(r_{h+1})} = w_{h+1}$ which in turn implies that

$$a_{e+1}^{(k)} = w_{h+1} \quad ((h+1)q^{e+1} \le k \le (h+2)q^{e+1} - 1).$$

Invoking upon the VWDWO property, we arrive at $a_{e+1}^{((h+2)q^{e+1})} \notin \{w_0, \ldots, w_{h+1}\}$, which completes the induction on h.

So far we have found that

- $a_{e+1}^{(0)} = \cdots = a_{e+1}^{(q^{e+1}-1)} = w_0$
- $a_{e+1}^{(q^{e+1})} = \cdots = a_{e+1}^{(2q^{e+1}-1)} = w_1$
- $a_{e+1}^{((h+1)q^{e+1})} = \cdots = a_{e+1}^{((h+2)q^{e+1}-1)} = w_{h+1}$, $a_{e+1}^{(h+2)q^{e+1}} \notin \{w_0, \ldots, w_{h+1}\}$ $(2 \le h+1 \le q-2)$.

By the VWDWO property modulo $\mathfrak{m}^{e+2}$, we must have

$$a_{e+1}^{((q-1)q^{e+1}+s)} = w_{q-1} \quad (0 \le s \le q^e - 1).$$

Since $\{w_n\}$ is a VWDWO sequence, considering modulo $\mathfrak{m}^{e+2}$, we get

$$w_{q^{e+2}+i} \equiv w_i \pmod{\mathfrak{m}^{e+2}} \quad (0 \le i \le q^{e+2} - 1);$$

proceeding successively through the VWDWO property, we arrive at

$$w_{jq^{e+2}+i} \equiv w_{(j-1)q^{e+2}+i} \equiv \cdots \equiv w_{q^{e+2}+i} \equiv w_i \pmod{\mathfrak{m}^{e+2}},$$

for each $j \in \mathbb{N}_0$ and $0 \le i \le q^{e+2} - 1$. Thus, for any $n = n_0 + n_1 q + \cdots + n_{d(n)} q^{d(n)} \ge q^{e+2}$ (for the case where $n \le q^{e+2} - 1$, the required result has already been found), we have, from what we have found,

$$\begin{aligned} a_0^{(n)} + a_1^{(n)} T + \cdots + a_{e+1}^{(n)} T^{e+1} &\equiv w_n \equiv w_{n_0+\cdots+n_{e+1}q^{e+1}} \\ &\equiv a_0^{(n_0+\cdots+n_{e+1}q^{e+1})} + \cdots + a_e^{(n_0+\cdots+n_{e+1}q^{e+1})} + a_{e+1}^{(n_0+\cdots+n_{e+1}q^{e+1})} T^{e+1} \\ &= w_{n_0} + \cdots + w_{n_e} T^e + w_{n_{e+1}} T^{e+1} \pmod{\mathfrak{m}^{e+2}}. \end{aligned}$$

Equating the coefficients of T^{e+1}, we conclude that $a_{e+1}^{(n)} = w_{n_{e+1}}$, which completes the induction on e and finishes the proof of the theorem. □

Applying Theorem 2.4 to the case of function field, we immediately obtain.

Corollary 2.5 *Let $\mathbb{F}_q(x)$ be the field of rational functions over $\mathbb{F}_q$ (the finite field with q elements) equipped with the x-adic valuation. Let $\{w_0 = 0, w_1, w_2, \ldots\}$ be a g-IVP sequence in the corresponding discrete valuation domain of $\mathbb{F}_q(x)$ whose associated w-polynomial sequence is $\{B_n(t)\}$. Assume that*

- *the sequence $\{w_n\}$ is a VWDWO sequence;*
- *the sequence $\{B_n(t)\}$ satisfies the Lucas property modulo the principal ideal (x)*

Then

$$w_n = w_{n_0} + w_{n_1}x + \cdots + w_{n_{d(n)}}x^{d(n)}, \tag{2.26}$$

where the base q-representation of $n \in \mathbb{N}_0$ is as in (1.2).

In passing, it is easily checked that the following converse of Corollary 2.5 is valid: if the relation (2.26) holds and $\{w_n\}$ is a VWDWO sequence, then the sequence $\{B_n(t)\}$ satisfies the Lucas property modulo (x).

Applying Theorem 2.4 to the case of rational number field together with an extra condition about the representative set U, more precise information can be obtained as shown next.

Corollary 2.6 *Let p be a prime, let V_p be the valuation domain of $\mathbb{Q}$ with respect to the p-adic valuation, and let $\{w_n\}$ be a g-IVP sequence in V_p whose associated w-polynomial sequence is $\{B_n(t)\}$. Assume that*

- *the sequence $\{w_n\}$ is a VWDWO sequence;*
- *the sequence $B_n(t)$ satisfies Lucas property modulo the principal ideal (p).*

Then

$$w_n = w_{n_0} + w_{n_1}p + \cdots + w_{n_{d(n)}}p^{d(n)}, \tag{2.27}$$

where the base p-representation of $n \in \mathbb{N}_0$ is as in (1.2).

Moreover, if

$$w_0 = 0,\ w_1 = 1,\ \ldots,\ w_{p-1} = p-1,$$

then $w_n = n \quad (n \in \mathbb{N}_0)$.

Proof The first part is immediate from Theorem 2.4. To check the last assertion, we assume that $w_i = i \in \{0, 1, \ldots, p-1\}$. With the base p-representation (1.2) of n, we get

$$w_n = w_{n_0} + w_{n_1}p + \cdots + w_{n_{d(n)}}p^{d(n)} = n_0 + n_1p + \cdots + n_{d(n)}p^{d(n)} = n.$$

□

Similar to the remark after the preceding corollary, the following converse of Corollary 2.6 is true: if the relation (2.27) holds and $\{w_n\}$ is a VWDWO sequence, then the sequence $\{B_n(t)\}$ satisfies the Lucas property modulo (p).

3. The second problem

As mention in Section 1, Carlitz proved that the sequence $\{G_n(t)/g_n\}$ is a basis for the $\mathbb{F}_q[x]$-module $\mathrm{Int}(\mathbb{F}_q[x])$; this sequence is different from the basis $\{B_n(t)\}$ in Section 2. In this section, we first confirm that $\{G_n(t)/g_n\}_{n\geq 0}$ satisfies the Lucas property. Then we derive conditions on the sequence $\{w_n\}$ generating a basis $\{\mathcal{G}_n(t)\}$ of Carlitz-like polynomials which satisfies the Lucas property.

We proceed now to verify our first objective.

Theorem 3.1 *The sequence of Carlitz polynomials $\{G_n(t)/g_n\}_{n\geq 0}$ satisfies the Lucas property modulo the principal ideal (x).*

Proof Recall from Section 1 that the sequence $\{G_n(t)/g_n\}$, with $G_0(t)/g_0 = 1$, is a basis for the $\mathbb{F}_q[x]$-module $\mathrm{Int}(\mathbb{F}_q[x])$. When $n = 0$, the Lucas property holds because both sides of (1.3) are equal to 1. For $n \geq 1$ with base q-representation as in (1.2), from (1.6) and (1.7), we have

$$\frac{G_n(t)}{g_n} = \frac{\psi_0^{n_0}(t)\psi_1^{n_1}(t)\cdots\psi_{d(n)}^{n_{d(n)}}(t)}{F_0^{n_0}F_1^{n_1}\cdots F_{d(n)}^{n_{d(n)}}}.$$

Let $A = A_0 + A_1x + \cdots \in \mathbb{F}_q[x]$. If $\deg A < d(n)$, by (1.5), we get $\psi_{d(n)}(A) = 0$. Since $A_{d(n)} = 0$, from (1.6), we have $G_{n_{d(n)}}(A_{d(n)})/g_{d(n)} = 0$, and so

$$\frac{G_n(A)}{g_n} = 0 = \frac{G_{n_0}(A_0)}{g_{n_0}}\cdots\frac{G_{n_{d(n)}}(A_{d(n)})}{g_{n_{d(n)}}}.$$

Assume henceforth that $\deg(A) \geq d(n)$. If there is an index $k \in \{1, 2, \ldots, d(n)\}$ such that $A_k = 0$, then

$$(A - (A_0 + A_1x + \cdots + A_{k-1}x^{k-1})) = A_{k+1}x^{k+1} + A_{k+2}x^{k+2} + \cdots \equiv 0 \pmod{(x)},$$

and so $\psi_k(A) = \prod_{\deg M<k}(A - M) \equiv 0 \pmod{(x)}$. Note also that $\psi_0(A_k)/F_0 = 0$. Thus,

$$\frac{G_n(A)}{g_n} = \prod_{i=0}^{d(n)}\left(\frac{\psi_i(A)}{F_i}\right)^{n_i} \equiv 0 = \prod_{i=0}^{d(n)}\left(\frac{\psi_0(A_i)}{F_0}\right)^{n_i} = \prod_{i=0}^{d(n)}\frac{G_{n_i}(A_i)}{g_{n_i}} \pmod{(x)},$$

validating the Lucas property in this case. There remains the case where $A_k \neq 0$ for all $k \in \{1, 2, \ldots, d(n)\}$. Since F_k is the product of all monic polynomial in $\mathbb{F}_q[x]$ of degree k, we see that

$$\begin{aligned}\psi_k(A) &= \prod_{\deg M<k}(A - M) = \prod_{\deg M<k}((A_kx^k + \cdots + A_1x + A_0 - M) + A_{k+1}x^{k+1}) \\ &= \prod_{\substack{\deg M'=k \\ M' \text{monic}}}(A_kM' + A_{k+1}x^{k+1} + \text{terms with higher powers of } x) \\ &= A_k^{q^k}F_k + N_kx^{\deg(F_k)+1} = A_kF_k + N_kx^{\deg(F_k)+1},\end{aligned}$$

for some $N_k \in \mathbb{F}_q[x]$. From [6, Lemma1], we know that $\psi_k(t)/F_k$ is an integer-valued polynomial, and so

$\psi_k(A)/F_k = A_k + N'_k x$ for some $N'_k \in \mathbb{F}_q[x]$. Using $\psi_0(A) = A,\ F_0 = 1$, we have

$$\begin{aligned}\frac{G_n(t)}{g_n} &= \left(\frac{\psi_0(A)}{F_0}\right)^{n_0} \prod_{k=1}^{d(n)} \left(\frac{\psi_k(A)}{F_k}\right)^{n_k} = A^{n_0} \prod_{k=1}^{d(n)} (A_k + N'_k x)^{n_k} \equiv A_0^{n_0} A_1^{n_1} \cdots A_{d(n)}^{n_{d(n)}} \\ &= \left(\frac{\psi_0(A_0)}{F_0}\right)^{n_0} \left(\frac{\psi_0(A_1)}{F_0}\right)^{n_1} \cdots \left(\frac{\psi_0(A_{d(n)})}{F_0}\right)^{n_{d(n)}} \\ &= \frac{G_{n_0}(A_0)}{g_{n_0}} \cdot \frac{G_{n_1}(A_1)}{g_{n_1}} \cdots \frac{G_{n_{d(n)}}(A_{d(n)})}{g_{n_{d(n)}}} \pmod{(x)},\end{aligned}$$

showing finally that the Carlitz polynomials basis satisfies the Lucas property modulo (x). □

To extend Theorem 3.1, we introduce:

Definition 3.2 *Let $\{w_n\}_{n\geq 0}$ be a given sequence of distinct elements in $\mathbb{F}_q[x]$.*

- *Define the interpolating w-polynomial sequence $\{\varphi_n(t)\}_{n\geq 0}$ by*

$$\varphi_0(t) = \frac{t - w_0}{w_1 - w_0}, \quad \varphi_k(t) = \frac{(t - w_0)(t - w_1)\cdots(t - w_{q^k-1})}{(w_{q^k} - w_0)(w_{q^k} - w_1)\cdots(w_{q^k} - w_{q^k-1})} \quad (k \geq 1)$$

and define the w-Carlitz like polynomial (w-CLP) sequence $\{\mathcal{G}_n(t)\}_{n\geq 0}$ of $\mathbb{F}_q(x)[t]$ by

$$\mathcal{G}_0(t) = 1,\ \mathcal{G}_n(t) = \varphi_0^{n_0}(t)\varphi_1^{n_1}(t)\cdots\varphi_{d(n)}^{n_{d(n)}}(t) \quad (n \geq 1 \text{ as in (1.2)}),$$

- *If $w_0 = 0$ and if the w-CLP sequence is a basis for $Int(\mathbb{F}_q[x])$, then $\{w_n\}$ is called a g-CLP (generating Carlitz like polynomial) sequence.*

Observe from Definition 3.2 that

1. the sequence of Carlitz polynomials $\{G_n(t)/g_n\}$ is a special case of $\mathcal{G}_n(t)$ with $\{w_0 = 0, w_1 = 1, \ldots, w_{q-1}\} = \mathbb{F}_q$ and $w_n = w_{n_0} + w_{n_1} x + w_{n_{d(n)}} x^{d(n)}$;
2. though the polynomials $\mathcal{G}_n(t)$ and $B_n(t)$ (in Section 2) are of the same degree n, they are not the same because all factors of $B_n(t)$ are distinct, while $\mathcal{G}_n(t)$ contains repeated factors.

Keeping the notation set out in Section 1, we first prove an auxiliary result.

Lemma 3.3 *Let*

$$A = A_0 + A_1 T + \cdots + A_j T^j + \cdots \in U[[T]]$$
$$B = B_0 + B_1 T + \cdots + B_j T^j + \cdots \in U[[T]]$$

be two nonzero elements in V. If B is a divisor of A in V, then $\nu(A) \geq \nu(B)$ and

$$\frac{A}{B} \equiv \frac{A_{\nu(B)}}{B_{\nu(B)}} \pmod{\mathfrak{m}}. \tag{3.1}$$

Proof Let $r=\nu(A)$ and $s=\nu(B)$. If $r<s$, then

$$\frac{A}{B}=\frac{A_rT^r+A_{r+1}T^{r+1}+\cdots}{B_sT^s+B_{s+1}T^{s+1}+\cdots}=\frac{A_r+A_{r+1}T+\cdots}{T^{s-r}(B_s+B_{s+1}T\cdots)}\notin V,$$

which is a contradiction. Thus, $r\geq s$, and we see that

$$\frac{A}{B}=\frac{A_rT^{r-s}+A_{r+1}T^{r-s+1}+\cdots}{B_s+B_{s+1}T+\cdots}=\frac{A_r}{B_s}T^{r-s}+N'T^{r-s+1}$$

for some $N'\in V$. If $r=s$, (3.1) is immediate, while if $r>s$, both sides of (3.1) are $\equiv 0 \pmod{\mathfrak{m}}$. □

Our extension of Theorem 3.1 reads:

Theorem 3.4 *Given a g-CLP sequence $\{w_n\}$, let $\{\mathcal{G}_n(t)\}$ be its associated w-CLP sequence. If $\{\mathcal{G}_n(t)\}$ satisfies the Lucas property modulo (x), then for each $k\in\mathbb{N}$, we have*

1. *$\{w_0=0,\ldots,w_{q^k-1}\}$ is the set of all polynomials in $\mathbb{F}_q[x]$ of degree $<k$; in particular $\{w_0=0,w_1,\ldots,w_{q-1}\}=\mathbb{F}_q$;*
2. *the sequence element w_{q^k} is a polynomial in $\mathbb{F}_q[x]$ of degree k with leading coefficient w_1.*

Proof To prove the first assertion, we begin with the claim that the set $\{w_0=0,w_1,\cdots,w_{q^k-1}\}$ constitutes a complete residue system modulo $(x)^k$ in the ring $\mathbb{F}_q[x]$, or equivalently,

$$(w_i)_{\bmod x^k}:=a_0^{(i)}+a_1^{(i)}x+\cdots+a_{k-1}^{(i)}x^{k-1}\quad(0\leq i\leq q^k-1).$$

To verify this claim, consider $\mathcal{G}_1(t)=\varphi_0(t)=t/w_1$. Since $\mathcal{G}_1(t)\in \mathrm{Int}(\mathbb{F}_q[x])$, we get $\mathcal{G}_1(1)=1/w_1\in\mathbb{F}_q[x]$ showing that w_1 is a unit in $\mathbb{F}_q[x]$, i.e. $w_1\in\mathbb{F}_q^*$ which affirms the first assertion when $k=0$. Next, for the case $k=1$, since $\mathcal{G}_q(t)=\varphi_1(t)=\frac{t(t-w_1)\cdots(t-w_{q-1})}{w_q(w_q-w_1)\cdots(w_q-w_{q-1})}$, by the Lucas property modulo (x), for each $A=A_0+A_1x+\cdots\in\mathbb{F}_q[x]$, we get

$$\frac{\mathcal{A}_1}{\mathcal{B}_1}=:\frac{A(A-w_1)\cdots(A-w_{q-1})}{w_q(w_q-w_1)\cdots(w_q-w_{q-1})}=\mathcal{G}_q(A)\equiv\mathcal{G}_1(A_1)=\varphi_0(A_1)=\frac{A_1}{w_1}\pmod{(x)}.\tag{3.2}$$

The numerator and the denominator are

$$\begin{aligned}\mathcal{A}_1&=\prod_{i=0}^{q-1}\Big((A_0-a_0^{(i)})+(A_1-a_1^{(i)})x+(A_2-a_2^{(i)})x^2+\cdots\Big)\\&=\prod_{i=0}^{q-1}(A_0-a_0^{(i)})+\sum_{j=0}^{q-1}(A_1-a_1^{(j)})x\prod_{\substack{i=0\\i\neq j}}^{q-1}(A_0-a_0^{(i)})+(\text{terms with } x \text{ of powers}\geq 2)\\\mathcal{B}_1&=\prod_{i=0}^{q-1}(a_0^{(q)}-a_0^{(i)})+\sum_{j=0}^{q-1}(a_1^{(q)}-a_1^{(j)})x\prod_{\substack{i=0\\i\neq j}}^{q-1}(a_0^{(q)}-a_0^{(i)})+(\text{terms with } x \text{ of powers}\geq 2).\end{aligned}$$

If $\prod_{i=0}^{q-1}(A_0 - a_0^{(i)}) \neq 0$, then

$$\frac{A_1}{w_1} = \prod_{i-0}^{q-1} \frac{(A_0 - a_0^{(i)})}{(a_0^{(q)} - a_0^{(i)})};$$

this relation holds for any $A_1 \in \mathbb{F}_q$ on the left, while the right-hand side is independent of A_1, which is untenable. Thus, $\prod_{i=0}^{q-1}(A_0 - a_0^{(i)}) = 0$, implying that $A_0 \in \mathbb{F}_q$. This being true for any $A_0 \in \mathbb{F}_q$, we must have $\{a_0^{(0)},\ a_0^{(1)}, \ldots, a_0^{(q-1)}\} = \mathbb{F}_q$, affirming the first assertion when $k = 1$.

Proceeding to general k, consider the set $\{w_0 = 0, w_1, \ldots, w_{q^k-1}\}$ of $q^k - 1$ elements. Since

$$\mathcal{G}_{q^k}(t) = \varphi_k(t) = \frac{t(t - w_1)\cdots(t - w_{q^k-1})}{w_{q^k}(w_{q^k} - w_1)\cdots(w_{q^k} - w_{q^k-1})}.$$

satisfies the Lucas property modulo (x), we get

$$\frac{\mathcal{A}_k}{\mathcal{B}_k} =: \frac{A(A - w_1)\cdots(A - w_{q^k-1})}{w_{q^k}(w_{q^k} - w_1)\cdots(w_{q^k} - w_{q^k-1})} = \mathcal{G}_{q^k}(A) \equiv \mathcal{G}_1(A_k) = \frac{A_k}{w_1} \pmod{(x)}. \tag{3.3}$$

The numerator and the denominator are

$$\begin{aligned}
\mathcal{A}_k &= \prod_{i=0}^{q^k-1} \Big\{ \Big((A_0 + A_1x + \cdots + A_{k-1}x^{k-1}) - (a_0^{(i)} + a_1^{(i)}x + \cdots + a_{k-1}^{(i)}x^{k-1}) \Big) \\
&\qquad + (A_k - a_k^{(i)})x^k + (A_{k+1} - a_{k+1}^{(i)})x^{k+1} + \text{terms with higher powers of } x \Big\} \\
&= \prod_{i=0}^{q^k-1} \Big((A_0 + A_1x + \cdots + A_{k-1}x^{k-1}) - (a_0^{(i)} + a_1^{(i)}x + \cdots + a_{k-1}^{(i)}x^{k-1}) \Big) \\
&\quad + \sum_{j=0}^{q^k-1} (A_k - a_k^{(j)})x^k \prod_{\substack{i=0 \\ i\neq j}}^{q^k-1} \Big((A_0 + \cdots + A_{k-1}x^{k-1}) - (a_0^{(i)} + \cdots + a_{k-1}^{(i)}x^{k-1}) \Big) \\
&\quad + (\text{terms with higher powers of } x) \\
\mathcal{B}_k &= \prod_{i=0}^{q^k-1} \Big((a_0^{(q^k)} + a_1^{(q^k)}x + \cdots + a_{k-1}^{(q^k)}x^{k-1}) - (a_0^{(i)} + a_1^{(i)}x + \cdots + a_{k-1}^{(i)}x^{k-1}) \Big) \\
&\quad + \sum_{j=0}^{q^k-1} (a_k^{(q^k)} - a_k^{(j)})x^k \prod_{\substack{i=0 \\ i\neq j}}^{q^k-1} \Big((a_0^{(q^k)} + \cdots + a_{k-1}^{(q^k)}x^{k-1}) - (a_0^{(i)} + \cdots + a_{k-1}^{(i)}x^{k-1}) \Big) \\
&\quad + (\text{terms with higher powers of } x).
\end{aligned}$$

Let

$$\mathcal{N} = \prod_{i=0}^{q^k-1} \Big((A_0 + A_1x + \cdots + A_{k-1}x^{k-1}) - (a_0^{(i)} + a_1^{(i)}x + \cdots + a_{k-1}^{(i)}x^{k-1}) \Big) \tag{3.4}$$

$$\mathcal{D} = \prod_{i=0}^{q^k-1} \Big((a_0^{(q^k)} + a_1^{(q^k)}x + \cdots + a_{k-1}^{(q^k)}x^{k-1}) - (a_0^{(i)} + a_1^{(i)}x + \cdots + a_{k-1}^{(i)}x^{k-1}) \Big).$$

If $\mathcal{N} \neq 0$, then there is a least positive integer r such that $r = \nu_q(\mathcal{N})$. Lemma 3.3 now ensures that $\mathcal{D} \neq 0$ and together with (3.3), we deduce that $A_k/w_1 = \alpha_1/\alpha_2$, where α_1 and α_2 are the coefficients of x^r in $\mathcal{N}$ and $\mathcal{D}$, respectively. But α_1/α_2 is independent of A_k, which is untenable, implying that $\mathcal{N} = 0$. Appealing to (3.4), using the fact that $A_0, A_1, \ldots, A_{k-1}$ are arbitrary elements in $\mathbb{F}_q$, and their total number is equal to q^k, the number of elements in the set $\{(w_0)_{\bmod x^k}, (w_1)_{\bmod x^k}, \ldots, (w_{q^k-1})_{\bmod x^k}\}$, we conclude that this last set is identical with the set of all polynomials in $\mathbb{F}_q[x]$ of degree $< k$. This completes the proof of our claim.

Next, we claim that the mod x^k can be removed, i.e. the set $\{w_0, w_1, \ldots, w_{q^k-1}\}$ is indeed the set of all polynomials of degree $< k$. Assume to the contrary that there exists $n \leq q^k - 1$ such that $\deg w_n \geq k$. Writing

$$w_n = a_0^{(n)} + a_1^{(n)}x + \cdots + a_s^{(n)}x^s, \ s \geq k, \ a_s^{(n)} \neq 0,$$

and substituting for t by w_n in $\mathcal{G}_{q^s}(t)$, we get

$$0 = \mathcal{G}_{q^s}(w_n) \equiv \mathcal{G}_1(a_s^{(n)}) = \varphi_0(a_s^{(n)}) = \frac{a_s^{(n)}}{w_1} \pmod{(x)},$$

contradicting what found earlier that $a_s^{(n)}/w_1 \in \mathbb{F}_q^*$. Thus, the second claim is verified which in turn affirms the first assertion.

To establish the second assertion, note from the first assertion that $\{w_0, w_1, \ldots, w_{q^k-1}\}$ is the set of all polynomials of degree $< k$ and we have $\{w_0, w_1, \ldots, w_{q^{k+1}-1}\}$ is the set of all polynomials of degree $< k+1$, and so each element of the set $\{w_{q^k}, w_{q^k+1}, \ldots, w_{q^{k+1}-1}\}$ is of degree k, showing that $a_k^{(q^k)} \neq 0$. For $A = A_0 + A_1x + \cdots \in \mathbb{F}_q[x]$ with $A_k \neq 0$, we get

$$\begin{aligned}
\mathcal{G}_{q^k}(A) = \varphi_k(A) &= \prod_{i=0}^{q^k-1} \frac{A - w_i}{w_{q^k} - w_i} = \prod_{\deg M < k} \frac{A - M}{w_{q^k} - M} \\
&= \prod_{\deg M < k} \frac{\left(A_0 + \cdots + A_{k-1}x^{k-1} + A_kx^k - M\right) + A_{k+1}x^{k+1} + \cdots}{\left(a_0^{(q^k)} + \cdots + a_{k-1}^{(q^k)}x^{k-1} + a_k^{(q^k)}x^k - M\right) + a_{k+1}^{(q^k)}x^{k+1} + \cdots} \\
&= \frac{A_k^{q^k}F_k + N_1x^{1+\deg F_k}}{(a_k^{(q^k)})^{q^k}F_k + N_2x^{1+\deg F_k}} \frac{A_k}{a_k^{(q^k)}} \pmod{(x)},
\end{aligned}$$

where $N_1, N_2 \in \mathbb{F}_q[x]$. On the other hand, the Lucas property modulo (x) yields

$$\mathcal{G}_{q^k}(A) \equiv \mathcal{G}_1(A_k) = \varphi_0(A_k) = \frac{A_k}{w_1} \pmod{(x)}.$$

Thus, $a_k^{(q^k)} = w_1$ for all $k \in \mathbb{N}$ and the second assertion is established. □

Specializing the value of w_1, Theorem 3.4 yields at once:

Corollary 3.5 *If $\{w_n\}$ is a g-CLP sequence with $w_1 = 1$, then its associated w-polynomial sequence $\{\varphi_n(t)\}$ satisfies*

$$\varphi_n(t) = \frac{\psi_n(t)}{F_n} \quad (n \in \mathbb{N}_0),$$

and its associated w-CLP sequence $\{\mathcal{G}_n(t)\}$ is identical with the set of Carlitz polynomials $\{G_n(t)/g_n\}$.

4. The third problem

Keeping the notation set out in Section 1, as witnessed in [2, Remark 2.7, p. 309], there are bases of $\mathrm{Int}\,(V)$ that do not satisfy the Lucas property. One such basis is that of Fermat polynomials $\mathcal{F}_n(t)$, [2], defined, with $\mathfrak{m} = (T)$, by

$$\mathcal{F}_0(t) = 1,\ \mathcal{F}_1(t) = t,\ \mathcal{F}_q(t) = \frac{t - t^q}{T},\ \mathcal{F}_{q^{h+1}}(t) = \mathcal{F}_q(\mathcal{F}_{q^h}),$$

$$\mathcal{F}_n(t) = \prod_{j=0}^{d(n)} (\mathcal{F}_{q^j})^{n_j} \quad \text{for } n \in \mathbb{N} \text{ as in (1.2)}.$$

Note that Fermat polynomials are neither of the same form as the Lagrange-type interpolation polynomials $B_n(t)$ in Section 2, nor of the same form as the Carlitz-type polynomials in Section 3. This leads us to ask for necessary condition(s) on general polynomials which form a basis for $\mathrm{Int}\,(V)$ and satisfy the Lucas property.

For each $i \in \mathbb{N}_0$, let $\{P_i^{(n)}\}_{n\geq 0}$ be a sequence in V with $P_n^{(n)} \neq 0$, and let

$$\left\{Q_0 = 1,\ Q_n := Q_0^{(n)} + Q_1^{(n)}T + \cdots \in U[[T]] \quad (n \in \mathbb{N})\right\}$$

be a sequence in $V^* := V \setminus \{0\}$. Define $\{\mathcal{H}_n(t)\}_{n\geq 0} \subseteq K[t]$, a general sequence of polynomials associated with the sequences $\{P_i^{(n)}\}, \{Q_n\}$, by

$$\mathcal{H}_0(t) = 1, \quad \mathcal{H}_n(t) = \frac{P_0^{(n)} + P_1^{(n)}t + \cdots + P_n^{(n)}t^n}{Q_n} \quad (n \in \mathbb{N}).$$

Observe that $\deg \mathcal{H}_n(t) = n$. We shall find it convenient to use the notation

$$\left(P_0^{(n)} + P_1^{(n)}A + \cdots + P_n^{(n)}A^n\right)_{\bmod \mathfrak{m}^r}$$

to represent the residue of the expression $P_0^{(n)} + P_1^{(n)}A + \cdots + P_n^{(n)}A^n$ modulo the principal ideal $\mathfrak{m}^r$.

Our next theorem gives necessary conditions for $\mathrm{Int}\,(V)$.

Theorem 4.1 *Keeping the notation in Section 1 and as set out above, if $\{\mathcal{H}_n(t)\}$ is a basis of the V-module $Int(V)$, then for each $A = A_0 + A_1T + \cdots + A_jT^j + \cdots \in V$, the following statements hold:*

1. *if $Q_0^{(n)} \neq 0$, then $\mathcal{H}_n(A) \equiv \frac{P_0^{(n)} + P_1^{(n)}A_0 + \cdots + P_n^{(n)}A_0^n}{Q_0^{(n)}} \pmod{\mathfrak{m}}$;*

2. *for $r \geq 1$, if $Q_0^{(n)} = Q_1^{(n)} = \cdots = Q_{r-1}^{(n)} = 0,\ Q_r^{(n)} \neq 0$, then*

$$\left(P_0^{(n)} + P_1^{(n)}A + \cdots + P_n^{(n)}A^n\right)_{\bmod \mathfrak{m}^r} = 0.$$

Proof Since $\mathcal{H}_n(t) \in \mathrm{Int}\,(V)$, we have $\mathcal{H}_n(A) = \frac{P_0^{(n)} + P_1^{(n)}A + \cdots + P_n^{(n)}A^n}{Q_n} \in V$.

1. If $Q_0^{(n)} \neq 0$, by Lemma 3.3, we have

$$\begin{aligned}\mathcal{H}_n(A) =& \frac{P_0^{(n)} + P_1^{(n)}(A_0 + A_1T + \cdots) + \cdots + P_n^{(n)}(A_0 + A_1T + \cdots)^n}{Q_0^{(n)} + Q_1^{(n)}T + \cdots} \\ \equiv& \frac{P_0^{(n)} + P_1^{(n)}A_0 + \cdots + P_n^{(n)}A_0^n}{Q_0^{(n)}} \pmod{\mathfrak{m}}.\end{aligned}$$

2. If $Q_0^{(n)} = Q_1^{(n)} = \cdots = Q_{r-1}^{(n)} = 0,\ Q_r^{(n)} \neq 0$, then

$$\mathcal{H}_n(A) = \frac{P_0^{(n)} + P_1^{(n)}A + \cdots + P_n^{(n)}A^n}{Q_r^{(n)}T^r + Q_{r+1}^{(n)}T^{r+1} + \cdots}.$$

Since the numerator is a multiple of T^r, the assertion follows from the fact that $\mathcal{H}_n(A) \in V$. □

Using Theorem 4.1, we now derive a necessary condition for a basis of $\mathrm{Int}(V)$ to satisfy the Lucas property.

Corollary 4.2 *Keeping the notation of Theorem 4.1, assume that $\{\mathcal{H}_n(t)\}_{n\geq 0}$ is a basis of the V-module $Int(V)$. If $\{\mathcal{H}_n(t)\}$ satisfies the Lucas property modulo $\mathfrak{m}$, then for each $n \geq q$ with its base q representation as in (1.2) and $A = A_0 + A_1q + \cdots + A_jq^j + \cdots \in V$, we have*

$$\frac{\left(P_0^{(n)} + P_1^{(n)}A + \cdots + P_n^{(n)}A^n\right)_{\bmod \mathfrak{m}^{s+1}}}{Q_s^{(n)}T^s} \equiv \prod_{i=0}^{d(n)} \frac{P_0^{(n_i)} + P_1^{(n_i)}A_i + \cdots + P_{n_i}^{(n_i)}A_i^{n_i}}{Q_{n_i}} \pmod{\mathfrak{m}}, \tag{4.1}$$

where $s = \nu(Q_n)$.

Proof If $s = 0$, by Theorem 4.1 part 1 and Lemma 3.3, we get

$$\mathcal{H}_n(A) \equiv \frac{P_0^{(n)} + P_1^{(n)}A_0 + \cdots + P_n^{(n)}A_0^n}{Q_0^{(n)}} \equiv \frac{\left(P_0^{(n)} + P_1^{(n)}A + \cdots + P_n^{(n)}A^n\right)_{\bmod \mathfrak{m}}}{Q_0^{(n)}} \pmod{\mathfrak{m}}.$$

If $s \geq 1$, by Theorem 4.1 part 2, we can write

$$P_0^{(n)} + P_1^{(n)}A + \cdots + P_n^{(n)}A^n = R_sT^s + R_{s+1}T^{s+1} + \cdots \in U[[T]],$$

and invoking upon Lemma 3.3, we get

$$\mathcal{H}_n(A) = \frac{R_sT^s + R_{s+1}T^{s+1} + \cdots}{Q_s^{(n)}T^s + Q_{s+1}^{(n)}T^{s+1} + \cdots} \equiv \frac{R_s}{Q_s^{(n)}} = \frac{\left(P_0^{(n)} + P_1^{(n)}A + \cdots + P_n^{(n)}A^n\right)_{\bmod \mathfrak{m}^{s+1}}}{Q_s^{(n)}T^s} \pmod{\mathfrak{m}}. \tag{4.2}$$

Since $\{\mathcal{H}_n(t)\}$ satisfies the Lucas property modulo $\mathfrak{m}$, we have

$$\mathcal{H}_n(A) \equiv \mathcal{H}_{n_0}(A_0)\mathcal{H}_{n_1}(A_1)\cdots\mathcal{H}_{n_{d(n)}}(A_{d(n)}) = \prod_{i=0}^{d(n)} \frac{P_0^{(n_i)} + P_1^{(n_i)}A_i + \cdots + P_{n_i}^{(n_i)}A_i^{n_i}}{Q_{n_i}} \pmod{\mathfrak{m}}. \tag{4.3}$$

The desired result follows at once from (4.2) and (4.3). □

As an application of Corollary 4.2, we give another proof that the sequence of Fermat polynomials $\mathcal{F}_n(t)$ does not satisfy the Lucas property. Taking in this case, $K = \mathbb{F}_2(x)$ equipped with the x-adic valuation so that the discrete valuation domain is

$$V = \left\{ \frac{f(x)}{g(x)} \in \mathbb{F}_2(x) \ ; \ x \nmid g(x) \right\}.$$

Consider the Fermat polynomials

$$\mathcal{F}_0(t) = 1, \ \mathcal{F}_1(t) = t, \ \mathcal{F}_2(t) = \frac{t - t^2}{x}, \ \mathcal{F}_4(t) = \mathcal{F}_2(\mathcal{F}_2(t)) = \frac{0 + xt - (1+x)t^2 - 0 \cdot t^3 - t^4}{x^3}.$$

Let

$$\begin{aligned}
&n = 4 = 0 + 0 \cdot 2 + 1 \cdot 2^2, \\
&\frac{P_0^{(4)} + P_1^{(4)} t + P_2^{(4)} t^2 + P_3^{(4)} t^3 + P_4^{(4)} t^4}{Q_4} = \mathcal{H}_4(t) = \mathcal{F}_4(t) = \frac{0 + xt - (1+x)t^2 + 0 \cdot t^3 - t^4}{x^3}, \\
&\frac{P_0^{(0)}}{Q_0} = \mathcal{H}_0(t) = \mathcal{F}_0(t) = \frac{1}{1}, \quad \frac{P_0^{(1)} + P_1^{(1)} t}{Q_1} = \mathcal{H}_1(t) = \mathcal{F}_1(t) = \frac{t}{1}, \\
&\frac{P_0^{(2)} + P_1^{(2)} t + P_2^{(2)} t^2}{Q_2} = \mathcal{H}_2(t) = \mathcal{F}_2(t) = \frac{t - t^2}{x},
\end{aligned}$$

so that

$$\begin{aligned}
&d(4) = 2, \ n_0 = n_1 = 0, n_2 = 1, \\
&Q_0 = Q_1 = 1, Q_2 = x, Q_4 = x^3 = 0 + 0 \cdot x + 0 \cdot x^2 + 1 \cdot x^3, \ s = \nu(Q_4) = 3, \ Q_3^{(4)} = 1.
\end{aligned}$$

Taking $A = x = 0 + 1 \cdot x, \ A_1 = 1, A_i = 0 \ (i \neq 1)$, the left-hand expression of (4.1) is

$$\frac{\left(0 + x \cdot x - (1+x)x^2 + 0 \cdot x^3 - x^4\right) \bmod (x)^4}{1 \cdot x^3} = 1,$$

while the right-hand expression of (4.1) is

$$\prod_{i=0}^{2} \frac{P_0^{(n_i)} + P_1^{(n_i)} A_i + \cdots + P_{n_i}^{(n_i)} A_i^{n_i}}{Q_{n_i}} = \frac{P_0^{(0)}}{Q_0} \cdot \frac{P_0^{(0)}}{Q_0} \cdot \frac{P_0^{(1)} + P_1^{(1)} A_2}{Q_1} = 0.$$

These two values contradict the result of Corollary 4.2 implying that the sequence of Fermat polynomials does not satisfy the Lucas property.

Acknowledgment

The authors are grateful to the anonymous referees for suggestions and comments. The first author is financially supported by the Science Achievement Scholarship of Thailand (SAST).

References

[1] Bhargava M. P-orderings and polynomial functions on arbitrary subsets of Dedekind rings. Journal für die reine und angewandte Mathematik 1997; 490: 101-127. doi: 10.1515/crll.1997.490.101

[2] Boulanger J, Chabert J-L. An extension of the Lucas theorem. Acta Arithmetica 2001; 96: 303-312. doi: 10.4064/aa96-4-1

[3] Cahen P-J, Chabert J-L. Integer-valued polynomials. American Mathematical Society Surveys and Monographs Providence 1997; 48.

[4] Carlitz L. On polynomials in a Galois field. Bulletin of the American Mathematical Society 1932; 38: 736-744.

[5] Carlitz L. On certain functions connected with polynomials in a Galois field. Duke Mathematical Journal 1935; 1: 137-168. doi: 10.1215/s0012-7094-35-00114-4

[6] Carlitz L. A set of polynomials. Duke Mathematical Journal 1940; 6: 486-504. doi: 10.1215/S0012-7094-40-00639-1

[7] Fine NJ. Binomial coefficients modulo a prime. The American Mathematical Monthly 1947; 54: 589-592. doi: 10.2307/2304500

[8] McCarthy PJ. Algebraic Extension of Fields. New York, NY, USA: Dover, 1991.

[9] Narkiewicz W. Polynomial Mappings, Lecture Notes in Mathematics 1600. Berlin, Germany: Springer, 1995.