CARLETON UNIVERSITY

SCHOOL OF
MATHEMATICS AND STATISTICS

HONOURS PROJECT

TITLE: Counting Monic Polynomials over a Finite Field with Prescribed Degree, First Consecutive Coefficients, and Factorization

AUTHOR: Simon Kuttner

SUPERVISOR: Qiang Wang

DATE: May 4th, 2021

Counting Monic Polynomials over a Finite Field with Prescribed Degree, First Consecutive Coefficients, and Factorization

Simon Kuttner

May 4, 2021

Abstract

We use generating functions over group rings to count degree m monic polynomials over a finite field with fixed numbers of irreducible factors from different degrees when the first few coefficients are prescribed. Our method extends from the techniques used in [6, 7] to count degree m monic irreducible polynomials with prescribed coefficients. We obtain explicit formulas for the number of degree m monic polynomials with a given distribution of irreducible factors from different degrees when the first coefficient is prescribed. As a corollary, we obtain exact results for the number of degree m n-smooth monic with the first coefficient fixed.

Contents

1 Introduction

Let p and e be positive integers where p is prime. Let $\mathbb{F}_q$ be a finite field with $q = p^e$ elements. Let $\mathbb{F}_q[x]$ denote the set of polynomials over $\mathbb{F}_q$. Let M denote the set of monic polynomials over $\mathbb{F}_q$, and I denote the subset of these polynomials that are irreducible. For each positive integer d, let M_d denote the set of degree d monic polynomials over $\mathbb{F}_q$, and let I_d be the subset of these polynomials that are irreducible.

For monic polynomials f, let $d(f)$ denote the degree of f, let $r_i(f)$ denote the number of monic distinct degree i irreducible factors of f, and $l_i(f)$ denote the number of monic degree i irreducible factors of f counting multiplicity.

For a monic polynomial f, write

$$f(x) = x^{d(f)} + f_1 x^{d(f)-1} + \cdots + f_{d(f)}, \tag{1}$$

and set $f_j = 0$ if $j > d(f)$.

For $f \in M$ and $w \geq 0$, define

$$\begin{aligned} \langle f \rangle_w &= x^{d(f)} f(1/x) \pmod{x^{w+1}} \\ &= 1 + f_1 x + \cdots + f_w x^w \pmod{x^{w+1}}. \end{aligned} \tag{2}$$

In this project, we want to determine the number of degree m monic polynomials $f(x)$ with prescribed coefficients $f_1, \ldots, f_w$ and a given distribution of irreducible factors with different degrees, which is an important research problem in the theory of finite fields. First of all, we introduce the following definitions.

Definition 1 *Let us fix $w \geq 0$ and a finite set $T \subset \mathbb{N}$.*

- *Define* $N(m, \prod_{i \in T} I_i^{r_i}, \langle f \rangle_w)$ *as the number of degree* m *monic polynomials* g *over* $\mathbb{F}_q$ *with* $\langle g \rangle_w = \langle f \rangle_w$*, where* g *has* r_i *monic distinct degree* i *irreducible factors for each* $i \in T$*.*

- *Define* $N^*(m, \prod_{i \in T} I_i^{l_i}, \langle f \rangle_w)$ *as the number of degree* m *monic polynomials* g *over* $\mathbb{F}_q$ *with* $\langle g \rangle_w = \langle f \rangle_w$*, where* g *has* l_i *monic degree* i *irreducible factors counting multiplicity for each* $i \in T$*.*

The problem of counting monic irreducible degree m polynomials f over a finite field $\mathbb{F}_q$ with fixed coefficients $f_1, \ldots, f_w$ is a well studied subclass of our general problem. Let $I_m(\langle f \rangle_w)$ be the number of degree m monic irreducible polynomials g over $\mathbb{F}_q$, where $\langle g \rangle_w = \langle f \rangle_w$. Then

$$I_m(\langle f \rangle_w) = N^*(m, I_m^1, \langle f \rangle_w). \tag{3}$$

For typographic convenience, we omit the subscript of w, when the value of w is fixed.

If $w = 0$, for any monic polynomial f, we have $\langle f \rangle = 1 \pmod{x} = \langle 1 \rangle$. Thus, $I_m(\langle f \rangle) = |I_m|$, which is the total number of degree m monic irreducible polynomials over $\mathbb{F}_q$. This formula is known (see [12]) and is given by

$$|I_m| = \frac{1}{m} \sum_{k|m} \mu(k) q^{m/k}, \tag{4}$$

where μ is the möbius function, defined on the set of positive integers by $\mu(1) = 1$, $\mu(k) = 0$ if $k > 1$ and k has no repeated prime factors, and $\mu(k) = (-1)^r$ if $k = p_1 \cdots p_r$ for distinct primes $p_1, \ldots, p_r$.

The results for $w = 1$ can be found in [18, 19]. In this case, for each monic polynomial f, we have $\langle f \rangle = 1 + \alpha x \pmod{x^2} = \langle x + \alpha \rangle$ for some unique

$\alpha \in \mathbb{F}_q$. For $m \geq 1$, $I_m(\langle x+\alpha \rangle)$ counts the number of monic irreducible polynomials of the form $x^m + \alpha x^{m-1} + g(x)$ where $\alpha \in \mathbb{F}_q$ is fixed and $g(x) \in \mathbb{F}_q[x]$ is a polynomial of degree $m-2$ which is allowed to vary. When m is a multiple of p, the formula for $I_m(\langle x+\alpha \rangle)$ depends on whether $\alpha = 0$ or not. For convenience, we use the notation $[\![P]\!]$ to be equal to 1 if P is true and 0 otherwise. With this notation, we have $I_m(\langle x+\alpha \rangle) = a_m + b_m [\![\alpha = 0]\!]$, where

$$a_m = \frac{1}{mq} \sum_{p \nmid k \mid m} \mu(k) q^{m/k}, \text{ and } \; b_m = \frac{1}{m} \sum_{p \nmid k \mid m} \mu(k) q^{m/k}. \tag{5}$$

If $p \nmid m$, then for all $\alpha \in \mathbb{F}_q$, we have

$$I_m(\langle x+\alpha \rangle) = \frac{|I_m|}{q} = \frac{1}{mq} \sum_{k \mid m} \mu(k) q^{m/k}.$$

Formulas for $I_m(\langle f \rangle)$ exist for $w = 2$ (see [14]), and also for $w = 3$, when $q = 2$ (see [5]). Formulas for $I_m(\langle f \rangle)$ for are derived in [7], which is a paper in progress, using the generating functions method over group rings in some other cases including $q = 2$ and $w = 4$.

Another special case of the general problem of computing N and N^* is determining the number of monic polynomials $f(x)$ with prescribed coefficients $f_1, \ldots, f_w$ and a given number of distinct linear factors, or linear factors counting multiplicity. For $m \geq w$, $N(m, I_1^r, \langle f \rangle_w)$ counts the number of degree m polynomials of the form $x^m + f_1 x^{m-1} + \cdots + f_w x^{m-w} + g(x)$ with r distinct linear factors, where $f_1, \ldots, f_w \in \mathbb{F}_q$ are fixed, and $g(x) \in \mathbb{F}_q[x]$ is a polynomial of degree at most $m-w$ that varies.

This number is important and well studied due to its applications in Reed-Solomon codes. In general, if we write $\mathbb{F}_q = \{x_1, \ldots, x_q\}$, then a codeword

in a Reed Solomon code of dimension k and length q is of the form $F = (f(x_1), \ldots, f(x_q)) \in \mathbb{F}_q^q$, where $f(x)$ is a polynomial of degree at most $k-1$ over $\mathbb{F}_q$.

In general, a vector $V \in \mathbb{F}_q^q$ can be written as $(v(x_1), \ldots, v(x_q))$ for some unique polynomial $v(x)$ of degree at most $q-1$, with the Lagrange Interpolation formula. The distance between V and a codeword F is the number of non-zero components in the vector $V - F$, which is equal to the number of roots of the polynomial $v(x) - f(x)$.

An important problem in decoding messages in Reed-Solomon codes is to determine the number of codewords at a given distance of a received word. Suppose in the above example that the word V is received, and the polynomial $v(x)$ is a polynomial of degree $k+w$ for $w \geq 0$. Suppose without loss of generality that $v(x)$ is monic. Then the number of codewords of distance $q-r$ from the received word V is the number of polynomials f, not necessarily monic, of degree at most $k-1$ where $v(x) - f(x)$ has exactly r distinct roots. Writing $v(x) = x^{k+w} + v_1 x^{k+w-1} + \cdots + v_w x^k + c(x)$, for $v_1, \ldots, v_k \in \mathbb{F}_q$ and $c(x) \in \mathbb{F}_q[x]$ has degree at most $k-1$. The number of codewords at distance $q-r$ from V is the number of monic polynomials $v(x) - f(x)$ where f runs through all polynomials of degree at most $k-1$, and $v(x) - f(x)$ has r distinct roots in $\mathbb{F}_q$, which is equal to $N(k+w, I_1^r, \langle v \rangle_w)$.

Both numbers $N(m, I_1^r, \langle f \rangle_w)$ and $N^*(m, I_1^l, \langle f \rangle_w)$ are studied in [8] when $w = 0$ in order to obtain the distribution of zeros of a random monic polynomial of degree m, with and without multiplicity counted. When $w = 0$, for all monic polynomials f, we have $\langle f \rangle_w = 1 \pmod{x}$, so dropping the subscript of w and the modulo operation, we write $\langle f \rangle = 1$ for all $f \in M$. It

is shown in [8] that the number of degree m monic polynomials over $\mathbb{F}_q$ with l linear factors counting multiplicity is

$$N^*(m, I_1^l, 1) = q^{m-l}\binom{q+l-1}{l}\sum_{j=0}^{m-l}\binom{q}{j}(-1)^j q^{-j}.$$

If $m \geq q + l$, then the formula simplifies to

$$N^*(m, I_1^l, 1) = q^{m-l}\binom{q+l-1}{l}(1-1/q)^q.$$

The number of degree m monic polynomials over $\mathbb{F}_q$ with r distinct linear factors is also given in [8]. This number is

$$N(m, I_1^r, 1) = q^{m-r}\binom{q}{r}\sum_{j=0}^{m-r} q^{-j}\binom{q-r}{j}(-1)^j.$$

If $m \geq q$, this number becomes

$$N(m, I_1^r, 1) = q^{m-r}\binom{q}{r}(1-1/q)^{q-r}.$$

The problem of counting the number of degree m monic polynomials $f(x)$ with a given number of distinct roots has been extended in recent years to allow for prescribing coefficients $f_1, \ldots, f_w$, where $w \geq 0$ is arbitrary due to applications in Reed-Solomon codes (see [11, 20]). For the case $w = 1$, Zhou et al. [20] studied the number of degree $m \geq 1$ polynomials over $\mathbb{F}_q$ with r distinct roots of the form $x^m + \alpha x^{m-1} + g(x)$, where $\alpha \in \mathbb{F}_q$ is fixed, and $g(x) \in \mathbb{F}_q[x]$ is a varying polynomial of degree at most $m-2$. If $p \nmid m$, then the number is

$$N(m, I_1^r, \langle x+\alpha \rangle) = q^{m-r-1}\binom{q}{r}\sum_{j=0}^{m-r} q^{-j}\binom{q-r}{j}(-1)^j.$$

If $p \mid m$, then the number is

$$N(m, I_1^r, \langle x+\alpha \rangle) = q^{m-r-1}\binom{q}{r}\sum_{j=0}^{m-r} q^{-j}\binom{q-r}{j}(-1)^j + \frac{v(\alpha)}{q}\binom{q/p}{m/p}\binom{m}{r}(-1)^{m/p-r},$$

where $v(\alpha) = q[\![\alpha = 0]\!] - 1$.

Exact and more complicated expressions are obtained in [20] for the number of monic degree $m \geq 2$ polynomials with r distinct linear factors over $\mathbb{F}_q$ of the form $x^m + g(x)$ where $g(x) \in \mathbb{F}_q[x]$ is a varying polynomial of degree at most $m-3$. More recently, in [11], an asymptotic bound on the number of degree $m \geq w$ polynomials with r distinct linear factors over $\mathbb{F}_q$ of the form $x^m + b_1 x^{m-1} + \cdots + b_w x^{m-w} + g(x)$, for fixed $b_1, \ldots, b_w \in \mathbb{F}_q$, and varied $g(x) \in \mathbb{F}_q[x]$ is obtained for $m < q$. The arguments used in [11] can be extended to the case $m \geq q$ as well, in which case, simple explicit expressions can be obtained if $m \geq q + w$.

Degree m monic polynomials with a given number of irreducible factors of a specific degree with or without counting the multiplicity have been counted in [9] using ordinary generating functions. The number of degree m monic polynomials over $\mathbb{F}_q$ with r distinct degree i irreducible factors is

$$\begin{aligned} N(m, {I_i}^r, 1) &= q^{m-ir}\binom{|I_i|}{r}\sum_{j=0}^{\lfloor m/i \rfloor - r} q^{-ij}\binom{|I_i|-r}{j}(-1)^j \\ &= q^{m-ir}\binom{|I_i|}{r}(1-1/q^i)^{|I_i|-r} \text{ if } m \geq i|I_i|. \end{aligned}$$

Also, the number of degree m monic polynomials over $\mathbb{F}_q$ with l degree i

irreducible factors counting multiplicity is

$$N^*(m, I_i^l, 1) = q^{m-il}\binom{|I_i|+l-1}{l}\sum_{j=0}^{\lfloor m/i\rfloor - l}\binom{|I_i|}{j}(-1)^j q^{-ij}$$
$$= q^{m-il}\binom{|I_i|+l-1}{l}(1-1/q^i)^{|I_i|}. \text{ if } m \geq i(|I_i|+l).$$

Polynomials whose irreducible factors are all of degree at most n are called n-smooth and they have applications in security. The number of n-smooth polynomials of degree m over $\mathbb{F}_q$ has already been considered first by Odlyzko [16] who provided an asymptotic estimate when $m \to \infty$ for the case $q = 2$ and $m^{1/100} < n < m^{99/100}$ using the saddle point method. This generalizes to any prime power q; see [13]. For n large with respect to m, typically $n > cm(\log\log m)/\log m$, Car [2] has given an asymptotic expression for this number in terms of the Dickman function. Panario, Gourdon and Flajolet [17] extended this range to $n > (1+\epsilon)(\log m)^{1/k}$, for a positive integer constant k.

In this project, we adapt the general method of counting irreducible polynomials with prescribed coefficients as described in [6, 7], to count polynomials with prescribed coefficients and factorization type. In [6], generating functions over group rings were used to count degree m monic irreducible polynomials when the first and last terms are fixed. In [7], the method has been extended to the more general situation where the first few and last few consecutive coefficients are fixed.

Here, we adapt the method to allow for irreducible factors of different degrees. More specifically, we derive general expressions for N and N^* from the generating functions over group rings for any fixed $w \geq 0$ and finite set $T \subset \mathbb{N}$. These general expressions for N and N^* are provided in Theorems 1

and 2. These expressions have many corollaries that extend on known results.

We first focus on the case where the degree m of the polynomials is large compared to the degrees of the prescribed irreducible factors and the number of prescribed coefficients w. When the polynomial degree is large enough, we obtain simple general results for N and N^* (see Theorems 3 and 4). These results extend on formulas from papers such as [8, 9], by allowing for prescribed coefficients when m is large. Although m is too large to apply to coding-theory applications such as Reed-Solomon codes, we obtain new information on the distribution of monic polynomials with prescribed coefficients and factorization type.

Then we focus on the cases when $w = 0$ or $w = 1$, and thus obtain exact formulas for N and N^* in those cases. When $w = 0$, we simplify our formulas for N and N^* and recover several known results. We also find two different exact formulas for the number of monic n-smooth polynomials of degree m (see Corollaries 9 and 12), which we verify directly using the setup from [17]. When $w = 1$, we repeat a similar procedure to the case $w = 0$. The main difference between the two cases is that the case $w = 1$ is mostly new, and the manipulations involved when $w = 1$ are much more technical than the case $w = 0$. Simplifying the general expressions for N and N^* when $w = 1$, we obtain two different exact formulas for the number of n-smooth polynomials of degree m of the form $x^m + \alpha x^{m-1} + g(x)$ where g is a polynomial of degree at most $m-2$ (Corollary 15 and Corollary 19). Extending the setup from [17] by keeping track of the prescribed coefficient α, we verify that these formulas are equivalent.

The project is organized as follows. In Section 2 we provide background

definitions and preliminary results. In Section 3 we demonstrate the generating functions method over group rings to count irreducible polynomials with prescribed coefficients. Then in Section 4 we develop the general results on counting polynomials with prescribed coefficients and prescribed factorization pattern. We further demonstrate our general methodology in different special cases such as large degree, $w = 0$, and $w = 1$ respectively. These results can be found in Sections 5, 6, 7 respectively.

2 Definitions and Notations

A general combinatorial framework for counting irreducible polynomials with prescribed coefficients, using generating functions with coefficients from a group algebra, was developed in Section 2 of [7]. We review the notations and details.

First, we fix $w \geq 0$. For $f \in M$, write $f = x^{d(f)} + f_1 x^{d(f)-1} + \cdots + f_{d(f)}$, and set $f_j = 0$ if $j > d(f)$. According to the definition of $\langle f \rangle$, we have

$$\begin{aligned} \langle f \rangle &= x^{d(f)} f(1/x) \pmod{x^{w+1}} \\ &= 1 + f_1 x + \cdots + f_w x^w \pmod{x^{w+1}} \\ &= \langle x^w + f_1 x^{w-1} + \cdots + f_w \rangle. \end{aligned}$$

Fix $f \in M$ and $d \geq w$. Recall that M_d is the set of monic polynomials of degree d. For $g \in M_d$, $\langle g \rangle = \langle f \rangle$ if and only if $g = x^d + f_1 x^{d-1} + \cdots + f_w x^{d-w} + c(x)$ for some $c(x) \in \mathbb{F}_q[x]$ of degree at most $d - w - 1$. Therefore, there are q^{d-w} monic polynomials $g \in M_d$ that satisfy $\langle g \rangle = \langle f \rangle$. For convenience, define

$$G = \{\langle f \rangle : f \in M\} = \{\langle x^w + f_1 x^{w-1} + \cdots + f_w \rangle : f_1, \ldots, f_w \in \mathbb{F}_q\}. \quad (6)$$

Note that $|G| = q^w$. Moreover, for each $\langle f \rangle \in G$ and $d \geq w$, there are q^{d-w} monic polynomials $g \in M_d$ that satisfy $\langle g \rangle = \langle f \rangle$.

Proposition 1 (Proposition 1 [7]) *G is an abelian group under multiplication $\langle f \rangle \langle g \rangle = \langle fg \rangle$ with identity $\langle 1 \rangle$.*

Proof

We first verify that G is closed under the operation. For $f, g \in M$,

$$\begin{aligned}\langle f\rangle\langle g\rangle &= x^{d(f)} f(1/x) x^{d(g)} g(1/x) \pmod{x^{w+1}} \\ &= x^{d(f)+d(g)} fg(1/x) \pmod{x^{w+1}} \\ &= x^{d(fg)} fg(1/x) \pmod{x^{w+1}} \\ &= \langle fg\rangle.\end{aligned}$$

Using the fact that M is a commutative monoid with identity 1 and for $f, g \in M$, $\langle f\rangle\langle g\rangle = \langle fg\rangle$, we have that G is a commutative monoid with identity $\langle 1\rangle$.

For $f \in M$, $\langle f\rangle = 1 + f_1 x + \cdots + f_w x^w \pmod{x^{w+1}}$. Noting that $x \nmid 1 + f_1 x + \cdots + f_w x^w$, we have

$$\gcd(x^{k+1}, 1 + f_1 x + \cdots + f_w x^w) = 1.$$

Hence, there exists $g_0 + g_1 x + \cdots + g_w x^w$ where

$$(1 + f_1 x + \cdots + f_w x^w)(g_0 + g_1 x + \cdots + g_w x^w) \equiv 1 \pmod{x^{w+1}}.$$

It follows that $g_0 = 1 * g_0 = 1$. Let $g = x^w + g_1 x^{w+1} + \cdots + g_w \in M$. We have

$$\begin{aligned}\langle f\rangle\langle g\rangle &= (1 + f_1 x + \cdots + f_w x^w)(1 + g_1 x + \cdots + g_w x^w) \pmod{x^{w+1}} \\ &= (1 + f_1 x + \cdots + f_w x^w)(g_0 + g_1 x + \cdots + g x^w) \pmod{x^{w+1}} \\ &= 1 \pmod{x^{w+1}} \\ &= \langle 1\rangle.\end{aligned}$$

Hence, $\langle g\rangle$ is the multiplicative inverse of $\langle f\rangle$ in G. ∎

In order to make use of the group G, we introduce the notion of a group ring.

Definition 2 *Define* $\mathbb{C}[G]$ *to be the commutative ring of formal* $\mathbb{C}$*-linear combinations of elements of* G*. For convenience, write* 0 *as the additive identity of* $\mathbb{C}[G]$ *and* $1 = \langle 1 \rangle$ *as the multiplicative identity of* $\mathbb{C}[G]$*. The elements of* $\mathbb{C}[G]$ *are of the form*

$$v = \sum_{\langle f \rangle \in G} v_{\langle f \rangle} \langle f \rangle,$$

where $v_{\langle f \rangle} \in \mathbb{C}$*. For* $a = \sum_{\langle f \rangle \in G} a_{\langle f \rangle} \langle f \rangle, b = \sum_{\langle f \rangle \in G} b_{\langle f \rangle} \langle f \rangle \in \mathbb{C}[G]$*, define*

$$a + b = \sum_{\langle f \rangle \in G} (a_{\langle f \rangle} + b_{\langle f \rangle}) \langle f \rangle, \tag{7}$$

$$ab = \sum_{\langle f \rangle \in G} \sum_{\langle g \rangle \in G} a_{\langle g \rangle} b_{\langle f \rangle \langle g \rangle^{-1}} \langle f \rangle. \tag{8}$$

To help with counting, we introduce the following definition.

Definition 3 *Define*

$$E = \frac{1}{q^w} \sum_{\langle f \rangle \in G} \langle f \rangle, \tag{9}$$

$$J = 1 - E. \tag{10}$$

It is straightforward to verify that E and J are orthogonal idempotents.

Proposition 2 *The following properties of* E *and* J *hold:*

1) $E\langle g \rangle = E$ *for any* $\langle g \rangle \in G$*.*

2) $E^2 = E$*.*

3) $EJ = 0$*.*

4) $J^2 = J$*.*

Proof 1) Let $\langle g\rangle \in G$. For $\langle h\rangle \in G$, there exists a unique $\langle f\rangle \in G$ with $\langle f\rangle\langle g\rangle = \langle h\rangle$, Therefore,

$$E\langle g\rangle = \frac{1}{q^w}\sum_{\langle f\rangle\in G}\langle f\rangle\langle g\rangle = \frac{1}{q^w}\sum_{\langle h\rangle\in G}\langle h\rangle = E.$$

2) Using $|G| = q^w$, we have

$$E^2 = E\frac{1}{q^w}\sum_{\langle f\rangle\in G}\langle f\rangle = \frac{1}{q^w}\sum_{\langle f\rangle\in G}E\langle f\rangle = \frac{1}{q^w}\sum_{\langle f\rangle\in G}E = E.$$

3) $EJ = E(1-E) = E - E^2 = E - E = 0$.

4) $J^2 = (1-E)J = J - EJ = J - 0 = J$. ∎

We now derive more useful facts for doing computations in $\mathbb{C}[G]$.

Proposition 3 *The following properties hold:*

1) $E\sum_{f\in M_d}\langle f\rangle = q^d E$.

2) $\sum_{f\in M_d}\langle f\rangle = q^d E$ *for* $d \geq w$.

3) $J\sum_{f\in M_d}\langle f\rangle = 0$ *for* $d \geq w$.

Proof 1) For $f \in M_d$, $\langle f\rangle \in G$. From $|M_d| = q^d$ and Proposition 2, we obtain

$$E\sum_{f\in M_d}\langle f\rangle = \sum_{f\in M_d}E\langle f\rangle = \sum_{f\in M_d}E = q^d E.$$

2) Suppose $d \geq w$. For $\langle g\rangle \in G$, there are q^{d-w} polynomials $\langle f\rangle \in M_d$ such that $\langle f\rangle = \langle g\rangle$. From the definition of E, it follows that

$$\sum_{f\in M_d}\langle f\rangle = q^{d-w}\sum_{\langle h\rangle\in G}\langle h\rangle = q^d E.$$

3) Suppose $d \geq w$. Then using $EJ = 0$, we have

$$J\sum_{f\in M_d}\langle f\rangle = q^d EJ = 0.$$ ∎

Formal power series over the group ring $\mathbb{C}[G]$ are an important tool for counting polynomials. As such, the following proposition is useful.

Proposition 4 *Suppose $A(z)$ is a formal power series over $\mathbb{C}[G]$. Then we have the following result. 1) $KA(z) = KA(Kz)$ for $K \in \{E, J\}$.*
2) $A(z) = EA(Ez) + JA(Jz)$.

Proof 1) Write $A(z) = \sum_{j\geq 0} a_j z^j$, where $a_j \in \mathbb{C}[G]$. Suppose $K \in \{E, J\}$. Then $K^2 = K$. By induction, $K(K^j) = K$ for each $j \geq 0$, so

$$KA(z) = K\sum_{j\geq 0} a_j z^j = K\sum_{j\geq 0} a_j K^j z^j = KA(Kz).$$

2) $A(z) = EA(z) + JA(z) = EA(Ez) + JA(Jz)$. ∎

3 Counting Monic Irreducible Polynomials

In this section, we demonstrate the generating functions method over group rings to recover some known results about the number of degree m monic irreducible polynomials with the first few coefficients prescribed. In particular, we re-derive the total number of irreducible polynomials, and the number of irreducible polynomials of the form $x^m + \alpha x^{m-1} + g(x)$ where $\alpha \in \mathbb{F}_q$ is fixed, and $g(x) \in \mathbb{F}_q[x]$ of degree at most $m-2$ is varied. Materials in this section can be found in greater generality in [7].

We recall that I is the set of irreducible monic polynomials over $\mathbb{F}_q$. For $d \geq 1$, I_d be the set of degree d polynomials in I. For $f \in M$, $I_d(\langle f \rangle)$ is the number of polynomials $g \in I_d$ with $\langle g \rangle = \langle f \rangle$. Define the generating function (GF)

$$F(z) = \sum_{f \in M} \langle f \rangle z^{d(f)} = 1 + \sum_{d \geq 1} \sum_{f \in M_d} \langle f \rangle z^d. \tag{11}$$

From the unique factorization of polynomials, we have

$$F(z) = \prod_{f \in I} (1 - \langle f \rangle z^{d(f)})^{-1} \tag{12}$$

$$= \prod_{d \geq 1} \prod_{f \in I_d} (1 - \langle f \rangle z^d)^{-1} \tag{13}$$

$$= \prod_{d \geq 1} \prod_{\langle f \rangle \in G} (1 - \langle f \rangle z^d)^{-I_d(\langle f \rangle)}. \tag{14}$$

It follows that

$$\begin{aligned} \ln(F(z)) &= \sum_{d \geq 1} \sum_{f \in G} I_d(\langle f \rangle) \sum_{k \geq 1} \frac{\langle f \rangle^k z^{dk}}{k} \\ &= \sum_{m \geq 1} \sum_{d | m} \sum_{f \in G} \frac{d}{m} I_d(\langle f \rangle) \langle f \rangle^{m/d} z^m. \end{aligned}$$

Let $N(m, \langle f \rangle) = m[\langle f \rangle z^m] \ln(F(z))$. Then

$$N(m, \langle f \rangle) = \sum_{d|m} \sum_{\langle g \rangle \in G} dI_d(\langle g \rangle)[\![\langle g \rangle^{m/d} = \langle f \rangle]\!]. \tag{15}$$

Proposition 5 (Proposition 2 [7])

$$I_m(\langle f \rangle) = \frac{1}{m} \sum_{k|m} \sum_{\langle g \rangle \in G} \mu(k) N(m/k, \langle g \rangle)[\![\langle g \rangle^k = \langle f \rangle]\!]$$

Proof Using the fact that for $m \in \mathbb{N}$,

$$\sum_{d|m} \mu(d) = [\![m = 1]\!],$$

we obtain

$$\begin{aligned}
&\sum_{k|m} \sum_{\langle g \rangle \in G} \mu(k) N(m/k, \langle g \rangle)[\![\langle g \rangle^k = \langle f \rangle]\!] \\
&= \sum_{k|m} \sum_{\langle g \rangle \in G} \mu(k) \sum_{d|k} \sum_{h \in G} dI_d(\langle h \rangle)[\![\langle h \rangle^{m/kd} = \langle g \rangle]\!][\![\langle g \rangle^k = \langle f \rangle]\!] \\
&= \sum_{k|m} \mu(k) \sum_{d|\frac{m}{k}} \sum_{\langle h \rangle \in G} dI_d(\langle h \rangle)[\![\langle h \rangle^{m/d} = \langle f \rangle]\!] \\
&= \sum_{d|m} \sum_{\langle h \rangle \in G} dI_d(\langle h \rangle)[\![\langle h \rangle^{m/d} = \langle f \rangle]\!] \sum_{k|\frac{m}{d}} \mu(k) \\
&= \sum_{d|m} \sum_{\langle h \rangle \in G} dI_d(\langle h \rangle)[\![\langle h \rangle^{m/d} = \langle f \rangle]\!][\![d = m]\!] \\
&= mI_m(\langle f \rangle)
\end{aligned}$$

Dividing by m, we obtain the result. ∎

Next, we give the formula for $N(m, \langle f \rangle)$ in terms of GFs.

Proposition 6 (Lemma 1 [7])

$$N(m, \langle f \rangle) = q^{m-w} + m[\langle f \rangle z^m] J \ln \left(1 + \sum_{d=1}^{w-1} \sum_{f \in M_d} \langle f \rangle z^d \right)$$

Proof Using (11),

$$F(z) = 1 + \sum_{d\geq 1} \sum_{f\in M_d} \langle f\rangle z^d.$$

Since E and J are orthogonal idempotents, we have $1 = E + J$, $E^d = E$, and $J^d = J$. Hence, from Propositions 3 and 4, it follows that

$$\begin{aligned}
\ln(F(z)) &= E\ln(F(Ez)) + J\ln(F(Jz)) \\
&= E\ln\left(1 + \sum_{d\geq 1}\sum_{f\in M_d}\langle f\rangle E^d z^d\right) + J\ln\left(1 + \sum_{d\geq 1}\sum_{f\in M_d}\langle f\rangle J^d z^d\right) \\
&= E\ln\left(1 + \sum_{d\geq 1} q^d E^d z^d\right) + J\ln\left(1 + \sum_{d=1}^{w-1}\sum_{f\in M_d}\langle f\rangle J^d z^d\right) \\
&= E\ln\left(1 + \sum_{d\geq 1} q^d z^d\right) + J\ln\left(1 + \sum_{d=1}^{w-1}\sum_{f\in M_d}\langle f\rangle z^d\right) \\
&= E\ln\left(\frac{1}{1-qz}\right) + J\ln\left(1 + \sum_{d=1}^{w-1}\sum_{f\in M_d}\langle f\rangle z^d\right) \\
&= E\sum_{k\geq 1}\frac{1}{k}q^k z^k + J\ln\left(1 + \sum_{d=1}^{w-1}\sum_{f\in M_d}\langle f\rangle z^d\right).
\end{aligned}$$

Using the definition $E = \frac{1}{q^w}\sum_{\langle f\rangle\in G}\langle f\rangle$ and extracting the coefficient $m[\langle f\rangle z^m]$ from $\ln(F(z))$, the result follows. ∎

For $w = 0, 1$, $N(m, \langle f\rangle) = q^{m-w}$. If $w = 0$, then $G = \{1\}$. In this case, for $f \in M$, $\langle f\rangle = 1$. It follows that

$$|I_m| = I(m, 1) = \frac{1}{m}\sum_{k|m}\mu(k)q^{m/k}.$$

If $w = 1$, then $G = \{1 + \alpha x \pmod{x^2} : \alpha \in \mathbb{F}_q\} = \{\langle x + \alpha\rangle : \alpha \in \mathbb{F}_q\}$.

For $\alpha, \beta \in \mathbb{F}_q$,

$$\begin{aligned}\langle x+\beta\rangle^n &= (1+\beta x)^n \pmod{x^2} \\ &= (1+n\beta x) \pmod{x^2} \\ &= \langle x + n\beta\rangle = \langle x+\alpha\rangle\end{aligned}$$

if and only if $n\beta = \alpha$.

Suppose $\alpha \in \mathbb{F}_q$. Then

$$\#\{\beta \in \mathbb{F}_q : n\beta = \alpha\} = [\![p \nmid n]\!] + q[\![\alpha = 0]\!][\![p \mid n]\!]. \tag{16}$$

It follows that

$$\begin{aligned}I_m(\langle x+\alpha\rangle) &= \frac{1}{m}\sum_{k|m}\sum_{\alpha\in\mathbb{F}_q}\mu(k)q^{m/k-1}[\![\langle x+\beta\rangle^k = \langle x+\alpha\rangle]\!] \\ &= \frac{1}{mq}\sum_{k|m}\sum_{\beta\in\mathbb{F}_q}\mu(k)q^{m/k}[\![k\beta=\alpha]\!] \\ &= \frac{1}{mq}\sum_{p\nmid k|m}\mu(k)q^{m/k} + \frac{[\![\alpha=0]\!]}{m}\sum_{p|k|m}\mu(k)q^{m/k}. \\ &= a_m + b_m[\![\alpha=0]\!].\end{aligned}$$

4 Factorization Problem: General Theory

In this section, we develop the generating functions method to find the number of monic polynomials over $\mathbb{F}_q$ of degree m with their first w coefficients prescribed and specific pattern of degrees of irreducible factors prescribed. Let $T \subset \mathbb{N}$ be finite. For each $i \in T$ and $f \in M$, define $r_i(f)$ to be the number of distinct degree i monic irreducible factors of f, and $l_i(f)$ to be the number of degree i monic irreducible factors of f counting multiplicity. Then

$$r_i(f) = \sum_{g \in I_i} [\![g|f]\!], \tag{17}$$

$$l_i(f) = \sum_{g \in I_i} \max\{k : g^k | f\}. \tag{18}$$

From Definition 1, $N(m, \prod_{i \in T} I_i^{r_i}, \langle f \rangle)$ is the number of degree m monic polynomials over $\mathbb{F}_q$ with $\langle g \rangle = \langle f \rangle$, where g has r_i distinct factors in I_i for each $i \in T$. On the other hand, $N^*(m, \prod_{i \in T} I_i^{l_i}, \langle f \rangle)$ is the number of degree m monic polynomials g over $\mathbb{F}_q$ with $\langle g \rangle = \langle f \rangle$, where g has l_i factors in I_i counting multiplicity for each $i \in T$.

For $i \in T$, let u_i mark the irreducible monic polynomials of degree i. For $g \in I$, we define

$$u_g = \begin{cases} u_i & \text{if } g \in I_i \text{ for some } i \in T; \\ 1 & \text{otherwise.} \end{cases}$$

Let u be a vector of u_i. Define the GFs

$$G(z, u) = \sum_{f \in M} \langle f \rangle z^{d(f)} \prod_{g \in I, g|f} u_g = \sum_{f \in M} \langle f \rangle z^{d(f)} \prod_{i \in T} u_i^{r_i(f)}, \tag{19}$$

$$H(z,u) = \sum_{f\in M} \langle f\rangle z^{d(f)} \prod_{g\in I} u_g^{\max\{k:g^k|f\}} = \sum_{f\in M} \langle f\rangle z^{d(f)} \prod_{i\in T} u_i^{l_i(f)}. \qquad (20)$$

Note that

$$[\langle f\rangle z^m \prod_{i\in T} u_i^{r_i}]G(z,u) = N(m, \prod_{i\in T} I_i^{r_i}, \langle f\rangle), \qquad (21)$$

$$[\langle f\rangle z^m \prod_{i\in T} u_i^{l_i}]H(z,u) = N^*(m, \prod_{i\in T} I_i^{l_i}, \langle f\rangle). \qquad (22)$$

Proposition 7 *The expression for $G(z,u)$ can be written as follows:*

$$G(z,u) = F(z) \prod_{i\in T} \prod_{g\in I_i} (1 + \langle g\rangle z^i (u_i - 1)),$$

where $F(z) = \sum_{f\in M} \langle f\rangle z^{d(f)}$ is defined in (11).

Proof From the fact that every monic polynomial factors uniquely into a product of irreducible polynomials,

$$\begin{aligned}
G(z,u) &= \sum_{f\in M} \langle f\rangle z^{d(f)} \prod_{g\in I, g|f} u_g \\
&= \prod_{g\in I} \left(1 + \sum_{k\geq 1} \langle g^k\rangle z^{d(g^k)} u_g\right) \\
&= \prod_{g\in I} \left(1 + \sum_{k\geq 1} \langle g\rangle^k z^{k(d(g))} u_g\right) \\
&= \prod_{g\in I} \left(1 + \frac{u_g \langle g\rangle z^{d(g)}}{1 - \langle g\rangle z^{d(g)}}\right) \\
&= \prod_{g\in I} \left(\frac{1 - \langle g\rangle z^{d(g)} + u_g \langle g\rangle z^{d(g)}}{1 - \langle g\rangle z^{d(g)}}\right) \\
&= \prod_{g\in I} \left(\frac{1 + \langle g\rangle z^{d(g)}(u_g - 1)}{1 - \langle g\rangle z^{d(g)}}\right) \\
&= F(z) \prod_{g\in I} (1 + \langle g\rangle z^{d(g)}(u_g - 1)).
\end{aligned}$$

Using the definition of u_g we obtain the result. ∎

We now derive a more explicit formula for $G(z,u)$.

Lemma 1 *Under the same notations as above,*

$$G(z,u) = E\left(\sum_{d\geq 0} q^d z^d\right) \prod_{i\in T} \sum_{j_i=0}^{|I_i|} \sum_{r_i=0}^{j_i} \binom{|I_i|}{j_i} z^{ij_i} \binom{j_i}{r_i} u_i^{r_i} (-1)^{j_i - r_i}$$
$$+ J\left(\sum_{d=0}^{w-1} \sum_{f\in M_d} \langle f\rangle z^d\right) \prod_{i\in T} \prod_{g\in I_i} (1 + \langle g\rangle z^i (u_i - 1)).$$

Proof Using Proposition 7 and Equation (11), we have

$$G(z,u) = \left(\sum_{d\geq 0} \sum_{f\in M_d} \langle f\rangle z^d\right) \prod_{i\in T} \prod_{g\in I_i} (1 + \langle g\rangle z^i (u_i - 1)).$$

Using $E^2 = E$ and $E\langle f\rangle = E$, it follows that

$$\begin{aligned}
EG(z,u) &= E\left(\sum_{d\geq 0} \sum_{f\in M_d} \langle f\rangle z^d\right) \prod_{i\in T} \prod_{g\in I_i} (1 + \langle g\rangle z^i (u_i - 1)) \\
&= E\left(\sum_{d\geq 0} \sum_{f\in M_d} z^d\right) \prod_{i\in T} \prod_{g\in I_i} (1 + z^i (u_i - 1)) \\
&= E\left(\sum_{d\geq 0} q^d z^d\right) \prod_{i\in T} (1 + z^i (u_i - 1))^{|I_i|} \\
&= E\left(\sum_{d\geq 0} q^d z^d\right) \prod_{i\in T} \sum_{j_i=0}^{|I_i|} \binom{|I_i|}{j_i} z^{ij_i} (u_i - 1)^{j_i} \\
&= E\left(\sum_{d\geq 0} q^d z^d\right) \prod_{i\in T} \sum_{j_i=0}^{|I_i|} \sum_{r_i=0}^{j_i} \binom{|I_i|}{j_i} z^{ij_i} \binom{j_i}{r_i} u_i^{r_i} (-1)^{j_i - r_i}.
\end{aligned}$$

Using $J\sum_{f\in M_d} \langle f\rangle = 0$ for $d \geq w$, we have

$$\begin{aligned}
JG(z,u) &= J\left(\sum_{d\geq 0} \sum_{f\in M_d} \langle f\rangle z^d\right) \prod_{i\in T} \prod_{g\in I_i} (1 + \langle g\rangle z^i (u_i - 1)) \\
&= J\left(\sum_{d=0}^{w-1} \sum_{f\in M_d} \langle f\rangle z^d\right) \prod_{i\in T} \prod_{g\in I_i} (1 + \langle g\rangle z^i (u_i - 1)).
\end{aligned}$$

Using $G(z,u) = EG(z,u) + JG(z,u)$, we obtain the result. ∎

Theorem 1 *Let $T \subset \mathbb{N}$ be finite and I_i be the set of monic irreducible polynomials of degree i. Let f be a fixed polynomial over $\mathbb{F}_q$ with degree d and w be a fixed positive integer. The number of degree m monic polynomials g over $\mathbb{F}_q$ with the first w coefficients prescribed as those of f where g has r_i distinct factors in I_i for each $i \in T$ is*

$$\begin{aligned}
&N(m, \prod_{i\in T} I_i^{r_i}, \langle f\rangle) \\
&= q^{m-w} \prod_{i\in T} \binom{|I_i|}{r_i} q^{-ir_i} \sum_{j_i=0}^{|I_i|-r_i} q^{-ij_i} \binom{|I_i|-r_i}{j_i} (-1)^{j_i} [\![\sum_{i\in T} i(r_i+j_i) \le m]\!] \\
&+ [\langle f\rangle z^m \prod_{i\in T} u_i^{r_i}] J\left(\sum_{d=0}^{w-1} \sum_{f\in M_d} \langle f\rangle z^d \right) \prod_{i\in T} \prod_{g\in I_i} (1 + \langle g\rangle z^i (u_i - 1)).
\end{aligned}$$

Proof Note that

$$N(m, \prod_{i\in T} I_i^{r_i}, \langle f\rangle) = [\langle f\rangle z^m \prod_{i\in T} u_i^{r_i}] G(z,u),$$

and

$$\begin{aligned}
G(z,u) = E\left(\sum_{d\ge 0} q^d z^d \right) \prod_{i\in T} \sum_{j_i=0}^{|I_i|} \sum_{r_i=0}^{j_i} \binom{|I_i|}{j_i} z^{ij_i} \binom{j_i}{r_i} u_i^{r_i} (-1)^{j_i - r_i} \\
+ J\left(\sum_{d=0}^{w-1} \sum_{f\in M_d} \langle f\rangle z^d \right) \prod_{i\in T} \prod_{g\in I_i} (1 + \langle g\rangle z^i (u_i - 1)).
\end{aligned}$$

Note that for $0 \le r_i \le j_i \le |I_i|$,

$$\begin{aligned}
\binom{|I_i|}{j_i}\binom{j_i}{r_i} &= \frac{|I_i|!}{j_i!(|I_i|-j_i)!} \frac{j_i!}{r_i!(j_i-r_i)!} \\
&= \frac{|I_i|!}{r_i!(|I_i|-j_i)!(j_i-r_i)!} \\
&= \frac{|I_i|!}{r_i!(|I_i|-r_i)!} \frac{(|I_i|-r_i)!}{(j_i-r_i)!(|I_i|-j_i)!} \\
&= \binom{|I_i|}{r_i}\binom{|I_i|-r_i}{j_i-r_i}.
\end{aligned}$$

It follows that

$$\begin{aligned}
EG(z,u) &= E\left(\sum_{d\geq 0} q^d z^d\right) \prod_{i\in T} \sum_{j_i=0}^{|I_i|} \sum_{r_i=0}^{j_i} \binom{|I_i|}{r_i} z^{ij_i} \binom{|I_i|-r_i}{j_i-r_i} (-1)^{j_i-r_i} u_i^{r_i} \\
&= E\left(\sum_{d\geq 0} q^d z^d\right) \prod_{i\in T} \sum_{r_i=0}^{|I_i|} \binom{|I_i|}{r_i} u_i^{r_i} \sum_{j_i=r_i}^{|I_i|} z^{ij_i} \binom{|I_i|-r_i}{j_i-r_i} (-1)^{j_i-r_i} \\
&= E\left(\sum_{d\geq 0} q^d z^d\right) \prod_{i\in T} \sum_{r_i=0}^{|I_i|} \binom{|I_i|}{r_i} u_i^{r_i} z^{ir_i} \sum_{j_i=0}^{|I_i|-r_i} z^{ij_i} \binom{|I_i|-r_i}{j_i} (-1)^{j_i}.
\end{aligned}$$

Extracting the coefficient of $\prod_{i\in T} u_i^{r_i}$, we have

$$[\prod_{i\in T} u_i^{r_i}] EG(z,u) = E\left(\sum_{d\geq 0} q^d z^d\right) \prod_{i\in T} \binom{|I_i|}{r_i} z^{ir_i} \sum_{j_i=0}^{|I_i|-r_i} z^{ij_i} \binom{|I_i|-r_i}{j_i} (-1)^{j_i}.$$

Extracting z^m, we have

$$\begin{aligned}
&[z^m \prod_{i\in T} u_i^{r_i}] EG(z,u) \\
&= Eq^m \prod_{i\in T} \binom{|I_i|}{r_i} q^{-ir_i} \sum_{j_i=0}^{|I_i|-r_i} q^{-ij_i} \binom{|I_i|-r_i}{j_i} (-1)^{j_i} [\![\sum_{i\in T} i(r_i+j_i) \leq m]\!]
\end{aligned}$$

Hence, using the definition of E, extracting the coefficient of $\langle f \rangle$, we obtain

$$\begin{aligned}
&[\langle f \rangle z^m \prod_{i\in T} u_i^{r_i}] EG(z,u) \\
&= q^{m-w} \prod_{i\in T} \binom{|I_i|}{r_i} q^{-ir_i} \sum_{j_i=0}^{|I_i|-r_i} q^{-ij_i} \binom{|I_i|-r_i}{j_i} (-1)^{j_i} [\![\sum_{i\in T} i(r_i+j_i) \leq m]\!].
\end{aligned}$$

Adding $[\langle f \rangle z^m \prod_{i\in T} u_i^{r_i}] JG(z,u)$, we obtain the result. ∎

Similarly, we obtain the following.

Proposition 8 *The expression for $H(z,u)$ can be written as follows:*

$$H(z,u) = F(z) \prod_{i\in T} \prod_{g\in I_i} \left(\frac{1-\langle g \rangle z^i}{1-\langle g \rangle z^i u_i}\right).$$

Proof

$$\begin{aligned} H(z,u) &= \sum_{f\in M} \langle f\rangle z^{d(f)} \prod_{g\in I} u_g^{\max\{k:g^k|f\}} \\ &= \prod_{g\in I}\left(\sum_{k\geq 0}\langle g^k\rangle u_g^k z^{d(g^k)}\right) \\ &= \prod_{g\in I}\left(\sum_{k\geq 0}\langle g\rangle^k u_g^k z^{kd(g)}\right) \\ &= \prod_{g\in I}\left(\frac{1}{1-\langle g\rangle z^{d(g)}u_g}\right) \\ &= F(z)\prod_{g\in I}\left(\frac{1-\langle g\rangle z^{d(g)}}{1-\langle g\rangle z^{d(g)}u_g}\right). \end{aligned}$$

Using the definition of u_g, we obtain the result. ∎

Lemma 2 *We have the following formula for $H(z,u)$:*

$$\begin{aligned} H(z,u) = E\left(\sum_{d\geq 0} q^d z^d\right) \prod_{i\in T}\sum_{j_i=0}^{|I_i|}\binom{|I_i|}{j_i}(-1)^{j_i} z^{ij_i} \sum_{r_i\geq 0}\binom{|I_i|+r_i-1}{r_i} z^{ir_i}u_i^{r_i} \\ + J\left(\sum_{d=0}^{w-1}\sum_{f\in M_d}\langle f\rangle z^d\right)\prod_{i\in T}\prod_{g\in I_i}\left(\frac{1-\langle g\rangle z^i}{1-\langle g\rangle z^i u_i}\right). \end{aligned}$$

Proof Using Proposition 8 and Equation (11), we have

$$H(z,u) = \left(\sum_{d\geq 0}\sum_{f\in M_d}\langle f\rangle z^d\right)\prod_{i\in T}\prod_{g\in I_i}\left(\frac{1-\langle g\rangle z^i}{1-\langle g\rangle z^i u_i}\right).$$

It follows that

$$\begin{aligned}
EH(z,u) &= E\left(\sum_{d\geq 0}\sum_{f\in M_d}\langle f\rangle z^d\right)\prod_{i\in T}\prod_{g\in I_i}\left(\frac{1-\langle g\rangle z^i}{1-\langle g\rangle z^i u_i}\right)\\
&= E\left(\sum_{d\geq 0}\sum_{f\in M_d} z^d\right)\prod_{i\in T}\prod_{g\in I_i}\left(\frac{1-z^i}{1-z^i u_i}\right)\\
&= E\left(\sum_{d\geq 0} q^d z^d\right)\prod_{i\in T}\left(\frac{1-z^i}{1-z^i u_i}\right)^{|I_i|}\\
&= E\left(\sum_{d\geq 0} q^d z^d\right)\prod_{i\in T}\sum_{j_i=0}^{|I_i|}\binom{|I_i|}{j_i}(-1)^{j_i} z^{ij_i}\sum_{r_i\geq 0}\binom{|I_i|+r_i-1}{r_i} z^{ir_i}u_i^{r_i}.
\end{aligned}$$

Using $J\sum_{f\in M_d}\langle f\rangle = 0$ for $d \geq w$, we have

$$\begin{aligned}
JH(z,u) &= J\left(\sum_{d\geq 0}\sum_{f\in M_d}\langle f\rangle z^d\right)\prod_{i\in T}\prod_{g\in I_i}\left(\frac{1-\langle g\rangle z^i}{1-\langle g\rangle z^i u_i}\right)\\
&= J\left(\sum_{d=0}^{w-1}\sum_{f\in M_d}\langle f\rangle z^d\right)\prod_{i\in T}\prod_{g\in I_i}\left(\frac{1-\langle g\rangle z^i}{1-\langle g\rangle z^i u_i}\right).
\end{aligned}$$

Using $H(z,u) = EH(z,u) + JH(z,u)$, the result follows. ∎

Theorem 2 *Let $T \subset \mathbb{N}$ be finite and I_i be the set of monic irreducible polynomials of degree i. Let f be a fixed polynomial over $\mathbb{F}_q$ with degree d and w be a fixed positive integer. The number of degree m monic polynomials g over $\mathbb{F}_q$ with the first w coefficients prescribed as those of f where g has r_i factors in I_i counting multiplicity for each $i \in T$ is*

$$\begin{aligned}
&N^*(m, \prod_{i\in T} I_i^{l_i}, \langle f\rangle)\\
&= q^{m-w}\prod_{i\in T}\binom{|I_i|+l_i-1}{l_i} q^{-il_i}\sum_{j_i=0}^{|I_i|}\binom{|I_i|}{j_i}(-1)^{j_i} q^{-ij_i}[\![\sum_{i\in T} i(l_i+j_i)\leq m]\!]\\
&+ [\langle f\rangle z^m \prod_{i\in T} u_i^{l_i}] J\left(\sum_{d=0}^{w-1}\sum_{f\in M_d}\langle f\rangle z^d\right)\prod_{i\in T}\prod_{g\in I_i}\left(\frac{1-\langle g\rangle z^i}{1-\langle g\rangle z^i u_i}\right).
\end{aligned}$$

Proof We note that

$$N^*(m, \prod_{i\in T} I_i^{l_i}, \langle f\rangle) = [\langle f\rangle z^m \prod_{i\in T} u_i^{l_i}] H(z,u),$$

and

$$\begin{aligned} H(z,u) = E\left(\sum_{d\geq 0} q^d z^d\right) \prod_{i\in T} \sum_{j_i=0}^{|I_i|} \binom{|I_i|}{j_i} (-1)^{j_i} z^{ij_i} \sum_{r_i\geq 0} \binom{|I_i|+r_i-1}{r_i} z^{ir_i} u_i^{r_i} \\ + J\left(\sum_{d=0}^{w-1} \sum_{f\in M_d} \langle f\rangle z^d\right) \prod_{i\in T} \prod_{g\in I_i} \left(\frac{1-\langle g\rangle z^i}{1-\langle g\rangle z^i u_i}\right). \end{aligned}$$

For the first line, extracting the coefficient of $\prod_{i\in T} u_i^{l_i}$, we have

$$[\prod_{i\in T} u_i^{l_i}] EH(z,u) = E\left(\sum_{d\geq 0} q^d z^d\right) \prod_{i\in T} \binom{|I_i|+l_i-1}{l_i} z^{il_i} \sum_{j_i=0}^{|I_i|} \binom{|I_i|}{j_i} (-1)^{j_i} z^{ij_i}.$$

Extracting the coefficient of z^m, we have

$$\begin{aligned} &[z^m \prod_{i\in T} u_i^{l_i}] EH(z,u) \\ &= Eq^m \prod_{i\in T} \binom{|I_i|+l_i-1}{l_i} q^{-il_i} \sum_{j_i=0}^{|I_i|} \binom{|I_i|}{j_i} (-1)^{j_i} q^{-ij_i} [\![\sum_{i\in T} i(l_i+j_i) \leq m]\!] \end{aligned}$$

Using the definition of E and extracting $\langle f\rangle$, we have

$$\begin{aligned} &[\langle f\rangle z^m \prod_{i\in T} u_i^{l_i}] EH(z,u) \\ &= q^{m-w} \prod_{i\in T} \binom{|I_i|+l_i-1}{l_i} q^{-il_i} \sum_{j_i=0}^{|I_i|} \binom{|I_i|}{j_i} (-1)^{j_i} q^{-ij_i} [\![\sum_{i\in T} i(l_i+j_i) \leq m]\!]. \end{aligned}$$

Adding $[\langle f\rangle z^m \prod_{i\in T} u_i^{l_i}] JH(z,u)$, we obtain the result. ∎

5 Large Degree Monic Polynomials

In this section, we derive some simpler consequences under certain restrictions such as when the degree of polynomials are very large. The degree restrictions are too large to apply to some coding theory applications, such as the Reed-Solomon codes. However, the material extends results from [8, 9] by allowing for prescribed coefficients.

Theorem 3 *Suppose that* $\sum_{i\in T} i|I_i| \leq m-w$. *Then*

$$N(m, \prod_{i\in T} I_i^{r_i}, \langle f\rangle) = q^{m-w} \prod_{i\in T} \binom{|I_i|}{r_i} (1/q^i)^{r_i} (1-1/q^i)^{|I_i|-r_i}$$

Proof Suppose $\sum_{i\in T} i|I_i| \leq m-w$. Note that

$$\begin{aligned}
&N(m, \prod_{i\in T} I_i^{r_i}, \langle f\rangle) \\
&= q^{m-w} \prod_{i\in T} \binom{|I_i|}{r_i} q^{-ir_i} \sum_{j_i=0}^{|I_i|-r_i} q^{-ij_i} \binom{|I_i|-r_i}{j_i} (-1)^{j_i} [\![\sum_{i\in T} i(r_i+j_i) \leq m]\!] \\
&+ [\langle f\rangle z^m \prod_{i\in T} u_i^{r_i}] J \left(\sum_{d=0}^{w-1} \sum_{f\in M_d} \langle f\rangle z^d \right) \prod_{i\in T} \prod_{g\in I_i} (1+\langle g\rangle z^i (u_i-1)).
\end{aligned}$$

For the first line, if $j_i \leq |I_i| - r_i$, then $r_i + j_i \leq |I_i|$, so the bracket condition holds true.

The term on the second line is a polynomial in z of degree less than $w + \sum_{i\in T} i|I_i| \leq m$. Thus

$$[\langle f\rangle z^m \prod_{i\in T} u_i^{r_i}] J \left(\sum_{d=0}^{w-1} \sum_{f\in M_d} \langle f\rangle z^d \right) \prod_{i\in T} \prod_{g\in I_i} (1+\langle g\rangle z^i (u_i-1)) = 0.$$

Therefore,

$$\begin{aligned} N(m, \prod_{i\in T} I_i^{r_i}, \langle f\rangle) &= q^{m-w} \prod_{i\in T} \binom{|I_i|}{r_i} q^{-ir_i} \sum_{j_i=0}^{|I_i|-r_i} q^{-ij_i} \binom{|I_i|-r_i}{j_i} (-1)^{j_i} \\ &= q^{m-w} \prod_{i\in T} \binom{|I_i|}{r_i} (1/q^i)^{r_i} \sum_{j_i=0}^{|I_i|-r_i} (-1/q^i)^{j_i} \binom{|I_i|-r_i}{j_i} \\ &= q^{m-w} \prod_{i\in T} \binom{|I_i|}{r_i} (1/q^i)^{r_i} (1-1/q^i)^{|I_i|-r_i}. \ \blacksquare \end{aligned}$$

When we fix T to contain only one single degree i, the formula for N further simplifies, and the case $w = 0$ is well known.

Corollary 1 (Theorem 3 [9] when $w = 0$) *Fix $i \geq 1$. Suppose that $m \geq i|I_i| + w$. Then the number of polynomials $x^m + a_1 x_{m-1} + \cdots + a_w x^{m-w} + g(x)$ with $g(x) \in \mathbb{F}_q[x]$ of degree at most $m - w - 1$, that have r distinct irreducible factors of degree i, is*

$$N(m, {I_i}^r, \langle x^w + a_1 x^{w-1} + \cdots + a_w\rangle) = q^{m-w} \binom{|I_i|}{r} (1/q^i)^r (1-1/q^i)^{|I_i|-r}.$$

Setting $i = 1$, we obtain the following result about the number of monic polynomials with a given number of distinct linear factors with the highest few consecutive terms prescribed. This formula can also obtained using the sieve formula from [11].

Corollary 2 *Suppose that $m \geq q + w$. Fix $a_1, \ldots, a_w \in \mathbb{F}_q$. Then the number of polynomials $x^m + a_1 x_{m-1} + \cdots + a_w x^{m-w} + g(x)$ with $g(x) \in \mathbb{F}_q[x]$ of degree at most $m - w - 1$, that have r distinct linear factors, is*

$$N(m, {I_1}^r, \langle x^w + a_1 x^{w-1} + \cdots + a_w\rangle) = q^{m-w-r} \binom{q}{r} (1-1/q)^{q-r}.$$

Setting $w = 0$, we obtain a known result about polynomials.

Corollary 3 (Theorem 3 [8]) *Suppose that $m \geq q$. Then the number of degree m monic polynomials of degree at that have r distinct linear factors, is*

$$N(m, {I_1}^r, 1) = q^{m-w-r}\binom{q}{r}(1-1/q)^{q-r}.$$

Theorem 4 *Suppose that $\sum_{i\in T} i(|I_i|+l_i) \leq m-w$. Then*

$$N^*(m, \prod_{i\in T} I_i^{l_i}, \langle f\rangle) = q^{m-w}\prod_{i\in T}\binom{|I_i|+l_i-1}{l_i}(1/q^i)^{l_i}(1-1/q^i)^{|I_i|}.$$

Proof Suppose $\sum_{i\in T} i(|I_i|+l_i) \leq m-w$. Note that

$$\begin{aligned}
&N^*(m, \prod_{i\in T} I_i^{l_i}, \langle f\rangle)\\
&= q^{m-w}\prod_{i\in T}\binom{|I_i|+l_i-1}{l_i}q^{-il_i}\sum_{j_i=0}^{|I_i|}\binom{|I_i|}{j_i}(-1)^{j_i}q^{-ij_i}[\![\sum_{i\in T} i(l_i+j_i)\leq m]\!]\\
&+ [\langle f\rangle z^m \prod_{i\in T} u_i^{l_i}]J\left(\sum_{d=0}^{w-1}\sum_{f\in M_d}\langle f\rangle z^d\right)\prod_{i\in T}\prod_{g\in I_i}\left(\frac{1-\langle g\rangle z^i}{1-\langle g\rangle z^i u_i}\right).
\end{aligned}$$

For the first line, any term j_i in the sum satisfies $J_i \leq |I_i|$, so the bracket condition holds.

For the second line,

$$\prod_{g\in I_i}\frac{1}{1-\langle g\rangle z^i u_i} = \sum_{j\geq 0} a_{ij} z^{ji} u_i^j$$

with $a_{ij} \in \mathbb{C}[G]$. This means that

$$[\prod_{i\in T} u_i^{l_i}]J\left(\sum_{d=0}^{w-1}\sum_{f\in M_d}\langle f\rangle z^d\right)\prod_{i\in T}\prod_{g\in I_i}\left(\frac{1-\langle g\rangle z^i}{1-\langle g\rangle z^i u_i}\right)$$

is a polynomial in z over $\mathbb{C}[G]$ of degree less than $\sum_{i=i}^{n} i(|I_i|+l_i)+w \leq m$. Hence,

$$[\langle f\rangle z^m \prod_{i\in T} u_i^{l_i}]J\left(\sum_{d=0}^{w-1}\sum_{f\in M_d}\langle f\rangle z^d\right)\prod_{i\in T}\prod_{g\in I_i}\left(\frac{1-\langle g\rangle z^i}{1-\langle g\rangle z^i u_i}\right) = 0.$$

Therefore,

$$N^*(m, \prod_{i\in T} I_i^{l_i}, \langle f\rangle) = q^{m-w} \prod_{i\in T} \binom{|I_i|+l_i-1}{l_i} q^{-il_i} \sum_{j_i=0}^{|I_i|} \binom{|I_i|}{j_i} (-1)^{j_i} q^{-ij_i}$$
$$= q^{m-w} \prod_{i\in T} \binom{|I_i|+l_i-1}{l_i} (1/q^i)^{l_i} \sum_{j_i=0}^{|I_i|} \binom{|I_i|}{j_i} (-1/q^i)^{j_i}$$
$$= q^{m-w} \prod_{i\in T} \binom{|I_i|+l_i-1}{l_i} (1/q^i)^{l_i} (1-1/q^i)^{|I_i|}. \blacksquare$$

When we fix T to contain only one single degree i, the formula for N^* further simplifies. In addition, the case $w = 0$ is well known.

Corollary 4 (Theorem 1 [9] when $w = 0$) *Suppose that $m \geq i(|I_i| + l) + w$. Then the number of polynomials $x^m + a_1 x_{m-1} + \cdots + a_w x^{m-w} + g(x)$ with $g(x) \in \mathbb{F}_q[x]$ of degree at most $m - w - 1$, that have l degree i irreducible factors counting multiplicity, is*

$$N^*(m, I_i^l, \langle f\rangle) = q^{m-w} \binom{|I_i|+l-1}{l} (1/q^i)^l (1-1/q^i)^{|I_i|}.$$

Setting $i = 1$, we obtain the following results about the number of monic polynomials with a given number of linear factors counting multiplicity with the highest few consecutive terms prescribed.

Corollary 5 *Suppose that $m \geq q + l + w$. Fix $a_1, \ldots, a_w \in \mathbb{F}_q$. Then the number of polynomials $x^m + a_1 x_{m-1} + \cdots + a_w x^{m-w} + g(x)$ with $g(x) \in \mathbb{F}_q[x]$ of degree at most $m - w - 1$, that have l linear factors counting multiplicity, is*

$$N^*(m, {I_1}^l, \langle x^w + a_1 x^{w-1} + \cdots + a_w\rangle) = q^{m-w-l} \binom{q+l-1}{l} (1-1/q)^q.$$

Setting $w = 0$, we obtain a known result about polynomials.

Corollary 6 (Theorem 1 [8]) *Suppose that $m \geq q+l$. Then the number of monic degree m polynomials that have l linear factors counting multiplicity, is*

$$N^*(m, {I_1}^l, 1) = q^{m-l}\binom{q+l-1}{l}(1-1/q)^q.$$

6 General Results about Monic Polynomials

In this section, we focus on the special case when $w = 0$. In this case, no coefficients are prescribed, so we are simply counting monic polynomials that have a certain factorization pattern.

When $w = 0$, we have $G = \{1\}$. This means that for all $\langle f \rangle \in G, \langle f \rangle = 1$.

Theorem 5 *We have the following formula for* $N(m, \prod_{i \in T} I_i^{r_i}, \langle f \rangle)$ *when* $w = 0$*:*

$$\begin{aligned} &N(m, \prod_{i \in T} I_i^{r_i}, \langle f \rangle) \\ &= q^m \prod_{i \in T} \binom{|I_i|}{r_i} q^{-ir_i} \sum_{j_i=0}^{|I_i|-r_i} q^{-ij_i} \binom{|I_i| - r_i}{j_i} (-1)^{j_i} [\![\sum_{i \in T} i(r_i + j_i) \leq m]\!] \end{aligned}$$

Proof The result follows from Theorem 1 by setting $w = 0$. ∎

When we set $T = \{i\}$, we obtain the known results for the number of degree m monic polynomials with a given number of distinct degree i irreducible factors.

Corollary 7 (Theorem 3 [9]) *The number of degree* m *monic polynomials over* $\mathbb{F}_q$ *with* r *distinct irreducible degree* i *factors is*

$$N(m, {I_i}^r, 1) = q^{m-ir} \binom{|I_i|}{r} \sum_{j=0}^{\lfloor m/i \rfloor - r} q^{-ij} \binom{|I_i| - r}{j} (-1)^j.$$

Proof The result follows from Theorem 5 by setting $T = \{i\}$. ∎

Corollary 8 (Theorem 3 [8]) *The number of degree m monic polynomials over $\mathbb{F}_q$ with r distinct linear factors is*

$$N(m, {I_1}^r, 1) = q^{m-r}\binom{q}{r}\sum_{j=0}^{m-r} q^{-j}\binom{q-r}{j}(-1)^j.$$

Proof The result follows from Corollary 7 since $|I_1| = q$. ∎

In addition to these results, we can also obtain an exact formula for the number of n-smooth degree m monic polynomials by using Theorem 5. This formula is useful when n is close in size to m.

Corollary 9 *The number of n-smooth monic polynomials over $\mathbb{F}_q$ with degree m is*

$$N(m, \prod_{i=n+1}^{m} I_i^0, 1) = q^m \prod_{i=n+1}^{m}\sum_{j_i=0}^{|I_i|} q^{-ij_i}\binom{|I_i|}{j_i}(-1)^{j_i}[\![\sum_{i=n+1}^{m} ij_i \leq m]\!].$$

Proof A degree m polynomial is n-smooth if it contains no factors above degree n. Hence, we can obtain this result by setting $T = \{n+1, \ldots, m\}$ and then checking polynomials with no irreducible factors in T with Theorem 5. ∎

We can obtain a similar result to Theorem 5 when multiplicity of the factors are counted.

Theorem 6 *We have the following formula for $N^*(m, \prod_{i\in T} I_i^{l_i}, \langle f\rangle)$ when $w = 0$.*

$$\begin{aligned} &N^*(m, \prod_{i\in T} I_i^{l_i}, \langle f\rangle) \\ &= q^m \prod_{i\in T}\binom{|I_i| + l_i - 1}{l_i} q^{-il_i}\sum_{j_i=0}^{|I_i|}\binom{|I_i|}{j_i}(-1)^{j_i} q^{-ij_i}[\![\sum_{i\in T} i(l_i + j_i) \leq m]\!] \end{aligned}$$

Proof The result follows from Theorem 2 by setting $w = 0$. ∎

When we set $T = \{i\}$, we obtain the known expression for the number of degree m monic polynomials with a number of degree i irreducible factors counting multiplicity.

Corollary 10 (Theorem 3 [9]) *The number of degree m monic polynomials over $\mathbb{F}_q$ with l irreducible degree i factors counting multiplicity is*

$$N^*(m, I_i^l, 1) = q^{m-il}\binom{|I_i| + l - 1}{l}\sum_{j=0}^{\lfloor m/i \rfloor - l}\binom{|I_i|}{j}(-1)^j q^{-ij}$$

Setting $i = 1$ gives the known result on the number of degree m monic polynomials with a given number of linear factors counting multiplicity.

Corollary 11 (Theorem 1 [8]) *The number of degree m monic polynomials over $\mathbb{F}_q$ with l linear factors counting multiplicity is*

$$N^*(m, I_1^l, 1) = q^{m-l}\binom{q + l - 1}{l}\sum_{j=0}^{m-l}\binom{q}{j}(-1)^j q^{-j}$$

In addition to these results, we can obtain another exact formula for the number of $n - smooth$ degree m monic polynomials by using Theorem 6. This formula is useful when n is close in size to 1.

Corollary 12 *The number of monic n-smooth polynomials over $\mathbb{F}_q$ with degree m is*

$$\sum_{l_1 + 2l_2 + \cdots + nl_n = m} N^*(m, \prod_{i=1}^{n} I_i^{l_i}, 1) = \prod_{i=1}^{n}\sum_{l_i \geq 0}\binom{|I_i| + l_i - 1}{l_i}[\![\sum_{i=1}^{n} il_i = m]\!].$$

Proof A degree m monic polynomial is n-smooth if it contains no factors with degree greater than n. Hence, summing over all cases with $T =$

$\{1, \ldots, n\}$, where the polynomials are products of factors with degrees in T with Theorem 6, we obtain the result. ∎

As a result of Corollaries 9 and 12, we have an identity for the number of degree m n-smooth polynomials. This number is given by

$$q^m \prod_{i=n+1}^{m} \sum_{j_i=0}^{|I_i|} q^{-ij_i} \binom{|I_i|}{j_i} (-1)^{j_i} [\![\sum_{i=n+1}^{m} ij_i \leq m]\!]$$
$$= \prod_{i=1}^{n} \sum_{l_i \geq 0} \binom{|I_i| + l_i - 1}{l_i} [\![\sum_{i=1}^{n} il_i = m]\!].$$

We verify this identity can be proven in an elementary way from the unique factorization of monic polynomials, since

$$\prod_{i \geq 1} (1 - z^i)^{-|I_i|} = \sum_{k \geq 0} q^k z^k \tag{23}$$

Using generating functions, as mentioned in [17], the number of degree m n-smooth monic polynomials is

$$[z^m] \prod_{i=1}^{n} (1 - z^i)^{-|I_i|} = [z^m] \prod_{i=1}^{n} \sum_{l_i \geq 0} \binom{|I_i| + l_i - 1}{l_i} z^{il_i}$$
$$= \prod_{i=1}^{n} \sum_{l_i \geq 0} \binom{|I_i| + l_i - 1}{l_i} [\![\sum_{i=1}^{n} il_i = m]\!].$$

Using equation (23), we have that

$$\prod_{i=1}^{n} (1 - z^i)^{-|I_i|} = \sum_{k \geq 0} q^k z^k \prod_{i \geq n+1} (1 - z^i)^{|I_i|}.$$

Hence, as also mentioned in [17], the number of degree m n-smooth monic polynomials is also given by

$$[z^m] \sum_{k \geq 0} q^k z^k \prod_{i \geq n+1} (1 - z^i)^{|I_i|} = [z^m] \sum_{k \geq 0} q^k z^k \prod_{i \geq n+1} \sum_{j_i=0}^{|I_i|} \binom{|I_i|}{j_i} (-1)^{j_i} z^{ij_i}$$
$$= q^m \prod_{i=n+1}^{m} \sum_{j_i=0}^{|I_i|} q^{-ij_i} \binom{|I_i|}{j_i} (-1)^{j_i} [\![\sum_{i=n+1}^{m} ij_i \leq m]\!].$$

In general, exact results in this section, such as the number of degree m n-smooth monic polynomials, can be extended to the case where the second highest degree term of the polynomial is prescribed.

7 Results about Monic Polynomials with Second Highest Degree Term Prescribed

In this chapter, we consider the case where $w = 1$. In this case, we are able to obtain the exact formulas for the number of degree m polynomials of the form $f(x) = x^m + \alpha x^{m-1} + g(x)$, where $g(x) \in \mathbb{F}_q[x]$ has degree at most $m-2$, $\alpha \in \mathbb{F}_q$ is fixed, and f has a fixed number of irreducible factors of any degree, with or without multiplicity counted.

In order to do so, we use the formula for the number of degree m monic irreducible polynomials when the second highest degree term is prescribed. More explicitly, the number of degree i irreducible polynomials of the form $f(x) = x^i + \alpha x^{i-1} + g(x)$, for $g \in \mathbb{F}_q[x]$ of degree at most $i-2$ and fixed $\alpha \in \mathbb{F}_q$ is

$$|\{\langle f\rangle \in I_i, \langle f\rangle = \langle x+\alpha\rangle\}| = I_i(\langle x+\alpha\rangle) = a_i + b_i[\![\alpha = 0]\!], \tag{24}$$

where

$$a_i = \frac{1}{iq}\sum_{p\nmid k\mid i} \mu(k) q^{i/k}, \tag{25}$$

$$b_i = \frac{1}{i}\sum_{p\mid k\mid i} \mu(k) q^{i/k}. \tag{26}$$

In general, we can obtain answers that are in terms of a_i, b_i, and $|I_i|$. This turns out to be sufficient for obtaining the known formula for the number of degree m monic polynomials with r distinct roots when the second highest degree term is prescribed. In addition, we obtain an analogue of this formula when the multiplicity of the roots is counted.

We also obtain formulas for the number of monic n-smooth polynomials with degree m when the second highest degree term is prescribed in a similar way to the case $w = 0$ and obtain similar looking identities.

When $w = 1$, we have $G = \{\langle x + \alpha \rangle : \alpha \in \mathbb{F}_q\}$, and

$$\langle x + \alpha \rangle \langle x + \beta \rangle = \langle x + \alpha + \beta \rangle.$$

For $\alpha \in \mathbb{F}_q$, note that

$$\langle x + \alpha \rangle^k = \langle x + k\alpha \rangle.$$

Using $\langle x \rangle = 1$, it follows that

$$\begin{aligned}\sum_{\alpha \in \mathbb{F}_q} (\langle x + \alpha \rangle)^k &= \sum_{\alpha \in \mathbb{F}_q} (\langle x + k\alpha \rangle) = q\langle x \rangle [\![p \mid k]\!] + \sum_{\alpha \in \mathbb{F}_q} (\langle x + \alpha \rangle)[\![p \nmid k]\!] \\ &= q[\![p \mid k]\!] + qE[\![p \nmid k]\!].\end{aligned}$$

Using $EJ = 0$, it follows that

$$J \sum_{\alpha \in \mathbb{F}_q} (\langle x + \alpha \rangle)^k = qJ[\![p \mid k]\!].$$

For $k \geq 1$ using $J^k = J$, we have

$$J^k \sum_{\alpha \in \mathbb{F}_q} (\langle x + \alpha \rangle)^k = J^k q[\![p \mid k]\!]. \tag{27}$$

Using this formula, we obtain some facts which are useful for deriving results for N and N^* when $w = 1$.

Proposition 9 *We have the following facts:*

$$1) J \prod_{\alpha \in \mathbb{F}_q} (1 + \langle x + \alpha \rangle y) = J(1 - (-y)^p)^{\frac{q}{p}},$$

$$2) J \prod_{\alpha \in \mathbb{F}_q} \frac{1}{1 - \langle x + \alpha \rangle y} = J \left(\frac{1}{1 - y^p} \right)^{\frac{q}{p}}.$$

Proof 1) Using Proposition 4, Equation (27), and the power series definition for exp and log, we have

$$\begin{aligned}
J \prod_{\alpha \in \mathbb{F}_q} (1 + \langle x + \alpha \rangle y) &= J \prod_{\alpha \in \mathbb{F}_q} (1 + \langle x + \alpha \rangle Jy) \\
&= J \exp\left(\sum_{\alpha \in \mathbb{F}_q} \ln(1 + \langle x + \alpha \rangle Jy) \right) \\
&= J \exp\left(\sum_{\alpha \in \mathbb{F}_q} \sum_{k \geq 1} (-1)^{k-1} \frac{\langle x + \alpha \rangle^k J^k y^k}{k} \right) \\
&= J \exp\left(\sum_{k \geq 1} (-1)^{k-1} \frac{J^k y^k}{k} (q[\![p \mid k]\!]) \right) \\
&= J \exp\left(\sum_{k \geq 1} (-1)^{k-1} \frac{y^k}{k} (q[\![p \mid k]\!]) \right) \\
&= J \exp\left(\frac{-q}{p} \sum_{k \geq 1} \frac{(-y)^{pk}}{k} \right) \\
&= J \exp\left(\frac{q}{p} \ln(1 - (-y)^p) \right) \\
&= J(1 - (-y)^p)^{\frac{q}{p}}.
\end{aligned}$$

2) Similarly, we have

$$\begin{aligned}
J\prod_{\alpha\in\mathbb{F}_q}\frac{1}{1-\langle x+\alpha\rangle y} &= J\prod_{\alpha\in\mathbb{F}_q}\frac{1}{1-\langle x+\alpha\rangle Jy}\\
&= J\exp\left(\sum_{\alpha\in\mathbb{F}_q}\ln\left(\frac{1}{1-\langle x+\alpha\rangle Jy}\right)\right)\\
&= J\exp\left(\sum_{\alpha\in\mathbb{F}_q}\sum_{k\geq 1}\frac{\langle x+\alpha\rangle^k J^k y^k}{k}\right)\\
&= J\exp\left(\sum_{k\geq 1}\frac{J^k y^k}{k}(q[\![p\mid k]\!])\right)\\
&= J\exp\left(\frac{q}{p}\sum_{k\geq 1}\frac{y^{pk}}{k}\right)\\
&= J\exp\left(\frac{q}{p}\ln\left(\frac{1}{1-y^p}\right)\right)\\
&= J\left(\frac{1}{1-y^p}\right)^{\frac{q}{p}}. \ \blacksquare
\end{aligned}$$

Define the following numbers:

$$A_m(a,0)=\binom{aq/p}{m/p}(-1)^{m+m/p}[\![p\mid m]\!], \tag{28}$$

$$B_m(a,0)=\binom{aq/p+m/p-1}{m/p}[\![p\mid m]\!], \tag{29}$$

and, for $b\neq 0$,

$$A_m(a,b)=\sum_{j=0}^{\lfloor m/p\rfloor}\binom{aq/p}{j}\binom{b}{m-pj}(-1)^{j+pj}, \tag{30}$$

$$B_m(a,b)=\sum_{j=0}^{\lfloor m/p\rfloor}\binom{aq/p+j-1}{j}\binom{b+m-pj-1}{m-pj}. \tag{31}$$

Combining these numbers with (9), we obtain information related to the set of monic irreducible polynomials of degree i.

Proposition 10 *We have the following properties.*

$$1) J \prod_{f \in I_i} (1 + \langle f \rangle y) = J \sum_{m \geq 0} A_m(a_i, b_i) y^m.$$
$$2) J \prod_{f \in I_i} \frac{1}{1 - \langle f \rangle y} = J \sum_{m \geq 0} B_m(a_i, b_i) y^m.$$

Proof

1) Using $\langle x \rangle = 1$ and $I_i(\langle x + \alpha \rangle) = a_i + b_i [\![\alpha = 0]\!]$, $J^k = J$ for $k \geq 1$, and Proposition 9, we have

$$\begin{aligned}
J \prod_{f \in I_i} (1 + \langle f \rangle y) &= J \prod_{\alpha \in \mathbb{F}_q} (1 + \langle x + \alpha \rangle y)^{a_i + b_i [\![\alpha = 0]\!]} \\
&= J(1 + \langle x \rangle y)^{b_i} \prod_{\alpha \in \mathbb{F}_q} (1 + \langle x + \alpha \rangle y)^{a_i} \\
&= J(1 - (-y)^p)^{\frac{a_i q}{p}} (1 + y)^{b_i} \\
&= J \sum_{m \geq 0} \sum_{j=0}^{\lfloor m/p \rfloor} \binom{a_i q/p}{j} (-1)^j (-1)^{pj} \binom{b_i}{m - pj} y^m \\
&= J \sum_{m \geq 0} \sum_{j=0}^{\lfloor m/p \rfloor} \binom{a_i q/p}{j} \binom{b_i}{m - pj} (-1)^{j + pj} y^m \\
&= J \sum_{m \geq 0} A_m(a_i, b_i) y^m.
\end{aligned}$$

2) Similarly, we have

$$\begin{aligned}
J\prod_{f\in I_i}\frac{1}{1-\langle f\rangle y} &= J\prod_{\alpha\in\mathbb{F}_q}\left(\frac{1}{1-\langle x+\alpha\rangle y}\right)^{a_i+b_i[\![\alpha=0]\!]}\\
&= J\left(\frac{1}{1-\langle x\rangle y}\right)^{b_i}\prod_{\alpha\in\mathbb{F}_q}\left(\frac{1}{1-\langle x+\alpha\rangle y}\right)^{a_i}\\
&= J\left(\frac{1}{1-y^p}\right)^{\frac{a_iq}{p}}\left(\frac{1}{1-y}\right)^{b_i}\\
&= J\sum_{m\geq 0}\sum_{j=0}^{\lfloor m/p\rfloor}\binom{a_iq/p+j-1}{j}\binom{b_i+m-pj-1}{b_i}y^m\\
&= J\sum_{m\geq 0}B_m(a_i,b_i)y^m.\ \blacksquare
\end{aligned}$$

Using Proposition 10, we can obtain formulas for N and N^* when $w=1$.

Theorem 7 *Suppose $w=1$. Then*

$$\begin{aligned}
&N(m,\prod_{i\in T}I_i^{r_i},\langle x+\alpha\rangle)\\
&= q^{m-1}\prod_{i\in T}\binom{|I_i|}{r_i}q^{-ir_i}\sum_{j_i=0}^{|I_i|-r_i}q^{-ij_i}\binom{|I_i|-r_i}{j_i}(-1)^{j_i}[\![\sum_{i\in T}i(r_i+j_i)\leq m]\!]\\
&+\frac{v(\alpha)}{q}\prod_{i\in T}\sum_{k_i\geq 0}A_{k_i}(a_i,b_i)\binom{k_i}{r_i}(-1)^{k_i-r_i}[\![\sum_{i\in T}ik_i=m]\!],
\end{aligned}$$

where $v(\alpha)=q[\![\alpha=0]\!]-1$.

Proof Using Theorem 1, we have

$$\begin{aligned}
&N(m, \prod_{i\in T} I_i^{r_i}, \langle x+\alpha\rangle) \\
&= q^{m-1} \prod_{i\in T} \binom{|I_i|}{r_i} q^{-ir_i} \sum_{j_i=0}^{|I_i|-r_i} q^{-ij_i} \binom{|I_i|-r_i}{j_i} (-1)^{j_i} [\![\sum_{i\in T} i(r_i+j_i) \le m]\!] \\
&+ [\langle x+\alpha\rangle z^m \prod_{i\in T} u_i^{r_i}] J \prod_{i\in T} \prod_{g\in I_i} (1+\langle g\rangle z^i (u_i - 1)).
\end{aligned}$$

Using $J^k = J$ for any positive integer k and Proposition 10, we have

$$\begin{aligned}
&[\langle x+\alpha\rangle z^m \prod_{i\in T} u_i^{r_i}] J \prod_{i\in T} \prod_{g\in I_i} (1+\langle g\rangle z^i (u_i - 1)) \\
&= [\langle x+\alpha\rangle z^m \prod_{i\in T} u_i^{r_i}] J \prod_{i\in T} \sum_{k_i \ge 0} A_{k_i}(a_i, b_i) z^{ik_i} (u_i - 1)^{k_i}
\end{aligned}$$

Extracting coefficients of the u_i using the Binomial Theorem,

$$= [\langle x+\alpha\rangle z^m] J \prod_{i\in T} \sum_{k_i \ge 0} A_{k_i}(a_i, b_i) z^{ik_i} \binom{k_i}{r_i} (-1)^{k_i - r_i}$$

Extracting the coefficient of z,

$$= [\langle x+\alpha\rangle] J \prod_{i\in T} \sum_{k_i \ge 0} A_{k_i}(a_i, b_i) \binom{k_i}{r_i} (-1)^{k_i - r_i} [\![\sum_{i\in T} ik_i = m]\!].$$

Using $J = 1 - E = \frac{1}{q} \sum_{\alpha\in\mathbb{F}_q} v(\alpha)\langle x+\alpha\rangle$, and extracting $\langle x+\alpha\rangle$,

$$= \frac{v(\alpha)}{q} \prod_{i\in T} \sum_{k_i \ge 0} A_{k_i}(a_i, b_i) \binom{k_i}{r_i} (-1)^{k_i - r_i} [\![\sum_{i\in T} ik_i = m]\!],$$

Combining the pieces together, we have the result. ∎

In the following special case, we obtain a simpler result.

Corollary 13 *Suppose $w = 1$. Suppose that $p \nmid i$ for each i.*

If $p \nmid m$, then

$$N(m, \prod_{i\in T} I_i^{r_i}, \langle x+\alpha\rangle)$$
$$= q^{m-1} \prod_{i\in T} \binom{|I_i|}{r_i} q^{-ir_i} \sum_{j_i=0}^{|I_i|-r_i} q^{-ij_i} \binom{|I_i|-r_i}{j_i} (-1)^{j_i} [\![\sum_{i\in T} i(r_i+j_i) \le m]\!].$$

If $p \mid m$, then

$$N(m, \prod_{i\in T} I_i^{r_i}, \langle x+\alpha\rangle)$$
$$= q^{m-1} \prod_{i\in T} \binom{|I_i|}{r_i} q^{-ir_i} \sum_{j_i=0}^{|I_i|-r_i} q^{-ij_i} \binom{|I_i|-r_i}{j_i} (-1)^{j_i} [\![\sum_{i\in T} i(r_i+j_i) \le m]\!]$$
$$+ \frac{v(\alpha)}{q} \prod_{i\in T} \sum_{k_i=0}^{|I_i|/p} \binom{|I_i|/p}{k_i} \binom{pk_i}{r_i} (-1)^{k_i-r_i} [\![\sum_{i\in T} ik_i = m/p]\!],$$

where $v(\alpha) = q[\![\alpha = 0]\!] - 1$.

Proof The result follows from Theorem 7 by setting $b_i = 0$ for each i, and using (28), and noting that $qa_i = |I_i|$ for $p \nmid i$. ∎

Setting $T = \{1\}$, we obtain the known result for the number of monic polynomials with a given number of linear factors when the coefficient in front of the second highest ordered term is fixed.

Corollary 14 (Theorem 3.1 [20]) *The number of monic polynomials over $\mathbb{F}_q$ of the form $x^m + \alpha x^{m-1} + g(x)$ for fixed $\alpha \in \mathbb{F}_q$, where $g \in \mathbb{F}_q[x]$ has degree at most $m-2$, that have r distinct linear factors is given as follows:*

If $p \nmid m$, then

$$N(m, I_1^r, \langle x+\alpha\rangle) = q^{m-r-1} \binom{q}{r} \sum_{j=0}^{m-r} q^{-j} \binom{q-r}{j} (-1)^j.$$

If $p \mid m$, then

$$N(m, I_1^r, \langle x+\alpha \rangle) = q^{m-r-1}\binom{q}{r}\sum_{j=0}^{m-r} q^{-j}\binom{q-r}{j}(-1)^j + \frac{v(\alpha)}{q}\binom{q/p}{m/p}\binom{m}{r}(-1)^{m/p-r},$$

where $v(\alpha) = q[\![\alpha = 0]\!] - 1$.

Proof The result follows from Theorem 7 by taking $T = \{1\}$, and using $|I_1| = q$. ∎

Now, we state a result about degree m monic n-smooth polynomials with a prescribed coefficient in front of the second highest ordered term, which comes from Theorem 7. This formula is most useful when n is large.

Corollary 15 *The number of monic n-smooth polynomials over $\mathbb{F}_q$ of the form $x^m + \alpha x^{m-1} + g(x)$ for fixed $\alpha \in \mathbb{F}_q$, where $g \in \mathbb{F}_q[x]$ has degree at most $m-2$ is*

$$N(m, \prod_{i=n+1}^{m} I_i^0, \langle x+\alpha \rangle) = q^{m-1}\prod_{i=n+1}^{m}\sum_{j_i=0}^{|I_i|} q^{-ij_i}\binom{|I_i|}{j_i}(-1)^{j_i}[\![\sum_{i=n+1}^{m} ij_i \le m]\!] + \frac{v(\alpha)}{q}\prod_{i=n+1}^{m}\sum_{k_i \ge 0} A_{k_i}(a_i, b_i)(-1)^{k_i}[\![\sum_{i=n+1}^{m} ik_i = m]\!],$$

where $v(\alpha) = q[\![\alpha = 0]\!] - 1$.

Proof The result follows from Theorem 7 by setting $T = \{n+1, \ldots, m\}$ and using the fact that a monic polynomial is n-smooth if it has no irreducible factors with degree larger than n.

Next, we give the general theorem for N^*. That is the case where the multiplicity of the the factors is counted. The result is as follows.

Corollary 16 *Suppose $w = 1$. Then*

$$\begin{aligned}
&N^*(m, \prod_{i\in T} I_i^{l_i}, \langle x+\alpha\rangle)\\
&= q^{m-1}\prod_{i\in T}\binom{|I_i|+l_i-1}{l_i} q^{-il_i}\sum_{j_i=0}^{|I_i|}\binom{|I_i|}{j_i}(-1)^{j_i}q^{-ij_i}[\![\sum_{i\in T} i(l_i+j_i)\le m]\!]\\
&+ \frac{v(\alpha)}{q}\prod_{i\in T} B_{l_i}(a_i,b_i)\sum_{k_i\ge 0} A_{k_i}(a_i,b_i)(-1)^{k_i}[\![\sum_{i\in T} i(l_i+k_i)=m]\!],
\end{aligned}$$

where $v(\alpha) = q[\![\alpha = 0]\!] - 1$.

Proof Using Theorem 2, we have

$$\begin{aligned}
&N^*(m, \prod_{i\in T} I_i^{l_i}, \langle x+\alpha\rangle)\\
&= q^{m-1}\prod_{i\in T}\binom{|I_i|+l_i-1}{l_i} q^{-il_i}\sum_{j_i=0}^{|I_i|}\binom{|I_i|}{j_i}(-1)^{j_i}q^{-ij_i}[\![\sum_{i\in T} i(l_i+j_i)\le m]\!]\\
&+ [\langle a+\alpha\rangle z^m\prod_{i\in T} u_i^{l_i}]J\prod_{i\in T}\prod_{g\in I_i}\left(\frac{1-\langle g\rangle z^i}{1-\langle g\rangle z^i u_i}\right).
\end{aligned}$$

Using $J^k = J$ for any positive integer k, applying Proposition 10, and extracting coefficients of the u_i, z, and then $\langle x+\alpha\rangle$, we have

$$\begin{aligned}
&[\langle x+\alpha\rangle z^m\prod_{i\in T} u_i^{l_i}]J\prod_{i\in T}\prod_{g\in I_i}\left(\frac{1-\langle g\rangle z^i}{1-\langle g\rangle z^i u_i}\right)\\
&= [\langle x+\alpha\rangle z^m]J\prod_{i\in T} B_{l_i}(a_i,b_i) z^{il_i}\sum_{k_i\ge 0} A_{k_i}(a_i,b_i)(-z^i)^{k_i}\\
&= [\langle x+\alpha\rangle z^m]J\prod_{i\in T} B_{l_i}(a_i,b_i)\sum_{k_i\ge 0} A_{k_i}(a_i,b_i)(-1)^{k_i} z^{i(l_i+k_i)}\\
&= [\langle x+\alpha\rangle]J\prod_{i\in T} B_{l_i}(a_i,b_i)\sum_{k_i\ge 0} A_{k_i}(a_i,b_i)(-1)^{k_i}[\![\sum_{i\in T} i(l_i+k_i)=m]\!]\\
&= \frac{v(\alpha)}{q}\prod_{i\in T} B_{l_i}(a_i,b_i)\sum_{k_i\ge 0} A_{k_i}(a_i,b_i)(-1)^{k_i}[\![\sum_{i\in T} i(l_i+k_i)=m]\!],
\end{aligned}$$

since $J = 1 - E = \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q} v(\alpha)\langle x+\alpha\rangle$. Hence, the result follows. ∎

As a corollary to Theorem 16, we have the following simpler result.

Corollary 17 *Suppose $w = 1$. Suppose that $p \nmid i$ for each i.*
If $p \nmid m$ or $p \nmid l_i$ for some i, then

$$N^*(m, \prod_{i\in T} I_i^{l_i}, \langle x+\alpha\rangle)$$
$$= q^{m-1} \prod_{i\in T} \binom{|I_i|+l_i-1}{l_i} q^{-il_i} \sum_{j_i=0}^{|I_i|} \binom{|I_i|}{j_i} (-1)^{j_i} q^{-ij_i} [\![\sum_{i\in T} i(l_i+j_i) \le m]\!].$$

If $p \mid m$ and $p \mid l_i$ for each i, then

$$N^*(m, \prod_{i\in T} I_i^{l_i}, \langle x+\alpha\rangle)$$
$$= q^{m-1} \prod_{i\in T} \binom{|I_i|+l_i-1}{l_i} q^{-il_i} \sum_{j_i=0}^{|I_i|} \binom{|I_i|}{j_i} (-1)^{j_i} q^{-ij_i} [\![\sum_{i\in T} i(l_i+j_i) \le m]\!]$$
$$+ \frac{v(\alpha)}{q} \prod_{i\in T} \binom{|I_i|/p+l_i/p-1}{l_i/p} \sum_{k_i=0}^{|I_i|/p} \binom{|I_i|/p}{k_i} (-1)^{pk_i} [\![\sum_{i\in T} i(l_i/p+k_i) = m/p]\!]$$

where $v(\alpha) = q[\![\alpha = 0]\!] - 1$.

Proof The result follows from Theorem 16 by setting $b_i = 0$ for each i, using (28) and (29), and noting that $qa_i = |I_i|$ for $p \nmid i$. ∎

From this corollary, we can obtain the number of degree m monic polynomials $f(x)$ with a given number of roots counting multiplicity, with a fixed coefficient of x^{m-1}. The result is new and is similar in style to the distinct root case. The result is provided below.

Corollary 18 *The number of monic polynomials over $\mathbb{F}_q$ of the form $x^m + \alpha x^{m-1} + g(x)$ for fixed $\alpha \in \mathbb{F}_q$, where $g(x) \in \mathbb{F}_q[x]$ has degree at most $m-2$ that have l linear factors counting multiplicity is given as follows:*

If $p \nmid m$ or $p \nmid l$, then

$$N^*(m, I_1^l, \langle x+\alpha \rangle) = q^{m-l-1}\binom{q+l-1}{l}\sum_{j=0}^{m-l}\binom{q}{j}(-1)^j q^{-j}$$

If $p \mid m$ and $p \mid l$, then

$$N^*(m, I_1^l, \langle x+\alpha \rangle) = q^{m-l-1}\binom{q+l-1}{l}\sum_{j=0}^{m-l}\binom{q}{j}(-1)^j q^{-j} + \frac{v(\alpha)}{q}\binom{q/p+l/p-1}{l/p}\binom{q/p}{(m-l)/p}(-1)^{m-l}$$

where $v(\alpha) = q[\![\alpha = 0]\!] - 1$.

Proof The result follows from Corollary 17 by taking $T = \{1\}$, and using $|I_1| = q$. ∎

Using Theorem 16, we obtain another formula for the number of n-smooth degree m monic polynomials with a prescribed coefficient in front of the term of degree $m-1$. The result looks different from Theorem 15 and is useful when n is small.

Corollary 19 *The number of monic n-smooth polynomials over $\mathbb{F}_q$ of the form $x^m + \alpha x^{m-1} + g(x)$ for fixed $\alpha \in \mathbb{F}_q$, where $g \in \mathbb{F}_q[x]$ has degree at most $m-2$ is*

$$\sum_{l_1+2l_2+\cdots+nl_n=m} N^*(m, \prod_{i=1}^n I_i^{l_i}, \langle x+\alpha \rangle) = \frac{1}{q}\prod_{i=1}^n \sum_{l_i \geq 0}\binom{|I_i|+l_i-1}{l_i}[\![\sum_{i=1}^n il_i = m]\!] + \frac{v(\alpha)}{q}\prod_{i=1}^n \sum_{l_i \geq 0} B_{l_i}(a_i, b_i)[\![\sum_{i=1}^n il_i = m]\!],$$

where $v(\alpha) = q[\![\alpha = 0]\!] - 1$.

Proof A degree m monic polynomial is n-smooth if it contains no factors above degree n. Hence, summing over all cases with $T = \{1, \ldots, n\}$ with

Theorem 16, where the polynomials are products of factors with degrees in T, we obtain the result.

As a result of Corollaries 15 and 19, we have the following identity for the number of degree m monic n-smooth polynomials of the form $x^m + \alpha x^{m-1} + g(x)$, where $\alpha \in \mathbb{F}_q$ is fixed and $g(x) \in \mathbb{F}_q[x]$ has degree at most $m-2$. This number is given by

$$\begin{aligned}
&q^{m-1} \prod_{i=n+1}^{m} \sum_{j_i=0}^{|I_i|} q^{-ij_i} \binom{|I_i|}{j_i} (-1)^{j_i} [\![\sum_{i=n+1}^{m} ij_i \leq m]\!] \\
&+ \frac{v(\alpha)}{q} \prod_{i=n+1}^{m} \sum_{k_i \geq 0} A_{k_i}(a_i, b_i)(-1)^{k_i} [\![\sum_{i=n+1}^{m} ik_i = m]\!] \\
&= \frac{1}{q} \prod_{i=1}^{n} \sum_{l_i \geq 0} \binom{|I_i| + l_i - 1}{l_i} [\![\sum_{i=1}^{n} il_i = m]\!] \\
&+ \frac{v(\alpha)}{q} \prod_{i=1}^{n} \sum_{l_i \geq 0} B_{l_i}(a_i, b_i) [\![\sum_{i=1}^{n} il_i = m]\!]
\end{aligned}$$

where $v(\alpha) = q[\![\alpha = 0]\!] - 1$.

This result can be verified directly using generating functions in a similar way to the case $w = 0$. From generating functions, the number of degree m n-smooth polynomials of the form $x^m + \alpha x^{m-1} + g(x)$, where $\alpha \in \mathbb{F}_q$ is fixed and $g(x) \in \mathbb{F}_q[x]$ has degree at most $m-2$, is given by

$$[\langle x + \alpha \rangle z^m] \prod_{i=1}^{n} \prod_{f \in I_i} (1 - \langle f \rangle z^i)^{-1}.$$

From unique factorization of monic polynomials, we have

$$F(z) = \prod_{i \geq 1} \prod_{f \in I_i} (1 - \langle f \rangle z^i)^{-1} = 1 + \sum_{k \geq 1} \sum_{f \in M_k} \langle f \rangle z^k. \tag{32}$$

Using $E\langle f \rangle = E$ and $E^2 = E$, we have

$$EF(z) = E \prod_{i \geq 1} (1 - z^i)^{-|I_i|} = E \sum_{k \geq 0} q^k z^k. \tag{33}$$

Using $J\sum_{f\in M_k}\langle f\rangle = 0$ for $k \geq w = 1$, we have

$$JF(z) = J\prod_{i\geq 1}\prod_{f\in I_i}(1-\langle f\rangle z^i)^{-1} = J. \tag{34}$$

Applying $F(z) = \prod_{i\geq 1}\prod_{f\in I_i}(1-\langle f\rangle z^i)^{-1}$ to equations (33) and (34), we obtain

$$E\prod_{i=1}^{n}\prod_{f\in I_i}(1-\langle f\rangle z^i)^{-1} = E\prod_{i=1}^{n}(1-z^i)^{-|I_i|} = E\sum_{k\geq 0}q^k z^k \prod_{i\geq n+1}(1-z^i)^{|I_i|},$$
$$J\prod_{i=1}^{n}\prod_{f\in I_i}(1-\langle f\rangle z^i)^{-1} = J\prod_{i\geq n+1}\prod_{f\in I_i}(1-\langle f\rangle z^i).$$

From Proposition 10, we have

$$J\prod_{i=1}^{n}\prod_{f\in I_i}(1-\langle f\rangle z^i)^{-1} = J\prod_{i\geq 1}\sum_{k\geq 0}B_k(a_i,b_i)z^{ik},$$
$$J\prod_{i\geq n+1}\prod_{f\in I_i}(1-\langle f\rangle z^i) = \prod_{i\geq n+1}\sum_{k\geq 0}A_k(a_i,b_i)(-1)^k z^{ik}.$$

Hence, using $E + J = 1$, we obtain

$$\begin{aligned}
&\prod_{i=1}^{n}\prod_{f\in I_i}(1-\langle f\rangle z^i)^{-1}\\
&= E\prod_{i=1}^{n}(1-z^i)^{-|I_i|} + J\prod_{i\geq 1}\sum_{k\geq 0}B_k(a_i,b_i)z^{ik}\\
&= E\sum_{k\geq 0}q^k z^k\prod_{i\geq n+1}(1-z^i)^{|I_i|} + J\prod_{i\geq n+1}\sum_{k\geq 0}A_k(a_i,b_i)(-1)^k z^{ik}.
\end{aligned}$$

Using $E = \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q}\langle x+\alpha\rangle$ and $J = 1-E = \frac{1}{q}\sum_{\alpha\in\mathbb{F}_q} v(\alpha)\langle x+\alpha\rangle$, we obtain

$$\begin{aligned}
&[\langle x+\alpha\rangle z^m]\prod_{i=1}^{n}\prod_{f\in I_i}(1-\langle f\rangle z^i)^{-1}\\
&=\frac{1}{q}\prod_{i=1}^{n}\sum_{l_i\geq 0}\binom{|I_i|+l_i-1}{l_i}[\![\sum_{i=1}^{n} il_i = m]\!]\\
&+\frac{v(\alpha)}{q}\prod_{i=1}^{n}\sum_{l_i\geq 0}B_{l_i}(a_i,b_i)[\![\sum_{i=1}^{n} il_i = m]\!]\\
&=q^{m-1}\prod_{i=n+1}^{m}\sum_{j_i=0}^{|I_i|}q^{-ij_i}\binom{|I_i|}{j_i}(-1)^{j_i}[\![\sum_{i=n+1}^{m} ij_i \leq m]\!]\\
&+\frac{v(\alpha)}{q}\prod_{i=n+1}^{m}\sum_{k_i\geq 0}A_{k_i}(a_i,b_i)(-1)^{k_i}[\![\sum_{i=n+1}^{m} ik_i = m]\!],
\end{aligned}$$

as desired.

8 Conclusion

In this project, we adapted the generating functions method from [6, 7] in order to find the number of degree m monic polynomials f whose first w coefficients are fixed, when f has a given distribution of irreducible factors from different degrees. From our general results, we were able to recover and extend formulas from numerous research papers, such as [2, 7, 8, 9, 20]. For polynomials of sufficiently large degree, we extended the known results to allow for any number of consecutive prescribed leading coefficients w given any factorization pattern. For polynomials of arbitrary degree, we found general formulas when $w \leq 1$ for any factorization. For the case $w = 0$, we recovered known results from several papers. For the case $w = 1$, we obtained some new results, including two formulas for the number of n-smooth monic degree m polynomials with the first coefficient fixed.

In the future, it could be interesting to try to extend the results from the case $w = 1$ to the case $w = 2$. This could help further develop our generating functions method in order to address coding theory applications. The case $w = 2$ is known in general for irreducible degree m monic polynomials, and in special cases for degree m monic polynomials with a given number of distinct linear factors. Given that the case $w = 1$ harder than the case $w = 0$, we expect the case $w = 2$ to be more difficult than than the case $w = 1$. However, given the known results on the case $w = 2$, we expect this case to be feasible for a future project. Polynomials used in Reed-Solomon codes have degree less than the size of the field. Thus, we plan to study the case $w = 2$ for low degree polynomials in the future.

References

[1] X. Cao, M. Liu, D. Wan, L. Wang, Q. Wang, Linearized Wenger graphs, *Discrete Math.* 338 (2015), 1595-1602.

[2] M. Car, Théorèmes de densité dans $\mathbb{F}_q[X]$. (French) [Density theorems in $\mathbb{F}_q[X]$], *Acta Arith.* 48 (1987), no. 2, 145-165.

[3] L. Carlitz, A theorem of Dickson on irreducible polynomials, *Proc. Amer. Math. Soc.* 3 (1952), 693-700.

[4] S.M. Cioaba, F. Lazebnic, W. Li, On the spectrum of Wegner graphs, *J. Combin. Theory Ser. B* 107 (2014), 132-139.

[5] R. W. Fitzgerald and J. L. Yucas, Irreducible polynomials over GF(2) with three prescribed coefficients, *Finite Fields Appl.* 9 (2003), 286-299.

[6] Z. Gao, S. Kuttner, Q. Wang, On enumeration of irreducible polynomials and related objects over a finite field with respect to their trace and norm, *Finite Fields Appl.* 69 (2021), 101770, 25pp.

[7] Z. Gao, S. Kuttner, Q. Wang, Counting irreducible polynomials with prescribed coefficients over a finite field, preprint.

[8] A. Knopmacher, J. Knopmacher, Counting polynomials with a given number of zeros in a finite field, *Linear Multilinear Algebra* 26 (1990), 267-292.

[9] A. Knopmacher, J. Knopmacher, Counting irreducible factors of polynomials over a finite field, *Discrete Math. 112* (1993), 103-118.

[10] S. Kuttner and Q. Wang, On the enumeration of polynomials with prescribed factorization pattern, preprint.

[11] J. Li, D. Wan, Distance distribution in Reed-Solomon codes, *IEEE Trans. Inform. Theory* 66 (2020), no. 5, 2743-2750.

[12] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.

[13] R. Lovorn, Rigourous, subexponential algorithms for discrete logarithm algorithms in $\mathbb{F}_{p^2}$. PhD thesis University of Georgia, 1992.

[14] M. Moisio and K. Ranto, Elliptic curves and explicit enumeration of irreducible polynomials with two coefficients prescribed, *Finite Fields Appl.* 14 (2008), 798-815.

[15] G. L. Mullen, D. Panario, *Handbook of Finite Fields*, Discrete Mathematics and its Applications (Boca Raton). CRC Press, Boca Raton, FL, 2013.

[16] A. Odlyzko, Discrete logarithms and their cryptographic significance. In Advances in Cryptology, Proceedings of Eurocrypt 1984 (1985), vol. 209 of Lecture Notes in Computer Science, Springer-Verlag, pp. 224-314.

[17] D. Panario, X. Gourdon, P. Flajolet, An analytic approach to smooth polynomials over finite fields. Algorithmic number theory (Portland, OR, 1998), 226-236, Lecture Notes in Comput. Sci., 1423, Springer, Berlin, 1998.

[18] F. Ruskey, C. R. Miers, J. Sawada, The number of irreducible polynomials and Lyndon words with given trace. *SIAM J. Discrete Math.* 14 (2001), no. 2, 240-245.

[19] J. L. Yucas, Irreducible polynomials over finite fields with prescribed trace/prescribed constant term, *Finite Fields Appl.* 12 (2006), 211-221.

[20] H. Zhou, L. Wang, W. Wang, Counting polynomials with distinct zeros in finite fields, *J. Number Theory* 174 (2017), 118-135.