ON THE ENUMERATION OF POLYNOMIALS WITH PRESCRIBED FACTORIZATION PATTERN

SIMON KUTTNER AND QIANG WANG

Abstract. We use generating functions over group rings to count polynomials over finite fields with the first few coefficients prescribed and a factorization pattern prescribed. In particular, we obtain different exact formulas for the number of monic \( n \)-smooth polynomial of degree \( m \) over a finite field, as well as the number of monic \( n \)-smooth polynomial of degree \( m \) with the prescribed trace coefficient.

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 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 a monic polynomial \( f \), let \( d(f) \) denote the degree of \( f \), \( r_i(f) \) denote the number of monic distinct irreducible factors of \( f \) with degree \( i \), and \( l_i(f) \) denote the number of monic degree \( i \) irreducible factors of \( f \) counting multiplicity. In particular, we write

\[
f(x) = x^{d(f)} + f_1 x^{d(f)-1} + \cdots + f_d(f),
\]

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

For \( f \in M \) and \( w \geq 0 \), we define

\[
\langle f \rangle_w = x^{d(f)} f(1/x) \quad \text{mod} \quad x^{w+1}
\]

\[
= 1 + f_1 x + \cdots + f_w x^w \quad \text{mod} \quad x^{w+1}.
\]

In this paper, we want to determine the number of monic polynomials \( f(x) \) of degree \( m \) with prescribed coefficients \( f_1, \ldots, f_w \) and a given pattern of irreducible factors in terms of their degrees. First of all, we introduce the following definitions.

Definition 1. Let \( w \geq 0 \) be a fixed integer and \( T \subseteq \mathbb{N} \) be a finite set.

1. Define \( N(m, \prod_{i \in T} I_i^r_i, \langle f \rangle_w) \) as the number of monic polynomial \( g \) over \( \mathbb{F}_q \) of degree \( m \) with \( \langle g \rangle_w = \langle f \rangle_w \), where \( g \) has \( r_i \) distinct monic degree \( i \) irreducible factors for each \( i \in T \). In particular, if \( m = \sum_T r_i \), then \( N(m, \prod_{i \in T} I_i^r_i, \langle f \rangle_w) \) is the number of monic polynomials over \( \mathbb{F}_q \) of degree \( m \) with both the first \( w \) coefficients \( f_1, \ldots, f_w \) and a factorization pattern in terms of their degrees are prescribed.

Date: May 18, 2021.

Key words and phrases. Finite fields, irreducible polynomials, factorization, smooth polynomials.

This research is partially supported by NSERC of Canada (RGPIN-2017-06410).
(2) Define $N^*(m, \prod_{i \in T} I_i^l, \langle f \rangle_w)$ as the number of degree $m$ monic polynomial $g$ 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 $i \in T$. In particular, if $m = \sum_T l_i$, then $N^*(m, \prod_{i \in T} I_i^l, \langle f \rangle_w)$ is the number of monic polynomials over $\mathbb{F}_q$ of degree $m$ with both the first $w$ coefficients $f_1, \ldots, f_w$ and a factorization pattern in terms of their degrees counting multiplicity are prescribed.

Finding these numbers answers many previous known questions in the literature. For example, the problem of counting monic irreducible polynomials $f$ over $\mathbb{F}_q$ of degree $m$ with prescribed coefficients $f_1, \ldots, f_w$ is well studied. Denote by $I(m, \langle f \rangle_w)$ the number of degree $m$ monic irreducible polynomial $g$ over $\mathbb{F}_q$, where $\langle g \rangle_w = \langle f \rangle_w$. Then

\[
I(m, \langle f \rangle_w) = N^*(m, I_m^1 \prod_{i \neq 1} I_i^0, \langle f \rangle_w).
\]

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 $\langle f \rangle \equiv 1 \pmod{x} = (1)$. 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 [1]) and is given by

\[
|I_m| = \frac{1}{m} \sum_{k|m} \mu(m/k)q^k,
\]

where $\mu$ is the Möbius function.

The results for $w = 1$ can be found in [19]. In this case, for each monic polynomial $f$, we have $\langle f \rangle = 1 + \beta x \pmod{x^2} = \langle x + \beta \rangle$ for some unique $\beta \in \mathbb{F}_q$. For $m \geq 1$, $I(m, \langle x + \beta \rangle)$ counts the number of monic irreducible polynomials of the form $x^m + \beta x^{m-1} + g(x)$ where $\beta \in \mathbb{F}_q$ is fixed and $g(x) \in \mathbb{F}_q[x]$ is a polynomial of degree at most $m - 2$ which is allowed to vary. When $m$ is a multiple of $p$, the formula for $I(m, \langle x + \beta \rangle)$ depends on whether $\beta = 0$ or not. Explicitly, if $m = p^j n_0$ with $j > 0$, then we have

\[
I(m, \langle x + \beta \rangle) = \frac{1}{mq} \sum_{k|n_0} \mu(k)q^{m/k} - \frac{v(\beta)}{mq} \sum_{k|n_0} \mu(k)q^{m/kp},
\]

where $v(\beta) = q$ if $\beta = 0$ and 0 otherwise.

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

\[
I(m, \langle x + \beta \rangle) = \frac{|I_m|}{q} = \frac{1}{mq} \sum_{k|m} \mu(m/k)q^k.
\]

We also note that there are formulas for $I(m, \langle f \rangle)$ for $w = 2$ (see [13]), and also for $w = 3$, when $q = 2$ (see [4]).

Another special case of our general problem of computing $N$ and $N^*$ in Definition 1 is to determine 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 $m \geq w$, $N(m, I_1^1, \langle f \rangle_w)$ 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 \( m - w - 1 \) that varies.

This number is important 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 \( f \) of degree at most \( k - 1 \) where \( v(x) - f(x) \) has at exactly \( r \) distinct roots. Writing \( v(x) = x^w + v_1 x^{w-1} + \cdots + v_w x + c(x) \), for \( v_1, \ldots, v_w \in \mathbb{F}_q \) 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, which is equal to \( N(k + w, I^l_w) \).

Both numbers \( N(m, I^l_w, \langle f \rangle_w) \) and \( N^*(m, I^l_w, \langle f \rangle_w) \) 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 \( \langle f \rangle_w \equiv 1 \pmod{\alpha x} \), 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

\[
N^*(m, I^l_1, 1) = q^{m-l} \left( \frac{q + l - 1}{l} \right) \sum_{j=0}^{m-l} \left( \frac{q}{j} \right) (-1)^j q^{-j}.
\]

If \( m \geq q + l \), the formula simplifies to

\[
N^*(m, I^l_1, 1) = q^{m-l} \left( \frac{q + l - 1}{l} \right) (1 - 1/q)^q.
\]

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

\[
N(m, I^l_r, 1) = q^{m-r} \left( \frac{q}{r} \right) \sum_{j=0}^{m-r} q^{-j} \left( \frac{q}{j} \right) (-1)^j.
\]

If \( m \geq q \), this number becomes

\[
N(m, I^l_r, 1) = q^{m-r} \left( \frac{q}{r} \right) (1 - 1/q)^{q-r}.
\]

These results have been extended in recent years to allow for prescribing coefficients \( f_1, \ldots, f_w \), where \( w \geq 1 \) is arbitrary, due to applications in Reed-Solomon codes (see [20, 10]). 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

\[
N(m, I^*_1, (x + \alpha)) = q^{m-r-1} \left( \frac{q}{r} \right) \sum_{j=0}^{m-r} q^{-j} \binom{q-r}{j} (-1)^j.
\]

If \( p \mid m \), then the number is

\[
N(m, I^*_1, (x + \alpha)) = q^{m-r-1} \left( \frac{q}{r} \right) \sum_{j=0}^{m-r} q^{-j} \binom{q-r}{j} (-1)^j + \frac{v(\alpha)}{q} \left( \frac{q/p}{m/p} \right) \binom{m}{r} \left( -1 \right)^{m/p-r},
\]

where \( v(\alpha) = q[\alpha = 0] - 1 \). Here we use the notation \([P]\), which is equal to 1 if \( P \) is true and \([P] = 0\) otherwise.

The 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 [10], 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 \( m \leq q \).

In this paper, we derive a general expression for \( N \) and \( N^* \) from the generating functions over group-rings for any fixed \( w \geq 0 \) and any fixed \( T \subset \mathbb{N} \). Namely, we can use this to find the number of monic polynomials over \( \mathbb{F}_q \) of degree \( m \) with their first \( w \) coefficients prescribed and specific factorization pattern prescribed, counting multiplicity or not (see Theorems 11, 12). These general results for \( N \) and \( N^* \) both have many corollaries that improve known results. In particular, we obtain some simpler consequences when the degree of polynomials is sufficiently large (see Theorems 13, 14). Then we focus on the cases when \( w = 0 \) or \( w = 1 \), and thus obtain some exact formulas for \( N \) and \( N^* \) in those cases.

We also apply our results to the study of smooth polynomials. 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 [15] 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 [12]. For \( n \) large with respect to \( m \), typically \( n > cm \log \log m / \log m \), Car [11] has given an asymptotic expression for this number in terms of the Dickman function. Panario, Gourdon and Flajolet [16] extended this range to \( n > (1+\epsilon)(\log m)^{1/k} \), for a positive integer constant \( k \). All these results are asymptotic results and no exact formula is known previously.

When \( w = 0 \), we can simplify our general results and obtain two exact formulas for the number of monic \( n \)-smooth polynomials of degree \( m \) (see Corollaries 11, 14). Similarly, when \( w = 1 \), we obtain two exact formulas for the number of degree \( m \)-smooth polynomials of the form \( x^m + \alpha x^{m-1} + g(x) \) where \( g \) is a polynomial of degree at most \( m - 2 \) (see Corollaries 17 and 20). We also show that the corresponding different formulas are equivalent.
The paper is organized as follows. In Section 2 we provide background definitions and preliminary results that were first introduced in [3, 5], such as generating functions defined on the group algebra of the equivalent classes for polynomials over finite fields. In Section 3 we demonstrate the generating function method over group rings to count irreducible polynomials with prescribed coefficients, which were explored in [3, 5] earlier. In Section 4 we develop the general results on counting polynomials with prescribed coefficients and prescribed factorization pattern. Then 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

In this section, we introduce the necessary background to be able to count monic polynomials with the first $w$ prescribed coefficients using the generating functions method. A general combinatorial framework for counting irreducible polynomials with prescribed coefficients, using generating functions with coefficients from a group algebra, was developed in [3, 5] and Section 2 of [6].

First, we fix $w \geq 0$. Recall that $M$ is set of monic polynomials over $\mathbb{F}_q$. For $f \in M$, we let $d(f)$ denote the degree of $f$, write $f = x^{d(f)} + f_1 x^{d(f) - 1} + \cdots + f_{d(f)}$, and set $f_j = 0$ if $j > d(f)$. We also recall the notation

$$\langle f \rangle = x^{d(f)} f(1/x) \pmod{x^{w+1}}$$

$$= 1 + f_1 x + \cdots + f_w x^w \pmod{x^{w+1}}.$$

Fix $f \in M$ and $d \geq w$. 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 $g \in M_d$ satisfying $\langle g \rangle = \langle f \rangle$. For convenience, we define

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

From this definition, we have the following result.

**Proposition 1.** (Proposition 1, [6]) $G$ 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 $f, g \in M$,

$$\langle f \rangle \langle g \rangle = x^{d(f)} f(1/x) x^{d(g)} g(1/x) \pmod{x^{w+1}}$$

$$= x^{d(f)+d(g)} f(1/x) g(1/x) \pmod{x^{w+1}}$$

$$= x^{d(fg)} (fg)(1/x) \pmod{x^{w+1}}$$

$$= \langle fg \rangle.$$

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 \( g_0 + g_1 x + \cdots + g_w x^w \) such that
\[
(1 + f_1 x + \cdots + f_w x^w)(g_0 + g_1 x + \cdots + g_w x^w) \equiv 1 \pmod{x^{w+1}}.
\]
It follows that \( g_0 = 1 \ast g_0 = 1 \). Let \( g = x^w + g_1 x^{w+1} + \cdots + g_w \in M \). We have
\[
\langle f \rangle \langle g \rangle = (1 + f_1 x + \cdots + f_w x^w)(1 + g_1 x + \cdots + g_w x^w) \pmod{x^{w+1}}
= (1 + f_1 x + \cdots + f_w x^w)(g_0 + g_1 x + \cdots + g x^w) \pmod{x^{w+1}}
= 1 \pmod{x^{w+1}}
= (1).
\]
Hence, \( \langle g \rangle \) is the multiplicative inverse of \( \langle f \rangle \) in \( G \).

Let \( \mathbb{C} \) be the field of complex numbers. In order to make use of the group \( G \), it is convenient to define the following.

**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 = (1) 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
\[
a + b = \sum_{\langle f \rangle \in G} (a_{\langle f \rangle } + b_{\langle f \rangle }) \langle f \rangle ,
\]
\[
ab = \sum_{\langle f \rangle \in G} \sum_{\langle g \rangle \in G} a_{\langle g \rangle } b_{\langle f \rangle \langle g \rangle ^{-1} } \langle f \rangle .
\]

To help with counting, the following elements in \( \mathbb{C}[G] \) are useful.

**Definition 3.** Define
\[
E = \frac{1}{q^w} \sum_{\langle f \rangle \in G} \langle f \rangle
\]
\[
J = 1 - E
\]

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

**Proposition 2.** The following properties of \( E \) and \( J \) hold:
\begin{itemize}
  \item[i)] \( E \langle g \rangle = E \) for any \( \langle g \rangle \in G \).
  \item[ii)] \( E^2 = E \).
  \item[iii)] \( E J = 0 \).
  \item[iv)] \( J^2 = J \).
\end{itemize}

To connect to the polynomial counting problem, we recall that \( M_d \) is the set of degree \( d \) monic polynomials over \( \mathbb{F}_q \), so \( |M_d| = q^d \). Suppose \( f \in M \). Then for \( d \geq w \), any \( g \in M_d \) satisfies \( \langle g \rangle = \langle f \rangle \) if and only if \( g = x^d + f_1 x^{d-1} + \cdots + f_w x^{d-w} + c(x) \) for some polynomial \( c(x) \) of degree at most \( d - w - 1 \) over \( \mathbb{F}_q \). There are \( q^{d-w} \) polynomials over \( \mathbb{F}_q \) of degree at most \( d - w - 1 \). Therefore, the number of polynomials \( g \in M_d \) with \( \langle g \rangle = \langle f \rangle \) is \( q^{d-w} \). It follows that every \( \langle f \rangle \in G \) is uniquely defined by the polynomial \( h \in M_w \) that satisfies \( \langle h \rangle = \langle f \rangle \). We can therefore write
\[
G = \{ \langle x^w + h_1 x^{w-1} + \cdots + h_w \rangle : h_1, \ldots, h_w \in \mathbb{F}_q \}. 
\]
Using the above defined notations and Proposition 2, we can derive more facts that are useful when performing computations in \( \mathbb{C}[G] \).

**Proposition 3.** The following properties hold:

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

ii) \( \sum_{f \in M_d} \langle f \rangle = q^d E \) for \( d \geq w \).

iii) \( J \sum_{f \in M_d} \langle f \rangle = 0 \) for \( d \geq w \).

**Proof**

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

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

ii) Suppose \( d \geq w \) and \( h \in M_w \). We note that there are \( q^{d-w} \) polynomials \( g \in M_d \) with \( \langle g \rangle = \langle h \rangle \). It follows from the definition of \( E \) that

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

iii) Suppose \( d \geq w \). Then using \( EJ = 0 \), we have

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

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

**Proposition 4.** Suppose \( A(z) \) is a formal power series over \( \mathbb{C}[G] \). If \( K \in \mathbb{C}[G] \) satisfies \( K^2 = K \), then \( KA(z) = KA(Kz) \). In particular, we have \( EA(z) = EA(Ez) \), \( JA(z) = JA(Jz) \), and \( A(z) = EA(Ez) + JA(Jz) \).

**Proof**

Write \( A(z) = \sum_{j \geq 0} a_j z^j \), where \( a_j \in \mathbb{C}[G] \). Since \( K^2 = K \), we have

\[
KA(z) = K \sum_{j \geq 0} a_j z^j
\]

\[
= K \sum_{j \geq 0} K a_j z^j
\]

\[
= K \sum_{j \geq 0} K a_j K^j z^j
\]

\[
= K \sum_{j \geq 0} K a_j (K z)^j
\]

\[
= K \sum_{j \geq 0} a_j (K z)^j
\]

\[
= KA(K z).
\]

The rest of proof follows from Proposition 2.
3. Counting 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 $x^m + \beta x^{m-1} + g(x)$ where $\beta \in \mathbb{F}_q$ is fixed, and $g(x) \in \mathbb{F}_q[x]$ of degree at most $m - 2$ is varied. More details can be found in [5, 6], where this method was first introduced, and different cases such as prescribed trace and norm, or prescribed multiple coefficients were considered respectively.

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)

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

From the unique factorization of polynomials, we have

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

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

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

It follows that

$$\ln(F(z)) = \sum_{d \geq 1} \sum_{(f) \in G} I(d, \langle f \rangle) \sum_{k \geq 1} \frac{\langle f \rangle^k z^{dk}}{k}$$

$$= \sum_{m \geq 1} \sum_{d|m} \sum_{(f) \in G} \frac{d}{m} I(d, \langle f \rangle) \langle f \rangle^{m/d} z^m.$$

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

$$N(m, \langle f \rangle) = \sum_{d|m} \sum_{(g) \in G} dI(d, \langle g \rangle) \langle g \rangle^{m/d} = \langle f \rangle].$$  

Proposition 5. (Proposition 2, [6])

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

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

$$\sum_{d|m} \mu(d) = [m = 1].$$
we obtain

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

\[
= \sum_{k|m} \sum_{\langle g \rangle \in G} \mu(m/k) \sum_{d|k} \sum_{\langle h \rangle \in G} dI(d, \langle h \rangle) \langle h \rangle^{k/d} = \langle g \rangle \langle g \rangle^{m/k} = \langle f \rangle
\]

\[
= \sum_{k|m} \mu(m/k) \sum_{d|k} dI(d, \langle h \rangle) \langle h \rangle^{k/d} = \langle f \rangle
\]

\[
= \sum_{k|m} \mu(k) \sum_{d|k} dI(d, \langle h \rangle) \langle h \rangle^{m/d} = \langle f \rangle \sum_{k|m} \mu(k)
\]

\[
= \sum_{d|m} dI(d, \langle h \rangle) \langle h \rangle^{m/d} = \langle f \rangle \sum_{d|m} \mu(k)
\]

\[
= mI(m, \langle f \rangle).
\]

Dividing by \( m \), we obtain the result. \( \blacksquare \)

Proposition 6.

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

Proof Using (10),

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

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
\[
\ln(F(z)) = E \ln(F(Ez)) + J \ln(F(Jz)) \\
= E \ln \left(1 + \sum_{d \geq 1} \sum_{f \in M_d} \langle f \rangle E_d z^d \right) + J \ln \left(1 + \sum_{d \geq 1} \sum_{f \in M_d} \langle f \rangle J_d z^d \right) \\
= E \ln \left(1 + \sum_{d \geq 1} q^d E_d z^d \right) + J \ln \left(1 + \sum_{d = 1}^{w-1} \sum_{f \in M_d} \langle f \rangle z^d \right) \\
= E \ln \left(1 + \sum_{d \geq 1} q^d z^d \right) + J \ln \left(1 + \sum_{d = 1}^{w-1} \sum_{f \in M_d} \langle f \rangle z^d \right) \\
= E \sum_{k \geq 1} \frac{1}{k} q^k z^k + J \ln \left(1 + \sum_{d = 1}^{w-1} \sum_{f \in M_d} \langle f \rangle z^d \right).
\]

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

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

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

If \( w = 1 \), then \( G = \{1 + \alpha x \pmod{x^2} : \alpha \in \mathbb{F}_q \} = \{x + \alpha) : \alpha \in \mathbb{F}_q \} \). For \( \alpha, \beta \in \mathbb{F}_q \), and \( n \geq 1 \), we have \( (x + \alpha)^n = (1 + \alpha x)^n \pmod{x^2} = 1 + n\alpha x \pmod{x^2} \)

= \langle x + n\alpha \rangle. \) Hence \( \langle x + \alpha \rangle^n = \langle x + \beta \rangle \) if and only if \( n\alpha = \beta \).

Suppose \( \beta \in \mathbb{F}_q \) and \( n \geq 1 \). Then

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

If \( w = 1 \), then \( G = \{1 + \alpha x \pmod{x^2} : \alpha \in \mathbb{F}_q \} = \{x + \alpha) : \alpha \in \mathbb{F}_q \} \). For \( \alpha, \beta \in \mathbb{F}_q \), and \( n \geq 1 \), we have \( (x + \alpha)^n = (1 + \alpha x)^n \pmod{x^2} = 1 + n\alpha x \pmod{x^2} \)

\[ \langle x + \alpha \rangle^n = \langle x + \beta \rangle \] if and only if \( n\alpha = \beta \).

Suppose \( \beta \in \mathbb{F}_q \) and \( n \geq 1 \). Then

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

It follows from Proposition 4 that

\[ I(m, \langle x + \beta \rangle) = \frac{1}{m} \sum_{k|m} \sum_{\alpha \in \mathbb{F}_q} \mu(k) q^{m/k} \left\lfloor \langle x + \alpha \rangle^k = \langle x + \beta \rangle \right\rfloor \]

\[ = \frac{1}{mq} \sum_{k|m} \sum_{\alpha \in \mathbb{F}_q} \mu(k) q^{m/k} \left\lfloor k\alpha = \beta \right\rfloor \]

\[ = \frac{1}{mq} \sum_{p|k|m} \mu(k) q^{m/k} + \frac{\left\lfloor \beta = 0 \right\rfloor}{m} \sum_{p|k|m} \mu(k) q^{m/k}. \]
This is equivalent to Equation 5 due to Yucas [10]; see also [17]. In particular, if \( p \nmid m \) and \( w = 1 \), then for all \( \beta \in \mathbb{F}_q \),
\[
I(m, (x + \beta)) = \frac{|I_m|}{q} = \frac{1}{mq} \sum_{k|m} \mu(k)q^{m/k}.
\]

4. Factorization Problem: General Theory

In this section, we develop the generating function method to find the number of monic polynomials over \( \mathbb{F}_q \) of degree \( m \) with their first \( w \) coefficients prescribed and the factorization pattern in terms of the degrees of irreducible factors prescribed. One can refer to [3] [7] [15] and references therein for related results on general decomposable structures with prescribed patterns.

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
\[
(16) \quad r_i(f) = \sum_{g \in I_i} \|g|f\],
\[
(17) \quad l_i(f) = \sum_{g \in I_i} \max\{k : g^k|f\}.
\]

From Definition \( \text{I} \) \( N(m, \prod_{i \in T} I^i, \langle f \rangle) \) 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, \( N^*(m, \prod_{i \in T} I^i, \langle f \rangle) \) 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
\[
u_g = \begin{cases} u_i & \text{if } g \in I_i \text{ for some } i \in T; \\ 1 & \text{otherwise}. \end{cases}
\]

Define the GFs
\[
(18) \quad G(z, u) = \sum_{f \in M} \langle f \rangle z^{d(f)} \prod_{g \in I, g|f} u_g = \sum_{f \in M} \langle f \rangle z^{d(f)} \prod_{i \in T} u_i^{r_i(f)},
\]
\[
(19) \quad H(z, u) = \sum_{f \in M} \langle f \rangle z^{d(f)} \prod_{g \in I} u_g^{\max\{k : g^k|f\}} = \sum_{f \in M} \langle f \rangle z^{d(f)} \prod_{i \in T} u_i^{l_i(f)}.
\]

Note that
\[
(20) \quad [\langle f \rangle z^m \prod_{i \in T} u_i^{r_i}] G(z, u) = N(m, \prod_{i \in T} I^i, \langle f \rangle),
\]
\[
(21) \quad [\langle f \rangle z^m \prod_{i \in T} u_i^{l_i}] H(z, u) = N^*(m, \prod_{i \in T} I^i, \langle f \rangle).
\]

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 (10).

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

\[
G(z, u) = \sum_{f \in M} \langle f \rangle z^{d(f)} \prod_{g \in I \setminus \{ f \}} u_g
\]

\[
= \prod_{g \in I} \left( 1 + \sum_{k \geq 1} \langle g \rangle^k z^{k(d(g))} u_g \right)
\]

\[
= \prod_{g \in I} \left( 1 + \sum_{k \geq 1} \langle g \rangle^k z^{k(d(g))} u_g \right)
\]

\[
= \prod_{g \in I} \left( 1 + \frac{u_g \langle g \rangle z^{d(g)}}{1 - \langle g \rangle z^{d(g)}} \right)
\]

\[
= \prod_{g \in I} \left( \frac{1 + \langle g \rangle z^{d(g)} - u_g \langle g \rangle z^{d(g)}}{1 - \langle g \rangle z^{d(g)}} \right)
\]

\[
= F(z) \prod_{g \in I} (1 + \langle g \rangle z^{d(g)}(u_g - 1)).
\]

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,

\[
G(z, u) = E \left( \sum_{d \geq 0} q^d z^d \prod_{i \in T} \sum_{j_i = 0, r_i = 0}^{|I_i|} \sum_{\substack{I_i \cap I_j = 0, \ j_i = 0, \ r_i = 0 \ \text{for all} \ i \neq j \ \text{and} \ j_i < r_i} \left( \sum_{f \in M_d} \langle f \rangle z^{d(f)} \prod_{i \in T} \prod_{g \in I_i} (1 + \langle g \rangle z^i(u_g - 1)) \right. \right.
\]

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

**Proof** Using Proposition 7 and Equation (10), we have

\[
G(z, u) = \left( \sum_{d \geq 0} q^d z^d \right) \prod_{i \in T} \prod_{g \in I_i} (1 + \langle g \rangle z^i(u_i - 1)).
\]
Using \( E^2 = E \) and \( E(f) = E \), the follows that

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

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

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

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

**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 monic 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 \( f \) and \( g \) has \( r_i \) distinct factors in \( I_i \) for each \( i \in T \) is

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

**Proof** First we note that

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

\[ G(z, u) = E \left( \sum_{d \geq 0} q^d z^d \right) \prod_{i \in T} \prod_{j_i = 0} \sum_{r_i = 0}^{\lfloor |I_i| \rfloor} \left( \frac{|I_i|!}{j_i! (|I_i| - j_i)! r_i! (j_i - r_i)!} \right) z^{j_i} \left( \frac{|I_i| - r_i}{j_i - r_i} \right) (-1)^{j_i - r_i} + J \left( \sum_{d=0}^{m-1} \sum_{f \in M_d} (f) z^d \right) \prod_{i \in T} \prod_{g \in I_i} (1 + (g) z^i (u_i - 1)). \]

Note that for \( 0 \leq r_i \leq j_i \leq |I_i| \),

\[ \left( \frac{|I_i|!}{j_i! (|I_i| - j_i)! r_i! (j_i - r_i)!} \right) \]

\[ = \frac{|I_i|!}{r_i! (|I_i| - r_i)! (j_i - r_i)!} \]

\[ = \left( \frac{|I_i|!}{|I_i| - r_i! (|I_i| - j_i)! (j_i - r_i)!} \right) \]

\[ = \binom{|I_i|}{r_i} \binom{|I_i| - r_i}{j_i - r_i}. \]

It follows that

\[ EG(z, u) = E \left( \sum_{d \geq 0} q^d z^d \right) \prod_{i \in T} \sum_{j_i = 0}^{\lfloor |I_i| \rfloor} \left( \frac{|I_i|!}{j_i! (|I_i| - j_i)! r_i! (j_i - r_i)!} \right) z^{j_i} \left( \frac{|I_i| - r_i}{j_i - r_i} \right) (-1)^{j_i - r_i} u_i^{r_i} \]

\[ = E \left( \sum_{d \geq 0} q^d z^d \right) \prod_{i \in T} \frac{|I_i|!}{r_i! (|I_i| - r_i)! (j_i - r_i)!} \sum_{j_i=r_i}^{\lfloor |I_i| - r_i \rfloor} \left( \frac{|I_i| - r_i}{j_i - r_i} \right) (-1)^{j_i - r_i} \]

\[ = E \left( \sum_{d \geq 0} q^d z^d \right) \prod_{i \in T} \frac{|I_i|!}{r_i! (|I_i| - r_i)! (j_i - r_i)!} \sum_{j_i=0}^{\lfloor |I_i| - r_i \rfloor} \left( \frac{|I_i| - r_i}{j_i} \right) (-1)^{j_i}. \]

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

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

Extracting \( z^m \), we have

\[ [z^m \prod_{i \in T} u_i^{r_i}] EG(z, u) \]

\[ = Eq^m \prod_{i \in T} \left( \frac{|I_i|!}{r_i! (|I_i| - r_i)!} \sum_{j_i=0}^{\lfloor |I_i| - r_i \rfloor} q^{-j_i} \left( \frac{|I_i| - r_i}{j_i} \right) (-1)^{j_i} \left[ \sum_{i \in T} i (r_i + j_i) \leq m \right] \].

Hence, using the definition of \( E \), extracting the coefficient of \( (f) \), we obtain
\[ [(f) z^m \prod_{i \in T} u_i^{r_i}] E G(z, u) \]
\[ = q^{m-w} \prod_{i \in T} \left( \binom{|I_i|}{r_i} q^{-i=r_i} \sum_{j_i=0}^{r_i} q^{-i=r_i} \left( \frac{|I_i| - r_i}{j_i} \right) \right) (-1)^{r_i} \left[ \sum_{i \in T} i(r_i + j_i) \leq m \right]. \]

Adding \([(f) z^m \prod_{i \in T} u_i^{r_i}] J G(z, u)\), we obtain the result.\[ \square \]

Similarly, we obtain the following.

Proposition 8. The expression for \(H(z, u)\) can be written as follows:
\[ H(z, u) = F(z) \prod_{i \in T} \prod_{g \in I_i} \left( \frac{1 - \langle g \rangle z^{|I_i|}}{1 - \langle g \rangle z^{|I_i|} u_i} \right). \]

Proof
\[ H(z, u) = \sum_{f \in M} \langle f \rangle z^{d(f)} \prod_{g \in I} u_g^{\max\{k : g^k \mid f\}} \]
\[ = \prod_{g \in I} \left( \sum_{k \geq 0} \langle g \rangle^k u_g^k z^{d(g)} \right) \]
\[ = \prod_{g \in I} \left( \sum_{k \geq 0} \langle g \rangle^k u_g^k z^{kd(g)} \right) \]
\[ = \prod_{g \in I} \left( \frac{1}{1 - \langle g \rangle z^{d(g)} u_g} \right) \]
\[ = F(z) \prod_{g \in I} \left( \frac{1 - \langle g \rangle z^{d(g)}}{1 - \langle g \rangle z^{d(g)} u_g} \right). \]

Using the definition of \(u_g\), we obtain the result.\[ \square \]

Lemma 2. We have the following formula for \(H(z, u)\):
\[ H(z, u) = E \left( \sum_{d \geq 0} g^d z^d \prod_{i \in T} \sum_{j_i=0}^{|I_i|} \binom{|I_i|}{j_i} (-1)^{j_i} z^{j_i} \sum_{r_i \geq 0} \left( \binom{|I_i| + r_i - 1}{r_i} \right) z^{r_i} u_i^{r_i} \right) \]
\[ + J \left( \sum_{d=0}^{u-1} \sum_{f \in M_d} \langle f \rangle z^d \right) \prod_{i \in T} \prod_{g \in I_i} \left( \frac{1 - \langle g \rangle z^i}{1 - \langle g \rangle z^i u_i} \right). \]

Proof Using Proposition 8 and Equation (10), we have
\[ H(z, u) = \left( \sum_{d \geq 0} \sum_{f \in M_d} \langle f \rangle z^d \prod_{i \in T} \prod_{g \in I_i} \left( \frac{1 - \langle g \rangle z^i}{1 - \langle g \rangle z^i u_i} \right) \right). \]
It follows that

\[
EH(z, u) = E \left( \sum_{d \geq 0} \sum_{f \in M_d} \langle f \rangle z^d \right) \prod_{i \in T} \prod_{g \in I_i} \left( \frac{1 - \langle g \rangle z^l}{1 - \langle g \rangle z^l u_i} \right)
= E \left( \sum_{d \geq 0} \sum_{f \in M_d} z^d \right) \prod_{i \in T} \prod_{g \in I_i} \left( \frac{1 - z^l}{1 - z^l u_i} \right)
= E \left( \sum_{d \geq 0} q^d z^d \right) \prod_{i \in T} \left( \frac{1 - z^l}{1 - z^l u_i} \right)^{|I_i|}
= E \left( \sum_{d \geq 0} q^d z^d \right) \prod_{i \in T} \sum_{j_i = 0}^{|I_i|} \left( -1 \right)^{j_i} z^{j_i} \sum_{r_i \geq 0} \left( |I_i| + r_i - 1 \right) \frac{1}{r_i} \right) z^{i r_i u_i}.
\]

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

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

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 monic 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 \( f \) and \( g \) has \( r_i \) factors in \( I_i \) counting multiplicity for each \( i \in T \) is

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

**Proof** We note that

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

\[ H(z, u) = E \left( \sum_{d=0}^{\infty} q^d z^d \right) \prod \sum_{i \in T, j_i=0}^{\left| I_i \right|} \left( \frac{\left| I_i \right|}{j_i} \right) (-1)^{j_i} z^{j_i} \sum_{r_i \geq 0} \left( \frac{\left| I_i \right| + r_i - 1}{r_i} \right) z^{r_i} u_i^{r_i} \]

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

For the first line, extracting the coefficient of \( \prod_{i \in T} u_i^{r_i} \), we have

\[ [\prod_{i \in T} u_i^{r_i}] EH(z, u) = E \left( \sum_{d=0}^{\infty} q^d z^d \right) \prod \left( \frac{\left| I_i \right| + l_i - 1}{l_i} \right) z^{l_i} \sum_{j_i=0}^{\left| I_i \right|} \left( \frac{\left| I_i \right|}{j_i} \right) (-1)^{j_i} z^{j_i}. \]

Extracting the coefficient of \( z^m \), we have

\[ [z^m \prod_{i \in T} u_i^{l_i}] EH(z, u) \]

\[ = Eq^m \prod_{i \in T} \left( \frac{\left| I_i \right| + l_i - 1}{l_i} \right) q^{-d_i} \sum_{j_i=0}^{\left| I_i \right|} \left( \frac{\left| I_i \right|}{j_i} \right) (-1)^{j_i} q^{-ij_i} \llbracket \sum_{i \in T} i(l_i + j_i) \leq m \rrbracket. \]

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

\[ \langle f \rangle z^m \prod_{i \in T} u_i^{l_i} EH(z, u) \]

\[ = q^{m-w} \prod_{i \in T} \left( \frac{\left| I_i \right| + l_i - 1}{l_i} \right) q^{-d_i} \sum_{j_i=0}^{\left| I_i \right|} \left( \frac{\left| I_i \right|}{j_i} \right) (-1)^{j_i} q^{-ij_i} \llbracket \sum_{i \in T} i(l_i + j_i) \leq m \rrbracket. \]

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

5. Large Degree Polynomials

In this section, we derive some simpler consequences under certain restrictions such that the degree \( m \) of the desired polynomials is very large, comparing to the factorization pattern and the number of prescribed coefficients.

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

\[ N(m, \prod_{i \in T} f_i^{r_i}, \langle f \rangle) = q^{m-w} \prod_{i \in T} \left( \frac{\left| I_i \right|}{r_i} \right) (1/q^i)^{r_i} (1 - 1/q^i)^{|I_i|-r_i}. \]
Proof. By Theorem 1, we have

\[ N(m, \prod_{i \in T} I_i^{r_i}, (f)) \]

\[ = q^{m-w} \prod_{i \in T} \left( \frac{|I_i|}{r_i} \right)^{r_i} \left[ \sum_{j_i=0}^{|I_i|-r_i} q^{-ij_i} \left( \frac{|I_i|-r_i}{j_i} \right) \right] \]

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

If \( j_i \leq |I_i|-r_i \), then \( r_i+j_i \leq |I_i| \) and thus \( \sum_{i \in T} i(r_i+j_i) \leq \sum_{i \in T} i|I_i| \leq m \). Hence the bracket condition for the first line holds. 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

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

Therefore,

\[ N(m, \prod_{i \in T} I_i^{r_i}, (f)) = q^{m-w} \prod_{i \in T} \left( \frac{|I_i|}{r_i} \right)^{r_i} \left[ \sum_{j_i=0}^{|I_i|-r_i} q^{-ij_i} \left( \frac{|I_i|-r_i}{j_i} \right) \right] \]

\[ = q^{m-w} \prod_{i \in T} \left( \frac{|I_i|}{r_i} \right)^{r_i} \left[ \sum_{j_i=0}^{|I_i|-r_i} q^{-ij_i} \left( \frac{|I_i|-r_i}{j_i} \right) \right] \]

\[ = q^{m-w} \prod_{i \in T} \left( \frac{|I_i|}{r_i} \right)^{r_i} (1-1/q^{i|I_i|-r_i}). \]

When we fix \( T \) to contain only one single degree \( i \), the formula for \( N \) further simplifies.

Corollary 1. 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

\[ N(m, I_i^r, (x^w + a_1 x^{w-1} + \cdots + a_w)) = q^{m-w} \left( \frac{|I_i|}{r} \right)^r (1-1/q^{i|I_i|-r}). \]

Setting \( i = 1 \), we obtain the following results about the number of monic polynomials with a given number of distinct linear factors with the highest few consecutive terms prescribed.

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

\[ N(m, I_i^r, (x^w + a_1 x^{w-1} + \cdots + a_w)) = q^{m-w-r} \left( \frac{q}{r} \right) (1-1/q)^{q-r}. \]

Furthermore, setting \( w = 0 \), we obtain the following known result.
Corollary 3 (Theorem 3 [3]). Suppose that \( m \geq q \). Then the number of monic polynomials of degree \( m \) that have \( r \) distinct linear factors is

\[
N(m, I^r, 1) = q^{m-w-r} \left( \frac{q}{r} \right)^r (1 - 1/q)^{q-r}.
\]

Similarly, we obtain the analogous result when considering possible repeated factors.

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

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

Proof. From Theorem 2 we obtain

\[
N^*(m, \prod_{i \in T} I_i, \langle f \rangle) = q^{m-w} \prod_{i \in T} \left( \frac{|I_i| + l_i - 1}{l_i} \right) \sum_{j_i=0}^{\lfloor |I_i| / l_i \rfloor} (-1)^{j_i} q^{-j_i} \sum_{i \in T} i(l_i + j_i) \leq m
\]

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

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,

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

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

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

is a polynomial in \( z \) over \( \mathbb{C}[G] \) of degree less than \( \sum_{i=1}^n i(|I_i| + l_i) + w \leq m \). Hence,

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

Therefore,

\[
N^*(m, \prod_{i \in T} I_i, \langle f \rangle) = q^{m-w} \prod_{i \in T} \left( \frac{|I_i| + l_i - 1}{l_i} \right) q^{-i} \sum_{j_i=0}^{\lfloor |I_i| / l_i \rfloor} (-1)^{j_i} q^{-j_i}
\]

\[
= q^{m-w} \prod_{i \in T} \left( \frac{|I_i| + l_i - 1}{l_i} \right) (1/q^i)^{l_i} \sum_{j_i=0}^{\lfloor |I_i| / l_i \rfloor} (-1/q^i)^{l_i}
\]

\[
= q^{m-w} \prod_{i \in T} \left( \frac{|I_i| + l_i - 1}{l_i} \right) (1/q^i)^{l_i} (1 - 1/q^i)^{|I_i|}.
\]

Again, when we fix \( T \) to contain only one single degree \( i \), the formula for \( N^* \) further simplifies.
Corollary 4. Suppose that \( m \geq q + l + w \). 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

\[
N^*(m, I_1^l, \langle f \rangle) = q^{m-w} \left( \prod_{i=1}^{l} |I_i| + 1 \right) (1/q)^i (1 - 1/q)^{|I_i|}.
\]

Setting \( i = 1 \), we obtain the following results about the number of monic polynomials with a given number of distinct degree \( l \) irreducible 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

\[
N^*(m, I_1^l, \langle x^w + a_1 x^{w-1} + \cdots + a_w \rangle) = q^{m-w-1} \left( \prod_{i=1}^{l} |I_i| + 1 \right) (1 - 1/q)^q.
\]

Setting \( w = 0 \), we obtain the following known result.

Corollary 6 (Theorem 1 [3]). Suppose that \( m \geq q + l \). Then the number of monic degree \( m \) polynomials that have \( l \) linear factors counting multiplicity, is

\[
N^*(m, I_1^l, 1) = q^{m-1} \left( \prod_{i=1}^{l} |I_i| + 1 \right) (1 - 1/q)^q.
\]

6. \( w = 0 \): No prescribed coefficients

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 has certain factorization pattern.

In fact, when \( w = 0 \), we have \( G = \{1\} \). This means that for all \( \langle f \rangle \in G, \langle f \rangle = 1 \).

Hence we have the following consequence from Theorem 4.

Corollary 7. We have the following formula for \( N(m, \prod_{i \in T} I_i^r, \langle f \rangle) \) when \( w = 0 \):

\[
N(m, \prod_{i \in T} I_i^r, 1) = q^m \prod_{i \in T} \left( |I_i| \right)^{r_i - 1} \sum_{j_k = 0}^{r_k} q^{-j_k} \left( \sum_{i \in T} \left( I_i - 1 \right) \right)^j \left( \sum_{i \in T} i(r_i + j_i - m) \right).
\]

When we set \( T = \{i\} \), we obtain an expression for the number of degree \( m \) monic polynomials with a given number of distinct degree \( i \) irreducible factors.

Corollary 8 (Theorem 3 [3]). The number of degree \( m \) monic polynomials over \( \mathbb{F}_q \) that contains \( r \) distinct irreducible factors of degree \( i \) is

\[
N(m, I_i^r, 1) = q^{m-ir} \left( \prod_{i=1}^{r} |I_i| \right)^{m/i - r} \sum_{j=0}^{i} q^{-j} \left( \prod_{i=1}^{r} \left( |I_i| - r \right) \right)^j (-1)^j.
\]

The case when \( i = 1 \) was known in [3].
Corollary 9 (Theorem 3 [8]). The number of degree $m$ monic polynomials over $\mathbb{F}_q$ with $r$ distinct linear factors is

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

In addition to these results, we can also obtain an exact formula for the number of monic $n$-smooth polynomials of degree $m$ by using Corollary 7. This formula is useful when $n$ is close in size to $m$.

Corollary 10. The number of monic $n$-smooth polynomials over $\mathbb{F}_q$ with degree $m$ is

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

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 Corollary 7.

We can obtain a similar result to Corollary 7 when multiplicity of the factors are counted. Indeed, the following result follows from Theorem 2.

Corollary 11. Let $w = 0$. Then

$$N^*(m, \prod_{i \in T} I_i^l, 1) = q^m \prod_{i \in T} \left( |I_i| + l_i - 1 \right) q^{-il_i} \sum_{j_i=0}^{\lfloor |I_i|/l_i \rfloor} \binom{|I_i|}{j_i} (-1)^{j_i} q^{-j_i} \prod_{i \in T} i(l_i + j_i) \leq m].$$

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

Corollary 12 (Theorem 1 [9]). The number of degree $m$ monic polynomials over $\mathbb{F}_q$ with $l$ irreducible degree $i$ factors counting multiplicity is

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

The case when $i = 1$ was known in [8].

Corollary 13 (Theorem 1 [8]). The number of degree $m$ monic polynomials over $\mathbb{F}_q$ with $l$ linear factors counting multiplicity is

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

In addition to these results, we can obtain another exact formula for the number of monic $n$-smooth polynomials of degree $m$ by using Corollary 11. This formula is useful when $n$ is small.
Corollary 14. The number of monic $n$-smooth polynomials over $\mathbb{F}_q$ with degree $m$ is
\[
\sum_{l_1+2l_2+\cdots+nl_n=m} N^*(m, \prod_{i=1}^n l_i^{l_i}, 1) = q^m \prod_{i=1}^n \sum_{l_i \geq 0} \left(\frac{|I_i| + l_i - 1}{l_i}\right) q^{-il_i} \left[\sum_{i=1}^n il_i = m\right].
\]

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 polynomial is a product of factors with degrees in $T$ with Corollary 11, we obtain the result.

As a consequence of Corollaries 10 and 11, we have an identity for the number of monic $n$-smooth polynomials of degree $m$ over $\mathbb{F}_q$. This number is given by
\[
q^m \prod_{i=1}^n \sum_{l_i \geq 0} \left(\frac{|I_i| + l_i - 1}{l_i}\right) q^{-il_i} \left[\sum_{i=1}^n il_i = m\right].
\]

This identity can be proven in an elementary way. Indeed, by the unique factorization of monic polynomials, we have
\[
(\sum_{k \geq 0} q^k z^k)(1 - z^k)^{-|I_i|} = \prod_{i \geq 1} (1 - z^i)^{-|I_i|} = \sum_{k \geq 0} q^k z^k.
\]
Using generating functions, the number of monic $n$-smooth polynomials of degree $m$ is
\[
[z^n] \prod_{i=1}^n (1 - z^i)^{-|I_i|} = [z^n] \prod_{i=1}^n \sum_{l_i \geq 0} \left(\frac{|I_i| + l_i - 1}{l_i}\right) z^{il_i} = \prod_{i=1}^n \sum_{l_i \geq 0} \left(\frac{|I_i| + l_i - 1}{l_i}\right) \left[\sum_{i=1}^n il_i = m\right].
\]
Using equation (22), 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, the number of monic $n$-smooth polynomials of degree $m$ is also given by
\[
[z^m] \sum_{k \geq 0} q^k z^k \prod_{i \geq n+1} (1 - z^i)^{|I_i|} = [z^m] \sum_{k \geq 0} q^k z^k \prod_{i \geq n+1} \sum_{j_i=0}^{l_i} \left(\frac{|I_i|}{j_i}\right) (-1)^{j_i} z^{j_i} = q^m \prod_{i=1}^n \sum_{j_i=0}^{l_i} q^{-j_i} \left(\frac{|I_i|}{j_i}\right) (-1)^{j_i} \left[\sum_{i=1}^n j_i \leq m\right].
\]

7. $w = 1$: Polynomials with Prescribed Trace Term

In this section, 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 prescribed factorization pattern in terms of degrees of irreducible factors, with or without multiplicity counted.
In order to do so, we use the formula from Section 3 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

\[
|\{ (f) \in I_i, (f) = (x + \alpha) \} | = I(i, (x + \alpha)) = a_i + b_i \| \alpha = 0 \|
\]

where

\[
a_i = \frac{1}{iq} \sum_{p \mid k} \mu(k)q^{i/k}, \quad b_i = \frac{1}{q} \sum_{p \mid k} \mu(k)q^{i/k}.
\]

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 monic polynomials of 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 \( G = \{ (x + \alpha) : \alpha \in \mathbb{F}_q \} \), and

\[
(x + \alpha)(x + \beta) = (x + \alpha + \beta).
\]

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

\[
(x + \alpha)^k = (x + k\alpha).
\]

Using \( \langle x \rangle = 1 \), it follows that

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

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

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

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:

(i) \( J \prod_{\alpha \in \mathbb{F}_q} (1 + (x + \alpha)y) = J(1 - (y)^p)^{2p} \),

(ii) \( J \prod_{\alpha \in \mathbb{F}_q} \frac{1}{1 - (x+\alpha)y} = J \left( \frac{1}{1-y^p} \right)^{2p} \).
Proof 1) Using Proposition 4, Equation (25), and the power series definition for \( \exp \) and \( \log \), we have

\[
J \prod_{\alpha \in \mathbb{F}_q} (1 + \langle x + \alpha \rangle y) = J \prod_{\alpha \in \mathbb{F}_q} (1 + (x + \alpha)Jy)
\]

\[
= J \exp \left( \sum_{\alpha \in \mathbb{F}_q} \ln(1 + (x + \alpha)Jy) \right)
\]

\[
= J \exp \left( \sum_{\alpha \in \mathbb{F}_q} \sum_{k \geq 1} (-1)^{k-1} \frac{(x + \alpha)^k J^k J^k y^k}{k} \right)
\]

\[
= J \exp \left( \sum_{k \geq 1} (-1)^{k-1} \frac{J^k J^k y^k}{k} \left(qJ[p \mid k]\right) \right)
\]

\[
= J \exp \left( \sum_{k \geq 1} (-1)^{k-1} \frac{y^k}{k} \left(q[p \mid k]\right) \right)
\]

\[
= J \exp \left( \frac{q}{p} \sum_{k \geq 1} \frac{(-y)^p}{k} \right)
\]

\[
= J \exp \left( \frac{q}{p} \ln(1 - (-y)^p) \right)
\]

\[
= J \left(1 - (-y)^p\right)^{\frac{q}{p}}.
\]

2) Similarly, we have

\[
J \prod_{\alpha \in \mathbb{F}_q} \frac{1}{1 - \langle x + \alpha \rangle y} = J \prod_{\alpha \in \mathbb{F}_q} \frac{1}{1 - (x + \alpha)Jy}
\]

\[
= J \exp \left( \sum_{\alpha \in \mathbb{F}_q} \ln \left( \frac{1}{1 - \langle x + \alpha \rangle Jy} \right) \right)
\]

\[
= J \exp \left( \sum_{\alpha \in \mathbb{F}_q} \sum_{k \geq 1} \frac{(x + \alpha)^k J^k y^k}{k} \right)
\]

\[
= J \exp \left( \sum_{k \geq 1} \frac{J^k y^k}{k} \left(qJ[p \mid k]\right) \right)
\]

\[
= J \exp \left( \sum_{k \geq 1} \frac{y^k}{k} \left(q[p \mid k]\right) \right)
\]

\[
= J \exp \left( \frac{q}{p} \ln \left( \frac{1}{1 - y^p} \right) \right)
\]

\[
= J \left( \frac{1}{1 - y^p} \right)^{\frac{q}{p}}.
\]
Define the following numbers

\[ A_m(a, 0) = \left(\frac{aq}{m/p}\right)(-1)^{m/m/p} \left\lfloor \frac{m}{p} \right\rfloor, \]  

\[ B_m(a, 0) = \left(\frac{aq + m/p - 1}{m/p}\right) \left\lfloor \frac{m}{p} \right\rfloor, \]  

and, for \( b \neq 0, \)

\[ A_m(a, b) = \sum_{j=0}^{[m/p]} \left(\frac{aq}{j}\right) \left(\frac{b}{m - pj}\right)(-1)^{j + pj}, \]  

\[ B_m(a, b) = \sum_{j=0}^{[m/p]} \left(\frac{aq + j - 1}{j}\right) \left(\frac{b + m - pj - 1}{m - pj}\right). \]

Combining these numbers with (24), we obtain information related to the set of monic irreducible polynomials of degree \( i. \)

**Proposition 10.** Let \( a_i, b_i \) defined in (24) and \( A_m(a_i, b_i), B_m(a_i, b_i) \) be defined in (28) and (29). Then

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

(ii) \( \frac{1}{J} = J \sum_{m \geq 0} B_m(a_i, b_i)y^m. \)

**Proof.** 1) Using \( \langle x \rangle = 1 \) and \( I(i, (x + \alpha)) = a_i + b_i[\alpha = 0], J^k = J \) for \( k \geq 1, \) and Proposition 9, we have

\[ J \prod_{f \in I_i} (1 + \langle f \rangle y) = J \prod_{\alpha \in \mathbb{F}_q} (1 + \langle x + \alpha \rangle y)^{a_i + b_i[\alpha = 0]} \]

\[ = J(1 + \langle x \rangle y)^{b_i} \prod_{\alpha \in \mathbb{F}_q} (1 + \langle x + \alpha \rangle y)^{a_i} \]

\[ = J(1 - (-y)^{\frac{a_i}{b_i}} + \sum_{m \geq 0} \left(\frac{aq/p}{j}\right)(-1)^{j + pj} \left(\frac{b_i}{m - pj}\right)y^m \]

\[ = J \sum_{m \geq 0} \sum_{j=0}^{[m/p]} \left(\frac{aq/p}{j}\right)(-1)^{j + pj} \left(\frac{b_i}{m - pj}\right)y^m \]

\[ = J \sum_{m \geq 0} A_m(a_i, b_i)y^m. \]
2) Similarly, we have

\[ J \prod_{j \in I} \frac{1}{1 - \langle j \rangle y} = J \prod_{\alpha \in \mathbb{F}_q} \left( \frac{1}{1 - \langle x + \alpha \rangle y} \right)^{a_i + b_i[\alpha = 0]} \]

\[ = J \left( \frac{1}{1 - \langle x \rangle y} \right)^b \prod_{\alpha \in \mathbb{F}_q} \left( \frac{1}{1 - \langle x + \alpha \rangle y} \right)^{a_i} \]

\[ = J \left( \frac{1}{1 - y^p} \right)^{\frac{a}{r}} \left( \frac{1}{1 - y} \right)^b \]

\[ = J \sum_{m \geq 0} \sum_{j = 0}^{\lceil m/p \rceil} \left( a_i q/p + j - 1 \right) \left( b_i + m - pj - 1 \right) y^m \]

\[ = J \sum_{m \geq 0} B_m(a_i, b_i) y^m. \]

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

**Theorem 5.** Suppose \( w = 1 \). Then

\[ N(m, \prod_{i \in T} I_{r_i}, \langle x + \alpha \rangle) \]

\[ = q^{m-1} \prod_{i \in T} \left( \frac{|I_i|}{r_i} \right) q^{-ir_i} \sum_{j_i = 0}^{\lfloor |I_i| - r_i \rfloor} q^{-i j_i} \left( \frac{|I_i| - r_i}{j_i} \right) (-1)^{j_i} \sum_{i \in T} i(r_i + j_i) \leq m \]

\[ + \frac{v(\alpha)}{q} \prod_{i \in T} \sum_{k_i \geq 0} A_{k_i}(a_i, b_i) \left( \frac{k_i}{r_i} \right) (-1)^{k_i - r_i} \sum_{i = 1}^{n} i k_i = m, \]

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

**Proof** Using Theorem 11 we have

\[ N(m, \prod_{i \in T} I_{r_i}, \langle x + \alpha \rangle) \]

\[ = q^{m-1} \prod_{i \in T} \left( \frac{|I_i|}{r_i} \right) q^{-ir_i} \sum_{j_i = 0}^{\lfloor |I_i| - r_i \rfloor} q^{-i j_i} \left( \frac{|I_i| - r_i}{j_i} \right) (-1)^{j_i} \sum_{i \in T} i(r_i + j_i) \leq m \]

\[ + [(x + \alpha) z^m \prod_{i \in T} u_i^{r_i}] J \prod_{i \in T} \prod_{g \in I_i} (1 + (g) z^i(u_i - 1)). \]

Using \( J^k = J \) for any positive integer \( k \) and Proposition 10, we have

\[ [(x + \alpha) z^m \prod_{i \in T} u_i^{r_i}] J \prod_{i \in T} \prod_{g \in I_i} (1 + (g) z^i(u_i - 1)) \]

\[ = [(x + \alpha) z^m \prod_{i \in T} u_i^{r_i}] J \prod_{i \in T} \sum_{k_i \geq 0} A_{k_i}(a_i, b_i) z^{j k_i} (u_i - 1)^{k_i}. \]
Extracting coefficients of the $u_i$ by using the Binomial Theorem, the latter equals

$$[(x + \alpha)z^m]J \prod_{i \in T} \sum_{k_i \geq 0} A_k(i, b_i)z^{ik_i} \left(\frac{k_i}{r_i}\right)(-1)^{k_i-r_i}. $$

Extracting the coefficient of $z$, we obtain

$$[(x + \alpha)]J \prod_{i \in T} \sum_{k_i \geq 0} A_k(i, b_i) \left(\frac{k_i}{r_i}\right)(-1)^{k_i-r_i}[\sum_{i=1}^n ik_i = m].$$

Using $J = 1 - E = \sum_{\alpha \in F_q} \frac{v(\alpha)}{q}(x + \alpha)$, and extracting $(x + \alpha)$, this simplifies to

$$\frac{v(\alpha)}{q} \prod_{i \in T} \sum_{k_i \geq 0} A_k(i, b_i) \left(\frac{k_i}{r_i}\right)(-1)^{k_i-r_i}[\sum_{i=1}^n ik_i = m],$$

The proof is complete by combining all the pieces together. \[ \]

Corollary 15. Suppose $w = 1$. Suppose that $p \nmid i$ for each $i \in T$.

If $p \not| m$, then

$$N(m, \prod_{i \in T} I_{r_i}, \langle x + \alpha \rangle)$$

$$= q^{m-1} \prod_{i \in T} \left(\frac{|I_i|}{r_i}\right)q^{-ir_i} \sum_{j_i=0}^{\frac{|I_i|-r_i}{i}} q^{-ij_i} \left(\frac{|I_i|-r_i}{j_i}\right)(-1)^{j_i}[\sum_{i \in T} i(r_i + j_i) \leq m].$$

If $p \mid m$, then

$$N(m, \prod_{i \in T} I_{r_i}, \langle x + \alpha \rangle)$$

$$= q^{m-1} \prod_{i \in T} \left(\frac{|I_i|}{r_i}\right)q^{-ir_i} \sum_{j_i=0}^{\frac{|I_i|-r_i}{i}} q^{-ij_i} \left(\frac{|I_i|-r_i}{j_i}\right)(-1)^{j_i}[\sum_{i \in T} i(r_i + j_i) \leq m]$$

$$+ \frac{v(\alpha)}{q} \prod_{i \in T} \sum_{k_i \geq 0} \left(\frac{|I_i|/p}{k_i}\right) \left(\frac{pk_i}{r_i}\right)(-1)^{k_i-r_i}[\sum_{i=1}^n ik_i = m/p],$$

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

Proof. The result follows from Theorem 3 by setting $b_i = 0$ for each $i$, and using (20), 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 trace term is fixed.

Corollary 16 (Theorem 3.1 [20]). The number of monic polynomials over $F_q$ of the form $x^m + \alpha x^{m-1} + g(x)$ for fixed $\alpha \in F_q$, where $g \in F_q[x]$ has degree at most $m - 2$, that have $r$ distinct linear factors is given as follows:

If $p \not| m$, then

$$N(m, I^r, \langle x + \alpha \rangle) = q^{m-r-1} \left(\binom{q}{r}\right) \sum_{j=0}^{m-r} q^{-j} \left(\binom{q}{j}\right)(-1)^j.$$
If $p \mid m$, then
\[
N(m, I^r, \langle x + \alpha \rangle) = q^{m-r-1} \left( \frac{q}{r} \right) \sum_{j=0}^{m-r} q^{-j} \binom{q - r}{j} (-1)^j + \frac{v(\alpha)}{q} \left( \frac{q/p}{m/p} \right) \left( \frac{m}{r} \right) (-1)^{m/p-r},
\]
where $v(\alpha) = q[\alpha = 0] - 1$.

**Proof** The result follows from Theorem 5 by taking $T = \{1\}$, and using $|I_1| = q$. \hfill \square

Now, we state a result about degree $m$ monic $n$-smooth polynomials with a prescribed trace coefficient, which comes from Theorem 5. This formula is most useful when $n$ is close to $m$.

**Corollary 17.** 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
\[
N(m, \prod_{i=n+1}^m I^0_i, \langle x + \alpha \rangle) = q^{m-1} \prod_{i=n+1}^m q^{-\ell_i} \sum_{j_i=0}^{\ell_i} \binom{\ell_i}{j_i} \sum_{i=n+1} m ij_i \leq m]
+ \frac{v(\alpha)}{q} \prod_{i \in T} B_{l_i}(a_i, b_i) \sum_{k_i \geq 0} A_{k_i}(a_i, b_i)(-1)^{k_i} \sum_{i \in T} i(l_i + k_i) = m],
\]
where $v(\alpha) = q[\alpha = 0] - 1$.

**Proof** The result follows from Theorem 5 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 $n$. \hfill \square

Next, we give a general formula for $N^*$. That is the case where the multiplicity of the trace factors is counted.

**Theorem 6.** Suppose $w = 1$. Then
\[
N^*(m, \prod_{i \in T} I^l_i, \langle x + \alpha \rangle)
= q^{m-1} \prod_{i \in T} \left( \binom{\ell_i}{l_i} + \ell_i - 1 \right) q^{-\ell_i} \sum_{j_i=0}^{\ell_i} \binom{\ell_i}{j_i} \sum_{i \in T} i(l_i + j_i) \leq m]
+ \frac{v(\alpha)}{q} \prod_{i \in T} B_{l_i}(a_i, b_i) \sum_{k_i \geq 0} A_{k_i}(a_i, b_i)(-1)^{k_i} \sum_{i \in T} i(l_i + k_i) = m],
\]
where $v(\alpha) = q[\alpha = 0] - 1$.

**Proof** Using Theorem 5, we have
\[
N^*(m, \prod_{i \in T} I^l_i, \langle x + \alpha \rangle)
= q^{m-1} \prod_{i \in T} \left( \binom{\ell_i}{l_i} + \ell_i - 1 \right) q^{-\ell_i} \sum_{j_i=0}^{\ell_i} \binom{\ell_i}{j_i} \sum_{i \in T} i(l_i + j_i) \leq m]
+ [a + \alpha > z^m \prod_{i \in T} u^l_i] J \prod_{i \in T} \prod_{g \in I_i} \left( \frac{1 - \langle g \rangle z^{l_i}}{1 - \langle g \rangle z^{l_i} u_i} \right).
\]
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

$$[\langle x + \alpha \rangle^m \prod_{i \in T} u_i^{l_i}] J \prod_{i \in T} \prod_{y \in L_i} \left( \frac{1 - \langle g \rangle z^i}{1 - \langle g \rangle z} u_i \right)$$

$$= [\langle x + \alpha \rangle^m \prod_{i \in T} B_i(a_i, b_i) z^{l_i} \sum_{k_i \geq 0} A_{k_i}(a_i, b_i)(-z^i)^{k_i}$$

$$= [\langle x + \alpha \rangle^m \prod_{i \in T} B_i(a_i, b_i) \sum_{k_i \geq 0} A_{k_i}(a_i, b_i)(-1)^{k_i} z^{l_i + k_i}$$

$$= [\langle x + \alpha \rangle^m \prod_{i \in T} B_i(a_i, b_i) \sum_{k_i \geq 0} A_{k_i}(a_i, b_i)(-1)^{k_i} \sum_{i \in T} i(l_i + k_i) = m]$$

$$= \frac{\nu(\alpha)}{q} \prod_{i \in T} B_i(a_i, b_i) \sum_{k_i \geq 0} A_{k_i}(a_i, b_i)(-1)^{k_i} \sum_{i \in T} i(l_i + k_i) = m],$$

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

As a corollary to Theorem 6, we have the following simpler result.

**Corollary 18.** Suppose $w = 1$. Suppose that $p \nmid i$ for each $i \in T$.

If $p \nmid m$ or $p \nmid l_i$ for some $i$, then

$$N^*(m, \prod_{i \in T} I_i^l, \langle x + \alpha \rangle)$$

$$= q^{m-1} \prod_{i \in T} \left( |I_i| + l_i - 1 \right) q^{-l_i} \sum_{j_i = 0}^{\lfloor |I_i| \rfloor} \left( \frac{|I_i|}{j_i} \right) (-1)^{j_i} q^{-j_i} \left[ \sum_{i \in T} i(l_i + j_i) \leq m \right].$$

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

$$N^*(m, \prod_{i \in T} I_i^l, \langle x + \alpha \rangle)$$

$$= q^{m-1} \prod_{i \in T} \left( |I_i| + l_i - 1 \right) q^{-l_i} \sum_{j_i = 0}^{\lfloor |I_i| \rfloor} \left( \frac{|I_i|}{j_i} \right) (-1)^{j_i} q^{-j_i} \left[ \sum_{i \in T} i(l_i + j_i) \leq m \right]$$

$$+ \frac{\nu(\alpha)}{q} \prod_{i \in T} \left( \frac{|I_i|}{p} + l_i/p - 1 \right) q^{l_i/p} \sum_{k_i = 0}^{\lfloor |I_i|/p \rfloor} \left( \frac{|I_i|/p}{k_i} \right) (-1)^{p k_i} \left[ \sum_{i \in T} i(l_i/p + k_i) = m/p \right],$$

where $\nu(\alpha) = q^{[\alpha = 0]} - 1$.

**Proof.** The result follows from Theorem 6 by setting $b_i = 0$ for each $i$, using (20) and (27), and noting that $q a_i = |I_i|$ for $p \nmid i$. \( \blacksquare \)

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 $x^{m-1}$.

**Corollary 19.** 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
\[
N^*(m, \prod_{i \in T} I_i^l, (x + \alpha)) = q^{m-l-1} \binom{q + l - 1}{l} \sum_{j=0}^{m-l} \binom{q}{j} (-1)^j q^{-j}.
\]

If \( p \mid m \) and \( p \mid l \), then
\[
N^*(m, \prod_{i \in T} I_i^l, (x + \alpha)) = q^{m-l-1} \binom{q + l - 1}{l} \sum_{j=0}^{m-l} \binom{q}{j} (-1)^j q^{-j} + \frac{v(\alpha)}{q} \left( \frac{q/p + l/p - 1}{l/p} \right) \left( \frac{q/p}{(m-l)/p} \right) (-1)^{m-l},
\]
where \( v(\alpha) = q[\alpha = 0] - 1 \).

**Proof** The result follows from Corollary 13 by taking \( T = \{1\} \), and using \( |I_1| = q \).

Using Corollary 6, we obtain another formula for the number of \( n \)-smooth degree \( m \) monic polynomials with a prescribed trace coefficient. The result looks different from Theorem 17 and it is useful when \( n \) is small.

**Corollary 20.** 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
\[
\sum_{l_1 + 2l_2 + \cdots + nl_n = m} N^*(m, \prod_{i=1}^{n} I_i^{l_i}, 1) = q^m \prod_{i=1}^{n} \sum_{l_i \geq 0} \binom{I_i + l_i - 1}{l_i} q^{-il_i} \llbracket \sum_{i=1}^{n} il_i = m \rrbracket
\]
\[
+ \frac{v(\alpha)}{q} \prod_{i=1}^{n} \sum_{l_i \geq 0} B_{il_i}(a_i, b_i) \llbracket \sum_{i=1}^{n} il_i = m \rrbracket,
\]
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 6 where the polynomial is a product of factors with degrees in \( T \), we obtain the result.

Corollaries 17 and 20 give two different looking expressions 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 \( m - 2 \). In order to use these formulas in computation, one should check the size of \( n \) compared to \( m \). If \( n \) is much bigger than 1, it is likely faster to use Corollary 17 while if \( n \) is much closer to 1 than \( m \), it is probably faster to use Corollary 20.

The equivalence of these two formulas can be verified directly using generating functions in a similar way to the case \( w = 0 \). Indeed, the number of \( n \)-smooth polynomials of degree \( m \) 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
\[
[(x + \alpha)z^m] \prod_{i=1}^{n} \prod_{f \in I_i} (1 - (f)z^i)^{-1}.
\]

From unique factorization of monic polynomials, we have
\[
F(z) = \prod_{i \geq 1} \prod_{f \in I_i} (1 - (f)z^i)^{-1} = 1 + \sum_{k \geq 1} \sum_{f \in M_k} (f)z^k.
\]
Using $E(f) = E$ and $E^2 = E$, we have

\[(31) \quad EF(z) = E \prod_{i \geq 1} (1 - z^i)^{-|I_i|} = E \sum_{k \geq 0} q^k z^k.\]

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

\[(32) \quad JF(z) = J \prod_{i \geq 1} \prod_{f \in I_i} (1 - \langle f \rangle z^i)^{-1} = J.\]

Applying $F(z) = \prod_{i \geq 1} \prod_{f \in I_i} (1 - \langle f \rangle z^i)^{-1}$ to Equations (31) and (32), we obtain

\begin{align*}
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).
\end{align*}

From Proposition 10 we have

\begin{align*}
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_i(a_i, b_i) z^{ik}, \\
J \prod_{i \geq n+1} \prod_{f \in I_i} (1 - \langle f \rangle z^i)^{-1} & = \prod_{i \geq n+1} \sum_{k \geq 0} A_i(a_i, b_i)(-1)^{ik} z^{ik}.
\end{align*}

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

\begin{align*}
\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_i(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_i(a_i, b_i)(-1)^{ik} z^{ik}.
\end{align*}

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

\begin{align*}
[(x + \alpha) z^m] \prod_{i=1}^{n} \prod_{f \in I_i} (1 - \langle f \rangle z^i)^{-1} & = \frac{1}{q} \sum_{i=1}^{n} l_i \prod_{l_i \geq 0} (|I_i| + l_i - 1) \left[ \sum_{i=1}^{n} i l_i = m \right] \\
& + \frac{v(\alpha)}{q} \prod_{i=1}^{n} \sum_{l_i \geq 0} B_i(a_i, b_i) \left[ \sum_{i=1}^{n} i l_i = m \right] \\
& = q^{m-1} \prod_{i=n+1}^{m} \sum_{j_i=0}^{\frac{|I_i|}{j_i}} q^{-ij_i} \left( \frac{|I_i|}{j_i} \right) (-1)^{ij_i} \left[ \sum_{i=n+1}^{m} ij_i \leq m \right] \\
& + \frac{v(\alpha)}{q} \prod_{i=n+1}^{m} \sum_{k_i \geq 0} A_i(a_i, b_i)(-1)^{ik_i} \left[ \sum_{i=n+1}^{m} ik_i = m \right],
\end{align*}

as desired.
ACKNOWLEDGMENT

We thank Zhicheng Gao for many helpful discussions.

REFERENCES

[1] M. Car, Théorèmes de densité dans $F_q[X]$. (French) (Density theorems in $F_q[X]$), Acta Arith. 48 (1987), no. 2, 145-165.
[2] L. Carlitz, A theorem of Dickson on irreducible polynomials, Proc. Amer. Math. Soc. 3 (1952), 693-700.
[3] L. Dong, Z. Gao, D. Panario, Enumeration of decomposable combinatorial structures with restricted patterns. Ann. Comb. 12 (2009), no. 4, 357-372.
[4] R. W. Fitzgerald and J. L. Yucas, Irreducible polynomials over GF(2) with three prescribed coefficients, Finite Fields Appl. 9 (2003), 286-299.
[5] 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.
[6] Z. Gao, S. Kuttner, Q. Wang, Counting irreducible polynomials with prescribed coefficients over a finite field, preprint.
[7] Z. Gao, D. Panario, Degree distribution of the greatest common divisor of polynomials over $F_q$. Random Structures Algorithms 29 (2006), no. 1, 26-37.
[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] J. Li, D. Wan, Distance distribution in Reed-Solomon codes, IEEE Trans. Inform. Theory 66 (2020), no. 5, 2743-2750.
[11] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
[12] R. Lovorn, Rigorous, subexponential algorithms for discrete logarithm algorithms in $F_{p^2}$. PhD thesis University of Georgia, 1992.
[13] M. Moisio and K. Ranto, Elliptic curves and explicit enumeration of irreducible polynomials with two coefficients prescribed, Finite Fields Appl. 14 (2008), 798-815.
[14] G. L. Mullen, D. Panario, Handbook of Finite Fields, Discrete Mathematics and its Applications (Boca Raton), CRC Press, Boca Raton, FL, 2013.
[15] 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.
[16] 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.
[17] F. Ruskey, C. R. Mers, J. Sawada, The number of irreducible polynomials and Lyndon words with given trace. SIAM J. Discrete Math. 14 (2001), no. 2, 240-245.
[18] R. Sedgewick and P. Flajolet, An Introduction to the Analysis of Algorithms, Addison Wesley, 1996.
[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.

School of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada K1S5B6
Email address: SimonKuttner@cmail.carleton.ca, wang@math.carleton.ca