พหุนามค่าจำนวนเต็มเหนือโดเมนกำหนดค่าแบบวิยุต

นางสาวรัตติยา มีษา

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรดุษฎีบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2564

INTEGER-VALUED POLYNOMIALS OVER DISCRETE VALUATION DOMAINS

Miss Rattiya Meesa

A Dissertation Submitted in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy Program in Mathematics
Department of Mathematics and Computer Science
Faculty of Science
Chulalongkorn University
Academic Year 2021

Thesis Title	INTEGER-VALUED POLYNOMIALS OVER DISCRETE VALUATION DOMAINS
By	Miss Rattiya Meesa
Field of Study	Mathematics
Thesis Advisor	Associate Professor Tuangrat Chaichana, Ph.D.
Thesis Co-advisor	Professor Vichian Laohakosol, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Doctoral Degree

.... Dean of the Faculty of Science
(Professor Polkit Sangvanich, Ph.D.)

THESIS COMMITTEE

.... Chair External Committee
(Associate Professor Narakorn Kanasri, Ph.D.)

.... Advisor
(Associate Professor Tuangrat Chaichana, Ph.D.)

.... Co-Advisor
(Professor Vichian Laohakosol, Ph.D.)

.... Committee
(Professor Yotsanan Meemark, Ph.D.)

.... Committee
(Assistant Professor Kirati Sriamorn, Ph.D.)

.... Committee
(Nithi Rungtanapirom, Ph.D.)

รัตติยา มีษา : พหุนามค่าจำนวนเต็มบนโดเมนกำหนดค่าแบบวิยุต (INTEGER-VALUED POLYNOMIALS OVER DISCRETE VALUATION DOMAINS) อ.ที่ปรึกษาวิทยานิพนธ์หลัก : รองศาสตราจารย์ ดร.ตวงรัตน์ ไชยชนะ, อ.ที่ปรึกษาวิทยานิพนธ์ร่วม : ศาสตราจารย์ ดร. วิเชียร เลาหโกศล, 57 หน้า.

ทฤษฎีบทแบบฉบับของลูคัสกล่าวว่า พหุนามทวินามซึ่งเป็นฐานหลักของพหุนามค่าจำนวนเต็มสอดคล้องสมภาคมอดุโลจำนวนเฉพาะที่เกี่ยวข้องกับเลขโดดจากการกระจายจำนวนเต็มฐานจำนวนเฉพาะนั้น ในวิทยานิพนธ์นี้ เรานิยามสมบัติลูคัสภายใต้โครงสร้างที่ถูกกำหนดค่าแบบวิยุต และศึกษาว่าเมื่อใดพหุนามจะสอดคล้องกับสมบัตินี้ เราได้หาหลักเกณฑ์ทั่วไปในการตรวจสอบฐานหลักของพหุนามค่าจำนวนเต็มในโครงสร้างนี้ที่สอดคล้องกับสมบัติลูคัส ทั้งยังนำเสนอตัวอย่างของฐานหลักดังกล่าวที่อยู่ในรูปแบบลากรองจ์และพหุนามคล้ายคาร์ลิทซ์อีกด้วย

นอกจากนี้สมบัติที่รู้จักกันดีของพหุนามทวินามในกรณีแบบฉบับคือ สมการสามเหลี่ยมปาสคาลที่แสดงค่าของสัมประสิทธิ์ทวินาม ในรูปผลรวมของอีกสองสัมประสิทธิ์ทวินาม ในส่วนที่สองของวิทยานิพนธ์นี้ เราจึงนิยามสมบัติปาสคาลทั่วไป และพิสูจน์คุณลักษณะของพหุนามที่สอดคล้องสมบัติปาสคาลดังกล่าว มากไปกว่านั้นเราแสดงตัวอย่างของฐานหลักของพหุนามค่าจำนวนเต็มที่สอดคล้องกับสมบัติปาสคาล ซึ่งครอบคลุมกรณีแบบฉบับอีกด้วย

ภาควิชา คณิตศาสตร์และวิทยาการคอมพิวเตอร์ ลายมือชื่อนิสิต ....

สาขาวิชา ....คณิตศาสตร์.......... ลายมือชื่อ อ.ที่ปรึกษาหลัก ....

ปีการศึกษา ....2564.......... ลายมือชื่อ อ.ที่ปรึกษาร่วม ....

6172844023 : MAJOR MATHEMATICS
KEYWORDS : INTEGER-VALUED POLYNOMIAL/ DISCRETE VALUATION DOMAIN/ LUCAS PROPERTY / PASCAL PROPERTY

RATTIYA MEESA : INTEGER-VALUED POLYNOMIALS OVER DISCRETE VALUATION DOMAINS
ADVISOR : ASSOC. PROF. TUANGRAT CHAICHANA, Ph.D.,
CO-ADVISOR : PROF. VICHIAN LAOHAKOSOL, Ph.D., 57 pp.

The classical theorem of Lucas states that binomial polynomials, which form a basis for integer-valud polynomials, satisfy a congruence relation, modulo a prime, related to their digits in the base prime representation. In this thesis, we define the Lucas property in the setting of discrete-valued structures and investigate when and where the Lucas property holds. General criteria are derived for bases of integer-valued polynomials in this setting to satisfy the Lucas property. Examples of bases including those of Lagrange type and of Carlitz-like polynomials are worked out.

In addition, one of the best known properties of binomial polynomials in the classical case is the Pascal triangle equality, which equates the sum of two binomial coefficients to the one in the following line. In the second part of the thesis, we define a general Pascal property and prove a characterization for polynomials which satisfy this Pascal property. Examples of bases of integer-valued polynomials satisfying such a Pascal property, which embrace the classical case, are derived.

Department : Mathematics and Computer Science Student's Signature ....

Field of Study : Mathematics Advisor's Signature ....

Academic Year : 2021 Co-Advisor's Signature ....

ACKNOWLEDGEMENTS

My deepest gratitude goes to my thesis advisor, Associate Professor Tuangrat Chaichana, and thesis co-advisor, Professor Vichian Laohakosol, Ph.D., for their continuous guidance and support throughout the time of my thesis research. I deeply thank my thesis committee members, Professor Yotsanan Meemark, Ph.D., Assistant Professor Kirati Sriamorn, Ph.D., Nithi Rungtanapirom, Ph.D. and Associate Professor Narakorn Kanasri, Ph.D., for their constructive comments and suggestions. Moreover, I feel very thankful to all of my teachers who have taught me for my knowledge.

I would like to express my gratitude to my beloved family for their love and encouragement throughout my study. In particular, I wish to thank my friends for a great friendship.

Finally, I am grateful to the Human Resource Development in Science Project (Science Achievement Scholarship of Thailand, SAST) for financial support throughout my graduate study.

CONTENTS

CHAPTER I
INTRODUCTION

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

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

There has been numerous studies to investigate some properties of $\operatorname{Int}(D)$. For example, it was shown in [4, Chapter I.1] and [12] that the set $\operatorname{Int}(D)$ is a subring of $K[t]$ containing $D[t]$ and is also a D-module.

In the classical case where $D = \mathbb{Z}$, [4, Proposition I.1.1] the $\mathbb{Z}$-module $\operatorname{Int}(\mathbb{Z})$ is free and one best known regular basis of free $\mathbb{Z}$-module $\operatorname{Int}(\mathbb{Z})$ is the set of binomial polynomials $\left\{\binom{t}{n}\right\}_{n\in\mathbb{N}_0}$, defined by

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

One of the famous results concerning binomial polynomials is the Lucas theorem, [10]: let p be a prime number and let m and n be nonnegative integers. Then

$$\binom{m}{n} \equiv \binom{m_0}{n_0}\binom{m_1}{n_1}\cdots\binom{m_{d(n)}}{n_{d(n)}} \pmod{p}, \tag{1.1}$$

where

$$\begin{aligned} n &= n_0 + n_1p + n_2p^2 + \cdots + n_{d(n)}p^{d(n)} && \text{with } 0 \le n_i < p \ \ (n_{d(n)} \neq 0),\\ m &= m_0 + m_1p + m_2p^2 + \cdots + m_{d(m)}p^{d(m)} && \text{with } 0 \le m_j < p \ \ (m_{d(m)} \neq 0) \end{aligned}$$

are base p expansions of n and m, respectively.

There is a simple short proof of this theorem in [10], where some results on the number and conditions for binomial coefficients to be divisible by p are also obtained. Another famous identity related to binomial polynomials is the Pascal identity, [8, Theorem 26]: for $n \in \mathbb{N}$ and $k \in \mathbb{N}_0$, we have

$$\binom{k+1}{n} = \binom{k}{n-1} + \binom{k}{n},$$

which asserts that coefficient of the x^n in the expansion of $(1+x)^{k+1}$ is resulted from the sum of two neighboring coefficients of $(1+x)^k$.

For $D = V$, a discrete-valuation domain of the field K with finite residue field, the unique principal maximal ideal of V is denoted by $\mathfrak{m}$. Let T be a generator of $\mathfrak{m}$, and let q be the cardinality of the residue field $V/\mathfrak{m}$. Denote the set of representatives of $V/\mathfrak{m}$ by $U = \{u_0 = 0, u_1, \dots, u_{q-1}\}$. The running index of the sequence $\{u_n\}_{n \in \mathbb{N}_0}$ is enlarged from $q-1$ to the entire $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ by the following construction. For $n \in \mathbb{N}, n \geq q$, if the base q-representation of n is $n = n_0 + n_1 q + \cdots + n_{d(n)} q^{d(n)}$ $(0 \leq n_i < q)$, define

$$u_n = u_{n_0} + u_{n_1} T + \cdots + u_{n_{d(n)}} T^{d(n)}.$$

Using the sequence $\{u_n\}_{n \in \mathbb{N}_0}$, a regular basis $\{C_n(t)\}_{n \in \mathbb{N}_0}$ of the V-module $\mathrm{Int}(V)$ is defined along the same line as that of **Lagrange interpolating polynomials**, namely,

$$C_0(t) = 1, \qquad C_n(t) = \frac{(t-u_0)(t-u_1)\cdots(t-u_{n-1})}{(u_n-u_0)(u_n-u_1)\cdots(u_n-u_{n-1})} \quad (n \in \mathbb{N}).$$

In 2001, Boulanger and Chabert [3] generalized Lucas's theorem from $\mathbb{Z}$ to V by showing that $\{C_n(t)\}_{n \in \mathbb{N}_0}$ satisfies the congruence relation analogous to Lucas theorem: if

$$n = n_0 + n_1 q + \cdots + n_{d(n)} q^{d(n)} \quad \text{and} \quad A = A_0 + A_1 T + \cdots$$

are the q-adic expansion of a positive integer n, and the T-adic expansion of an element A of V, respectively, then

$$C_n(A) \equiv C_{n_0}(A_0)C_{n_1}(A_1)\cdots C_{n_{d(n)}}(A_{d(n)}) \pmod{\mathfrak{m}}. \tag{1.2}$$

In particular, if we replace V by $\mathbb{Z}$, ν by ν_p (the p-adic order), and $\mathfrak{m}$ by $p\mathbb{Z}$, by taking

$$u_n = n \quad (n \in \mathbb{N}_0),$$

the basis element $C_n(k)$ becomes the binomial polynomial $\binom{k}{n}$, which shows that the congruence relation (1.2) does indeed imply (1.1).

In the case of $K = \mathbb{F}_q(x)$, the field of rational functions over the finite field $\mathbb{F}_q$ of q elements, with the x-adic valuation whose discrete valuation domain is V, and whose maximal ideal is $\mathfrak{m} = (x) := xV$. In [5], [6], and [7], Carlitz introduced the following set of polynomials over $\mathbb{F}_q[x]$:

$$\psi_0(t) = t, \quad \psi_n(t) = \prod_{\deg M < n} (t - M) \quad (n \in \mathbb{N}),$$

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

$$F_0 = 1, \quad F_n = \langle n\rangle\langle n-1\rangle^q \cdots \langle 1\rangle^{q^{n-1}} \quad (n \in \mathbb{N}),$$

where $\langle n\rangle := x^{q^n} - x$. The polynomials $\psi_n(t)$ is generalized to the polynomials $G_n(t)$ defined by

$$G_0(t) = 1, \quad G_n(t) = \psi_0^{n_0}(t)\psi_1^{n_1}(t)\cdots\psi_{d(n)}^{n_{d(n)}}(t) \quad (n \in \mathbb{N}),$$

where $n = n_0 + n_1 q + \cdots + n_{d(n)}q^{d(n)}$ is its base q-representation. Correspondingly, the factorial-like elements generalizing the F_n's are defined by

$$g_0 = 1, \quad g_n = F_0^{n_0} F_1^{n_1} \cdots F_{d(n)}^{n_{d(n)}} \quad (n \in \mathbb{N}).$$

Carlitz proved that $\{G_n(t)/g_n\}$ is a regular basis of the $\mathbb{F}_q[x]$-module $\operatorname{Int}(\mathbb{F}_q[x])$.

Our thesis is organized as follows. Chapter II consists of some notations, definitions and related results using the entire thesis without proofs. In Chapter III, the shapes of Lagrange type interpolation polynomials similar to $\{C_n(t)\}$ which constitute bases for $\operatorname{Int}(V)$ and satisfy Lucas property are presented. Our results give an extension to a result of Boulanger and Chabert in 2001. Moreover, we show that the basis obtained by Carlitz satisfies Lucas property. The generalization of Carlitz polynomials, namely, Carlitz-like polynomials are introduced. Criteria guaranteeing that Carlitz-like polynomials which constitute a basis for $\operatorname{Int}(\mathbb{F}_q[x])$ enjoy the Lucas Theorem are derived. The necessary and/or sufficient conditions on arbitrary polynomials over K of degree n which form a basis for $\operatorname{Int}(V)$ and satisfy Lucas property are also investigated. In the final chapter, a generalization of Pascal property and criteria on polynomials satisfying Pascal property which form a regular basis for $\operatorname{Int}(V)$ are also established. An interesting application, another horizontal recurrence relation related to Stirling numbers of the first kind, is also presented.

CHAPTER II
PRELIMINARIES

2.1 Discrete valuation domains

We begin this section by recalling some basic knowledge in valuation theory. For the general reference, we refer to [9] and [11]. Let K be a field.

Definition 2.1. A **valuation** of K is a function $|\cdot| : K \longrightarrow \mathbb{R}^+ \cup \{0\}$ satisfying these properties: for all $a,\ b \in K$

1. $|a| = 0$ if and only if $a = 0$,
2. $|ab| = |a||b|$,
3. $|a+b| \leq |a| + |b|$. (Triangle inequality)

There is always at least one valuation on K given by setting $|a| = 1$ for all $a \in K^*$ and $|0| = 0$. This valuation is called the **trivial valuation**.

Definition 2.2. A valuation $|\cdot|$ is called **non-Archimedean** if it satisfies

$$|a+b| \leq \max\{|a|,\ |b|\} \quad \text{for all } a,\ b \in K.$$

Otherwise, the valuation $|\cdot|$ is called **Archimedean**.

The previous inequality becomes an equality under the following condition.

Theorem 2.3. *Let $|\cdot|$ be a non-Archimedean valuation. If $|a| \neq |b|$, then*

$$|a+b| = \max\{|a|,\ |b|\}.$$

Definition 2.4. Let $|\cdot|_1$ and $|\cdot|_2$ be two valuations on K. They are **equivalent** if and only if there exists a positive real number s such that

$$|a|_1 = |a|_2^s \quad \text{for all } a \in K.$$

Some examples of certain fields with their valuations are shown as follows:

Example 2.5.

1. The usual absolute value on the real number $\mathbb{R}$ or the complex number $\mathbb{C}$ is an Archimedean valuation.

2. Let $K = \mathbb{Q}$. If we fix a prime number p, any non-zero rational number c can be written in the form
$$c = p^v \cdot \frac{m}{n},$$
where $v \in \mathbb{Z},\ m \in \mathbb{Z},\ n \in \mathbb{N}$ and $p \nmid mn$. We then put
$$|c|_p = p^{-v} \quad \text{and} \quad |0|_p = 0.$$
This defines a non-Archimedean valuation on $\mathbb{Q}$, which is called the p**-adic valuation**.

3. Let $K = k(x)$, where k is any field, and $p(x)$ an irreducible polynomial in $k[x]$. Any non-zero rational function ϕ in x over k can be written as
$$\phi = p^v \cdot \frac{f}{g},$$
where $v \in \mathbb{Z},\ f, g \in k[x]$ and $p \nmid fg$. Then we obtain a non-Archimedean valuation on the rational function field $k(x)$ defined by
$$|\phi|_{p(x)} = 2^{-v} \quad \text{and} \quad |0|_{p(x)} = 0.$$
Moreover, the number 2 can be replaced by any real number greater than 1 and a new valuation is equivalent to the old one.

Next, we introduce the symbol ∞ that $\infty+\infty=\infty$ and $r+\infty=\infty$ for all $r\in\mathbb{R}$ and define an exponential valuation on K as follows.

Definition 2.6. An **exponential valuation on** K is a function $\nu : K \longrightarrow \mathbb{R}\cup\{\infty\}$ satisfying these properties, for all $a,\ b\in K$:

1. $\nu(a)=\infty$ if and only if $a=0$,
2. $\nu(ab)=\nu(a)+\nu(b)$,
3. $\nu(a+b)\geq \min\{\nu(a),\ \nu(b)\}$.

Note that if we set $\nu(a)=0$ for all $a\in K^*$ and $\nu(0)=\infty$, we have an exponential valuation corresponding to the trivial valuation on K and we call it the **trivial exponential valuation**.

Proposition 2.7. *Let ν be an exponential valuation on K. For all $a,b\in K$, if $\nu(a)\neq\nu(b)$, then*

$$\nu(a+b)=\min\{\nu(a),\ \nu(b)\}.$$

We continue with two important definitions.

Definition 2.8. An exponential valuation ν on K is called **discrete** if $\nu(K^*)=s\mathbb{Z}$ for some real number $s>0$. Moreover, ν is **normalized** if $s=1$.

Definition 2.9. Two exponential valuations ν_1 and ν_2 are **equivalent** if there exists a real $s>0$ such that $\nu_1=s\nu_2$.

Notice that if ν is a discrete valuation on K, then there exists a uniquely determined normalized valuation of K that is equivalent to ν. Thus, throughout this thesis, the term "discrete valuation" means "normalized discrete exponential valuation". Next, relations between the non-Archimedean valuations and the exponential valuations on K are shown.

Theorem 2.10. *Let $|\cdot|$ be a non-Archimedean valuation on K and $s\in\mathbb{R}^+$, then the function $\nu_s : K\longrightarrow\mathbb{R}\cup\{\infty\}$ defined by*

$$\nu_s(a)=\begin{cases}-s\log|a| & \textit{if } a\neq 0,\\ \infty & \textit{if } a=0\end{cases}$$

is an exponential valuation on K. Furthermore, if $s,\ s' \in \mathbb{R}^+$ and $s \neq s'$, then ν_s is equivalent to $\nu_{s'}$. Conversely, if ν is an exponential valuation on K and $q > 1$, then the function $|\cdot|_q : K \longrightarrow \mathbb{R}$ defined by

$$|a|_q = \begin{cases} q^{-\nu(a)} & \textit{if } a \neq 0, \\ 0 & \textit{if } a = 0 \end{cases}$$

is a non-Archimedean valuation on K. Moreover, if $q,\ q' > 1$ and $q \neq q'$, then $|\cdot|_q$ is equivalent to $|\cdot|_q'$.

From the above relation, we always get the corresponding valuation when a non-Archimedean valuation on K is given and vice versa. This leads us to consider three important sets in the following theorems.

Theorem 2.11. *Let ν be a discrete valuation on K and denote by $|\cdot|$ a corresponding non-Archimedean valuation. Then*

1. *the set*

$$V := \{a \in K \mid \nu(a) \in \mathbb{N}_0\} = \{a \in K \mid |a| \leq 1\}$$

is an integral domain, called the ***discrete valuation domain****. Moreover for all $a \in K^*$, we have $a \in V$ or $a^{-1} \in V$,*

2. *the set*

$$\mathfrak{m} := \{a \in K \mid \nu(a) > 0\} = \{a \in K \mid |a| < 1\} = \left\{a \in V \mid a^{-1} \notin V\right\}$$

is the unique principal maximal ideal of V,

3. *the set*

$$V \smallsetminus \mathfrak{m} := \{a \in K \mid \nu(a) = 0\} = \{a \in K \mid |a| = 1\}$$

is the group of units of V.

Note that each element in the discrete valuation domain can be uniquely represented in terms of a fixed generator of the maximal ideal $\mathfrak{m}$. Some examples of discrete valuation corresponding to certain valuations are presented as follows.

Example 2.12.

1. Let $K = \mathbb{Q}$. From Example 2.5(2), a discrete p-adic valuation corresponding to the p-adic valuation $|\cdot|_p$ is a function $\nu_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$ defined by

$$\nu_p(0) := \infty \quad \text{and} \quad \nu_p(c) := -\log_p |c|_p = v,$$

for all $c = p^v \cdot \frac{m}{n} \in \mathbb{Q}^*$. Therefore, we have

$$\begin{aligned} V &= \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; a, b \in \mathbb{Z},\ (a,b) = 1,\ \text{and } p \nmid b \right\}, \\ \mathfrak{m} &= \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; a, b \in \mathbb{Z},\ (a,b) = 1,\ p \mid a,\ \text{and } p \nmid b \right\}, \\ V \smallsetminus \mathfrak{m} &= \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; a, b \in \mathbb{Z},\ (a,b) = 1,\ \text{and } p \nmid ab \right\}. \end{aligned}$$

2. Let $K = k(x)$, where k is any field. From Example 2.5(3), a discrete valuation corresponding to the valuation $|\cdot|_{p(x)}$ is a function $\nu_{p(x)} : k(x) \longrightarrow \mathbb{Z} \cup \{\infty\}$ defined by

$$\nu_{p(x)}(0) := \infty \quad \text{and} \quad \nu_{p(x)}(\phi) := -\log_2 |\phi|_{p(x)} = v,$$

for all $\phi = p^v \cdot \frac{f}{g} \in k(x)^*$. So, we have

$$\begin{aligned} V &= \left\{ \frac{f(x)}{g(x)} \in k(x) \;\middle|\; f, g \in k[x],\ (f,g) = 1,\ \text{and } p \nmid g \right\}, \\ \mathfrak{m} &= \left\{ \frac{f(x)}{g(x)} \in k(x) \;\middle|\; f, g \in k[x],\ (f,g) = 1,\ p \mid f,\ \text{and } p \nmid g \right\}, \\ V \smallsetminus \mathfrak{m} &= \left\{ \frac{f(x)}{g(x)} \in k(x) \;\middle|\; f, g \in k[x],\ (f,g) = 1,\ \text{and } p \nmid fg \right\}. \end{aligned}$$

Let V be a discrete valuation domain corresponding to a discrete valuation ν, $\mathfrak{m}$ the unique principal maximal ideal of V generated by T, and $V/\mathfrak{m}$ is the finite residue field of cardinal $q > 1$. Let $U := \{a_0 = 0,\ a_1, \ldots, a_{q-1}\}$ be a set of representative of $V/\mathfrak{m}$. Each element in V can be uniquely represented as power series in T with coefficients in U.

Theorem 2.13. *For each $A \in V$, we can write*

$$A = A_0 + A_1T + A_2T^2 + \cdots \quad (A_i \in U).$$

Next, we introduce the notion of very well distributed and well ordered sequence in V as defined in [4].

Definition 2.14. Denote by $\nu_q(\ell)$ the largest power of q that divides $\ell \in \mathbb{N}$. 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

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

According to [4], some examples of VWDWO sequences are presented as follows.

Example 2.15.

1. For each prime number p, the natural sequence of positive integers is a VWDWO sequence for the p-adic valuation of $\mathbb{Q}$.

2. Let $U := \{a_0 = 0,\ a_1, \ldots, a_{q-1}\}$ be a set of representative of $V/\mathfrak{m}$ and T a generator of maximal ideal $\mathfrak{m}$. Taking q as the basis of the numeration, that is, decomposing n $\in \mathbb{N}$ as,

   $$n = n_rq^r + \cdots + n_1q + n_0 \quad (0 \leq n_i < q),$$

   and letting

   $$u_n = a_{n_r}T^r + \cdot + a_{n_1}T + a_{n_0},$$

   then $\{u_n\}$ is a VWDWO sequence in V.

Moreover, an important property of VWDWO sequences is also established.

Proposition 2.16. *Let $\{u_n\}$ be a sequence in V. The sequence $\{u_n\}$ is VWDWO if and only if for all $s \in \mathbb{N}$, any choice of q^s consecutive terms provides a complete set of residues of $\mathfrak{m}^s$ in V.*

2.2 Integer-valued polynomials

In this section, we give some notations, definitions and results concerning integer valued polynomials. For general references, we refer to [1], [2], [4] and [12]. Throughout, let D be an integral domain with quotient field K.

Definition 2.17. An **integer-valued polynomial over** D is a polynomial over K which maps the set D to itself. The set of all integer-valued polynomials over D is denoted by

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

Example 2.18.

1. Each polynomial over D is an integer-valued polynomial over D.

2. The binomial polynomials, defined by

$$\binom{t}{n} = \frac{t(t-1)\cdots(t-n+1)}{n!} \quad (n \in \mathbb{N}),$$

   are polynomial over $\mathbb{Q}$ and also form a subset of $\mathrm{Int}(\mathbb{Z})$.

3. Consider the **Lagrange interpolation polynomials**: let n be a positive integer and, for $0 \leq h \leq n$, let π_h be a polynomial of degree n such that $\pi_h(k) = \delta_{hk} \quad (0 \leq k \leq n)$, where δ_{hk} is a Kroneker symbol. They may be written

$$\pi_h(t) = \prod_{0 \leq k \leq n, k \neq h} \frac{t-k}{h-k} = (-1)^{n-h}\binom{t}{h}\binom{t-h-1}{n-h}. \tag{2.1}$$

   These polynomials are integer-valued polynomials over $\mathbb{Z}$.

4. Let $\{u_n\}_{n\in\mathbb{N}_0}$ be a VWDWO sequence of V. The sequence of polynomials $\{f_n\}_{n\in\mathbb{N}_0}$, constructed as Lagrange-type interpolation polynomial in the same manner as in (2.1), i.e.,

$$f_0(t) = 1 \quad \text{and} \quad f_n(t) = \prod_{i=0}^{n-1} \frac{(t-u_0)(t-u_1)\cdots(t-u_{n-1})}{(u_n-u_0)(u_n-u_1)\cdots(u_n-u_{n-1})} \quad (n \in \mathbb{N}),$$

forms a subset of $\operatorname{Int}(V)$.

Let B be a domain which $D[t] \subset B \subset K[t]$.

Definition 2.19. A basis $\{f_n\}_{n\in\mathbb{N}_0}$ of the D-module B is said to be a **regular basis** if, for each n, the polynomial f_n has degree n.

The **fractional ideal** J of D is a D-submodule of K which is fractional subset, that is, there exists a nonzero element d of D such that dJ is an ideal of D. Then the set of leading coefficients of polynomials in B forming the fractional ideal is defined in the following.

Definition 2.20. For every $n \in \mathbb{N}_0$, the **nth characteristic ideal of** B is the fractional ideal $J_n(B)$ which is the set of leading coefficients of polynomials in B of degree $\leq n$ (including 0):

$$J_n(B) = \{0\} \cup \{\alpha \in K \mid \exists f \in B,\ f = \alpha t^n + \alpha_{n-1}t^{n-1} + \cdots\}.$$

The relation between regular basis and fractional ideal $J_n(B)$ is characterized in [4, Proposition II.1.4] as follows.

Proposition 2.21. *A sequence $\{f_n(t)\}_{n\in\mathbb{N}_0}$ of elements of B is a regular basis of B if and only if, for each n, f_n is a polynomial of degree n whose leading coefficient generates the nth characteristic ideal of B as a D-module.*

Now let V be a discrete valuation domain with finite residue field of q elements and K its quotient field. Assume that T is a fixed generator of the unique principal maximal ideal of V. Next, we define an arithmetic function $w_q(n)$ on the positive integers by

$$w_q(n) = \sum_{k\in\mathbb{N}} \left\lfloor \frac{n}{q^k} \right\rfloor .$$

Recall Bhargava's notion of T-ordering on V [1] and [2]:

Definition 2.22. A sequence $\{u_n\}_{n\in\mathbb{N}_0}$ of elements of V is a **T-ordering** of V if, one has

$$\nu\left(\prod_{k=0}^{n-1}(u_n - u_k)\right) \leq \nu\left(\prod_{k=0}^{n-1}(t_0 - u_k)\right) \quad \text{for all } n \in \mathbb{N},\ t_0 \in V.$$

Two forms of regular bases for $\operatorname{Int}(V)$ are constructed by using t-ordering sequence $\{u_n\}$, see [2, Theorem 9] and [1, Propostition7], respectively.

Proposition 2.23. *Let $\{u_n\}_{n\in\mathbb{N}_0}$ be a T-ordering of V. The V-module Int(V) has a regular basis*

$$f_n(t) = \prod_{k=0}^{n-1} \frac{t-u_k}{u_n-u_k} \quad (n \in \mathbb{N}_0).$$

Conversely, the set of polynomials $\{f_n(t)\}$ forms a regular basis for Int(V) only if $\{u_n\}_{n\geq 0}$ be a T-ordering of V.

Proposition 2.24. *Let $\{u_n\}_{n\in\mathbb{N}_0}$ be a T-ordering of V. The sequence of polynomials associated to the T-ordering $\{u_n\}_{n\in\mathbb{N}_0}$*

$$f_n(t) = T^{-w_q(n)} \prod_{k=0}^{n-1}(t-u_k)$$

is a regular basis of Int(V).

It is noticed that any two T-ordering $\{u_n\}$ and $\{u'_n\}$ of V result in the same minimum condition:

$$\nu\left(\prod_{k=0}^{n-1}(u_n - u_k)\right) = \nu\left(\prod_{k=0}^{n-1}(u'_n - u'_k)\right) \quad (n \in \mathbb{N}).$$

By Proposition 2.24, Proposition 2.23 and Proposition 2.21, both $T^{-w_q(n)}$ and $\prod_{k=0}^{n-1} \frac{1}{u_n - u_k}$ are generators of $J_n(\mathrm{Int}(V))$. Therefore, for each T-ordering $\{u_n\}$ of V,

$$w_q(n) = \nu \left(\prod_{k=0}^{n-1} (u_n - u_k) \right). \tag{2.2}$$

Moreover, if a sequence $\{u_n\}$ satisfies (2.2), it becomes a T-ordering by Bhargava [2].

The other basis of $\mathrm{Int}(V)$ is defined as follows.

Definition 2.25. Let $\mathcal{F}_q$ be a polynomial

$$\mathcal{F}_0(t) = 1, \quad \mathcal{F}_1(t) = t, \quad \text{and} \quad \mathcal{F}_q(t) = \frac{t - t^q}{T}.$$

Then, taking q as the basis of the numeration, and writing

$$n = n_0 + n_1 q + \cdots + n_s q^s \quad (0 \neq n_i < q),$$

we let

$$\mathcal{F}_n(t) = \prod_{i=0}^{s} (\mathcal{F}_q^i(t))^{n_i} \quad (n \in \mathbb{N}).$$

where $\mathcal{F}^1(t) = \mathcal{F}(t)$ and $\mathcal{F}^i(t) = \mathcal{F}(\mathcal{F}^{i-1}(t))$. [4, Propositon II.2.12] We say that $\mathcal{F}_n$ is the **nth Fermat polynomial of** V and it is an integer-valued polynomial over V.

Theorem 2.26. *The Fermat polynomials $\mathcal{F}_n(t)$ form a regular basis of V-module Int(V).*

For the case of function field, let $\mathbb{F}_q[x]$ be the ring of polynomials over $\mathbb{F}_q$, a finite field of q elements, and $\mathbb{F}_q(x)$ its quotient field. In [5], [6] and [7], Carlitz defined the polynomials $\psi_k(t)$ for all $k \in \mathbb{N}_0$ in $\mathbb{F}_q[t]$, referred to as Carlitz poynomials, which play the role analogous to the binomial expansions in $\mathbb{Z}$ as follows: define

$\psi_0(t) = t$ and, for $k \in \mathbb{N}$, define

$$\psi_k(t) = \prod_{\deg M < k} (t - M), \tag{2.3}$$

where the product extends over all polynomials M (including 0) in an indeterminate x with coefficients in $\mathbb{F}_q$ of degree less than k. He also defined the following plays in $\mathbb{F}_q[x]$ which play the role analogous to the factorials in $\mathbb{Z}$: define $F_0 = 1$ and for $k \in \mathbb{N}$, define

$$F_k = [k][k-1]^q[k-2]^{q^2} \cdots [1]^{q^{k-1}},$$

where $[r] = x^{q^r} - x$ for all $r \in \mathbb{N}$. As mentioned in [6], $\psi_k(x^k) = \psi_k(M) = F_k$ 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. In [7], Carlitz generalized $\psi_k(t)$ to the polynomial $G_k(t)$ and F_k to the polynomial g_k defined as follows: define $G_0(t) = 1$ and $g_0 = 1$. For $k \in \mathbb{N}$, if k is expressed with respect to base q as

$$k = \alpha_0 + \alpha_1 q + \alpha_2 q^2 + \cdots + \alpha_{d(k)} q^{d(k)} \quad (0 \leqslant \alpha_i < q),$$

then define

$$G_k(t) = \psi_0^{\alpha_0}(t)\psi_1^{\alpha_1}(t) \cdots \psi_{d(k)}^{\alpha_{d(k)}}(t)$$

and

$$g_k = F_0^{\alpha_0} F_1^{\alpha_1} \cdots F_{d(k)}^{\alpha_{d(k)}}.$$

From these polynomials, a basis of $\mathrm{Int}(\mathbb{F}_q[x])$ is established.

Theorem 2.27. *Let $k \in \mathbb{N}_0$. For each $K \in \mathbb{F}_q[x]$, $G_k(K)/g_k$ is polynomials over $\mathbb{F}_q[x]$. Moreover, the polynomials $G_k(t)/g_k$ form a regular basis of $\mathbb{F}_q[x]$-module Int$(\mathbb{F}_q[x])$.*

CHAPTER III
LUCAS PROPERTY

From now on, let V be a discrete valuation domain with respect to normalized discrete valuation ν and a finite residue field, and let K be its quotient field. Let $\mathfrak{m} = (T)$ be the unique principal 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

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

By Theorem 2.13, each element $A \in V$ can be uniquely represented as a base T-representation (or power series in T over U) of the form

$$A_0 + A_1 T + A_2 T^2 + \cdots \qquad (A_i \in U).$$

The valuation $\nu(A)$ of $A \in V^* := V \smallsetminus \{0\}$ 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 $\ell \in \mathbb{N}$.

We first define the congruence relation analogous to Lucas theorem, referred to as Lucas property in the following.

Definition 3.1. Let $\{B_n(t)\}_{n\in\mathbb{N}_0} \subset K[t]$ 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 for $n \in \mathbb{N}_0$ with base q-representation

$$n = n_0 + n_1 q + \cdots + n_{d(n)} q^{d(n)} \quad (0 \le n_i < q,\ n_{d(n)} \ne 0 \text{ if } n \in \mathbb{N}), \tag{3.1}$$

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

$$A = A_0 + A_1 T + \cdots \qquad (A_i \in U),$$

the congruence relation

$$B_n(A) \equiv B_{n_0}(A_0) B_{n_1}(A_1) \cdots B_{n_{d(n)}}(A_{d(n)}) \pmod{\mathfrak{m}} \tag{3.2}$$

holds.

3.1 Lagrange-type interpolation polynomials

Let the polynomials $\{B_n(t)\}$ be constructed as Lagrange-type interpolation polynomials, i.e., there is a sequence $\{w_n\}_{n\in\mathbb{N}_0}$ of distinct elements in V such that

$$B_0(t) = 1, \qquad B_n(t) = \frac{(t-w_0)(t-w_1)\cdots(t-w_{n-1})}{(w_n-w_0)(w_n-w_1)\cdots(w_n-w_{n-1})} \quad (n \in \mathbb{N}).$$

Definition 3.2. 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 $\mathrm{Int}(V)$.

In this section, we determine those g-IVP sequences whose associated polynomials satisfy the Lucas property. The results give an extension to a result of Boulanger and Chabert [3]. Any g-IVP sequence $\{w_n\}$ is characterized by the next theorem.

Theorem 3.3. *If $\{w_n\}$ is a g-IVP sequence with $w_0 = 0$, then $w_1, \ldots, w_{q-1}$ are units, each of which belonging 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 on k, 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

$$\nu(w_i - w_j) = 0 \qquad (1 \leq i < j \leq k).$$

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

$$\nu(A - w_i) = 0 \qquad (0 \leq i \leq k).$$

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., $\nu(B_{k+1}(A)) \in \mathbb{N}_0$) 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 $w_1, \dots, w_k$ in $V/\mathfrak{m}$, and the induction is complete. The second assertion follows immediately from the first. $\square$

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

Lemma 3.4. *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 $\{w_0 = 0, w_1, \dots, w_{q-1}\} = U$, and denote any other element by*

$$w_n = a_0^{(n)} + a_1^{(n)}T + \cdots + a_j^{(n)}T^j + \cdots \quad (a_j^{(n)} \in U,\ n \geq q) \tag{3.3}$$

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

$$A = A_0 + A_1T + \cdots + A_jT^j + \cdots \in V. \tag{3.4}$$

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

$$a_0^{(n)} = w_{n_0},\ a_1^{(n)} = w_{n_1},\ \dots,\ a_m^{(n)} = w_{n_m}, \tag{3.5}$$

holds for all $n \in \mathbb{N}_0$ whose base q-representation is (3.1)*, then for each $k \in \{0, 1, \dots, q-2\}$, 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 $r_s \in \{0, 1, \dots, q^{m+1}-1\}$ are uniquely determined and satisfy the relation

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

Proof. Assume that $a_0^{(n)} = w_{n_0},\ a_1^{(n)} = w_{n_1},\ \dots,\ a_m^{(n)} = w_{n_m}$. For $0 \leq k \leq q-2$, replacing A and w_i by the expressions in (3.4), respectively, (3.3), we write

$$B_{(k+1)q^{m+1}}(A) = \prod_{s=0}^{k} \Omega_s,$$

where

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

The numerator of Ω_s is

$$\begin{aligned}\Lambda_1(s) = &\prod_{i=sq^{m+1}}^{(s+1)q^{m+1}-1} ((A_0 + \cdots + A_m T^m) - (a_0^{(i)} + \cdots + a_m^{(i)} T^m)) \\ &+ (A_{m+1} - a_{m+1}^{(i)})T^{m+1} + \ldots \\ = &\prod_{\substack{N \in U[T] \\ \deg N \leq m}} (A_0 + \cdots + A_m T^m - N) + \Sigma_0 \cdot \Pi_0 \\ &+ (\text{terms with powers of } T \geq 2m+2), \qquad (3.6)\end{aligned}$$

where

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

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

Since N and M run through all elements in $U[T]$ (including 0) of degree $\leq m$ and $M \neq a_0^{(i)} + \cdots + a_m^{(i)} T^m$, in the right-hand expression of (3.6) the first term vanishes, while the second term reduces to

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

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

$$a_i^{(r_s)} = A_i \quad (0 \le i \le m). \tag{3.7}$$

Thus,

$$\begin{aligned}\Lambda_1(s) = (A_{m+1} - a_{m+1}^{(r_s)})\, T^{m+1} \prod_{\substack{\deg M \le m \\ M \ne A_0 + \cdots + A_m T^m}} (A_0 + \cdots + A_m T^m - M) \\ + \text{(terms with powers of } T \ge 2m+2). \end{aligned} \tag{3.8}$$

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 (3.8) for $\Lambda_2(s)$, the first term of expansion vanishes and the second term reduces to

$$(a_{m+1}^{((s+1)q^{m+1})} - a_{m+1}^{(r'_s)})T^{m+1} \prod_{\substack{M' \in U[T],\, \deg M' \le m \\ M' \ne a_0^{((s+1)q^{m+1})} + \cdots + a_m^{((s+1)q^{m+1})} T^m}} \left(\sum_{i=0}^{m} a_i^{((s+1)q^{m+1})} T^i - M' \right)$$

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

$$a_i^{(r'_s)} = a_i^{((s+1)q^{m+1})} \quad (0 \le i \le m). \tag{3.9}$$

By the assumption (3.5), 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 (3.9) shows that $r'_s = sq^{m+1}$, and the second term of Λ_2 becomes

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

Thus,

$$\Lambda_2(s) = (a_{m+1}^{((s+1)q^{m+1})} - a_{m+1}^{(sq^{m+1})})T^{m+1} \prod_{\substack{\deg M' \leq m \\ M' \neq 0}} (0 - M')$$
$$+ \text{(terms with powers of } T \geq 2m+2). \qquad (3.10)$$

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 non-vanishing 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., belongs to 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

$$\prod_{\substack{\deg M \leq m \\ M \neq A_0 + \cdots + A_mT^m}} (A_0 + \cdots + A_mT^m - M) \equiv \prod_{\substack{\deg M' \leq m \\ M' \neq 0}} (0 - M') \pmod{\mathfrak{m}^{m+1}}. \quad (3.11)$$

By (3.8), (3.10) and (3.11), 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 (3.3) and (3.7), we get $a_i^{(r_s)} = A_i$ $(0 \leq i \leq m)$, i.e.,

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

as required. □

The explicit shape of a g-IVP sequence $\{w_n\}$ which is VWDWO, stated in Definition 2.14, and satisfies the Lucas property is obtained in the following theorem.

Theorem 3.5. *Let $\{w_n\} := \{w_0 = 0, w_1, w_2, \ldots\}$ be a g-IVP sequence whose associated w-polynomial sequence is $\{B_n(t)\}_{n\in\mathbb{N}_0}$. Assume that*

1. *the sequence $\{B_n(t)\}$ satisfies the Lucas property modulo $\mathfrak{m}$, and*

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 (3.1)*, we have*

$$w_n = w_{n_0} + w_{n_1} T + \cdots + w_{n_{d(n)}} T^{d(n)}. \tag{3.12}$$

(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 subjected to this dependence.)

Proof. Since $\{w_n\}$ is a g-IVP sequence with $w_0 = 0$, by Theorem 3.3, we can take its first q elements to be those of U, i.e.,

$$\{w_0 = 0, w_1, \ldots, w_{q-1}\} = U. \tag{3.13}$$

Using the notation as set out in (3.3) of Lemma 3.4, the set (3.13) shows that

$$a_0^{(0)}(=0),\ a_0^{(1)},\ \cdots,\ a_0^{(q-1)} \in U, \tag{3.14}$$

$$a_i^{(0)} = a_i^{(1)} = \cdots = a_i^{(q-1)} = 0 \quad (i). \tag{3.15}$$

We prove the theorem by establishing (3.12) component-wise that $a_j^{(n)} = w_{n_j}$.

As the first step, we show that

$$a_0^{(n)} = w_{n_0} \quad \text{for all } n \in \mathbb{N}_0. \tag{3.16}$$

This clearly holds for $n \in \{0, 1, \ldots, q-1\}$ because of (3.14). Since $\{w_n\}$ is a VWDWO sequence, by Proposition 2.16, any q consecutive terms in the sequence form a complete set of residues modulo $\mathfrak{m}$. Thus, for $0 \leq i \leq q-1$, we get

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

and so

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

proceeding inductively, we have

$$w_{jq+i} \equiv w_{(j-1)q+i} \equiv \cdots \equiv w_{q+i} \equiv w_i \pmod{\mathfrak{m}} \qquad (j \in \mathbb{N}). \tag{3.17}$$

Using the notation (3.1), we deduce from (3.17) for $n \in \mathbb{N}_0$ that

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

Being elements of U shows then that (3.16) is fulfilled.

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

$$a_{e+1}^{(n)} = w_{n_{e+1}} \quad \text{for all } n \in \mathbb{N}_0. \tag{3.18}$$

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

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

with the case $e = 0$ being just verified above. Taking any $A = A_0 + A_1T + \cdots \in V$, using Lemma 3.4 with $m = e, k = 0$ and (3.15), we have

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

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

$$B_{q^{e+1}}(A) \equiv 0 \pmod{\mathfrak{m}}. \tag{3.19}$$

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

$$a_{e+1}^{(n)} = 0 = w_{n_{e+1}} \quad (0 \leq n \leq q^{e+1} - 1). \tag{3.20}$$

Next, using Lemma 3.4 with $k = 1, m = e$, we have

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

where

$$\alpha_0 := \frac{A_{e+1} - a_{e+1}^{(r_0)}}{a_{e+1}^{(2q^{e+1})} - a_{e+1}^{(0)}}, \ \alpha_1 := \frac{A_{e+1} - a_{e+1}^{(q^{e+1}+r_1)}}{a_{e+1}^{(2q^{e+1})} - a_{e+1}^{(q^{e+1})}} \tag{3.21}$$

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

$$w_{r_i} \equiv A_0 + \cdots + A_e T^e \pmod{\mathfrak{m}^{e+1}}. \tag{3.22}$$

Using (3.15) and (3.20), 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, by Proposition 2.16, the set $\{w_0 = 0, w_1, \ldots, w_{q^{e+2}-1}\}$ constitutes a residue class modulo $\mathfrak{m}^{e+2}$. Thus, from (3.20), for larger n in the next range, i.e., for $q^{e+1} \leq n \leq q^{e+2} - 1$ 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 (3.21), we have

$$\alpha_1 = 0. \tag{3.23}$$

However, the Lucas property implies that

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

contradicting (3.23), and so $a_{e+1}^{(q^{e+1}+r_1)} = w_1$. Since r_1 satisfies (3.22) 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

$$a_{e+1}^{(n)} = w_1 = w_{n_{e+1}} \quad (q^{e+1} \leq n \leq 2q^{e+1} - 1). \tag{3.24}$$

From the VWDWO property modulo $\mathfrak{m}^{e+2}$, because of (3.20) and (3.24), 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

$$a_{e+1}^{n} \notin \{w_0, w_1\} \quad \text{for all } n \in \{2q^{e+1},\ 2q^{e+1} + 1,\ \ldots,\ q^{e+2} - 1\}. \tag{3.25}$$

We pause here to remark that the ongoing proof of (3.18) for $q = 2$ is now complete from (3.20), (3.24) and the VWDWO property, while for $q = 3$, since there are three residue classes, the proof of (3.18) is also complete from (3.20), (3.24), (3.25) 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 $0 \leq s \leq q^{e+1}-1$, 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 (3.20), (3.24) and (3.25). Applying Lemma 3.4 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

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

Turning now to α_{h+1}, by arguments similar to those leading to (3.24), we deduce that $a_{e+1}^{(r_{h+1})} = w_{h+1}$ which in turn implies that

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

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

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

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

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

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,

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

Comparing 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 3.5 to the case of function field, we immediately obtain

Corollary 3.6. *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 ideal (x)*

Then

$$w_n = w_{n_0} + w_{n_1} x + \cdots + w_{n_{d(n)}} x^{d(n)}, \tag{3.26}$$

where the base q-representation of $n \in \mathbb{N}_0$ is as in (3.1).

In passing, it is easily checked that the following converse of Corollary 3.6 is valid: if the relation (3.26) holds and $\{w_n\}$ is a VWDWO sequence, then the sequence $\{B_n(t)\}$ satisfies the Lucas property modulo (x).

Applying Theorem 3.5 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 3.7. *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

$$w_n = w_{n_0} + w_{n_1}p + \cdots + w_{n_{d(n)}}p^{d(n)}, \tag{3.27}$$

where the base p-representation of $n \in \mathbb{N}_0$ is as in (3.1)*.*

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 3.5. To check the last assertion, we assume that $w_i = i \in \{0, 1, \ldots, p-1\}$. With the base p-representation (3.1) of n, we get

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

Similar to the remark after the preceding corollary, the following converse of Corollary 3.7 is true: if the relation (3.27) holds and $\{w_n\}$ is a VWDWO sequence, then the sequence $\{B_n(t)\}$ satisfies the Lucas property modulo (p).

3.2 Carlitz and Carlitz-like polynomials

From Theorem 2.27, 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 3.1. In this section, we first confirm that $\{G_n(t)/g_n\}_{n\in\mathbb{N}_0}$ 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 3.8. *The sequence of Carlitz polynomials $\{G_n(t)/g_n\}_{n\in\mathbb{N}_0}$ satisfies the Lucas property modulo the principal ideal (x).*

Proof. Recall 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 (3.2) are equal to 1. For $n \in \mathbb{N}$ with base q-representation as in (3.1), 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 (2.3), we get $\psi_{d(n)}(A) = 0$. Since $A_{d(n)} = 0$, we have

$$\frac{G_{n_{d(n)}}(A_{d(n)})}{g_{d(n)}} = 0,$$

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

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

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

$$\begin{aligned}
\psi_k(A) = \prod_{\deg M<k} (A - M) &= \prod_{\deg M<k} ((A_k x^k + \cdots + A_1 x + A_0 - M) + A_{k+1}x^{k+1}) \\
&= \prod_{\substack{\deg M'=k \\ M' \text{monic}}} (A_k M' + A_{k+1}x^{k+1} + \text{terms with higher powers of } x) \\
&= A_k^{q^k} F_k + N_k x^{\deg(F_k)+1} = A_k F_k + N_k x^{\deg(F_k)+1},
\end{aligned}$$

for some $N_k \in \mathbb{F}_q[x]$. From [7, 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 3.8, we introduce:

Definition 3.9. Let $\{w_n\}_{n\in\mathbb{N}_0}$ be a given sequence of distinct elements in $\mathbb{F}_q[x]$.

- Define the **interpolating w-polynomial sequence** $\{\phi_n(t)\}_{n\in\mathbb{N}_0}$ by

$$\phi_0(t) = \frac{t-w_0}{w_1-w_0}, \quad \phi_k(t) = \frac{(t-w_0)(t-w_1)\cdots(t-w_{q^k-1})}{(w_{q^k}-w_0)(w_{q^k}-w_1)\cdots(w_{q^k}-w_{q^k-1})} \quad (k\in\mathbb{N})$$

  and define the **w-Carlitz like polynomial (w-CLP) sequence** $\{\mathcal{G}_n(t)\}_{n\in\mathbb{N}_0}$ of $\mathbb{F}_q(x)[t]$ by

$$\mathcal{G}_0(t) = 1,\ \mathcal{G}_n(t) = \phi_0^{n_0}(t)\phi_1^{n_1}(t)\cdots\phi_{d(n)}^{n_{d(n)}}(t) \quad (n\in\mathbb{N} \text{ as in } (3.1)),$$

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

Observe from Definition 3.9 that

1. the sequence of Carlitz polynomials $\{G_n(t)/g_n\}$ is a special case of w-CLP sequence 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 3.10. *Let*

$$A = A_0 + A_1T + A_2T^2 + \cdots \quad (A_i \in U)$$
$$B = B_0 + B_1T + B_2T^2 + \cdots \quad (B_i \in U)$$

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

$$\frac{A}{B} \equiv \frac{A_{\nu(B)}}{B_{\nu(B)}} \pmod{\mathfrak{m}}. \tag{3.28}$$

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

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

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

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

for some $N' \in V$. If $r = s$, (3.28) is immediate, while if $r > s$, both sides of (3.28) are congruent to 0 modulo $\mathfrak{m}$. □

Our extension of Theorem 3.8 reads:

Theorem 3.11. *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. We first claim that $\{w_0 = 0, w_1, \cdots, w_{q^k-1}\}$ constitute a complete residue system modulo $(x)^k$ in the ring $\mathbb{F}_q[x]$, or equivalently,

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

To verify this claim, consider $\mathcal{G}_1(t) = \phi_0(t) = t/w_1$. Since $\mathcal{G}_1(t) \in \text{Int}(\mathbb{F}_q[x])$, 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

$$\mathcal{G}_q(t) = \phi_1(t) = \frac{t(t-w_1)\cdots(t-w_{q-1})}{w_q(w_q-w_1)\cdots(w_q-w_{q-1})},$$

by the Lucas property modulo (x), for each $A = A_0 + A_1x + \cdots \in \mathbb{F}_q[x]$, we get

$$\frac{\mathcal{A}_1}{\mathcal{B}_1} =: \frac{A(A-w_1)\cdots(A-w_{q-1})}{w_q(w_q-w_1)\cdots(w_q-w_{q-1})} = \mathcal{G}_q(A) \equiv \mathcal{G}_1(A_1) = \phi_0(A_1) = \frac{A_1}{w_1} \pmod{(x)}.$$

The numerator and the denominator are

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

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

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

satisfies the Lucas property modulo (x), we get

$$\frac{\mathcal{A}_k}{\mathcal{B}_k} =: \frac{A(A-w_1)\cdots(A-w_{q^k-1})}{w_{q^k}(w_{q^k}-w_1)\cdots(w_{q^k}-w_{q^k-1})} = \mathcal{G}_{q^k}(A) \equiv \mathcal{G}_1(A_k) = \frac{A_k}{w_1} \pmod{(x)}. \tag{3.29}$$

The numerator is

$$\begin{aligned}
\mathcal{A}_k = \prod_{i=0}^{q^k-1} \Big\{ \Big(& (A_0 + A_1 x + \cdots + A_{k-1}x^{k-1}) - (a_0^{(i)} + a_1^{(i)}x + \cdots + a_{k-1}^{(i)}x^{k-1}) \Big) \\
& + (A_k - a_k^{(i)})x^k + (A_{k+1} - a_{k+1}^{(i)})x^{k+1} + \text{terms with higher powers of } x \Big\} \\
= \prod_{i=0}^{q^k-1} & \Big((A_0 + A_1 x + \cdots + A_{k-1}x^{k-1}) - (a_0^{(i)} + a_1^{(i)}x + \cdots + a_{k-1}^{(i)}x^{k-1}) \Big) \\
& + \sum_{j=0}^{q^k-1} (A_k - a_k^{(j)})x^k \prod_{\substack{i=0 \\ i\neq j}}^{q^k-1} \Big((A_0 + \cdots + A_{k-1}x^{k-1}) - (a_0^{(i)} + \cdots + a_{k-1}^{(i)}x^{k-1}) \Big) \\
& + (\text{terms with higher powers of } x),
\end{aligned}$$

and the denominator is

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

Let

$$\mathcal{N} = \prod_{i=0}^{q^k-1} \Big((A_0 + A_1 x + \cdots + A_{k-1}x^{k-1}) - (a_0^{(i)} + a_1^{(i)}x + \cdots + a_{k-1}^{(i)}x^{k-1}) \Big) \tag{3.30}$$

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

If $\mathcal{N} \neq 0$, then there is a least positive integer r such that $r = \nu_q(\mathcal{N})$. Lemma 3.10

now ensures that $\mathcal{D} \neq 0$ and together with (3.29), 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 (3.30), 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

$$0 = \mathcal{G}_{q^s}(w_n) \equiv \mathcal{G}_1(a_s^{(n)}) = \phi_0(a_s^{(n)}) = \frac{a_s^{(n)}}{w_1} \pmod{(x)},$$

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

Next, we prove the second assertion. We 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 that $\{w_0, w_1, \ldots, w_{q^{k+1}-1}\}$ 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

$$\mathcal{G}_{q^k}(A) = \phi_k(A) = \prod_{i=0}^{q^k-1} \frac{A - w_i}{w_{q^k} - w_i} = \prod_{\deg M < k} \frac{A - M}{w_{q^k} - M}$$

$$= \prod_{\deg M<k} \frac{\big(A_0+\cdots+A_{k-1}x^{k-1}+A_kx^k-M\big)+A_{k+1}x^{k+1}+\cdots}{\Big(a_0^{(q^k)}+\cdots+a_{k-1}^{(q^k)}x^{k-1}+a_k^{(q^k)}x^k-M\Big)+a_{k+1}^{(q^k)}x^{k+1}+\cdots}$$

$$= \frac{A_k^{q^k}F_k+N_1x^{1+\deg F_k}}{(a_k^{(q^k)})^{q^k}F_k+N_2x^{1+\deg F_k}} \frac{A_k}{a_k^{(q^k)}} \pmod{(x)},$$

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

$$\mathcal{G}_{q^k}(A) \equiv \mathcal{G}_1(A_k) = \phi_0(A_k) = \frac{A_k}{w_1} \pmod{(x)}.$$

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 3.11 yields at once:

Corollary 3.12. *If $\{w_n\}$ is a g-CLP sequence with $w_1 = 1$, then its associated w-polynomial sequence $\{\phi_n(t)\}$ satisfies*

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

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

3.3 Polynomials in additive expansion

There are bases of $\mathrm{Int}(V)$ that do not satisfy the Lucas property. One such basis is that of Fermat polynomials $\mathcal{F}_n(t)$, defined in Definition 2.25, by

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

$$\mathcal{F}_n(t) = \prod_{j=0}^{d(n)} (\mathcal{F}_{q^j})^{n_j} \quad \text{for } n \in \mathbb{N} \text{ as in (3.1).}$$

Note that Fermat polynomials are neither of the same form as the Lagrange-type interpolation polynomials $B_n(t)$, nor of the same form as the Carlitz-type polynomials. 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 $\{P_i^{(n)}\}_{n\in\mathbb{N}_0}$ be a sequence in V with $P_n^{(n)} \neq 0$, and let

$$\Big\{Q_0 = 1,\ Q_n := Q_0^{(n)} + Q_1^{(n)}T + \cdots \quad (n \in \mathbb{N})\Big\}$$

be a sequence in V^*. Define $\{\mathcal{H}_n(t)\}_{n\in\mathbb{N}_0} \subseteq K[t]$, 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

$$\Big(P_0^{(n)} + P_1^{(n)}A + \cdots + P_n^{(n)}A^n\Big)_{\text{mod } \mathfrak{m}^r}$$

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 3.13. *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 $r \in \mathbb{N}$, if $Q_0^{(n)} = Q_1^{(n)} = \cdots = Q_{r-1}^{(n)} = 0,\ Q_r^{(n)} \neq 0$, then*

$$\Big(P_0^{(n)} + P_1^{(n)}A + \cdots + P_n^{(n)}A^n\Big)_{\text{mod } \mathfrak{m}^r} = 0.$$

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 3.10, 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 3.13, we now derive a necessary condition for a basis of Int(V) to satisfy the Lucas property.

Corollary 3.14. *Assume that $\{\mathcal{H}_n(t)\}_{n\in\mathbb{N}_0}$ 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* (3.1) *and $A = A_0 + A_1q + \cdots + A_jq^j + \cdots \in V$, we have*

$$\begin{aligned}&\frac{\left(P_0^{(n)} + P_1^{(n)}A + \cdots + P_n^{(n)}A^n\right)_{\text{mod } \mathfrak{m}^{s+1}}}{Q_s^{(n)}T^s} \\ &\equiv \prod_{i=0}^{d(n)} \frac{P_0^{(n_i)} + P_1^{(n_i)}A_i + \cdots + P_{n_i}^{(n_i)}A_i^{n_i}}{Q_{n_i}} \pmod{\mathfrak{m}}, \qquad (3.31)\end{aligned}$$

where $s = \nu(Q_n)$.

Proof. If $s = 0$, by Theorem 3.13 part 1 and Lemma 3.10, we get

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

If $s \in \mathbb{N}$, by Theorem 3.13 part 2, we can write

$$P_0^{(n)} + P_1^{(n)} A + \cdots + P_n^{(n)} A^n = R_s T^s + R_{s+1} T^{s+1} + \cdots \quad (R_i \in U),$$

and invoking upon Lemma 3.10, we get

$$\begin{aligned} \mathcal{H}_n(A) &= \frac{R_s T^s + R_{s+1} T^{s+1} + \cdots}{Q_s^{(n)} T^s + Q_{s+1}^{(n)} T^{s+1} + \cdots} \\ &\equiv \frac{R_s}{Q_s^{(n)}} \\ &= \frac{\left(P_0^{(n)} + P_1^{(n)} A + \cdots + P_n^{(n)} A^n\right)_{\text{mod } \mathfrak{m}^{s+1}}}{Q_s^{(n)} T^s} \pmod{\mathfrak{m}}. \end{aligned} \tag{3.32}$$

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

$$\begin{aligned} \mathcal{H}_n(A) &\equiv \mathcal{H}_{n_0}(A_0) \mathcal{H}_{n_1}(A_1) \cdots \mathcal{H}_{n_{d(n)}}(A_{d(n)}) \\ &= \prod_{i=0}^{d(n)} \frac{P_0^{(n_i)} + P_1^{(n_i)} A_i + \cdots + P_{n_i}^{(n_i)} A_i^{n_i}}{Q_{n_i}} \pmod{\mathfrak{m}}. \end{aligned} \tag{3.33}$$

The desired result follows at once from (3.32) and (3.33). □

As an application of Corollary 3.14, 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

$$\mathcal{F}_0(t) = 1, \quad \mathcal{F}_1(t) = t, \quad \mathcal{F}_2(t) = \frac{t - t^2}{x},$$

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

Let $n = 4 = 0 + 0 \cdot 2 + 1 \cdot 2^2$ and

$$\frac{P_0^{(0)}}{Q_0} = \mathcal{H}_0(t) = \mathcal{F}_0(t) = \frac{1}{1},$$

$$\frac{P_0^{(1)} + P_1^{(1)}t}{Q_1} = \mathcal{H}_1(t) = \mathcal{F}_1(t) = \frac{t}{1},$$

$$\frac{P_0^{(2)} + P_1^{(2)}t + P_2^{(2)}t^2}{Q_2} = \mathcal{H}_2(t) = \mathcal{F}_2(t) = \frac{t - t^2}{x},$$

$$\frac{P_0^{(4)} + P_1^{(4)}t + \cdots + P_4^{(4)}t^4}{Q_4} = \mathcal{H}_4(t) = \mathcal{F}_4(t) = \frac{0 + xt - (1+x)t^2 + 0 \cdot t^3 - t^4}{x^3},$$

so that

$$d(4) = 2, \quad n_0 = n_1 = 0, \quad n_2 = 1,$$

$$Q_0 = Q_1 = 1, \quad Q_2 = x, \quad Q_4 = x^3 = 0 + 0 \cdot x + 0 \cdot x^2 + 1 \cdot x^3,$$

$$s = \nu(Q_4) = 3, \quad Q_3^{(4)} = 1.$$

Taking $A = x = 0 + 1 \cdot x,\ A_1 = 1, A_i = 0\ (i \neq 1)$, the left-hand expression of (3.31) is

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

while the right-hand expression of (3.31) 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 3.14 implying that the sequence of Fermat polynomials does not satisfy the Lucas property.

CHAPTER IV
PASCAL PROPERTY

Throughout this chapter, let K be a field of characteristic 0. The generalization of Pascal property is defined as follows.

Definition 4.1. Let $u = \{u_k\}_{k\geq 0}$ be a sequence of distinct elements in K and $\mathcal{P} = \{P_n(t)\}_{n\geq 0}$ be a sequence of polynomials in $K[t]$ with $P_0(t) = 1$ and $\deg P_n(t) = n$ for all n. We say that the pair $(\mathcal{P}, u)$ satisfies the **Pascal property** (or the sequence $\mathcal{P}$ satisfies the Pascal property with respect to $\{u_k\}$) if, for each $n \in \mathbb{N}$,

$$P_n(u_{k+1}) = P_n(u_k) + P_{n-1}(u_k) \quad (k \in \mathbb{N}_0).$$

4.1 Pascal property for polynomials

Let $\{u_k\}_{k\geq 0}$ be a sequence of distinct elements in K. Set the polynomials $P_n(t)$ over K in the following.

$$P_0(t) = 1 \quad \text{and} \quad P_n(t) = \frac{1}{d_n}\sum_{i=0}^{n} a_{n,i}t^i \qquad (n \in \mathbb{N}), \tag{4.1}$$

where $d_n \in K$ and $a_{n,n} = 1$ for all $n \in \mathbb{N}$. The sequence of polynomials $\{P_n(t)\}$ is denoted by $\mathcal{P}$. A characterization of the pair $(\mathcal{P}, u)$ satisfying Pascal property is presented in the following theorem.

Theorem 4.2. *Let $\mathcal{P}$ be a sequence of polynomials over K as in* (4.1)*. The pair $(\mathcal{P}, u)$ satisfies the Pascal property if and only if all of following conditions are true: for each $k \in \mathbb{N}$ and $n \in \mathbb{N}$,*

1. $u_k = u_0 + kd_1$,

2. $d_n = n! \cdot d_1^n$,

3. for $0 \leq m \leq n$,

$$a_{n,m} = \frac{1}{n+1} \sum_{i=0}^{n-m} \binom{m+1+i}{m} a_{n+1,m+1+i} d_1^i. \tag{4.2}$$

Proof. Assume that $(\mathcal{P}, u)$ satisfies the Pascal property. Then we obtain the following results.

For each $k \in \mathbb{N}$, we have

$$1 = P_0(u_{k-1}) = P_1(u_k) - P_1(u_{k-1}) = \frac{u_k + a_{1,0}}{d_1} - \frac{u_{k-1} + a_{1,0}}{d_1} = \frac{u_k - u_{k-1}}{d_1},$$

i.e.,

$$u_k = u_{k-1} + d_1 \quad (k \in \mathbb{N}). \tag{4.3}$$

By (4.3), for each $k \in \mathbb{N}$, we obtain

$$u_k = u_{k-1} + d_1 = u_{k-2} + 2d_1 = \cdots = u_0 + kd_1;$$

which completes *1.*

Next, let $n \in \mathbb{N}$. For each $k \in \mathbb{N}_0$, consider

$$\begin{aligned} \frac{1}{d_n} \sum_{m=0}^{n} a_{n,m} u_k^m &= P_n(u_k) = P_{n+1}(u_{k+1}) - P_{n+1}(u_k) \\ &= \frac{1}{d_{n+1}} \sum_{j=0}^{n+1} a_{n+1,j}(u_k + d_1)^j - \frac{1}{d_{n+1}} \sum_{j=0}^{n+1} a_{n+1,j}(u_k)^j. \end{aligned}$$

Then, the right hand side becomes

$$\begin{aligned} \frac{1}{d_{n+1}} \sum_{j=1}^{n+1} a_{n+1,j}((u_k + d_1)^j - u_k^j) &= \frac{1}{d_{n+1}} \sum_{j=1}^{n+1} a_{n+1,j} \left(\sum_{r=0}^{j-1} \binom{j}{r} d_1^{j-r} u_k^r \right) \\ &= \frac{1}{d_{n+1}} \sum_{j=0}^{n} \left(\sum_{r=0}^{j} \binom{j+1}{r} a_{n+1,j+1}\ d_1^{j+1-r} u_k^r \right) \end{aligned}$$

$$\begin{aligned} &= \frac{1}{d_{n+1}} \sum_{m=0}^{n} \left(\sum_{i=m+1}^{n+1} \binom{i}{m} a_{n+1,i}\; d_1^{i} \right) u_k^m \\ &= \frac{1}{d_{n+1}} \sum_{m=0}^{n} \left(\sum_{i=0}^{n-m} \binom{m+1+i}{m} a_{n+1,m+1+i} d_1^{i+1} \right) u_k^m. \end{aligned}$$

We then have

$$\sum_{m=0}^{n} a_{n,m} u_k^m = \frac{d_n}{d_{n+1}} \sum_{m=0}^{n} \left(\sum_{i=0}^{n-m} \binom{m+1+i}{m} a_{n+1,m+1+i} d_1^{i+1} \right) u_k^m \quad (k \in \mathbb{N}_0). \quad (4.4)$$

We can rewrite (4.4) in the form

$$A_0 + A_1 u_k + \cdots + A_n u_k^n = 0 \quad (k \in \mathbb{N}_0),$$

where

$$A_m = a_{n,m} - \frac{d_n}{d_{n+1}} \sum_{i=0}^{n-m} \binom{m+1+i}{m} a_{n+1,m+1+i}\; d_1^{i+1} \quad (0 \le m \le n).$$

Since n is arbitrary, we obtain the system of equations:

$$\begin{aligned} A_0 + A_1 u_0 + \cdots + A_n u_0^n &= 0 \\ A_0 + A_1 u_1 + \cdots + A_n u_1^n &= 0 \\ &\vdots \\ A_0 + A_1 u_n + \cdots + A_n u_n^n &= 0, \end{aligned}$$

which is equivalent to

$$\begin{bmatrix} 1 & u_0 & u_0^2 & \cdots & u_0^n \\ 1 & u_1 & u_1^2 & \cdots & u_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & u_n & u_n^2 & \cdots & u_n^n \end{bmatrix} \begin{bmatrix} A_0 \\ A_1 \\ \vdots \\ A_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Since $\{u_k\}$ is the sequence of distinct elements in K, the determinant of coefficient matrix is not equal to 0 by Vandermonde determinant. This implies that $(A_0,\ A_1, \dots, A_n)$ has the unique solution, and so $0 = A_0 = A_1 = \cdots = A_n$. This implies that

$$a_{n,m} = \frac{d_n}{d_{n+1}} \sum_{i=0}^{n-m} \binom{m+1+i}{m} a_{n+1,m+1+i}\ d_1^{i+1} \qquad (0 \le m \le n). \tag{4.5}$$

Since $d_{n+1} = (n+1)d_1 d_n$, by (4.5), we get

$$a_{n,m} = \frac{1}{n+1} \sum_{i=0}^{n-m} \binom{m+1+i}{m} a_{n+1,m+1+i}\ d_1^{i} \qquad (0 \le m \le n);$$

this gives *3.* Since $a_{n,n} = 1$, by (4.5) again, we also obtain

$$1 = \frac{d_n}{d_{n+1}}(n+1)d_1.$$

Hence,

$$d_{n+1} = (n+1) \cdot d_1 d_n \quad (n \in \mathbb{N}).$$

By iteration,

$$d_n = n \cdot d_1 d_{n-1} = n(n-1) \cdot d_1^2 d_{n-2} = \cdots = n! \cdot d_1^n \text{ for all } n \in \mathbb{N}.$$

This implies that *2.* is proved.

Conversely, assume that the statements *1.-3.* hold. Let $n \in \mathbb{N}_0$ and $k \in \mathbb{N}_0$. To show that the pair $(\mathcal{P}, u)$ satisfies the Pascal property, we consider

$$\begin{aligned}
P_{n+1}(u_{k+1}) - P_{n+1}(u_k) &= P_{n+1}(u_k + d_1) - P_{n+1}(u_k) && \text{(by 1.)} \\
&= \frac{1}{(n+1)! \cdot d_1^{n+1}} \sum_{j=0}^{n+1} a_{n+1,j}(u_k + d_1)^j \\
&\quad - \frac{1}{(n+1)d_1} \sum_{l=0}^{n+1} a_{n+1,l}(u_k)^l && \text{(by 2.)} \\
&= \frac{1}{(n+1)! \cdot d_1^{n+1}} \sum_{j=1}^{n+1} a_{n+1,j}((u_k + d_1)^j - u_k^j)
\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{(n+1)! \cdot d_1^{n+1}} \sum_{j=0}^{n} a_{n+1,j+1} \left(\sum_{r=0}^{j} \binom{j+1}{r} d_1^{j+1-r} u_k^r \right) \\
&= \frac{1}{(n+1)! \cdot d_1^{n+1}} \sum_{m=0}^{n} \left(\sum_{i=m+1}^{n+1} \binom{i}{m} a_{n+1,i}\ d_1^i \right) u_k^m \\
&= \frac{1}{(n+1)! \cdot d_1^{n+1}} \sum_{m=0}^{n} \left(\sum_{i=0}^{n-m} \binom{m+1+i}{m} a_{n+1,m+1+i}\ d_1^{i+1} \right) u_n^k \\
&= \frac{1}{(n+1)! \cdot d_1^{n}} \sum_{m=0}^{n} \left(\sum_{i=0}^{n-m} \binom{m+1+i}{m} a_{n+1,m+1+i}\ d_1^{i} \right) u_k^m \\
&= \frac{1}{(n+1)! \cdot d_1^{n}} \sum_{m=0}^{n} (n+1) a_{n,m} u_k^m && \text{(by 3.)} \\
&= \frac{1}{n! \cdot d_1^{n}} \sum_{m=0}^{n} a_{n,m} u_k^m = \frac{1}{d_n} \sum_{m=0}^{n} a_{n,m} u_k^m \\
&= P_n(u_k),
\end{aligned}$$

as desired. □

The next corollary shows that the pair $(\mathcal{P}, u)$ satisfying the Pascal property is a generalization of binomial polynomials.

Corollary 4.3. *Let $K = \mathbb{Q}$. Let $\{u_k\}$ be a sequence of distinct elements in K with $u_0 = 0$ and $\mathcal{P} = \{P_n(t)\}$ a sequence of polynomial over K as in* (4.1)*. Assume that the pair $(\mathcal{P}, u)$ satisfying the Pascal property. If $d_1 = 1$ and $a_{n,0} = 0$ for all $n \in \mathbb{N}$, then*

$$P_n(t) = \binom{t}{n} \qquad (n \in \mathbb{N}_0).$$

Proof. Clearly, the identity holds for $n = 0$. Since $a_{1,0} = 0$ and $d_1 = 1$, we obtain

$$P_1(t) = t = \binom{t}{1}.$$

Note that, by $d_1 = 1$, $u_0 = 0$ and Theorem 4.2, we get

$$d_n = n! \text{ and } u_k = k \quad (n \in \mathbb{N}_0,\ k \in \mathbb{N}_0).$$

Let $n \geq 2$. Assume that $P_{n-1}(t) = \binom{t}{n-1}$. We will show that $P_n(t) = \binom{t}{n}$, by comparing their coefficients. Observe that

$$\binom{k}{n-1} = P_{n-1}(k) = P_n(k+1) - P_n(k) \quad (k \in \mathbb{N}_0).$$

Therefore, for $k \in \mathbb{N}_0$,

$$\begin{aligned}\frac{k(k-1)\cdots(k-(n-2))}{(n-1)!} &= \frac{1}{n!}\sum_{r=0}^{n} a_{n,r}(k+1)^r - \frac{1}{n!}\sum_{r'=0}^{n} a_{n,r'}k^{r'} \\ &= \frac{1}{n!}\sum_{r=0}^{n} a_{n,r}((k+1)^r - k^r).\end{aligned}$$

Since $a_{n,0} = 0$, we deduce that

$$n(k)(k-1)\cdots(k-(n-2)) = \sum_{r=1}^{n} a_{n,r}((k+1)^r - k^r) \quad (k \in \mathbb{N}_0).$$

Substituting $k = 0,\ 1, \ldots, n-2$, we get the system of equations

$$\begin{aligned} 0 &= (1^n - 0^n) + (1^{n-1} - 0^{n-1})a_{n,n-1} + \cdots + (1^1 - 0^1)a_{n,1}, \\ 0 &= (2^n - 1^n) + (2^{n-1} - 1^{n-1})a_{n,n-1} + \cdots + (2^1 - 1^1)a_{n,1}, \\ &\vdots \\ 0 &= ((n-1)^n - (n-2)^n) + ((n-1)^{n-1} - (n-2)^{n-1})a_{n,n-1} \\ &\quad + \cdots + ((n-1)^1 - (n-2)^1)a_{n,1}, \end{aligned}$$

which equivalent to

$$\begin{bmatrix} -1^n + 0^n \\ -2^n + 1^n \\ \vdots \\ -(n-1)^n + (n-2)^n \end{bmatrix} = A \begin{bmatrix} a_{n,1} \\ a_{n,2} \\ \vdots \\ a_{n,n-1} \end{bmatrix},$$

where

$$A = \begin{bmatrix} 1^1 - 0^1 & 1^2 - 0^2 & \cdots & 1^{n-1} - 0^{n-1} \\ 2^1 - 1^1 & 2^2 - 1^2 & \cdots & 2^{n-1} - 1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ (n-1)^1 - (n-2)^1 & (n-1)^2 - (n-2)^2 & \cdots & (n-1)^{n-1} - (n-2)^{n-1} \end{bmatrix}.$$

Consider the matrix

$$\begin{aligned} A &= \begin{bmatrix} 1^1 - 0^1 & 1^2 - 0^2 & \cdots & 1^{n-1} - 0^{n-1} \\ 2^1 - 1^1 & 2^2 - 1^2 & \cdots & 2^{n-1} - 1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ (n-1)^1 - (n-2)^1 & (n-1)^2 - (n-2)^2 & \cdots & (n-1)^{n-1} - (n-2)^{n-1} \end{bmatrix} \\ &\sim \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 2^1 & 2^2 & \cdots & 2^{n-1} \\ 3^1 - 2^1 & 3^2 - 2^2 & \cdots & 3^{n-1} - 2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ (n-1)^1 - (n-2)^1 & (n-1)^2 - (n-2)^2 & \cdots & (n-1)^{n-1} - (n-2)^{n-1} \end{bmatrix} \\ &\vdots \\ &\sim \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 2^1 & 2^2 & \cdots & 2^{n-1} \\ 3^1 & 3^2 & \cdots & 3^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ (n-1)^1 & (n-1)^2 & \cdots & (n-1)^{n-1} \end{bmatrix} = B. \end{aligned}$$

Since B is a Vandermonde matrix, $\det A = \det B \neq 0$. So, the system of equations has the unique solution, say $(a_{n,1},\ a_{n,2}, \ldots, a_{n,n-1})$. Since $\binom{k}{n-1} = \binom{k+1}{n} - \binom{k}{n}$, by repeating the same process, all coefficients of $\binom{t}{n}$ form a solution of the system. This implies that

$$P_n(t) = \binom{t}{n}. \qquad \square$$

The following example shows an interesting application of our results in the classical case $K = \mathbb{Q}$.

Example 4.4. Recall the notion of Stirling numbers of the first kind. Consider the falling factorial polynomials of degree n:

$$(t)_n := n! \cdot \binom{t}{n} = t(t-1)\cdots(t-n+1).$$

Expanding the multiplications and arranging the terms of powers of indeterminate t, we get

$$(t)_n = \sum_{m=0}^{n} s(n,m)\, t^m \qquad (n \in \mathbb{N}_0). \tag{4.6}$$

The coefficients $s(n,m)$ of expression (4.6) of the falling factorial $(t)_n$ are called **Stirling numbers of the first kind**. Clearly, the definition implies $s(n,m) = 0$ if $m > n$ and $s(n,n) = 1$ for all $n \in \mathbb{N}_0$.

As the result of and Corollary 4.3, if we substitute $d_1 = 1$, $u_0 = 0$ and $a_{n,0} = 0$ $(n \in \mathbb{N}_0)$,

$$P_n(t) = \binom{t}{n} = \frac{(t)_n}{n!} = \frac{1}{n!}\sum_{m=0}^{n} s(n,m)t^m \quad (n \in \mathbb{N}_0).$$

By (4.1) and Theorem 4.2, for each $n \in \mathbb{N}_0$, we have

$$P_n(t) = \frac{1}{n!}\sum_{m=0}^{n} a_{n,m}t^m.$$

Comparing the coefficients of t^m, we conclude that

$$a_{n,m} = s(n,m) \quad (0 \le m \le n).$$

By (4.2), we obtain a recurrence relation on the Stirling numbers of the first kind $s(n,m)$:

$$s(n,m) = \frac{1}{n+1}\sum_{i=0}^{n-m}\binom{m+1+i}{m} s(n+1, m+1+i). \tag{4.7}$$

By [8, Theorem 8.7], the Stirling numbers of the first kind $s(n,m)$ satisfy the triangular recurrence relation

$$s(n+1,m) = s(n,m-1) - n \cdot s(n,m). \tag{4.8}$$

Combining (4.7) and (4.8), we get

$$\begin{aligned}
(n+1)\cdot s(n,m) &= \sum_{i=0}^{n-m} \binom{m+1+i}{m} s(n+1,m+1+i) \\
&= \sum_{i=0}^{n-m} \binom{m+1+i}{m} \left(s(n,m+i) - k \cdot s(n,m+1+i)\right) \\
&= (m+1)s(n,m) + \sum_{i=1}^{n-m} \binom{m+1+i}{m} s(n,m+i) \\
&\quad - n \sum_{i=0}^{n-m} \binom{m+1+i}{m} s(n,m+1+i) \\
&= (m+1)s(n,m) + \sum_{i=1}^{n-m} \left(\binom{m+1+i}{m} - n\binom{m+i}{m} \right) s(n,m+i).
\end{aligned}$$

Finally, we also obtain another horizontal recurrence relation

$$s(n,m) = \frac{1}{n-m} \sum_{i=1}^{n-m} \left(\binom{m+1+i}{m} - n\binom{m+i}{m} \right) s(n,m+i).$$

4.2 Pascal property for bases of integer-valued polynomials

In this section, criteria on polynomials forming a basis of $\mathrm{Int}(V)$ having Pascal property is characterized. By the same setting as in (4.1), we immediately obtain from the definition of $\mathrm{Int}(V)$ and Theorem 4.2 that if, for each $t_0 \in V$,

$$\nu(t_0^n + t_0^{n-1}a_{n,n-1} + \cdots + a_{n,0}) \geq \nu(d_1^n \cdot n!),$$

then

$$P_n(t) = \frac{1}{d_n} \sum_{i=0}^{n} a_{n,i} t^i \in \mathrm{Int}(V).$$

A characterization of $P_n(t)$ states as follows.

Theorem 4.5. *Let $(\mathcal{P}, u)$ be a pair satisfying the Pascal property. Let $P = \mathcal{P} \cap Int(V)$ and $Q \subset P$. Then the elements of Q form a regular basis for V-module $Int(V)$ if and only if the following three conditions are fulfilled:*

1. *the set Q contains exactly one polynomial of each degree $n \in \mathbb{N}_0$,*
2. *the element d_1 (in the first degree polynomial of Q) is a unit in V,*
3. *the valuation values $\nu(k!) = w_q(k)$ hold for all $k \in \mathbb{N}$.*

Proof. Assume that Q is a regular basis for V-module $\mathrm{Int}(V)$. Based on the definition of regular basis, we get *1.* By Proposition 2.21, for each n, $\frac{1}{d_n}$ generates $J_n(\mathrm{Int(V)})$. Since $T^{-w_q(n)}$ generates $J_n(\mathrm{Int(V)})$ and generators of any fractional ideal are unique up to multiplication by units, we deduce that $\nu(d_n) = w_q(n)$. We then have $\nu(d_1) = w_q(1) = 0$, i.e., d_1 is a unit in V. This implies that, for each n,

$$w_q(n) = \nu(d_n) = \nu(d_1^n \cdot n!) = \nu(d_1^n) + \nu(n!) = \nu(n!).$$

Conversely, assume that *1.-3.* hold. From *2.* and *3.*, we have

$$w_q(n) = \nu(n! \cdot d_1^n) = \nu(d_n).$$

In view of Proposition 2.24, $\frac{1}{d_n}$ generates $J_n(\mathrm{Int(V)})$. By Proposition 2.21 and assumption *1.*, the set Q is a regular basis for V-module $\mathrm{Int}(V)$. □

Next, let $\{u_n\}_{n \geq 0}$ be a sequence of distinct elements of V with $u_0 = 0$. Define polynomials $C_n(t)$ over K in the shape of the Lagrange-type by

$$C_0(t) = 1 \quad \text{and} \quad C_n(t) = \prod_{i=0}^{n-1} \frac{t - u_i}{u_n - u_i} \quad (n \in \mathbb{N}). \tag{4.9}$$

Theorem 4.6. *The sequence of Lagrange-type polynomials $C_n(t)$ as defined in (4.9) satisfy the Pascal property with respect to $\{u_k\}$ if and only if $u_k = ku_1$ for all $n \in \mathbb{N}_0$.*

Proof. Assume that the sequence $\{C_n(t)\}$ satisfies the Pascal property with respect to $\{u_k\}$, that is,

$$C_n(u_k) + C_{n-1}(u_k) = C_n(u_{k+1}) \text{ for all } n \in \mathbb{N} \text{ and } k \in \mathbb{N}_0.$$

Substituting $n = 1$, we get

$$C_1(u_k) + C_0(u_k) = C_1(u_{k+1}) \quad (k \in \mathbb{N}_0),$$

and so,

$$\frac{u_k}{u_1} + 1 = \frac{u_{k+1}}{u_1} \quad (k \in \mathbb{N}_0).$$

Thus, $u_k + u_1 = u_{k+1}$ for all $k \geq 0$. By iteration and the assumption $u_0 = 0$, we have

$$u_k = u_{k-1} + u_1 = u_{k-2} + 2u_1 = \cdots = u_0 + ku_1 = ku_1 \quad (k \in \mathbb{N}_0).$$

To prove the converse, assume that $u_k = ku_1$ for all $k \geq 0$. We first have

$$C_1(u_k) + C_0(u_k) = \frac{u_k}{u_1} + 1 = \frac{(k+1)u_1}{u_1} = \frac{u_{k+1}}{u_1} = C_1(u_{k+1}).$$

For each $n \geq 2$, we consider

$$\begin{aligned} C_n(u_k) + C_{n-1}(u_k) &= \prod_{i=0}^{n-1} \frac{u_k - u_i}{u_n - u_i} + \prod_{j=0}^{n-2} \frac{u_k - u_j}{u_{n-1} - u_j} \\ &= \prod_{i=0}^{n-1} \frac{ku_1 - iu_1}{nu_1 - iu_1} + \prod_{j=0}^{n-2} \frac{ku_1 - ju_1}{(n-1)u_1 - ju_1} \\ &= \prod_{i=0}^{n-1} \frac{k-i}{n-i} + \prod_{j=0}^{n-2} \frac{k-j}{n-1-j} \end{aligned}$$

$$
\begin{aligned}
&= \binom{k}{n} + \binom{k}{n-1} = \binom{k+1}{n} \\
&= \prod_{i=0}^{n-1} \frac{(k+1-i)u_1}{(n-i)u_1} = \prod_{i=0}^{n-1} \frac{u_{k+1}-u_i}{u_n-u_i} \\
&= C_n(u_{k+1}),
\end{aligned}
$$

as desired. □

Remark that $u_{pn} = 0$ for all $n \in \mathbb{N}_0$, if the domain V has characteristic p. This implies that $C_{np}(t)$ are non-defined.

Now, we ready to determine Lagrange type polynomials which satisfy Pascal property and form a regular basis of $\text{Int}(V)$. Let $u \in V^*$. With $u_k = ku$ for all $k \in \mathbb{N}_0$, by Theorem 4.6, the Lagrange-type polynomials

$$
\binom{t}{0}_u := 1 \quad \text{and} \quad \binom{t}{n}_u := \prod_{i=0}^{n-1} \frac{t-iu}{(n-i)u} \quad (n \in \mathbb{N}) \tag{4.10}
$$

satisfy the Pascal property. Next, the characterization of $\binom{t}{n}_u$ to be a regular basis of $\text{Int}(V)$ is presented as follows..

Theorem 4.7. *The sequence* $\{\binom{t}{n}_u\}_{n\geq 0}$ *as defined in* (4.10) *is a regular basis of* V*-module Int*(V) *if and only if* u *is a unit in* V *and* $\nu(n!) = w_q(n)$ *for all* $n \in \mathbb{N}$.

Proof. Assume that polynomials $\binom{t}{n}_u = \frac{t(t-u)(t-2u)\cdots(t-(n-1)u)}{u^n \cdot n!}$ form a basis of V-module $\text{Int}(V)$. By Proposition 2.23, the sequence $\{ku\}_{k\in\mathbb{N}}$ is T-ordering and so a g-IVP sequence. Then, by Theorem 3.3, the first $q-1$ terms of the sequence $\{nu\}_{n\in\mathbb{N}}$ are units in V. This implies that u is a unit in V. It remains to show that $\nu(n!) = w_q(n)$ for all $n \in \mathbb{N}$. Since $\frac{1}{u^n \cdot n!}$ is a generator of $J_n(\text{Int}(V))$ and $\nu(u) = 0$, by the same argument as in (2.2), we have

$$
w_q(n) = \nu(u^n \cdot n!) = \nu(u^n) + \nu(n!) = \nu(n!) \quad (n \in \mathbb{N}).
$$

On the other hand, assume that u is a unit of V and $\nu(n!) = w_q(n)$ for all $n \in \mathbb{N}_0$. By Proposition 2.24, it suffices to show that $\{0, u, 2u, \ldots\}$ is a T-ordering of V by showing that $\nu(\prod_{i=0}^{n-1}(n-i)u) = w_q(n)$ for all $n \in \mathbb{N}$. For each $n \in \mathbb{N}$, we have

$$\nu\left(\prod_{i=0}^{n-1}(n-i)u\right) = \nu\left(\prod_{i=0}^{n-1}(n-i)\right) + \nu(u) = \nu(n!) + 0 = w_q(n).$$

□

Return to the polynomials $C_n(t)$ as in (4.9). From [4, Theorem II.2.7], the polynomials $C_n(t)$ form a regular basis for V-module Int(V) if the corresponding sequence $\{u_k\}$ agrees with VWDWO condition defined in (2.14). Recall the result of [3, Theorem 2.2] on $C_n(t)$ with the setting of VWDWO sequence $\{u_k\}$:

Theorem 4.8. *If $n = n_0 + n_1 q + \cdots + n_{d(n)}q^{d(n)}$ is a q-adic expansion of a positive integer n, and if $A = A_0 + A_1 T + \cdots$ is a T-adic expansion of an element A of V, then*

$$C_n(A) \equiv C_{n_0}(A_0)C_{n_1}(A_1)\cdots C_{n_{d(n)}}(A_{d(n)}) \pmod{\mathfrak{m}}.$$

In the case of $K = \mathbb{Q}$, let V_q be a discrete valuation domain of the field of rational number $\mathbb{Q}$. We have that the number q, the cardinal of residue field, becomes a prime number and $\nu = \nu_q$, a q-adic valuation. A unit u in V_q^* is of the form $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $q \nmid ab$. It easy to see that

$$\nu_q(nu - mu) = \nu_q\left(n\cdot\frac{a}{b} - m\cdot\frac{a}{b}\right) = \nu_q\left((n-m)\cdot\frac{a}{b}\right) = \nu_q(n-m) \quad (n, m \in \mathbb{N}_0).$$

This implies that $\{0, u, 2u, \ldots\}$ is a VWDWO sequence. The final proposition shows that the polynomials $\binom{t}{n}_u$ satisfy the Lucas property modulo (q). Its proof is immediately from Theorem 4.8.

Proposition 4.9. *If $n = n_0 + n_1 q + \cdots + n_{d(n)}q^{d(n)}$ is the q-adic expansion of $n \in \mathbb{N}$, and if*

$$A = A_0 + A_1 q + A_2 q^2 + \cdots \qquad (A_i \in \{u_0 = 0, u_1, \cdots, u_{q-1}\})$$

is the q-adic expansion of an element A of V_q, then

$$\binom{A}{n}_u \equiv \binom{A_0}{n_0}_u \binom{A_1}{n_1}_u \cdots \binom{A_{d(n)}}{n_{d(n)}}_u \pmod{(q)}.$$

REFERENCES

[1] Adam, D.: Finite differences in finite characteristic, *J. Algebra* **296**, 285–300 (2006).

[2] Bhargava, M.: P-orderings and polynomial functions on arbitrary subsets of Dedekind rings, *J. Reine Angew. Math.* **490**, 101–127 (1997).

[3] Boulanger, J. and Chabert, J. L.: An extension of the Lucas theorem, *Acta Arith.* **96**, 303–312 (2001).

[4] Cahen, P. J., Chabert, J. L.: *Integer-Valued Polynomials*, Amer. Math. Soc. Surveys Monogr., Providence, 1997.

[5] Carlitz, L.: On polynomials in a Galois Field, *Bull. Amer. Math. Soc.* **38**, 736–744 (1932).

[6] Carlitz, L.: On certain functions connected with polynomials in a Galois field, *Duke Math. J.* **1**, 137–168 (1935).

[7] Carlitz, L.: A set of polynomials, *Duke Math. J.* **6**, 486–504 (1940).

[8] Charalambides, C. A.: *Enumerative Combinatorics*, CRC Press, New York, 2018.

[9] Cohn, P. M.: *Algebraic Numbers and Algebraic Functions*, CRC Press, New York, 2018.

[10] Fine, N. J.: Binomial coefficients modulo a prime, *Amer. Math. Monthly* **54**, 589–592 (1947).

[11] McCarthy, P. J.: *Algebraic Extension of Fields*, Dover, New York, 1991.

[12] Narkiewicz, W.: *Polynomial Mappings*, Lecture Notes in Math., Springer, Berlin, 1995.

VITA

Name	Miss Rattiya Meesa
Date of Birth	28 July 1993
Place of Birth	Narathiwas, Thailand
Education	† B.Sc. (Mathematics)(First Class Degree Honours), Prince of Songkla University, 2014 † M.Sc. (Mathematics), Chulalongkorn University, 2017
Scholarship	Science Achievement Scholarship of Thailand (SAST)