ON THE GENERATING POLYNOMIALS FOR THE DISTRIBUTION
OF GENERALIZED BINOMIAL COEFFICIENTS IN DISCRETE VALUATION
DOMAINS

DONG QUAN NGOC NGUYEN

CONTENTS

1. Introduction 1
2. An analogue of Lucas’ theorem for discrete valuation domains 2
3. Generating polynomials for generalized binomial coefficients 4
Acknowledgements 7
References 8

Abstract. For a discrete valuation domain $V$ with maximal ideal $m$ such that the residue field $V/m$ is finite, there exists a sequence of polynomials $(F_n(x))_{n \geq 0}$ defined over the quotient field $K$ of $V$ that forms a basis of the $V$-module $\text{Int}(V) = \{ f \in K[x] \mid f(V) \subseteq V \}$. This sequence of polynomials bears many resemblances to the classical binomial polynomials $(x^n)_{n \geq 0}$. In this paper, we introduce a generating polynomial to account for the distribution of the $V$-values of the polynomials $F_n(x)$ modulo the maximal ideal $m$, and prove a result that provides a method for counting exactly how many $V$-values of the polynomials $(F_n(x))_{n \geq 0}$ fall into each of the residue classes modulo $m$. Our main theorem in this paper can be viewed as an analogue of the classical theorem of Garfield and Wilf in the context of discrete valuation domains.

1. Introduction

For an integer $n \geq 0$, the classical binomial polynomial $(x^n) \in \mathbb{Q}[x]$ is defined as

$$x(x - 1)(x - 2) \cdots (x - n + 1) \over n!.$$ 

The sequence $(x^n)_{n \geq 0}$ plays an important role in studying the $\mathbb{Z}$-module $\text{Int}(\mathbb{Z}) = \{ f \in \mathbb{Q}[x] \mid f(\mathbb{Z}) \subseteq \mathbb{Z} \}$. Studying the $\mathbb{Z}$-values of these polynomials $(x^n)$ at integers $m \geq 0$ thus attracts special attention, and is an active research area. Many basic questions arise concerning with such $\mathbb{Z}$-values; for example, for a given prime $p$ and an integer $n \geq 0$, can one describe exactly which integers $m$ are such that the values of binomial polynomial $(x^n)$ at $m$ are divisible by $p$, or satisfy certain congruence conditions modulo $p$?

Motivated by such question, Garfield and Wilf [6] proposed a method using generating polynomials for studying the distribution of $\mathbb{Z}$-values of binomial polynomials modulo primes. More precisely, Garfield and Wilf [6] proved the following

Theorem 1.1. (Garfield–Wilf [6])

Let $p$ be a prime, and let $a$ be a primitive root modulo $p$. Let $n \geq 0$ be an integer, and let $t_j = t_j(n)$ be the number of times the digit $j$ appears in the $p$-ary expansion of $n$ for $0 \leq j \leq p - 1$. For each $i$, let $r_i(n)$ be the number of integers $k$, $0 \leq k \leq n$, for which the binomial coefficient $\binom{n}{k} \equiv a^i \pmod{p}$, and let $R_n(x) = \sum_{i=0}^{p-2} r_i(n)x^i$ be their generating function. Then

$$R_n(x) \equiv \prod_{j=1}^{p-1} R_j(x)^{t_j} \mod (x^{p-1} - 1).$$
There are many strong analogues between the integers $\mathbb{Z}$ and the ring of polynomials over a finite field $\mathbb{F}_q$, say $\mathbb{F}_q[t]$ (see, for example, Goss [7] and Weil [10]). Inspired by the work of Garfield and Wilf [6] and the analogies between $\mathbb{Z}$ and $\mathbb{F}_q[t]$, the author [9] proved a function field analogue of the Garfield–Wilf theorem with the classical binomial coefficients replaced by the Carlitz binomial coefficients (see Carlitz [3]).

In this paper, we further consider another analogy between $\mathbb{Z}$ and an arbitrary discrete valuation domain with finite residue field in view of the classical theorem of Garfield and Wilf. In such a discrete valuation domain $V$ with maximal ideal $m$, there exists a sequence of polynomials $(F_n(x))_{n \geq 0}$ (see (2) below for a precise notion of $F_n(x)$) defined over the quotient field $K$ of $V$ such that they form a basis of the $V$-module $\text{Int}(V) = \{ f \in K[x] \mid f(V) \subseteq V \}$ in a similar manner as the classical binomial polynomials $(\binom{x}{n})_{n \geq 0}$ do for the $\mathbb{Z}$-module $\text{Int}(\mathbb{Z})$. In view of this similarity, one can view $(F_n(x))_{n \geq 0}$ as an analogue in $V$ of the classical binomial polynomials $(\binom{x}{n})_{n \geq 0}$. One can ask for analogues of results about the classical binomial polynomials in the context of $V$ with $(F_n(x))_{n \geq 0}$ in place of the classical binomial polynomials; for illustration, a basic problem is to understand the divisibility properties of the $V$-values of $F_n(x)$ at elements $u \in V$. Regarding such a problem, it suffices to consider only the $V$-values of $F_n(x)$ at elements $u_n \in V$, where $(u_n)_{n \geq 0}$ forms a very well-distributed and well-ordered sequence in $V$ whose definition will be recalled in Section 2. Indeed, for such a sequence $(u_n)_{n \geq 0}$, it is well-known that a polynomial $f \in K[x]$ of degree $n$ belongs in $\text{Int}(V)$ if and only if the values of $f(x)$ at $u_0, u_1, \ldots, u_n$ belong in $V$ (see [2, Corollary II2.8]). Since the sequence $(F_n(x))_{n \geq 0}$ forms a basis of the $V$-module $\text{Int}(V)$, it suffices to study the $V$-values of $(F_n(x))_{n \geq 0}$ at the sequence $(u_n)_{n \geq 0}$. Based on this similarity with the $\mathbb{Z}$-values of the classical binomial polynomials $(\binom{x}{n})$ at integers $m \geq 0$, we call the values $F_n(u_m)$ for $n, m \geq 0$ the generalized binomial coefficients in $V$ in analogy with the classical binomial coefficients $(\binom{m}{n})$.

Motivated by the classical theorem of Garfield and Wilf [6] and the above discussion about analogies between the classical binomial polynomials in $\mathbb{Z}$ and the polynomials $(F_n(x))_{n \geq 0}$ in $V$, it is natural to ask whether there is an analogue of Garfield–Wilf theorem in the context of discrete valuation domains. We give an affirmative answer to this question, and our main theorem (see Theorem 3.5) in this paper can be viewed as an analogue of the theorem of Garfield and Wilf in the context of discrete valuation domains.

Our paper is structured as follows. In Section 2, we introduce some basic notions and notation that will be used throughout the paper. Furthermore, in the same section, we explain an analogue of Lucas’ theorem for discrete valuation domains which is due to Boulanger and Chabert [1]. In Section 3, we prove the main theorem in this paper (see Theorem 3.5). The proof of our main theorem is modeled on that of the classical theorem of Garfield and Wilf. Note that despite similarities between the classical binomial coefficients $(\binom{m}{n})$ and the generalized binomial coefficients $F_n(u_m)$, there is a distinct difference between these two values: both arguments $n, m$ in the classical binomial coefficients $(\binom{m}{n})$ belong in $\mathbb{Z}$ whereas one argument, say $u_m$, in the generalized binomial coefficients $F_n(u_m)$ belong in a discrete valuation domain $V$ which in general does not contain any ordering as $\mathbb{Z}$ does. The fact that the sequence $(u_n)_{n \geq 0}$ is a very well-distributed and well-ordered sequence in $V$, allows to view the elements $u_n$ in $V$ as the integers $n$.

Throughout the paper, $\mathbb{Z}$ denotes the set of integers, $\mathbb{Z}_{\geq 0}$ stands for the set of nonnegative integers, and $\mathbb{Z}_{>0}$ is the set of positive integers.

2. An analogue of Lucas’ theorem for discrete valuation domains

In this section, we introduce a few basic notions and notations that we will use throughout this paper. We also recall an analogue of Lucas’s theorem for discrete valuation domains which was proved by Boulanger and Chabert [1].

Let $V$ be a discrete valuation domain, and let $m$ be the maximal ideal of $V$. Throughout this paper, we assume that the residue field $V/m$ is finite, and isomorphic to the finite field $\mathbb{F}_q$ for some $q$. Let $\pi$ be a generator of $m$, $K$ the quotient field of $V$, and let $v$ the corresponding valuation of $K$, i.e., for each $x \in V \setminus \{0\}$, $v(x)$ is the largest integer $h$ such that $x \in m^h$. Let $\hat{V}, \hat{K}, \hat{m}$ be the completions of $V, K,$
and \( m \) with respect to the \( m \)-adic topology, respectively. By abuse of notation, we still use the same notation \( v \) to denote the extension of \( v \) to \( \hat{K} \).

For each integer \( \ell \), we denote by \( v_q(\ell) \) the largest power of \( q \) dividing \( \ell \). Recall from [8] that a sequence \( (u_n)_{n \in \mathbb{Z}_0} \) in \( V \) is a very well distributed and well-ordered sequence if for all integers \( m, n \),

\[
v(u_n - u_m) = v_q(n - m).
\]

The set formed by such a sequence is dense in \( V \) with respect to the topology induced by the valuation \( v \). There is a very well distributed and well-ordered sequence for every discrete valuation domain with finite residue field that is constructed as follows.

We choose elements \( u_0, \ldots, u_{q-1} \) in \( V \) such that \( u_0 = 0 \), and \( \mathcal{R} = \{u_0, u_1, \ldots, u_{q-1}\} \) is the set of representatives of \( V \) modulo \( m \). It is known (see [4, Chapter 2]) that each element \( x \in \hat{V} \) has a unique \( \pi \)-adic expansion of the form

\[
x = \sum_{j \geq 0} x_j \pi^j,
\]

where the \( x_j \) are some elements in \( R \). We extend the set \( \mathcal{R} \) as follows. For each integer \( n \geq 0 \), represent \( n \) in the \( q \)-adic expansion of the form

\[
n = n_0 + n_1 q + \cdots + n_k q^k,
\]

where the \( n_i \) are integers such that \( 0 \leq n_i \leq q - 1 \) for each \( i \). We define

\[
(1) \quad u_n = u_{n_0} + u_{n_1} \pi + \cdots + u_{n_k} \pi^k \in V.
\]

It is clear that for \( 0 \leq n \leq q - 1 \), the element \( u_n \) we just construct above is the same as in the set \( \mathcal{R} \). The sequence \( (u_n)_{n \geq 0} \) forms a very well distributed and well-ordered sequence in \( V \) (see [2, Definition II.2.1 and Proposition II.2.3]).

We construct a sequence of polynomials \( (F_n(x))_{n \geq 0} \subseteq K[x] \) (which can be viewed as an analogue of the classical binomial polynomials) by letting, for each \( n \geq 1 \),

\[
(2) \quad F_n(x) = \prod_{k=1}^{n-1} \frac{x - u_k}{u_n - u_k},
\]

and setting \( F_0(x) = 1 \).

The sequence \( (F_n(x))_{n \geq 0} \) shares several similar properties as the sequence of classical binomial polynomials \( \left( \binom{x}{n} \right)_{n \geq 0} \), where we recall that for each \( n \geq 0 \),

\[
\binom{x}{n} = \frac{x(x-1)(x-2)\cdots(x-n+1)}{n!}.
\]

One of the main resemblances between these two sequences (see Theorem II.2.7 in [2]) is that the sequence \( (F_n(x))_{n \geq 0} \) forms a basis of the \( V \)-module \( \text{Int}(V) = \{f \in K[x] \mid f(V) \subseteq V\} \), which is an analogue of the classical result that \( \left( \binom{x}{n} \right)_{n \geq 0} \) is a basis of the \( \mathbb{Z} \)-module \( \text{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[x] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\} \).

The pair \( \{(u_n)_{n \geq 0}, (F_n(x))_{n \geq 0}\} \) play a similar role for understanding \( \text{Int}(V) \) as the role of the pair \( \{(Z_{\geq 0}, (\binom{m}{n})_{n \geq 0}) \} \) for studying \( \text{Int}(\mathbb{Z}) \). This can be seen by recalling the fact (see [2, Corollary II.2.8]) that if \( f \) is a polynomial in \( K[x] \) of degree \( n \), then \( f \in \text{Int}(V) \) if and only if all the values \( f(u_0), \ldots, f(u_n) \) belong in \( V \). Since \( (F_n(x))_{n \geq 0} \) forms a basis of \( \text{Int}(V) \), the values of \( F_n(u_m) \) for \( n, m \in \mathbb{Z}_\geq 0 \) play an important role for studying the structure of \( \text{Int}(V) \) in a similar manner as the classical binomial coefficients \( \binom{m}{n} \) for understanding the structure of \( \text{Int}(\mathbb{Z}) \). In view of this analogy, it is natural to call the values of \( F_n(u_m) \) for \( n, m \in \mathbb{Z}_\geq 0 \) the generalized binomial coefficients in \( V \).

Another analogy between the sequence \( (F_n(x))_{n \geq 0} \) and the classical binomial polynomials \( \left( \binom{x}{n} \right)_{n \geq 0} \) which we need in the proof of our main theorem, is reflected in the following result which is due to Boulanger and Chabert (see [1, Theorem 2.2]).

**Theorem 2.1.** (analogue of Lucas’ theorem, see [1, Theorem 2.2])

Let \( x \) be an element of \( \hat{V} \) such that the \( \pi \)-adic expansion of \( x \) is of the form

\[
x = \sum_{j \geq 0} x_j \pi^j,
\]
where the \( x_j \) are some elements in \( R \). Let \( n \) be a positive integer whose \( q \)-adic expansion is of the form
\[
n = n_0 + n_1 q + \cdots + n_k q^k,
\]
where the \( n_i \) are integers such that \( 0 \leq n_i \leq q - 1 \) for each \( i \). Then
\[
F_n(x) \equiv F_{n_0}(x_0) F_{n_1}(x_1) \cdots F_{n_k}(x_k) \pmod{\hat{m}}.
\]

Since \( K \cap \hat{m} = m \) (see [5, Proposition 5, p.402]), and the \( F_n(x) \in K[x] \), the next result follows immediately from Theorem 2.1.

**Corollary 2.2.** Let \( x \) be an element of \( V \) such that the \( \pi \)-adic expansion of \( x \) is of the form
\[
x = \sum_{j \geq 0} x_j \pi^j,
\]
where the \( x_j \) are some elements in \( R \). Let \( n \) be a positive integer whose \( q \)-adic expansion is of the form
\[
n = n_0 + n_1 q + \cdots + n_k q^k,
\]
where the \( n_i \) are integers such that \( 0 \leq n_i \leq q - 1 \) for each \( i \). Then
\[
F_n(x) \equiv F_{n_0}(x_0) F_{n_1}(x_1) \cdots F_{n_k}(x_k) \pmod{m}.
\]

### 3. Generating polynomials for generalized binomial coefficients

In this section, we prove our main theorem (see Theorem 3.5 below) which signifies the distribution of generalized binomial coefficients modulo the maximal ideal in a discrete valuation domain. This result can be viewed as an analogue of a theorem of Garfield and Wilf (see [6]) in the setting of discrete valuation domains. We begin by describing how counting generalized binomial coefficients works in the setting of discrete valuation domains.

For the rest of this paper, we fix a primitive root, say \( \varphi \) modulo \( m \), i.e., \( \varphi \in V \) is a generator of the cyclic group \((V/m)^\times\).

For each \( n \in \mathbb{Z}_{\geq 0} \), and each integer \( j \in \mathbb{Z} \), define
\[
E_j(u_n) = \{ m \in \mathbb{Z} | 0 \leq m \leq n \text{ and } F_m(u_n) \equiv \varphi^j \pmod{m}\},
\]
and set
\[
\epsilon_j(u_n) = \text{card}(E_j(u_n))
\]
where \( \text{card}(\cdot) \) denotes the cardinality of a set.

For the \( q \)-adic representation of \( n \) of the form \( n = \sum_{i=0}^{r-1} n_i q^i \), define \( d^p(n) = r + 1 \) which is the number of digits \( n_i \) in the \( q \)-adic expansion of \( n \). We introduce a binary relation \( \ast \) on \( \mathbb{Z}_{\geq 0} \) under which \( \mathbb{Z}_{\geq 0} \) becomes a semigroup as follows: for all \( n', n'' \in \mathbb{Z}_{\geq 0} \), \( n' \ast n'' = n' + q^{d^p(n')} n'' \). We prove the following.

**Lemma 3.1.** For all \( n', n'' \in \mathbb{Z}_{\geq 0} \),
\[
F_m(u_{n' \ast n''}) \equiv F_{m'}(u_{n'}) \times F_{m''}(u_{n''}) \pmod{m},
\]
where \( m', m'' \) are nonnegative integers defined by \( m = m' + q^{d^p(n')} m'' \).

**Proof.** Let \( n', n'' \) be nonnegative integers, and write \( n = n' + n'' = \sum_i n_i q^i \), where
\[
n_i = \begin{cases} n_i' & \text{if } 0 \leq i < d^p(n') \\ n_i'' - d^p(n') & \text{if } d^p(n') \leq i \leq d^p(n') + d^p(n'') - 1. \end{cases}
\]

Then it follows from Corollary 2.2 that
\[
F_m(u_{n' \ast n''}) = \prod_{i=0}^{\infty} F_{m_i}(u_{n_i}) \equiv \left( \prod_{i=0}^{d^p(n')-1} F_{m_i}(u_{n_i'}) \right) \times \left( \prod_{i=d^p(n')}^{d^p(n') + d^p(n'') - 1} F_{m_j}(u_{n_i''}) \right) \pmod{m},
\]
where \( n' = \sum_i n_i' q^i \) and \( n'' = \sum_i n_i'' q^i \) are the \( q \)-adic expansions of \( n' \) and \( n'' \), respectively.

\[\square\]
Conversely, for $0 \leq \ell' \leq n'$ and $0 \leq \ell'' \leq n''$, since $\ell' \leq n' < q^{d(n')}$, one can consider $\ell = \ell' + q^{d(n')} \ell''$, and the next result follows immediately from Lemma 3.1.

**Corollary 3.2.**

$$F_{\ell}(u_{n'+n''}) \equiv F_{\ell'}(u_{n'}) \times F_{\ell''}(u_{n''}) \pmod{m}.$$  

We now prove the main lemma in this paper.

**Lemma 3.3.** Let $n \in \mathbb{Z}$. Then, for all $n', n'' \in \mathbb{Z}_{\geq 0}$, the set

$$\bigcup_{j=0}^{q-2} E_j(u_{n'}) \times E_{n-j}(u_{n''})$$

is in bijection with $E_n(u_{n'+n''})$.

**Proof.** We define a mapping $\psi : \bigcup_{j=0}^{q-2} E_j(u_{n'}) \times E_{n-j}(u_{n''}) \to E_n(u_{n'+n''})$ as follows. For a pair $(\ell', \ell'') \in E_j(u_{n'}) \times E_{n-j}(u_{n''})$ for some $0 \leq j \leq q - 2$, on letting $\ell = \ell' + q^{d(n')} \ell''$, we deduce from Corollary 3.2 that

$$F_{\ell}(u_{n'+n''}) \equiv F_{\ell'}(u_{n'}) \times F_{\ell''}(u_{n''}) \pmod{m}$$

$$\equiv \varphi^j \varphi^{n-j} \pmod{m}$$

$$\equiv \varphi^n \pmod{m},$$

which implies that $\ell \in E_n(u_{n'+n''})$. Set

$$(\ell', \ell'') = \ell.$$

We first verify that $\psi$ is surjective. Indeed, for an integer $\ell \in E_n(u_{n'+n''})$, let $\ell', \ell''$ be the unique nonnegative integers such that $\ell = \ell' + q^{d(n')} \ell''$. It is easy to see that $0 \leq \ell' \leq n'$ and $0 \leq \ell'' \leq n''$. By Lemma 3.1, $F_{\ell'}(u_{n'}) \times F_{\ell''}(u_{n''}) \equiv F_{\ell}(u_{n'+n''}) \equiv \varphi^n \pmod{m}$, which implies that $F_{\ell'}(u_{n'}) \equiv \varphi^j \pmod{m}$ and $F_{\ell''}(u_{n''}) \equiv \varphi^{n-j} \pmod{m}$ for some $0 \leq j \leq q - 2$ since $(V/m)^\times$ is the multiplicative cyclic group of order $q - 1$. Thus $(\ell', \ell'') \in E_j(u_{n'}) \times E_{n-j}(u_{n''})$, and therefore $\psi$ is surjective.

We now show that $\psi$ is injective. Suppose that $\psi(\ell', \ell'') = \psi(m', m'')$ for some $(\ell', \ell''), (m', m'') \in \bigcup_{j=0}^{q-2} E_j(u_{n'}) \times E_{n-j}(u_{n''})$, and thus $\ell' + q^{d(n')} \ell'' = m' + q^{d(n')} m''$. Without loss of generality, suppose that $\ell' \geq m'$. Therefore

$$\ell' - m' = q^{d(n')} (m'' - \ell'') \geq 0.$$

If $\ell' > m'$, then $m'' - \ell'' > 0$. Since $\ell', m' \leq n'$, $q^{d(n')} \leq \ell' - m' < q^{d(n')}$, a contradiction. Thus $\ell' = m'$ and hence $\ell'' = m''$, which proves that $\psi$ is injective. Therefore the lemma follows immediately.

Since $\epsilon_j(u_n) = \text{card}(E_j(n))$, the following result follows immediately from Lemma 3.3.

**Corollary 3.4.**

$$\epsilon_n(u_{n'+n''}) = \sum_{j=0}^{q-2} \epsilon_j(u_{n'}) \epsilon_{n-j}(u_{n''}).$$

Let $(\epsilon_j(u_n))_{j \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 0}}$ be the double sequence, where $\epsilon_j(u_n) = \text{card}(E_j(n))$. We are interested in computing the generating function for $(\epsilon_j(u_n))_{j \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 0}}$, which signifies the distribution of $F_m(u_n)$ modulo $m$ for $0 \leq m \leq n$. Since the constant $\epsilon_j(u_n)$ counts how many integers between 0 and $n$ for which the value $F_m(u_n)$ is congruent to $\varphi^j$ modulo $m$, we only need to compute the values $\epsilon_j(u_n)$ for $0 \leq j \leq q - 2$.

For each integer $n \geq 0$, let $G_n(x) \in \mathbb{Z}[x]$ be the polynomial defined by

$$G_n(x) = \sum_{j=0}^{q-2} \epsilon_j(u_n) x^j.$$
It follows from the definition of $\epsilon_j(n)$ that $G_0(x) = 1$. For each integer $n \geq 0$, the polynomial $G_n(x)$ is called the generating polynomial for the sequence $(\epsilon_j(u_n))_{j \in \mathbb{Z}}$.

In order to state the main theorem in this paper, we introduce a finite set of non-negative integers $\{e_j(n)\}_{0 \leq j \leq q-1}$ as follows.

For $n = 0$, define $e_0(0) = 1$ and $e_j(0) = 0$ for $1 \leq j \leq q - 1$. If $n > 0$, write $n$ in the $q$-adic expansion of the form $n = \sum_{i=1}^{r} n_i q^i$ for some $r \geq 0$, where the $n_i$ are in $\{0, \ldots, q - 1\}$, and $n_r > 0$. For each $0 \leq j \leq q - 1$, we define $e_j(n)$ to be the number of times the integer $j$ occurs in the set $\{n_0, n_1, \ldots, n_r\}$.

We now prove our main theorem which can be viewed as an analogue of the Garfield–Wilf theorem for discrete valuation domains.

**Theorem 3.5.** We maintain the same notation as above. Then for any $n \in \mathbb{Z}_{\geq 0}$,

$$G_n(x) \equiv \prod_{j=0}^{q-1} G_j(x)^{e_j(n)} \pmod{(x^{q-1} - 1)}.$$

**Proof.** Let $\mathcal{W}$ be the semigroup $\mathbb{Z}[x]/(x^{q-1} - 1)[x]$ equipped with the multiplication of polynomials modulo $(x^{q-1} - 1)$. Every element in $\mathcal{W}$ can be represented by a polynomial in $\mathbb{Z}[x]$ of degree $q - 2$.

For each $n \in \mathbb{Z}_{\geq 0}$, set $\Gamma(n) = G_n(x) \pmod{x^{q-1} - 1}$, i.e., $\Gamma : \mathbb{Z}_{\geq 0} \rightarrow \mathcal{W}$ be the mapping from the semigroup $\mathbb{Z}_{\geq 0}$ to the semigroup $\mathcal{W}$ defined by

$$\Gamma(n) = G_n(x) = \sum_{m=0}^{q-2} \epsilon_m(u_n)x^m \pmod{x^{q-1} - 1}, \quad n \in \mathbb{Z}_{\geq 0}.$$

We claim that $\Gamma$ is a semigroup homomorphism, i.e., $\Gamma(n' \ast n'') = \Gamma(n') \Gamma(n'')$ for any $n', n'' \in \mathbb{Z}_{\geq 0}$. Indeed, by Corollary 3.4,

$$\Gamma(n' \ast n'') = \sum_{m=0}^{q-2} \epsilon_m(u_{n' \ast n''})x^m = \sum_{m=0}^{q-2} \sum_{j=0}^{q-2} \epsilon_j(u_{n''}) \epsilon_{m-j}(u_{n'}) x^m.$$

By the definition of $(\epsilon_j(u_n))_{j \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 0}}$, it is easy to see that for a fixed integer $n \geq 0$, $\epsilon_j(u_n)$ is periodic of period $q - 1$ with respect to the index $j$ (since the group $(\mathcal{V}/m)^	imes$ is of order $q - 1$). Hence,

$$\epsilon_{m-j}(u_{n''}) = \epsilon_{q-1+(m-j)}(u_{n''}).$$

Since $x^{q-1+m} \equiv x^m \pmod{x^{q-1} - 1}$,

$$\Gamma(n' \ast n'') = \sum_{m=0}^{q-2} \sum_{j=0}^{q-2} \epsilon_j(u_{n''}) \epsilon_{q-1+(m-j)}(u_{n'}) x^{q-1+m} \equiv \sum_{j=0}^{q-2} \epsilon_j(u_{n''}) x^j \left( \sum_{m=0}^{q-2} \epsilon_{q-1+m-j}(u_{n'}) x^{q-1+m-j} \right) \pmod{x^{q-1} - 1},$$

(5)

where for each $0 \leq j \leq q - 2$,

$$A(j) = \sum_{m=0}^{q-2} \epsilon_{q-1+m-j}(u_{n'}) x^{q-1+m-j}.$$
We contend that
\[ A(j) \equiv A(j + 1) \pmod{x^{q-1} - 1}, \quad \text{for each } 0 \leq j \leq q - 3. \]

Indeed, one sees from (6) that
\[
A(j + 1) = \sum_{m=0}^{q-2} \epsilon_{q-1+(m-1)}(u_{n''})x^{q-1+m-(j+1)} \\
= \epsilon_{q-2-j}(u_{n''})x^{q-2-j} + \sum_{m=1}^{q-2} \epsilon_{q-1+(m-1)-j}(u_{n''})x^{q-1+(m-1)-j} \\
= \epsilon_{q-2-j}(u_{n''})x^{q-2-j} + \sum_{m=0}^{q-3} \epsilon_{q-1+j}(u_{n''})x^{q-1+m-j} \\
= \left( A(j) - \epsilon_{q-1+(q-2)-j}(u_{n''})x^{q-1+(q-2)-j} \right) + \epsilon_{q-2-j}(u_{n''})x^{q-2-j} \\
\equiv A(j) \pmod{x^{q-1} - 1} \quad \text{(since } (2q - 3 - j) - (q - 2 - j) = q - 1). \]

Thus \( A(j + 1) \equiv A(j) \pmod{x^{q-1} - 1} \) for every \( 0 \leq j \leq q - 3 \), and thus by induction, \( A(j) \equiv A(0) \pmod{x^{q-1} - 1} \) for all \( 0 \leq j \leq q - 2 \). It follows from (5) that
\[
\Gamma(n' + n'') \equiv \Gamma(n')A(0) \\
\equiv \Gamma(n') \sum_{m=0}^{q-2} \epsilon_{q-1+m}(u_{n''})x^{q-1+m} \\
\equiv \Gamma(n') \sum_{m=0}^{q-2} \epsilon_{m}(u_{n''})x^{m} \\
\equiv \Gamma(n') \Gamma(n'') \pmod{x^{q-1} - 1},
\]

and thus \( \Gamma \) is a semigroup homomorphism.

We are now ready to prove the theorem. The case \( n = 0 \) is trivially true. If \( n > 0 \), write \( n \) in the \( q \)-adic expansion of the form \( n = \sum_{i=0}^{r} n_i q^i \) for some \( r \in \mathbb{Z}_{\geq 0} \), where \( n_r > 0 \), and the \( n_i \) are in the finite set \( \{0, \ldots, q-1\} \). Thus
\[
\Gamma(n) = \Gamma(n_0 \ast n_1 \ast \cdots \ast n_r) = \Gamma(n_0) \cdots \Gamma(n_r),
\]

and it therefore follows from the definition of \( e_j(n) \) that
\[
G_n(x) \equiv G_{n_0}(x) \cdots G_{n_r}(x) \\
\equiv \prod_{i=0}^{q-1} G_j(x)^{e_i(n)} \pmod{x^{q-1} - 1}.
\]

\[\square\]

**Acknowledgements**

I am very grateful to the reviewer who provided a very detailed report that contains several great suggestions and comments, and that greatly helps shorten the paper and simplify many obscure points in the paper. I would particularly like to thank the reviewer very much for his/her important suggestion that I should work with a semigroup structure of \( \mathbb{Z}_{\geq 0} \) instead of the semigroup formed by the words on the alphabet \( R \).
REFERENCES


Department of Applied and Computational Mathematics and Statistics, University of Notre Dame, Notre Dame, Indiana 46556, USA

Email address: dongquan.ngoc.nguyen@nd.edu

URL: http://nd.edu/~dnguye15