ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 46, Number 5, 2016

THE NUMBER OF IRREDUCIBLE POLYNOMIALS WITH THE FIRST TWO PRESCRIBED COEFFICIENTS OVER A FINITE FIELD

MATILDE LALÍN AND OLIVIER LAROCQUE

ABSTRACT. We use elementary combinatorial methods, together with the theory of quadratic forms, over finite fields to obtain the formula, originally due to Kuz'min, for the number of monic irreducible polynomials of degree n over a finite field $\mathbb{F}_q$ with the first two prescribed coefficients. The formula relates the number of such irreducible polynomials to the number of polynomials that split over the base field.

1. Introduction. Let $\mathbb{F}_q$ be the finite field of q elements and characteristic p, and let $\mathbf{a} = (a_1, \ldots, a_\ell)$ be fixed. The problem of counting the number of irreducible polynomials,

$$x^n + a_1 x^{n-1} + \cdots + a_\ell x^{n-\ell} + t_{\ell+1} x^{n-\ell-1} + \cdots + t_n \in \mathbb{F}_q[x],$$

has been studied extensively. Asymptotic results were initiated by Artin [**1**] and answered in the most generality by Cohen [**7**]. In the domain of exact formulas Carlitz [**2**] and Yucas [**17**] have established formulas where the first or the last coefficient are fixed. This has also been studied by Omidi Koma, et al. [**16**]. Kuz'min [**10, 11**] has proved formulas where the first two coefficients are fixed and obtained partial results with three coefficients [**13**]. There is also work of Kuz'min [**12**], Cattell, et al. [**4**], Yucas and Mullen [**18**] and Fitzerald and Yucas [**8**] that expands solutions to three fixed coefficients in characteristic 2. More extensive results in characteristics 2 and 3 were proven by Moisio and Ranto [**15**]. We refer the reader to surveys of Cohen [**5, 6**] for more information.

2010 AMS *Mathematics subject classification.* Primary 11T06, 12E05.
Keywords and phrases. Irreducible polynomials, finite fields.
This work was supported by the Natural Sciences and Engineering Research Council of Canada, Discovery grant No. 355412-2013, the Fonds de recherche du Québec–Nature et technologies, Établissement de nouveaux chercheurs No. 144987 and Projet de recherche en équipe No. 166534.
Received by the editors on April 7, 2014, and in revised form on October 30, 2014.
DOI:10.1216/RMJ-2016-46-5-1587 Copyright ©2016 Rocky Mountain Mathematics Consortium

In this work, we examine the problem of two fixed coefficients. Let $H_n(a_1, a_2)$ be the number of irreducible polynomials of the form:

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + t_3 x^{n-3} + \cdots + t_n \in \mathbb{F}_q[x].$$

Kuz'min, building upon the ideas of Carlitz [**2**] and Hayes [**9**], proved the following result.

Theorem 1.1 ([**11,** Theorem 1], [**12**])**.** *Let $p > 2$ and a be nonzero. Then, for $n \geq 2$,*

$$H_n(0, a) = \frac{1}{n} \sum_{\substack{d \mid n \\ p \nmid d}} \mu(d) \delta_{n/d}(-a/d), \tag{1.1}$$

and

$$H_n(0, 0) = \frac{1}{n} \sum_{\substack{d \mid n \\ p \nmid d}} \mu(d) \delta_{n/d}(0) - \frac{\varepsilon}{n} \sum_{\substack{d \mid n/p \\ p \nmid d}} \mu(d) q^{n/dp}, \tag{1.2}$$

where $\varepsilon = 1$ if $p \mid n$ and 0, otherwise.

If $p \mid n$,

$$H_n(1, 0) = \frac{1}{q^2 n} \sum_{\substack{d \mid n \\ p \nmid d}} \mu(d) q^{n/d}. \tag{1.3}$$

Here, μ denotes the Möbius function defined as

$$\mu(n) = \begin{cases} (-1)^r & n \text{ square-free and} \\ n & \text{is a product of } r \text{ distinct primes,} \\ 0 & n \text{ is not square-free.} \end{cases}$$

For $n \geq 1$ and $a \in \mathbb{F}_q$,

$$\delta_n(a) = q^{n-2} + (-1)^n (q^{n-2} - Q_{n-1}(a)),$$

with $Q_n(a)$ being the number of solutions of the equation

$$\sum_{i=1}^{n} x_i^2 + \sum_{1 \leq i < j \leq n} x_i x_j = a. \tag{1.4}$$

For $p > 2$, $p \nmid n$,

$$\delta_n(a) = \begin{cases} q^{n-2} - \left(\frac{(-1)^l la}{q}\right) q^{l-1} & n = 2l, \\ \\ q^{n-2} + v(a)\left(\frac{(-1)^l n}{q}\right) q^{l-1} & n = 2l+1, \end{cases}$$

while, for $p \mid n$,

$$\delta_n(a) = \begin{cases} q^{n-2} - v(a)\left(\frac{(-1)^l}{q}\right) q^{l-1} & n = 2l, \\ \\ q^{n-2} + \left(\frac{(-1)^{l-1} 2a}{q}\right) q^{l} & n = 2l+1, \end{cases}$$

where

$$v(a) = \begin{cases} -1 & a \neq 0, \\ q-1 & a = 0. \end{cases}$$

When $p \nmid n$, the change of variables $x_1 = x + a_1/n$ allows us to write

$$H_n(a_1, a_2) = H_n\left(0, a_2 - \frac{n-1}{2n} a_1^2\right).$$

When $p \mid n$ and $a_1 \neq 0$, the change

$$x_1 = \frac{1}{a_1}\left(x - \frac{a_2}{a_1}\right)$$

implies

$$H_n(a_1, a_2) = H_n(1, 0).$$

Therefore, Theorem 1.1 provides a complete answer for the value of $H_n(a_1, a_2)$ in all cases. A similar result for $p = 2$ is also proven in **[11, 12]**.

Let $X_{(d^{n/d})}(0, a)$ denote the number of polynomials of the form $f^{n/d}$ with f irreducible, and such that $a_1 = 0$ and $a_2 = a$. The key to the proof of Theorem 1.1 lies in the equation:

$$\sum_{d \mid n} d X_{(d^{n/d})}(0, a) = \delta_n(-a). \tag{1.5}$$

The final result is then proven by means of Möbius inversion.

The first cases of Theorem 1.1 for $n \leq 7$ are analyzed **[10]** by elementary combinatorial methods, while the general case is proven **[11, 12]** by using L-functions and Gauss sums.

The goal of this paper is to complete the work of **[10]**, namely, to show that the elementary combinatorial methods introduced by Kuz'min can also be used to prove equation (1.5) and ultimately Theorem 1.1 completely. This is analogous to the work of Yucas **[17]** who gave elementary proofs for results of Carlitz **[2]** for fixed first or constant coefficient.

The combinatorial method has great potential for finding formulas in other cases, most notably in the cases of different prescribed factorization type. This method is also promising for formulas involving a higher number of fixed coefficients, although it should be noted that proving such formulas would be quite involved from the combinatorial point of view. Finally, we remark that the combinatorial part of the method works for any characteristic as reflected in the statement of equation (1.5). We focus on the case of $p > 2$ for simplicity, but the central proof is independent of the characteristic.

2. Notation. Let $\mathbf{a} = (a_1, \dots, a_\ell)$ with $\ell \leq n$. Let $\mathcal{P}_n(\mathbf{a})$ be the set of polynomials of the form $x^n + a_1x^{n-1} + \cdots + a_\ell x^{n-\ell} + t_{\ell+1}x^{n-\ell-1} + \cdots + t_n \in \mathbb{F}_q[x]$. Let $H_n(\mathbf{a})$ be the number of polynomials in $\mathcal{P}_n(\mathbf{a})$ that are irreducible. We write $\mathcal{P}_n$ and H_n when no conditions are imposed on the coefficients.

By the *type* of a polynomial in $\mathbb{F}_q[x]$ we refer to the collection of degrees of irreducible factors together with their multiplicities in the canonical decomposition of the polynomial over $\mathbb{F}_q[x]$. For example, $x^2(x+1)$ has type $(1^2, 1)$. We denote by $X_{\mathbf{v}}(\mathbf{a})$ the number of polynomials of type $\mathbf{v}$ in $\mathcal{P}_n(\mathbf{a})$. For example, $X_{(1^2,1)}$ (with no condition on the coefficients) denotes the number of polynomials of type $(1^2, 1)$, i.e., polynomials of the form $(x+\alpha)^2(x+\beta)$ with $\alpha \neq \beta$. Then we have that $X_{(1^2,1)} = q(q-1)$.

In this paper, we are going to work mainly with the specific case of $\ell = 2$. Accordingly, $n \geq 2$.

3. Results and strategy. Our goal is to prove equation (1.1). We are going to obtain this result as a corollary to the following identity.

(3.1)
$$\sum_{\substack{d|n\\ p\nmid n/d}} dH_d\left(0,\frac{ad}{n}\right)+(-1)^n\sum_{e_1+\cdots+e_k=n}\frac{n!}{e_1!\cdots e_k!}X_{(1^{e_1},\ldots,1^{e_k})}(0,a) = q^{n-2}+(-1)^n q^{n-2}.$$

This equation reduces to equation (1.1) by an application of the Möbius inversion because of the following result:

$$\sum_{e_1+\cdots+e_k=n}\frac{n!}{e_1!\cdots e_k!}X_{(1^{e_1},\ldots,1^{e_k})}(0,a)=Q_{n-1}(-a). \tag{3.2}$$

One can easily see that the left hand side of (3.2) is equivalent to the number of solutions of

$$\begin{cases}\displaystyle\sum_{i=1}^{n} x_i=0,\\ \displaystyle\sum_{1\le i<j\le n} x_i x_j = a,\end{cases}$$

which can be seen to be the same as the number of solutions of (1.4) (with the opposite sign for a). Then the number $Q_{n-1}(-a)$ is found by using Minkowski's method from the theory of quadratic forms over finite fields, see **[3, 14]** for more details.

Equation (3.1) is analogous to
(3.3)
$$\sum_{d|n} dH_d+(-1)^n\sum_{e_1+\cdots+e_k=n}\frac{n!}{e_1!\cdots e_k!}X_{(1^{e_1},\ldots,1^{e_k})}=q^n+(-1)^n q^n,$$

and

$$\sum_{\substack{d|n\\ p\nmid n/d}} dH_d\left(\frac{ad}{n}\right)+(-1)^n\sum_{e_1+\cdots+e_k=n}\frac{n!}{e_1!\cdots e_k!}X_{(1^{e_1},\ldots,1^{e_k})}(a) = q^{n-1}+(-1)^n q^{n-1}. \tag{3.4}$$

Notice that, in the case of equation (3.3), we have that

$$\sum_{e_1+\cdots+e_k=n} \frac{n!}{e_1!\cdots e_k!} X_{(1^{e_1},\ldots,1^{e_k})} = q^n, \tag{3.5}$$

since this is equivalent to all of the possible products of linear factors that one can form by choosing n ordered linear factors among q possibilities. By equation (3.4), we have, for $p \nmid n$ and $a \neq 0$,

$$\sum_{e_1+\cdots+e_k=n} \frac{n!}{e_1!\cdots e_k!} X_{(1^{e_1},\ldots,1^{e_k})}(a) = q^{n-1}, \tag{3.6}$$

since this is the number of solutions of

$$\sum_{i=1}^{n} x_i = -a.$$

By Möbius inversion, equations (3.3) and (3.4) imply the well known results:

$$H_n = \frac{1}{n}\sum_{d|n} \mu(d) q^{n/d}, \tag{3.7}$$

$$H_n(a) = \begin{cases} \frac{1}{qn}\sum_{\substack{d|n \\ p\nmid d}} \mu(d)q^{n/d} & a \neq 0, \\ \frac{1}{qn}\sum_{\substack{d|n \\ p\nmid d}} \mu(d)q^{n/d} - \frac{\varepsilon}{n}\sum_{\substack{d|n/p \\ p\nmid d}} \mu(d)q^{n/dp} & a = 0, \end{cases} \tag{3.8}$$

where $\varepsilon = 1$ if $p \mid n$ and 0 otherwise. See, for example, **[17]**.

Proof of Theorem 1.1. Equations (3.1) and (3.2) combined yield

$$\sum_{\substack{d|n \\ p\nmid n/d}} dH_d\left(0, \frac{ad}{n}\right) = \delta_n(-a).$$

Write $n = mp^r$ with $p \nmid m$. Thus, we write, more precisely,

$$\sum_{d|m} dp^r H_{dp^r}(0, a_1 d) = \delta_{mp^r}(-a_1 m),$$

where $a_1 = a/m$.

By Möbius inversion,

$$mp^r H_{mp^r}(0, a_1 m) = \sum_{d|m} \delta_{dp^r}(-a_1 d),$$

which translates into (1.1) by reversing all changes of variable.

Now equations (1.1) and (3.8) give us

$$\begin{aligned} H_n(0,0) &= H_n(0) - \sum_{a\neq 0} H_n(0,a) \\ &= \frac{1}{qn}\sum_{\substack{d\mid n\\ p\nmid d}} \mu(d)q^{n/d} \\ &\quad - \frac{\varepsilon}{n}\sum_{\substack{d\mid n/p\\ p\nmid d}} \mu(d)q^{n/dp} - \frac{1}{n}\sum_{\substack{d\mid n\\ p\nmid d}} \mu(d)\sum_{a\neq 0}\delta_{n/d}(-a/d). \end{aligned}$$

By observing that $\sum_a Q_{n/d-1}(-a/d)$ is simply the number of possibilities of choosing $n/d-1$ elements in $\mathbb{F}_q$, $q^{n/d-1}$, we conclude

$$\sum_{a\neq 0}\delta_{n/d}(-a/d) = \sum_a \delta_{n/d}(-a/d) - \delta_{n/d}(0) = q^{n/d-1} - \delta_{n/d}(0).$$

Thus,

$$H_n(0,0) = \frac{1}{n}\sum_{\substack{d\mid n\\ p\nmid d}} \mu(d)\delta_{n/d}(0) - \frac{\varepsilon}{n}\sum_{\substack{d\mid n/p\\ p\nmid d}} \mu(d)q^{n/dp}.$$

If $p \mid n$, we have

$$\begin{aligned} H_n &= \sum_{a_1,a_2} H_n(a_1,a_2) \\ &= \sum_{a_1\neq 0,a_2} H_n(a_1,a_2) + \sum_{a_2} H_n(0,a_2) \\ &= (q-1)qH_n(1,0) + H_n(0) \\ &= (q-1)qH_n(1,0) + H_n - (q-1)H_n(1). \end{aligned}$$

Thus,

$$H_n(1,0) = \frac{1}{q}H_n(1) = \frac{1}{q^2 n}\sum_{\substack{d\mid n\\ p\nmid d}} \mu(d)q^{n/d}.$$

This completes the proof of Theorem 1.1 from equation (3.1). □

The rest of the paper is devoted to giving a combinatorial proof of equation (3.1).

4. A family of equations. The following lemma is the starting point for generating relationships among the $X_{\mathbf{v}}(\mathbf{a})$'s.

Lemma 4.1. *Let $0 \le k \le n-\ell$. A monic polynomial of degree k divides $q^{n-\ell-k}$ polynomials in $\mathcal{P}_n(\mathbf{a})$.*

Proof. For a generic polynomial,

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_\ell x^{n-\ell} + t_{\ell+1}x^{n-\ell-1} + \cdots + t_n \in \mathcal{P}_n(\mathbf{a}),$$

and a fixed polynomial,

$$g(x) = x^k + b_1x^{k-1} + \cdots + b_{k-1}x + b_k,$$

such that $g(x) \mid f(x)$, we write $f(x) = g(x)h(x)$ with

$$h(x) = x^{n-k} + c_1x^{n-k-1} + \cdots + c_{n-k-1}x + c_{n-k}.$$

Given the values $b_1, \ldots, b_k$, the numbers $c_1, \ldots, c_{n-k}$ must satisfy the equations

$$\begin{cases} b_1 + c_1 = a_1 \\ b_2 + b_1c_1 + c_2 = a_2 \\ \cdots \\ b_\ell + b_{\ell-1}c_1 + \cdots + b_1c_{\ell-1} + c_\ell = a_\ell, \end{cases}$$

where we set $b_i = 0$ if $i > k$.

Thus, $g(x)$ fixes the first ℓ coefficients of $h(x)$. There are $n-k-\ell$ choices for the remaining coefficients of $h(x)$. ☐

Given a factorization type $\mathbf{v}$, the *degree*, denoted $\deg(\mathbf{v})$, is simply the degree of the resulting polynomial.

We note that there is a more precise way of describing a certain factorization type $\mathbf{v}$ of degree n by means of an $n \times n$ matrix $V = (v_{i,j})$, where the entry $v_{i,j}$ indicates the number of factors of the form i^j in the factorization type. Then the matrix V must satisfy:

$$\deg(V) := \sum_{i,j} ijv_{i,j} = n.$$

Accordingly, we use the notation $X_V(\mathbf{a})$ as equivalent to the notation $X_{\mathbf{v}}(\mathbf{a})$.

The *length* of $\mathbf{v}$, denoted $\lg(\mathbf{v})$ or $\lg(V)$ is defined as:

$$\lg(V) := \sum_{i,j} j v_{i,j}.$$

Our goal is to find a formula for $X_{(n)}(0,a)$. In order to do that we are going to consider the equations that we can form with the $X_{\mathbf{v}}(\mathbf{a})$.

Let V and W be $n \times n$ matrices with integral entries. We say that W is majorized by V (written $W \preceq V$), if and only if

$$\begin{cases} w_{i,n} \leq v_{i,n} \\ w_{i,n} + w_{i,n-1} \leq v_{i,n} + v_{i,n-1} \\ \cdots \\ w_{i,n} + \cdots + w_{i,1} \leq v_{i,n} + \cdots + v_{i,1}, \end{cases}$$

for each $i = 1, \ldots, n$.

Any factorization type $\mathbf{w}$ of total degree k less than or equal to $n-\ell$ may be represented by a matrix W with

$$\sum_{i,j} ij w_{i,j} = k.$$

For any such factorization of type $\mathbf{w}$ we may consider all the factorization types $\mathbf{v}$ of degree n such that $\mathbf{w}$ is a factor. This is simply the set of $\mathbf{v}$ such that $W \preceq V$. Counting the number of polynomials of each of these types and using Lemma 4.1 yield the following equation:

$$\sum_{V \succeq W} \prod_{i=1}^{n} \binom{v_{i,n}}{w_{i,n}} \binom{v_{i,n} + v_{i,n-1} - w_{i,n}}{w_{i,n-1}} \cdots \binom{v_{i,n} + \cdots + v_{i,1} - w_{i,n} - \cdots w_{i,2}}{w_{i,1}} X_V(\mathbf{a}) = q^{n-\ell-k} \prod_{i=1}^{n} \binom{H_i}{w_{i,1} \cdots w_{i,n}}, \tag{4.1}$$

where H_i denotes the number of irreducible polynomials of degree i, with no restrictions.

We refer to equation (4.1) as $\mathcal{E}_{\mathbf{w}}(\mathbf{a})$ or $\mathcal{E}_W(\mathbf{a})$.

5. A combination of equations. We are going to consider a certain combination of equations of the form $\mathcal{E}_{\mathbf{w}}(\mathbf{a})$. From now on, we are going to assume that $\ell = 2$. However, the combination we find also works for smaller values $\ell = 0, 1$.

Consider the following set:

$$\mathcal{W}_a = \{\mathbf{w} \text{ factorization type} \mid \deg(\mathbf{w}) \leq n-2, w_{i,j} = 0, j > 1\}.$$

Then we write

$$A : \sum_{\mathbf{w} \in \mathcal{W}_a} (-1)^{\lg(\mathbf{w})} (n - \deg(\mathbf{w})) \mathcal{E}_{\mathbf{w}}(\mathbf{a}).$$

Observe that this is a combination of equations.

Now, define

$$\mathcal{W}_b = \{\mathbf{w} \text{ factorization type} \mid \deg(\mathbf{w}) \leq n-2, w_{i,j} = 0, j > 1, w_{11} \neq 0\},$$

and

$$B : -\sum_{\mathbf{w} \in \mathcal{W}_b} (-1)^{\lg(\mathbf{w})} \mathcal{E}_{\mathbf{w}}(\mathbf{a}).$$

Finally, consider the set

$$\mathcal{W}_c = \{\mathbf{w} \text{ factorization type} \mid \deg(\mathbf{w}) \leq n-2, w_{i,j} = 0, \\ i, j > 1, \text{ there exists } j_0, w_{1,j_0} \neq 0\}.$$

We will work with the sequence given by

$$\alpha_s = \sum_{j=0}^{s} j! \binom{s}{j}.$$

Let γ be a function on n-vectors with nonnegative integral entries given by the following recurrence.

- For $s_1 \geq 0$,
$$\gamma(s_1, 0, 0, \ldots, 0) = \alpha_{s_1}.$$
- When there is an $i > 1$ with $s_i \neq 0$, we have

$$\gamma(s_1, s_2, \ldots, s_{n-1}, s_n) = \sum_{j=1}^{n} \gamma(s_1, \ldots, s_{j-1} + 1, s_j - 1, \ldots, s_n) s_j.$$

Notice that the sum starts with $\gamma(s_1 - 1, s_2, \ldots, s_{n-1}, s_n)$ if $s_1 \neq 0$.

Now, set

$$C : \sum_{\mathbf{w} \in \mathcal{W}_c} (-1)^{\lg(\mathbf{w})} \gamma(w_{1,1}, w_{1,2}, \ldots, w_{1,n}) \mathcal{E}_{\mathbf{w}}(\mathbf{a}).$$

We will see in Section 7 that $A + B + C$ gives us the desired result, namely, equation (3.1). Before that, we need to prove certain properties of γ.

6. A property of γ. In this section, we are going to prove the following.

Proposition 6.1. *Let $s_1, \ldots, s_n$ be nonnegative integers. Define*

$$f(s_1, \ldots, s_n) := \sum_{t_i \geq 0} \gamma(t_1, t_2, \ldots, t_n) \times (-1)^{t_1 + \cdots + n t_n} \binom{s_n}{t_n} \binom{s_n + s_{n-1} - t_n}{t_{n-1}} \cdots \binom{s_n + \cdots + s_1 - t_n - \cdots - t_2}{t_1}.$$

Then, we have

$$f(s_1, \ldots, s_n) = (-1)^{s_1 + 2s_2 + \cdots + n s_n} \frac{(s_1 + 2s_2 + \cdots + n s_n)!}{(1!)^{s_1} (2!)^{s_2} \cdots (n!)^{s_n}}. \tag{6.1}$$

Before proceeding to the proof of this result, we need to consider the following lemma.

Lemma 6.2. *For $(s_1, \ldots, s_n) \neq (0, \ldots, 0)$, We have the following recurrence relation.*

$$f(s_1, \ldots, s_n) = -\sum_{j=1}^{n} s_j f(s_1, \ldots, s_{j-1} + 1, s_j - 1, \ldots, s_n). \tag{6.2}$$

Proof. First notice that, for $s > 0$,

$$\begin{aligned} f(s,0,\dots,0) &= \sum_{0\le t\le s} \gamma(t,0,\dots,0)(-1)^t \binom{s}{t} \\ &= \sum_{0\le t\le s} \alpha_t (-1)^t \binom{s}{t} \\ &= \alpha_0 + \sum_{1\le t\le s} (\alpha_{t-1} t + 1)(-1)^t \binom{s}{t} \\ &= \sum_{0\le t\le s} (-1)^t \binom{s}{t} + s \sum_{1\le t\le s} \alpha_{t-1}(-1)^t \binom{s-1}{t-1} \\ &= -sf(s-1,0,\dots,0). \end{aligned}$$

By applying the recurrence of γ,

$$\begin{aligned} f(s_1,\dots,s_n) = \sum_{t_i\ge 0} \sum_{j=1}^{n} &\gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n) t_j \\ &\times (-1)^{t_1+\dots+nt_n} \binom{s_n}{t_n} \binom{s_n+s_{n-1}-t_n}{t_{n-1}} \\ &\qquad \cdots \binom{s_n+\dots+s_1-t_n-\dots-t_2}{t_1}. \end{aligned}$$

We remark that it is correct to apply the recurrence relation for the part of the sum involving the terms $\gamma(t_1,0,\dots,0)$ due to the case $f(s,0,\dots,0)$ analyzed above.

We now look at the term for a fixed value of j. First notice that

$$\begin{aligned} &\gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n) t_j \binom{s_n+\dots+s_j-t_n-\dots-t_{j+1}}{t_j} \\ &\qquad \times \prod_{i=j+1}^{n} \binom{s_n+\dots+s_i-t_n-\dots-t_{i+1}}{t_i} \\ &= \gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n)(s_n+\dots+s_j-t_n-\dots-t_{j+1}) \\ &\times \binom{s_n+\dots+s_j-t_n-\dots-t_{j+1}-1}{t_j-1} \end{aligned}$$

$$\times \prod_{i=j+1}^{n} \binom{s_n + \cdots + s_i - t_n - \cdots - t_{i+1}}{t_i},$$

where we have manipulated the j-binomial coefficient. Now we isolate the factor s_j in order to obtain

$$\begin{aligned}
&= \gamma(t_1, \ldots, t_{j-1}+1, t_j-1, \ldots, t_n) s_j \binom{s_n + \cdots + s_j - t_n - \cdots - t_{j+1} - 1}{t_j - 1} \\
&\quad \times \prod_{i=j+1}^{n} \binom{s_n + \cdots + s_i - t_n - \cdots - t_{i+1}}{t_i} \\
&\quad + \gamma(t_1, \ldots, t_{j-1}+1, t_j-1, \ldots, t_n)(s_n! + \cdots + s_{j+1} - t_n - \cdots -! t_{j+1}) \\
&\quad \times \binom{s_n + \cdots + s_j - t_n - \cdots - t_{j+1} - 1}{t_j - 1} \\
&\quad \times \prod_{i=j+1}^{n} \binom{s_n + \cdots + s_i - t_n - \cdots - t_{i+1}}{t_i}.
\end{aligned}$$

By manipulating the $j+1$-binomial coefficient, we find

$$\begin{aligned}
&= \gamma(t_1, \ldots, t_{j-1}+1, t_j-1, \ldots, t_n) s_j \binom{s_n + \cdots + s_j - t_n - \cdots - t_{j+1} - 1}{t_j - 1} \\
&\quad \times \prod_{i=j+1}^{n} \binom{s_n + \cdots + s_i - t_n - \cdots - t_{i+1}}{t_i} \\
&\quad + \gamma(t_1, \ldots, t_{j-1}+1, t_j-1, \ldots, t_n)(s_n + \cdots + s_{j+1} - t_n - \cdots - t_{j+2}) \\
&\quad \times \binom{s_n + \cdots + s_j - t_n - \cdots - t_{j+1} - 1}{t_j - 1} \\
&\quad \times \binom{s_n + \cdots + s_{j+1} - t_n - \cdots - t_{j+2} - 1}{t_{j+1}} \\
&\quad \times \prod_{i=j+2}^{n} \binom{s_n + \cdots + s_i - t_n - \cdots - t_{i+1}}{t_i}.
\end{aligned}$$

Again, we isolate the factor s_{j+1},

$$= \gamma(t_1, \ldots, t_{j-1}+1, t_j-1, \ldots, t_n) s_j \binom{s_n + \cdots + s_j - t_n - \cdots - t_{j+1} - 1}{t_j - 1}$$

$$\begin{aligned}
&\times \prod_{i=j+1}^{n} \binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}\\
&+\gamma(t_1,\ldots,t_{j-1}+1,t_j-1,\ldots,t_n)s_{j+1}\\
&\times \binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}\binom{s_n+\cdots+s_{j+1}-t_n-\cdots-t_{j+2}-1}{t_{j+1}}\\
&\times \prod_{i=j+2}^{n} \binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}\\
&\quad+\gamma(t_1,\ldots,t_{j-1}+1,t_j-1,\ldots,t_n)(s_n+\cdots+s_{j+2}-t_n-\cdots-t_{j+2})\\
&\times \binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}\\
&\times \binom{s_n+\cdots+s_{j+1}-t_n-\cdots-t_{j+2}-1}{t_{j+1}}\\
&\times \prod_{i=j+2}^{n} \binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}.
\end{aligned}$$

We rewrite the last row as two products:

$$\begin{aligned}
&=\gamma(t_1,\ldots,t_{j-1}+1,t_j-1,\ldots,t_n)s_j\binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}\\
&\times \prod_{i=j+1}^{n} \binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}\\
&+\gamma(t_1,\ldots,t_{j-1}+1,t_j-1,\ldots,t_n)s_{j+1}\\
&\times \binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}\\
&\times \binom{s_n+\cdots+s_{j+1}-t_n-\cdots-t_{j+2}-1}{t_{j+1}}\\
&\times \prod_{i=j+2}^{n} \binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}\\
&+\gamma(t_1,\ldots,t_{j-1}+1,t_j-1,\ldots,t_n)(s_n+\cdots+s_{j+2}-t_n-\cdots-t_{j+3})\\
&\times \binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}
\end{aligned}$$

$$\times \prod_{i=j+1}^{j+2} \binom{s_n + \cdots + s_i - t_n - \cdots - t_{i+1} - 1}{t_i}$$
$$\times \prod_{i=j+3}^{n} \binom{s_n + \cdots + s_i - t_n - \cdots - t_{i+1}}{t_i}.$$

This process is repeated until we reach the following:

$$\begin{aligned} &= \gamma(t_1, \ldots, t_{j-1} + 1, t_j - 1, \ldots, t_n) \\ &\quad \times \binom{s_n + \cdots + s_j - t_n - \cdots - t_{j+1} - 1}{t_j - 1} \\ &\quad \times \sum_{\ell=j}^{n} s_\ell \prod_{i=j+1}^{\ell} \binom{s_n + \cdots + s_i - t_n - \cdots - t_{i+1} - 1}{t_i} \\ &\quad \times \prod_{i=\ell+1}^{n} \binom{s_n + \cdots + s_i - t_n - \cdots - t_{i+1}}{t_i}. \end{aligned}$$

We now introduce the remaining factors

$$\begin{aligned} &\gamma(t_1, \ldots, t_{j-1} + 1, t_j - 1, \ldots, t_n) t_j \\ &\quad \prod_{i=1}^{n} \binom{s_n + \cdots + s_i - t_n - \cdots - t_{i+1}}{t_i} \\ &= \gamma(t_1, \ldots, t_{j-1} + 1, t_j - 1, \ldots, t_n) \\ &\quad \prod_{i=1}^{j-2} \binom{s_n + \cdots + s_i - t_n - \cdots - t_{i+1}}{t_i} \\ &\quad \times \binom{s_n + \cdots + s_{j-1} - t_n - \cdots - t_j}{t_{j-1}} \\ &\quad \times \binom{s_n + \cdots + s_j - t_n - \cdots - t_{j+1} - 1}{t_j - 1} \\ &\quad \times \sum_{\ell=j}^{n} s_\ell \prod_{i=j+1}^{\ell} \binom{s_n + \cdots + s_i - t_n - \cdots - t_{i+1} - 1}{t_i} \\ &\quad \times \prod_{i=\ell+1}^{n} \binom{s_n + \cdots + s_i - t_n - \cdots - t_{i+1}}{t_i}. \end{aligned}$$

We manipulate the $j-1$-binomial coefficient

$$
\begin{aligned}
&= \gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n) \\
&\quad \prod_{i=1}^{j-2}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i} \\
&\quad \times \binom{s_n+\cdots+s_{j-1}-t_n-\cdots-t_j+1}{t_{j-1}+1} \\
&\quad \times \binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1}\sum_{\ell=j}^{n}s_\ell \\
&\quad \times \prod_{i=j+1}^{\ell}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}-1}{t_i} \\
&\quad \times \prod_{i=\ell+1}^{n}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i} \\
&\quad - \gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n) \\
&\quad \prod_{i=1}^{j-2}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i} \\
&\quad \times \binom{s_n+\cdots+s_{j-1}-t_n-\cdots-t_j}{t_{j-1}+1}\binom{s_n+\cdots+s_j-t_n-\cdots-t_{j+1}-1}{t_j-1} \\
&\quad \times \sum_{\ell=j}^{n}s_\ell\prod_{i=j+1}^{\ell}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}-1}{t_i} \\
&\quad \times \prod_{i=\ell+1}^{n}\binom{s_n+\cdots+s_i-t_n-\cdots-t_{i+1}}{t_i}.
\end{aligned}
$$

Taking into account the signs, the terms containing $\gamma(t_1,\dots,t_{j-1}+1,t_j-1,\dots,t_n)$ with $j>2$ yield:

$$
-\sum_{\ell=j}^{n}s_\ell f(s_1,\dots,s_{j-1}+1,\dots,s_\ell-1,\dots,s_n) \\
+\sum_{\ell=j}^{n}s_\ell f(s_1,\dots,s_{j-2}+1,\dots,s_\ell-1,\dots,s_n).
$$

On the other hand, the term containing $\gamma(t_1-1,\dots,t_n)$ yields

$$-\sum_{\ell=1}^{n} s_\ell f(s_1,\dots,s_\ell-1,\dots,s_n),$$

while the one containing $\gamma(t_1+1,t_2-1,\dots,t_n)$ yields

$$-\sum_{\ell=2}^{n} s_\ell f(s_1+1,\dots,s_\ell-1,\dots,s_n)+\sum_{\ell=2}^{n} s_\ell f(s_1,\dots,s_\ell-1,\dots,s_n).$$

Putting all of this together, we get:

$$\begin{aligned}
f(s_1,\dots,s_n) &= -\sum_{j=1}^{n}\sum_{\ell=j}^{n} s_\ell f(s_1,\dots,s_{j-1}+1,\dots,s_\ell-1,\dots,s_n)\\
&\quad+\sum_{j=2}^{n}\sum_{\ell=j}^{n} s_\ell f(s_1,\dots,s_{j-2}+1,\dots,s_\ell-1,\dots,s_n)\\
&= -\sum_{j=1}^{n}\sum_{\ell=j}^{n} s_\ell f(s_1,\dots,s_{j-1}+1,\dots,s_\ell-1,\dots,s_n)\\
&\quad+\sum_{h=1}^{n-1}\sum_{\ell=h+1}^{n} s_\ell f(s_1,\dots,s_{h-1}+1,\dots,s_\ell-1,\dots,s_n)\\
&= -\sum_{j=1}^{n} s_j f(s_1,\dots,s_{j-1}+1,s_j-1,\dots,s_n).
\end{aligned}$$

This concludes the proof of the recurrence for $f(s_1,\dots,s_n)$. □

Proof of Proposition 6.1. Observe that, for $s=0$, $f(0,\dots,0)=1$. Now assume that $s>0$. We have:

$$f(s,0,\dots,0)=\sum_{t\geq 0}\alpha_t(-1)^t\binom{s}{t}=\sum_{t=0}^{s}\sum_{j=0}^{t} j!\binom{t}{j}(-1)^t\binom{s}{t}.$$

By exchanging the order of summation,

$$f(s,0,\dots,0)=\sum_{j=0}^{s} j!\binom{s}{j}\sum_{t=j}^{s}(-1)^t\binom{s-j}{t-j}.$$

Now notice that the inner sum equals zero unless $s = j$ and, in that case, it equals $(-1)^s$. Thus, we get

$$f(s,0,\ldots,0) = (-1)^s s! = (-1)^s \frac{s!}{(1!)^s}.$$

We proceed by induction on $k = s_1 + 2s_2 + \cdots + ns_n$. We remark that we have proved the case of $k = s_1$ for any value of k. We are going to apply the recurrence (6.2). Observe that, in the term $f(s_1,\ldots,s_{j-1}+1,s_j-1,\ldots,s_n)$, we have

$$s_1 + \cdots + (j-1)(s_{j-1}+1) + j(s_j - 1) + \cdots + ns_n = k-1.$$

Thus, by the induction hypothesis,

$$\begin{aligned}
f(s_1,\ldots,s_n) &= -\sum_{j=1}^n s_j f(s_1,\ldots,s_{j-1}+1,s_j-1,\ldots,s_n)\\
&= -\sum_{j=1}^n s_j (-1)^{s_1+2s_2+\cdots+ns_n-1}\\
&\quad\cdot \frac{(s_1+2s_2+\cdots+ns_n-1)!}{(1!)^{s_1}\cdots((j-1)!)^{s_{j-1}+1}(j!)^{s_j-1}\cdots(n!)^{s_n}}\\
&= (-1)^{s_1+2s_2+\cdots+ns_n}\frac{(s_1+2s_2+\cdots+ns_n-1)!}{(1!)^{s_1}\cdots(n!)^{s_n}}\\
&\quad + \sum_{j=1}^n s_j \tfrac{j!}{(j-1)!}\\
&= (-1)^{s_1+2s_2+\cdots+ns_n}\frac{(s_1+2s_2+\cdots+ns_n)!}{(1!)^{s_1}\cdots(n!)^{s_n}}.
\end{aligned}$$

This conclude the proof of Proposition 6.1. □

7. $A+B+C$.

In order to prove equation (3.1) we need to compute the coefficient of each $X_{\mathbf{v}}(\mathbf{a})$ in $A+B+C$. The following two equations are going to be key in this section:

$$\sum_{k=0}^{s}(-1)^k\binom{s}{k} = 0, \quad s \neq 0, \tag{7.1}$$

$$\sum_{k=0}^{s}(-1)^k k\binom{s}{k} = 0, \quad s \neq 1. \tag{7.2}$$

7.1. The term A. The coefficient of $X_{\mathbf{v}}(\mathbf{a})$ in A is given by:

$$\sum_{0\le w_{1,1}+\cdots+nw_{n,1}\le n-2}(n-(w_{1,1}+\cdots+nw_{n,1}))\prod_{i=1}^{n}(-1)^{w_{i,1}}\binom{v_{i,n}+\cdots+v_{i,1}}{w_{i,1}}.$$

Because of equations (7.1) and (7.2),

$$\sum_{0\le w_{1,1}+\cdots+nw_{n,1}\le n}(n-(w_{1,1}+\cdots+nw_{n,1}))\prod_{i=1}^{n}(-1)^{w_{i,1}}\binom{v_{i,n}+\cdots+v_{i,1}}{w_{i,1}}=0,$$

unless one of the following applies:

- $v_{i,n}+\cdots+v_{i,1}=0$ for all i, or
- there is an i_0 with $v_{i_0,n}+\cdots+v_{i_0,1}=1$ and $v_{i,n}+\cdots+v_{i,1}=0$ for all $i\neq i_0$.

The first case is impossible, since $n>0$. For the second case, since $\deg(\mathbf{v})=n$, the only possibility for this is $v_{i_0,n/i_0}=1$, and the rest is zero. We obtain the coefficient i_0 for $X_{(i_0^{n/i_0})}(\mathbf{a})$.

For the remaining $X_{\mathbf{v}}(\mathbf{a})$, the coefficient contributed by A must be

$$-\sum_{w_{1,1}+\cdots+nw_{n,1}=n-1}\prod_{i=1}^{n}(-1)^{w_{i,1}}\binom{v_{i,n}+\cdots+v_{i,1}}{w_{i,1}}.$$

Since we have $w_{i,1}\le v_{i,n}+\cdots+v_{i,1}$, we obtain

$$n-1=w_{1,1}+\cdots+nw_{n,1}\le\sum_{i,j}iv_{i,j}$$

and

$$\sum_{i,j}ijv_{i,j}-1\le\sum_{i,j}iv_{i,j},$$

which implies

$$\sum_{i,j}i(j-1)v_{i,j}\le 1.$$

This can only happen if $v_{i,j}=0$ for all $j>1$, with the exception of $v_{1,2}$ which can be equal to 1 or 0. In any of these cases $v_{i,1}$ can take any value. Thus, the contribution to the coefficient is given by:

$$-\sum_{w_{1,1}+\cdots+nw_{n,1}=n-1}(-1)^{w_{1,1}}\binom{v_{1,2}+v_{1,1}}{w_{1,1}}\prod_{i=2}^{n}(-1)^{w_{i,1}}\binom{v_{i,1}}{w_{i,1}}.$$

First assume that $v_{i,j}=0$ for $j>1$. Since $w_{i,1}\leq v_{i,1}$, the case $w_{1,1}+\cdots+nw_{n,1}=n-1$ occurs when $w_{i,1}=v_{i,1}$ for $i>1$ and $w_{1,1}=v_{1,1}-1$. We obtain

$$(-1)^{v_{1,1}+\cdots+v_{n,1}}v_{1,1}.$$

Now assume that $v_{i,j}=0$ for all $j>1$ except that $v_{1,2}=1$. Once again, we have $w_{i,1}\leq v_{i,1}$ for $i>1$ and $w_{1,1}\leq v_{1,1}+1$. The case $w_{1,1}+\cdots+nw_{n,1}=n-1$ occurs with $w_{1,1}=v_{1,1}+1$ and $w_{i,1}=v_{i,1}$ for $i>1$, and the coefficient equals

$$(-1)^{v_{1,1}+\cdots+v_{n,1}}.$$

7.2. The term B. We look at expression B. The coefficient of $X_{\mathbf{v}}(\mathbf{a})$ is given by:

$$-\sum_{\substack{0\leq w_{1,1}+\cdots+nw_{n,1}\leq n-2\\ w_{1,1}\neq 0}}\prod_{i=1}^{n}(-1)^{w_{i,1}}\binom{v_{i,n}+\cdots+v_{i,1}}{w_{i,1}}.$$

Because of equations (7.1) and (7.2),

$$-\sum_{0\leq w_{1,1}+\cdots+nw_{n,1}\leq n}\prod_{i=1}^{n}(-1)^{w_{i,1}}\binom{v_{i,n}+\cdots+v_{i,1}}{w_{i,1}}=0,$$

unless $v_{i,n}+\cdots+v_{i,1}=0$ for all i, which is impossible for $n>0$.

The case $w_{1,1}+2w_{2,1}+\cdots+nw_{n,1}\geq n-1$, together with the conditions $w_{i,1}\leq v_{i,n}+\cdots+v_{i,1}$ for all i, imply

$$\sum_{i,j}ijv_{i,j}-1=n-1\leq w_{1,1}+2w_{2,1}+\cdots+nw_{n,1}\leq\sum_{i,j}iv_{i,j},$$

which gives

$$\sum_{i,j}i(j-1)v_{i,j}\leq 1.$$

This can only happen if $v_{i,j} = 0$ for all $j > 1$ with the exception of $v_{1,2}$, which can be equal to 1 or 0. In addition, $v_{i,1}$ can take any value. Therefore, the contribution to the coefficient is:

(7.3)
$$\sum_{w_{1,1}+2w_{2,1}+\cdots+nw_{n,1}=n-1,n} (-1)^{w_{1,1}} \binom{v_{1,2}+v_{1,1}}{w_{1,1}} \prod_{i=2}^{n} (-1)^{w_{i,1}} \binom{v_{i,1}}{w_{i,1}}$$

(7.4)
$$+ \sum_{2w_{2,1}+\cdots+nw_{n,1}\le n-2} \prod_{i=2}^{n} (-1)^{w_{i,1}} \binom{v_{i,1}}{w_{i,1}}.$$

First, assume that $v_{i,j} = 0$ for $j > 1$. Since $w_{i,1} \le v_{i,1}$, the case $w_{1,1} + \cdots + nw_{n,1} = n-1$ occurs when $w_{i,1} = v_{i,1}$ for $i > 1$ and $w_{1,1} = v_{1,1} - 1$. The case $w_{1,1} + \cdots + nw_{n,1} = n$ can only occur if $w_{i,1} = v_{i,1}$ for all i. We obtain that the contribution from (7.3) is

$$-(-1)^{v_{1,1}+\cdots+v_{n,1}} v_{1,1} + (-1)^{v_{1,1}+\cdots+v_{n,1}}.$$

Now assume $v_{i,j} = 0$ for all $j > 1$, except that $v_{1,2} = 1$. Once again, we have $w_{i,1} \le v_{i,1}$ for $i > 1$ and $w_{1,1} \le v_{1,1} + 1$. The case $w_{1,1} + \cdots + nw_{n,1} = n-1$ occurs with $w_{1,1} = v_{1,1} + 1$ and $w_{i,1} = v_{i,1}$ for $i > 1$. The case $w_{1,1} + \cdots + nw_{n,1} = n$ never occurs. The contribution coming from (7.3) equals

$$-(-1)^{v_{1,1}+\cdots+v_{n,1}}.$$

The contribution from (7.4) will be analyzed in the more general case of $w_{1,1} = 0$. We have

$$\sum_{0\le 2w_{2,1}+\cdots+nw_{n,1}\le n-2} \prod_{i=2}^{n} (-1)^{w_{i,1}} \binom{v_{i,n}+\cdots+v_{i,1}}{w_{i,1}}.$$

Notice that

$$\sum_{0\le 2w_{2,1}+\cdots+nw_{n,1}\le n} \prod_{i=2}^{n} (-1)^{w_{i,1}} \binom{v_{i,n}+\cdots+v_{i,1}}{w_{i,1}} = 0,$$

unless $v_{i,n} + \cdots + v_{i,1} = 0$ for all $i > 1$ and, in that case, the above sum equals 1. Apart from that term, we obtain that the contribution to the coefficient is given by:

$$-\sum_{2w_{2,1}+\cdots+nw_{n,1}=n-1,n}\prod_{i=2}^{n}(-1)^{w_{i,1}}\binom{v_{i,n}+\cdots+v_{i,1}}{w_{i,1}}.$$

Because of the previous considerations and the fact that $v_{1,1}+\cdots+v_{1,n}$ must be positive for $X_{\mathbf{v}}(\mathbf{a})$ to appear in this sum, this contribution only appears if $v_{1,1}=1$ and $v_{i,j}=0$ for $j>1$. The only possibility is $w_{1,1}=0$ and $w_{i,1}=v_{i,1}$ for $i>1$, and we obtain

$$-(-1)^{v_{2,1}+\cdots+v_{n,1}}=(-1)^{v_{1,1}+\cdots+v_{n,1}}.$$

7.3. The term C. Finally, we look at expression C.

$$\sum_{\substack{0\le w_{1,1}+2w_{1,2}+\cdots+nw_{1,n}\le n-2\\ \exists j_0, w_{1,j_0}\neq 0}}\gamma(w_{1,1},w_{1,2},\dots,w_{1,n})$$
$$\times(-1)^{w_{1,1}+\cdots+nw_{1,n}}\binom{v_{1,n}}{w_{1,n}}\binom{v_{1,n}+v_{1,n-1}-w_{1,n}}{w_{1,n-1}}\cdots$$
$$\binom{v_{1,n}+\cdots+v_{1,1}-w_{1,n}-\cdots w_{1,2}}{w_{1,1}}$$
$$\times\sum_{0\le 2w_{2,1}+\cdots+nw_{n,1}\le n-2-(w_{1,1}+2w_{1,2}+\cdots+nw_{1,n})}$$
$$\times\prod_{i=2}^{n}(-1)^{w_{i,1}}\binom{v_{i,n}+\cdots+v_{i,1}}{w_{i,1}}.$$

Because of equations (7.1) and (7.2),

$$\sum_{0\le w_{1,1}+2w_{1,2}+\cdots+nw_{1,n}\le n}\gamma(w_{1,1},w_{1,2},\dots,w_{1,n})$$
$$\times(-1)^{w_{1,1}+\cdots+nw_{1,n}}\binom{v_{1,n}}{w_{1,n}}\binom{v_{1,n}+v_{1,n-1}-w_{1,n}}{w_{1,n-1}}\cdots$$
$$\binom{v_{1,n}+\cdots+v_{1,1}-w_{1,n}-\cdots w_{1,2}}{w_{1,1}}$$
$$\times\sum_{0\le 2w_{2,1}+\cdots+nw_{n,1}\le n-(w_{1,1}+2w_{1,2}+\cdots+nw_{1,n})}$$
$$\prod_{i=2}^{n}(-1)^{w_{i,1}}\binom{v_{i,n}+\cdots+v_{i,1}}{w_{i,1}}=0,$$

unless $v_{i,n} + \cdots + v_{i,1} = 0$ for all $i > 1$. In that case, we obtain

$$\begin{aligned}
&\sum_{\substack{0 \le w_{1,1}+2w_{1,2}+\cdots+nw_{1,n} \le n-2 \\ \exists j_0, w_{1,j_0} \neq 0}} \gamma(w_{1,1}, w_{1,2}, \ldots, w_{1,n}) \\
&\quad \times (-1)^{w_{1,1}+\cdots+nw_{1,n}} \binom{v_{1,n}}{w_{1,n}} \binom{v_{1,n}+v_{1,n-1}-w_{1,n}}{w_{1,n-1}} \cdots \\
&\qquad \binom{v_{1,n}+\cdots+v_{1,1}-w_{1,n}-\cdots w_{1,2}}{w_{1,1}} \\
&= f(v_{1,1}, \ldots, v_{1,n}) \\
&\quad - \sum_{0 \le w_{1,1}+2w_{1,2}+\cdots+nw_{1,n} = 0, n-1, n} \gamma(w_{1,1}, w_{1,2}, \ldots, w_{1,n}) \\
&\quad \times (-1)^{w_{1,1}+\cdots+nw_{1,n}} \binom{v_{1,n}}{w_{1,n}} \binom{v_{1,n}+v_{1,n-1}-w_{1,n}}{w_{1,n-1}} \cdots \\
&\qquad \binom{v_{1,n}+\cdots+v_{1,1}-w_{1,n}-\cdots w_{1,2}}{w_{1,1}}.
\end{aligned}$$

The case $w_{1,1} + 2w_{1,2} + \cdots + nw_{1,n} = n - 1$, together with the conditions $w_{1,i}+\cdots+w_{1,n} \le v_{1,i}+\cdots+v_{1,n}$ for all i and $v_{1,1}+2v_{1,2}+\cdots+nv_{1,n} = n$ imply that there is a $j_0 > 1$ such that $w_{1,j_0-1} = v_{1,j_0-1} + 1$ and $w_{1,j_0} = v_{1,j_0} - 1$, or $w_{1,1} = v_{1,1} - 1$. This term yields

$$\begin{aligned}
-\sum_{j=1}^{n} \gamma(v_{1,1}, \ldots, v_{1,j-1}+1, v_{1,j}-1, \ldots, v_{1,n})(-1)^{v_{1,1}+\cdots+nv_{1,n}-1} v_{1,j} \\
= (-1)^{v_{1,1}+\cdots+nv_{1,n}} \gamma(v_{1,1}, \ldots, v_{1,n})
\end{aligned}$$

by construction of γ, provided that there is an $i_0 > 1$ such that $v_{1,i_0} \neq 0$. Otherwise, we obtain

$$\begin{aligned}
&(-1)^{v_{1,1}} v_{1,1} \gamma(v_{1,1}-1, 0, \ldots, 0) \\
&\qquad = (-1)^{v_{1,1}} \alpha_{v_{1,1}} - (-1)^{v_{1,1}} = (-1)^{v_{1,1}} (\gamma(v_{1,1}, 0, \ldots, 0) - 1).
\end{aligned}$$

The case $w_{1,1}+2w_{1,2}+\cdots+nw_{1,n} = n$, together with the conditions $w_{1,i}+\cdots+w_{1,n} \le v_{1,i}+\cdots+v_{1,n}$ for all i and $v_{1,1}+2v_{1,2}+\cdots+nv_{1,n} = n$, imply that $w_{1,j} = v_{1,j}$ for all j, yields

$$-(-1)^{v_{1,1}+\cdots+nv_{1,n}} \gamma(v_{1,1}, \ldots, v_{1,n}).$$

We remark that the case $v_{1,j}=0$ for $j>1$ yields

$$-(-1)^{v_{1,1}}\alpha_{v_{1,1}}=-(-1)^{v_{1,1}}\gamma(v_{1,1},0,\dots,0).$$

The term with $w_{1,1}=\cdots=w_{1,n}=0$ will be considered in a more general setting.

If $v_{i_0,n}+\cdots+v_{i_0,1}\neq 0$, for some $i_0>1$, the contribution is given by

$$\begin{aligned}
&-\sum_{w_{1,1}+2w_{1,2}+\cdots+nw_{1,n}+2w_{2,1}+\cdots+nw_{n,1}=n-1,n}\gamma(w_{1,1},w_{1,2},\dots,w_{1,n})\\
&\quad\times(-1)^{w_{1,1}+\cdots+nw_{1,n}}\binom{v_{1,n}}{w_{1,n}}\binom{v_{1,n}+v_{1,n-1}-w_{1,n}}{w_{1,n-1}}\cdots\\
&\quad\times\binom{v_{1,n}+\cdots+v_{1,1}-w_{1,n}-\cdots w_{1,2}}{w_{1,1}}
\end{aligned}$$

$$\times\prod_{i=2}^{n}(-1)^{w_{i,1}}\binom{v_{i,n}+\cdots+v_{i,1}}{w_{i,1}} \tag{7.5}$$

$$-\gamma(0,\dots,0)\sum_{2w_{2,1}+\cdots+nw_{n,1}\leq n-2}\prod_{i=2}^{n}(-1)^{w_{i,1}}\binom{v_{i,n}+\cdots+v_{i,1}}{w_{i,1}}. \tag{7.6}$$

The case $w_{1,1}+2w_{1,2}+\cdots+nw_{1,n}+2w_{2,1}+\cdots+nw_{n,1}\geq n-1$ implies that

$$\begin{aligned}
\sum_{i,j}ijv_{i,j}-1=n-1\leq w_{1,1}+2w_{1,2}+\cdots+nw_{1,n}+2w_{2,1}+\cdots+nw_{n,1}\\
\leq\sum_{j}jv_{1,j}+\sum_{i>1,j}iv_{i,j},
\end{aligned}$$

which gives

$$\sum_{i>1,j}i(j-1)v_{i,j}\leq 1.$$

This can only happen if $v_{i,j}=0$ for $i,j>1$. Following equation (7.5),

$$-\sum_{w_{1,1}+2w_{1,2}+\cdots+nw_{1,n}+2w_{2,1}+\cdots+nw_{n,1}=n-1,n}\gamma(w_{1,1},w_{1,2},\dots,w_{1,n})$$

$$\times (-1)^{w_{1,1}+\cdots+nw_{1,n}} \binom{v_{1,n}}{w_{1,n}} \binom{v_{1,n}+v_{1,n-1}-w_{1,n}}{w_{1,n-1}} \cdots$$
$$\times \binom{v_{1,n}+\cdots+v_{1,1}-w_{1,n}-\cdots w_{1,2}}{w_{1,1}} \prod_{i=2}^{n} (-1)^{w_{i,1}} \binom{v_{i,1}}{w_{i,1}}.$$

We see that

$$w_{i,1} \le v_{i,1} \quad \text{for } i > 1,$$

and

$$w_{1,i} + \cdots + w_{1,n} \le v_{1,i} + \cdots + v_{1,n} \quad \text{for any } i.$$

The condition $w_{1,1} + 2w_{2,1} + \cdots + nw_{n,1} + 2w_{1,2} + \cdots + nw_{1,n} = n$ is only possible if $w_{i,1} = v_{i,1}$ for $i > 1$ and $w_{1,i} + \cdots + w_{1,n} = v_{1,i} + \cdots + v_{1,n}$ for all i, which implies $w_{1,i} = v_{1,i}$. The condition $w_{1,1} + 2w_{2,1} + \cdots + nw_{n,1} + 2w_{1,2} + \cdots + nw_{1,n} = n-1$ is only possible if $w_{i,1} = v_{i,1}$ for $i > 1$ and $w_{1,j_0} = v_{1,j_0} - 1$, and $w_{1,j_0-1} = v_{1,j_0-1} + 1$ for a unique j_0 fixed (this includes the case $j_0 = 1$, with the second condition empty) and $w_{1,j} = v_{1,j}$ for the other j.

Therefore, the contribution to the coefficient is given by

$$(-1)^{v_{2,1}+\cdots+v_{n,1}+v_{1,1}+\cdots+nv_{1,n}}$$
$$\times \sum_{j=1}^{n} \gamma(v_{1,1}, \ldots, v_{1,j-1}+1, v_{1,j}-1, \ldots, v_{1,n}) v_{1,j}$$
$$- (-1)^{v_{2,1}+\cdots+v_{n,1}+v_{1,1}+\cdots+nv_{1,n}} \gamma(v_{1,1}, v_{1,2}, \ldots, v_{1,n}).$$

This term equals 0, unless $v_{1,j} = 0$ for all $j > 1$. In that case, this term equals

$$-(-1)^{v_{1,1}+v_{2,1}+\cdots+v_{n,1}}.$$

The term $w_{1,1} = \cdots = w_{1,n} = 0$ yields equation (7.6):

$$-\gamma(0, \ldots, 0) \sum_{0 \le 2w_{2,1}+\cdots+nw_{n,1} \le n-2} \prod_{i=2}^{n} (-1)^{w_{i,1}} \binom{v_{i,n}+\cdots+v_{i,1}}{w_{i,1}}.$$

Notice that

$$-\gamma(0,\dots,0)\sum_{0\le 2w_{2,1}+\cdots+nw_{n,1}\le n}\prod_{i=2}^{n}(-1)^{w_{i,1}}\binom{v_{i,n}+\cdots+v_{i,1}}{w_{i,1}}=0,$$

unless $v_{i,n}+\cdots+v_{i,1}=0$ for all i and, in that case, the above sum equals $-\gamma(0,\dots,0)=-1$. In addition, we obtain a contribution given by

$$\gamma(0,\dots,0)\sum_{2w_{2,1}+\cdots+nw_{n,1}=n-1,n}\prod_{i=2}^{n}(-1)^{w_{i,1}}\binom{v_{i,n}+\cdots+v_{i,1}}{w_{i,1}}.$$

But the sum $2w_{2,1}+\cdots+nw_{n,1}\ge n-1$ implies that

$$\sum_{i,j} ijv_{i,j}-1=n-1\le 2w_{2,1}+\cdots+nw_{n,1}\le \sum_{i>1,j} iv_{i,j},$$

which implies

$$\sum_j jv_{1,j}+\sum_{i>1,j} i(j-1)v_{i,j}\le 1.$$

Thus, $v_{i,j}=0$ for $j>1$ and $v_{1,1}>0$ (it cannot be zero since one term of the form $v_{1,j}$ must be nonzero). In addition, since $w_{1,1}=0$, we have that $v_{1,1}=1$ and $2w_{2,1}+\cdots+nw_{n,1}=n-1$ can only happen if $w_{i,1}=v_{i,1}$, while the case $2w_{2,1}+\cdots+nw_{n,1}=n$ never occurs. The contribution is:

$$(-1)^{v_{2,1}+\cdots+v_{n,1}}=-(-1)^{v_{1,1}+\cdots+v_{n,1}}.$$

7.4. Putting the terms together. We compute the final coefficient for $X_{\mathbf{v}}(\mathbf{a})$ in $A+B+C$ by considering each case.

If $v_{i,j}\neq 0$ for some $i,j>1$, then the coefficient is 0 unless we are in the case of $X_{(d^{n/d})}$, in which the coefficient is d.

The remaining nonzero coefficients correspond to $v_{i,j}=0$ for all $i,j>1$. Table 1 contains a summary of the results in this case, taking into account that $n\ge 2$. Here $*$ indicates that any value is allowed and $v_{i,1}>0$ (respectively, $v_{1,j}>0$) indicates that the inequality is true for at least one subindex $i>1$ (respectively, $j>2$). Finally, f is short for $f(v_{1,1},\dots,v_{1,n})$.

We see that the final coefficient for $X_{\mathbf{v}}(\mathbf{a})$, such that $v_{i,j}=0$ for all $i,j>1$, is given by 0 if $v_{i_0,1}>0$ for some $i_0>1$ and

TABLE 1. Coefficient of $X_{\mathbf{v}}(\mathbf{a})$ in $A+B+C$.

$v_{1,1}$	$v_{1,2}$	$v_{1,j}$, $j>2$	$v_{i,1}$, $i>1$	A	B	C	$A+B+C$
0	$\neq 1$	$*$	>0	0	0	0	0
$*$	$*$	>0	0	0	1	$f-1$	f
0	1	0	0	1	0	$f-1$	f
$*$	1	0	>0	$(-1)^{v_{1,1}+\cdots+v_{n,1}}$	$-(-1)^{v_{1,1}+\cdots+v_{n,1}}$	0	0
0	1	>0	>0	0	0	0	0
0	>1	$*$	0	0	1	$f-1$	f
1	0	0	>0	$(-1)^{v_{1,1}+\cdots+v_{n,1}}$	$(-1)^{v_{1,1}+\cdots+v_{n,1}}$	$-2(-1)^{v_{1,1}+\cdots+v_{n,1}}$	0
$\neq 0$	$*$	>0	>0	0	0	0	0
1	1	0	0	-1	2	$f-1$	f
1	>1	0	0	0	1	$f-1$	f
$*$	>1	0	>0	0	0	0	0
>1	0	0	0	$(-1)^{v_{1,1}}v_{1,1}$	$1-(-1)^{v_{1,1}}v_{1,1}$ $+(-1)^{v_{1,1}}$	$f-1-(-1)^{v_{1,1}}$	f
>1	0	0	>0	$(-1)^{v_{1,1}+\cdots+v_{n,1}}v_{1,1}$	$-(-1)^{v_{1,1}+\cdots+v_{n,1}}v_{1,1}$ $+(-1)^{v_{1,1}+\cdots+v_{n,1}}$	$-(-1)^{v_{1,1}+\cdots+v_{n,1}}$	0
>1	1	0	0	$(-1)^{v_{1,1}}$	$1-(-1)^{v_{1,1}}$	$f-1$	f

$f(v_{1,1},\ldots,v_{1,n})$ otherwise. Now, Proposition 6.1 gives that the left hand side of $A+B+C$ equals

$$\sum_{d|n} dX_{(d^{n/d})}(\mathbf{a}) + \sum_{\substack{\mathbf{v} \\ v_{i,j}=0 \\ i>1}} (-1)^n \frac{n!}{(1!)^{v_{1,1}}(2!)^{v_{1,2}}\cdots(n!)^{v_{1,n}}} X_{\mathbf{v}}(\mathbf{a}).$$

Note that $X_{(1^n)}$ appears in both terms giving a final coefficient of $1+(-1)^n$.

Finally, we note that

$$X_{(d^{n/d})}(0,a) = \begin{cases} H_d(0,(ad)/n) & p \nmid n/d, \\ 0 & p \mid n/d. \end{cases}$$

We can then write

$$\sum_{\substack{d|n \\ p\nmid n/d}} dH_d\left(0, \frac{ad}{n}\right) + \sum_{\substack{\mathbf{v} \\ v_{i,j}=0 \\ i>1}} (-1)^n \frac{n!}{(1!)^{v_{1,1}}(2!)^{v_{1,2}} \cdots (n!)^{v_{1,n}}} X_{\mathbf{v}}(0,a),$$

which is the left hand side of equation (3.1).

The right hand side of $A+B+C$ can be computed quite easily by the following observation. If we take the equations with $\ell = 0$ (no conditions on the coefficients), then we must necessarily arrive at equation (3.3), which is true since it is the result of Möbius inversion on equation (3.7) combined with equation (3.5). The combination that we take with $\ell = 2$ (respectively, $\ell = 1$) is the result of dividing the right hand side of each equation by q^2 (respectively, q). In this way, we arrive at equation (3.1) (respectively, equation (3.4)).

8. Some particular cases. In this section, we consider the cases $n = 4$ and $n = 5$ (for $\ell = 2$) to illustrate how the proof works. In order to simplify the notation we omit the **a** part from $\mathcal{E}_{\mathbf{w}}(\mathbf{a})$.

8.1. Case $n = 4$. We can find that $\gamma(1,0) = \gamma(0,1) = 2$ and $\gamma(2,0) = 5$. In this case, we have

$$\begin{aligned} &A : 4\mathcal{E}_{(0)} - 3\mathcal{E}_{(1)} - 2\mathcal{E}_{(2)} + 2\mathcal{E}_{(1,1)}, \\ &B : \mathcal{E}_{(1)} - \mathcal{E}_{(1,1)}, \\ &C : -2\mathcal{E}_{(1)} + 2\mathcal{E}_{(1^2)} + 5\mathcal{E}_{(1,1)}. \end{aligned}$$

Thus,

$$A + B + C = 4\mathcal{E}_{(0)} - 4\mathcal{E}_{(1)} + 2\mathcal{E}_{(1^2)} - 2\mathcal{E}_{(2)} + 6\mathcal{E}_{(1,1)}. \tag{8.1}$$

Table 2 contains all the equations involved, separated by left hand side (LHS) and right hand side (RHS).

TABLE 2. Equations for the case $n = 4$.

$\mathbf{v}$	LHS $\mathcal{E}_{\mathbf{v}}$	RHS $\mathcal{E}_{\mathbf{v}}$
(0)	$X_{(1,1,1,1)} + X_{(1,1,1^2)} + X_{(1^2,1^2)}$ $+X_{(1,1^3)} + X_{(1^4)} + X_{(1,1,2)}$ $+X_{(1^2,2)} + X_{(2,2)} + X_{(2^2)} + X_{(1,3)} + X_{(4)}$	q^2
(1)	$4X_{(1,1,1,1)} + 3X_{(1,1,1^2)} + 2X_{(1^2,1^2)}$ $+2X_{(1,1^3)} + X_{(1^4)} + 2X_{(1,1,2)}$ $+X_{(1^2,2)} + X_{(1,3)}$	q^2
(1^2)	$X_{(1,1,1^2)} + 2X_{(1^2,1^2)} + X_{(1,1^3)} + X_{(1^4)} + X_{(1^2,2)}$	q
(2)	$X_{(1,1,2)} + X_{(1^2,2)} + 2X_{(2,2)} + X_{(2^2)}$	$\frac{q(q-1)}{2}$
$(1,1)$	$6X_{(1,1,1,1)} + 3X_{(1,1,1^2)} + X_{(1^2,1^2)} + X_{(1,1^3)} + X_{(1,1,2)}$	$\frac{q(q-1)}{2}$

We obtain

$$4X_{(4)} + 2X_{(2^2)} + X_{(1^4)} + 24X_{(1,1,1,1)} + 12X_{(1,1,1^2)} \\ + 4X_{(1,1^3)} + 6X_{(1^2,1^2)} + X_{(1^4)} = 2q^2,$$

which is the result predicted by Theorem 1.1.

8.2. Case $n = 5$. We find some values of γ.

$\gamma(1,0,0)$	$\gamma(0,1,0)$	$\gamma(0,0,1)$	$\gamma(2,0,0)$	$\gamma(1,1,0)$	$\gamma(3,0,0)$
2	2	2	5	7	16

In this case, we have

$$A : 5\mathcal{E}_{(0)} - 4\mathcal{E}_{(1)} - 3\mathcal{E}_{(2)} - 2\mathcal{E}_{(3)} + 3\mathcal{E}_{(1,1)} + 2\mathcal{E}_{(1,2)} - 2\mathcal{E}_{(1,1,1)},$$
$$B : \mathcal{E}_{(1)} - \mathcal{E}_{(1,1)} - \mathcal{E}_{(1,2)} + \mathcal{E}_{(1,1,1)},$$
$$C : -2\mathcal{E}_{(1)} + 2\mathcal{E}_{(1^2)} - 2\mathcal{E}_{(1^3)} + 5\mathcal{E}_{(1,1)} - 7\mathcal{E}_{(1,1^2)} + 2\mathcal{E}_{(1,2)} - 16\mathcal{E}_{(1,1,1)}.$$

Then

$$A + B + C = 5\mathcal{E}_{(0)} - 5\mathcal{E}_{(1)} + 2\mathcal{E}_{(1^2)} - 2\mathcal{E}_{(1^3)} - 3\mathcal{E}_{(2)} - 2\mathcal{E}_{(3)} \\ + 7\mathcal{E}_{(1,1)} + 3\mathcal{E}_{(1,2)} - 7\mathcal{E}_{(1,1^2)} - 17\mathcal{E}_{(1,1,1)}.$$

TABLE 3. Equations for the case $n = 5$.

$\mathbf{v}$	LHS $\mathcal{E}_{\mathbf{v}}$	RHS $\mathcal{E}_{\mathbf{v}}$
(0)	$X_{(1,1,1,1,1)} + X_{(1,1,1,1^2)} + X_{(1,1^2,1^2)}$ $+X_{(1,1,1^3)} + X_{(1,1^4)} + X_{(1^5)} + X_{(1,1,1,2)}$ $+X_{(1,1^2,2)} + X_{(1^3,2)} + X_{(1,2,2)} + X_{(1,2^2)}$ $+X_{(1,1,3)} + X_{(1^2,3)} + X_{(1,4)} + X_{(2,3)} + X_{(5)}$	q^3
(1)	$5X_{(1,1,1,1,1)} + 4X_{(1,1,1,1^2)} + 3X_{(1,1^2,1^2)}$ $+3X_{(1,1,1^3)} + 2X_{(1,1^4)} + X_{(1^5)} + 3X_{(1,1,1,2)}$ $+2X_{(1,1^2,2)} + X_{(1^3,2)} + X_{(1,2,2)} + X_{(1,2^2)}$ $+2X_{(1,1,3)} + X_{(1^2,3)} + X_{(1,4)}$	q^3
(1^2)	$X_{(1,1,1,1^2)} + 2X_{(1,1^2,1^2)} + X_{(1,1,1^3)}$ $+X_{(1,1^4)} + X_{(1^5)} + X_{(1,1^2,2)} + X_{(1^3,2)} + X_{(1^2,3)}$	q^2
(1^3)	$X_{(1,1,1^3)} + X_{(1,1^4)} + X_{(1^5)} + X_{(1^3,2)}$	q
(2)	$X_{(1,1,1,2)} + X_{(1,1^2,2)} + X_{(1^3,2)}$ $+2X_{(1,2,2)} + X_{(1,2^2)} + X_{(2,3)}$	$\frac{q^2(q-1)}{2}$
(3)	$X_{(1,1,3)} + X_{(1^2,3)} + X_{(2,3)}$	$\frac{q(q^2-1)}{3}$
$(1,1)$	$10X_{(1,1,1,1,1)} + 6X_{(1,1,1,1^2)} + 3X_{(1,1^2,1^2)}$ $+3X_{(1,1,1^3)} + X_{(1,1^4)} + 3X_{(1,1,1,2)}$ $+X_{(1,1^2,2)} + X_{(1,1,3)}$	$\frac{q^2(q-1)}{2}$
$(1,2)$	$3X_{(1,1,1,2)} + 2X_{(1,1^2,2)}$ $+X_{(1^3,2)} + 2X_{(1,2,2)} + X_{(1,2^2)}$	$\frac{q^2(q-1)}{2}$
$(1,1^2)$	$3X_{(1,1,1,1^2)} + 4X_{(1,1^2,1^2)}$ $+2X_{(1,1,1^3)} + X_{(1,1^4)} + X_{(1,1^2,2)}$	$q(q-1)$
$(1,1,1)$	$10X_{(1,1,1,1,1)} + 4X_{(1,1,1,1^2)}$ $+X_{(1,1^2,1^2)} + X_{(1,1,1^3)} + X_{(1,1,1,2)}$	$\frac{q(q-1)(q-2)}{6}$

Table 3 contains all of the equations involved in $A + B + C$.

Summing up according to the coefficients from equation (8.2), we obtain

$$5X_{(5)} + X_{(1^5)} - 120X_{(1,1,1,1,1)} - 60X_{(1,1,1,1^2)} - 30X_{(1,1^2,1^2)} - 20X_{(1,1,1^3)} - 5X_{(1,1^4)} - X_{(1^5)} = 0,$$

which is the result predicted by Theorem 1.1.

9. Conclusion. We have proved the formula for the number of irreducible polynomials with the first two prescribed coefficients by using combinatorial methods and results from the theory of quadratic forms over finite fields. Our method also gives a proof of the formula for the number of irreducible polynomials with the first prescribed coefficient and has the potential of leading results for other prescribed factorization types. In principle, this method could be extended to a higher number of fixed coefficients. This condition would restrict the number of equations $\mathcal{E}_{\mathbf{w}}$ that we can use, and the equivalent expression for $\sum_{\substack{d|n \\ p\nmid n/d}} dH_d$ would involve terms $X_{\mathbf{v}}(\mathbf{a})$ whose matrices V contain nonzero entries outside the first row. It should be interesting to explore the feasibility of this method for $\ell > 2$.

REFERENCES

1. E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen*, II, Math. Z. **19** (1924), 207–246.

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

3. W. Casselman, *Quadratic forms over finite fields*, notes available at `http://www.math.ubc.ca/~cass/siegel/Minkowski.pdf`.

4. K. Cattell, C.R. Miers, F. Ruskey, J. Sawada and M. Serra, *The number of irreducible polynomials over* GF (2) *with given trace and subtrace*, J. Comb. Math. Comb. Comp. **47** (2003), 31–64.

5. S.D. Cohen, *Explicit theorems on generator polynomials*, Finite Fields Appl. **11** (2005), 337–357.

6. ______, *Irreductible polynomials–Prescribed coefficients*, in *Handbook of finite fields*, G.L. Mullen and D. Panario, eds., CRC Press, Boca Raton, 2013.

7. ______, *Uniform distribution of polynomials over finite fields*, J. Lond. Math. Soc. **6** (1972), 93–102.

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

9. D.R. Hayes, *The distribution of irreducibles in $GF[q,x]$*, Trans. Amer. Math. Soc. **117** (1965), 101–127.

10. E.N. Kuz'min, *On irreducible polynomials over a finite field*, Sibirsk. Mat. Zh. **30** (1989), 98–109; Siberian Math. J. **30** (1990), 915–925 (in English).

11. ______, *A class of irreducible polynomials over a finite field*, Dokl. Akad. Nauk **313** (1990), 552–555; Soviet Math. Dokl. **42** (1991), 45–48.

12. ______, *Irreducible polynomials over a finite field and an analogue of Gauss sums over a field of characteristic* 2, Sibirsk. Mat. Zh. **32** (1991), 100–108, 205; Siberian Math. J. **32** (1992), 982–989 (in English).

13. E.N. Kuz'min, *Irreducible polynomials over a finite field*, I, Alg. Logic **33** (1995), 216–232.

14. H. Minkowski, *Grundlagen für eine Theorie der quadratischen Formen mit ganzzhligen Koeffizienten*, in *Gesammelte Abhandlungen*, AMS Chelsea Publishing, Philadelphia, 1967.

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

16. B. Omidi Koma, D. Panario and Q. Wang, *The number of irreducible polynomials of degree n over $\mathbb{F}_q$ with given trace and constant terms*, Discr. Math. **310** (2010), 1282–1292.

17. J.L. Yucas, *Irreducible polynomials over finite fields with prescribed trace/prescribed constant term*, Finite Fields Appl. **12** (2006), 21–221.

18. J.L. Yucas and G.L. Mullen, *Irreducible polynomials over $GF(2)$ with prescribed coefficients*, Discr. Math. **274** (2004), 265–279.

Département de mathématiques et de statistique, Université de Montréal, CP 6128, succ. Centre-ville, Montreal, QC H3C 3J7, Canada
Email address: **mlalin@dms.umontreal.ca**

Département de mathématiques et de statistique, Université de Montréal, CP 6128, succ. Centre-ville, Montreal, QC H3C 3J7, Canada
Email address: **olivier.larocque.1@umontreal.ca**