On the Number of Factorizations of Polynomials over Finite Fields

Rachel N. Berman Ron M. Roth

Computer Science Department, Technion, Haifa 3200003, Israel.
rachelinaka@gmail.com, ronny@cs.technion.ac.il

Abstract—Motivated by coding applications, two enumeration problems are considered: the number of distinct divisors of a degree- \( m \) polynomial over \( \mathbb{F} = \text{GF}(q) \), and the number of ways a polynomial can be written as a product of two polynomials of degree at most \( n \) over \( \mathbb{F} \). For the two problems, bounds are obtained on the maximum number of factorizations, and a characterization is presented for polynomials attaining that maximum. Finally, expressions are presented for the average and the variance of the number of factorizations, for any given \( m \) (resp., \( n \)).

I. INTRODUCTION

Throughout this work, we fix \( \mathbb{F} \) to be a finite field of size \( q \). Let \( \mathbb{F}[x] \) be the set of polynomials over \( \mathbb{F} \) and \( \mathcal{M}_n = \mathcal{M}_n(q) \) (resp., \( \mathcal{P}_m = \mathcal{P}_m(q) \)) be the set of all monic polynomials of degree exactly (resp., at most) \( n \) in \( \mathbb{F}[x] \).

Given \( m \in \mathbb{Z}^+ \) and \( s(x) \in \mathcal{P}_m \), let \( \Phi(s) \) be the number of distinct divisors of \( s(x) \) in \( \mathcal{P}_m \) and define

\[ \Upsilon_m = \Upsilon_m(q) = \max_{s(x) \in \mathcal{P}_m} \Phi(s). \]

It is easy to see that the maximum is attained only when \( \deg s = m \). Accordingly, we say that \( s(x) \in \mathcal{M}_m \) is maximal if \( \Phi(s) = \Upsilon_m \). Given \( (n, n') \in \mathbb{Z}^+ \times \mathbb{Z}^+ \) and \( s(x) \in \mathcal{P}_{n+n'} \), an \( (n, n') \)-factorization of \( s(x) \) is an ordered pair \( (u(x), v(x)) \in \mathcal{P}_n \times \mathcal{P}_{n'} \) such that \( s(x) = u(x) \cdot v(x) \).

The number of distinct \( (n, n') \)-factorizations of \( s(x) \) will be denoted by \( \Phi_{n,n'}(s) \) and we define

\[ \Upsilon_{n,n'} = \Upsilon_{n,n'}(q) = \max_{s(x) \in \mathcal{P}_{n+n'}} \Phi_{n,n'}(s). \]

We will assume hereafter that \( n = n' \) and abbreviate the notation \( \Phi_{n,n}(s) \) by \( \Phi_n(s) \). We say that \( s(x) \in \mathcal{P}_{2n} \) is \( n \)-maximal if \( \Phi_n(s) = \Upsilon_{n,n} \). Clearly, for all \( s(x) \in \mathcal{P}_{2n} \) we have \( \Phi_n(s) \leq \Phi(s) \), therefore \( \Upsilon_{n,n} \leq \Upsilon_{2n} \).

In this work we address two related combinatorial problems.

Problem 1 (Ordinary factorization). Given \( m \in \mathbb{Z}^+ \), compute \( \Upsilon_m \) and characterize the maximal polynomials in \( \mathcal{M}_m \).

Problem 2 ((\( n \), \( n \))-factorization). Given \( n \in \mathbb{Z}^+ \), compute \( \Upsilon_{n,n} \) and characterize the \( n \)-maximal polynomials in \( \mathcal{P}_{2n} \).

In particular, we show in Section III that

\[ \Upsilon_m = 2^{(m/\log_q m)(1+o_m(1))}, \]

where \( o_m(1) \) stands for an expression that goes to 0 as \( m \to \infty \), and that essentially the same expression holds for \( \Upsilon_{n,n} \):

\[ \Upsilon_{n,n} = 2^{(2n/\log_q n)(1+o_n(1))}. \]

A characterization of an \( (n) \)-maximal polynomial will be given in Sections IV and V.

For both problems, we also present in Section VI average case counterparts, and, inter alia, we compute the expectations and bound the variances of \( \Phi(s) \) and \( \Phi_n(s) \), when \( s(x) \) is drawn with respect to a particular uniform distribution defined precisely for each of the two problems in Section II.

The counterpart of Problem 1 for \emph{integers} is classical and was studied over 100 years ago [1, §4],[7],[9]. Polynomial factorization over finite fields, on the other hand, has hardly been considered. The enumeration of ordinary factorizations was investigated by Piret in [8] for \( q = 2 \). Specifically, he proved that \( \Upsilon_m(2) \leq (81/16)^{(m/\log_2 m)(1+o_m(1))} \), as part of an analysis that shows that most binary shortened cyclic codes approach the Gilbert–Varshamov bound. Enumeration of \( (n,n) \)-factorizations (Problem 2) is related to another coding problem, namely, the list decoding of a certain type of rank-metric codes [11, §4]. In recent years, there has been a growing interest in rank-metric codes [4],[12] and, in particular, in their list-decoding performance [3],[10],[11]. The value \( \Upsilon_{n,n} \) and the expected number of \( (n,n) \)-factorizations of a random polynomial in \( \mathcal{P}_{2n} \) are, respectively, the largest and average list sizes of a list decoder for the rank-metric code of \( (n+1) \times (n+1) \) arrays that was considered in [11], when the minimum rank distance is 2 and the decoding radius is 1. It was shown in [11] that for large fields (namely, \( q \geq 2n-1 \)), the list size is \( 4^{n-o_n(1)} \), but no analysis was carried out when the field size is small. In addition to these coding applications, we believe that our study of the structure of \( (n) \)-maximal polynomials is of independent mathematical interest. Our results demonstrate both similarities and differences between Problems 1 and 2.

Hereafter, \( [\ell : k] \) denotes the set \( \{i \in \mathbb{Z} : \ell \leq i \leq k \} \).

II. SUMMARY OF RESULTS

Bounds on \( \Upsilon_m \) and \( \Upsilon_{n,n} \). Our first set of results includes bounds on the values of \( \Upsilon_m \) and \( \Upsilon_{n,n} \).

Fix an ordering \( (p_i(x))_{i=1}^\infty \) on the monic irreducible polynomials over \( \mathbb{F} \) which is non-decreasing in degree and denote \( d_i = \deg p_i \). Given a monic \( s(x) \in \mathbb{F}[x] \), let \( s(x) = \prod_{i=1}^k p_i(x)^{r_i} \) be its irreducible factorization over \( \mathbb{F} \), where

\[ \prod_{i=1}^k p_i(x)^{r_i} \]

This work was supported in part by Grant 1396/16 from the Israel Science Foundation.
ri = \text{mult}_p_i(s) \text{ and } r_i > 0 \text{ (thus } r_i = 0 \text{ for every } i > t). \ \text{We will write } r(s) = (r_1 \ r_2 \ldots \ r_t) \text{ and define}
\rho(s) = \max_{i \in \mathbb{Z}^+ : d_i = 1} r_i.

It is easy to see that
\[ \Phi(s) = \prod_{i=1}^t (r_i + 1). \] (4)

The next three propositions present basic structural properties of maximal polynomials.

**Proposition 1.** Let \( s(x) \in \mathcal{M}_m \) be maximal and let \( r(s) = (r_i)_{i=1}^t \) and \( \rho = \rho(s). \) For every \( i \in [1 : t] \):
\[ r_i = \rho_i + 1 \leq d_i < \frac{\rho + 1}{r_i}. \] (5)
Equivalently: \( r_i \in \{ \lfloor \rho/d_i \rfloor, \lceil \rho/d_i \rceil - 1 \} \).

**Proposition 3.** Using the notation of Prop. 2,
\[ \log_2 q(m/8) < d_i \leq d_{i+1} \leq \log_2 m + 1. \] (6)

We then obtain the following two bounds.

**Theorem 4.** For all \( m \in \mathbb{Z}^+ \):
\[ \log_2 \Upsilon_m \leq \frac{m}{\log_2 m} \cdot \left( 1 + \mathcal{O} \left( \frac{\log_2 \log_2 m}{\log_2 m} \right) \right). \]

**Theorem 5.** For all \( n \in \mathbb{Z}^+ \):
\[ \log_2 \Upsilon_{n,n} \geq \frac{2n}{\log_2 n} \cdot \left( 1 - \mathcal{O} \left( \frac{1}{\log_2 n} \right) \right). \]

Thms. 4 and 5, along with \( \Upsilon_{n,n} \leq \Upsilon_{2n} \leq \Upsilon_{2n+1} \), imply (2) and (3).

**Finer characterization of maximal polynomials.** Our second set of results extends Prop. 2. First, we prove the following estimate for the value of \( \rho \).

**Proposition 6.** Using the notation of Prop. 2,
\[ \rho = \frac{\log_2 m}{\ln 2} + \mathcal{O} \left( \log_2 \log_2 m \right). \]

Then, we prove the following theorem, which improves on Prop. 2 for large degrees \( d_i \).

**Theorem 7.** Let \( s(x) \in \mathcal{M}_m \) be maximal. For every \( i \in [1 : t] \) such that \( d_i \geq \Theta \left( \log \log_2 m \right) \):
\[ \log_2 \left( 1 + \left( 1/\left( r_{i+1} \right) \right) \right) \cdot \log_2 m - \mathcal{O}(1) < d_i \leq \log_2 \left( 1 + \left( 1/r_i \right) \right) \cdot \log_2 m + \mathcal{O}(1). \]
Equivalently: \( r_i = \left[ \frac{1}{\left( 2^{d_i : \Theta(1)} \right) / \log_2 m - 1} \right] \).

**Characterization of \( n \)-maximal polynomials.** Our third set of results addresses the second part of Problem 2 and provides a characterization of an \( n \)-maximal polynomial.

For \( n \in \mathbb{Z}^+ \) and \( s(x) = \prod_{i=1}^t p_i(x) r_i \in \mathcal{P}_n \), let \( r_0 = 2n - \deg s \) and write \( r_n(s) = (r_i)_{i=0}^t \). Also, define
\[ \rho_n(s) = \max \{ \rho_0, \rho(s) \} = \max_{i \in \mathbb{Z}^+: d_i = 1} r_i, \]
where \( d_0 \equiv 1 \). Prop. 1 through Thm. 7 hold also for \( n \)-maximal polynomials, with \( m, r(s), \) and \( \rho(s) \) replaced by \( 2n, r_n(s), \) and \( \rho_n(s) \), respectively. In particular, the counterpart of Prop. 2 reads as follows.

**Proposition 8.** Let \( s(x) \in \mathcal{P}_{2n} \) be \( n \)-maximal and let \( r_n(s) = (r_i)_{i=0}^t \) and \( \rho_n = \rho_n(s). \) For every \( i \in [0 : t] \):
\[ \frac{\rho_n + 1}{r_i + 2} \leq d_i < \frac{\rho_n + 1}{r_i}. \] (7)
Equivalently: \( r_i \in \{ \lfloor \rho_n/d_i \rfloor, \lceil \rho_n/d_i \rceil - 1 \} \).

It follows from the \( n \)-maximal counterparts of Props. 2 and 6 that \( r_0 = \Theta(\log q) \); namely, any \( n \)-maximal polynomial \( s(x) \in \mathcal{P}_{2n} \) has degree \( 2n - \Theta(\log q) \) \((< 2n)\). In contrast, recall that the maximum in (1) is attained by a polynomial \( s(x) \) of degree exactly \( m \).

**Average-case analysis.** In our fourth set of results, we consider the probabilistic counterparts of Problems 1 and 2. In the case of ordinary factorizations, given \( m \in \mathbb{Z}^+ \), we take the sample space to be \( \mathcal{M}_m \), assume a uniform distribution over \( \mathcal{M}_m \), and define a random variable \( \Phi_m \) over \( s(x) \in \mathcal{M}_m \) by \( \Phi_m : s \mapsto \Phi(s) \).

**Theorem 9.**
\[ \mathbb{E} \{ \Phi_m \} = m + 1 \ \text{and} \ \mathbb{V} \{ \Phi_m \} = \frac{q - 1}{q} \left( \frac{m + 1}{3} \right). \]

Using the well-known Markov and Chebyshev inequalities we get that for every \( \varepsilon > 0 \),
\[ \mathbb{P} \{ \Phi_m \geq m^{1+\varepsilon} \} \leq \mathcal{O} \left( m^{-\max \{ 2, \varepsilon - 1 \}} \right). \]
In particular, the probability of \( \Phi_m \) being super-linear in \( m \) tends to 0 as \( m \to \infty \). Through a different approach, which uses the Chernoff bound, we are also able to prove the following result, which implies that the median of \( \Phi_m \) is sub-linear in \( m \).

**Proposition 10.** For any (fixed) \( \varepsilon > 0 \),
\[ \mathbb{P} \{ \Phi_m \geq m^{\varepsilon+1+\varepsilon} \} \leq \mathcal{O} \left( m^{-\kappa(\varepsilon)} \right), \]
where \( \kappa(\varepsilon) > 0 \).

In the case of \( (n, n) \)-factorizations, we consider a different probability model, which fits the coding application that was mentioned in Section I, namely, the list decoding of the rank-rank code of [11], assuming error arrays that are uniformly distributed conditioned on having rank 1. Accordingly, given \( n \in \mathbb{Z}^+ \), the sample space is defined to be \( \mathcal{P}_n^2 = \mathcal{P}_n \times \mathcal{P}_n \), over which we assume a uniform distribution. We define a random variable \( \Phi_{n,n} \) over \( (u, v) \in \mathcal{P}_n^2 \) by \( \Phi_{n,n} : (u, v) \mapsto \Phi_n(u \cdot v) \) (i.e., the number of \( (n, n) \)-factorizations of the product \( u \cdot v \)).

**Theorem 11.**
\[ \mathbb{E} \{ \Phi_{n,n} \} = (n+1)(1+\mathcal{O}(1/q)) \ \text{and} \ \mathbb{V} \{ \Phi_{n,n} \} = \mathcal{O}(n^4). \]

Thus, \( \Phi_{n,n} \), too, takes super-linear values in \( n \) with vanishing probability as \( n \to \infty \).

Due to space limitations, many proofs in this abstract are either sketched or omitted. The full text can be found in [2].
III. Bounds on υm and υn,n
For d ∈ ℤ+, let I(d) = I(d,q) be the number of monic irreducible polynomials of degree d over ℙ. It follows from [5, Thm. 3.25] that for any d ∈ ℤ+,
\[
\frac{1}{d} \left( q^d - 2q^{\lceil d/2 \rceil} \right) < I(d) < \frac{q^d}{d},
\]
(8)
and by induction on d we readily get:
\[
\sum_{\ell=1}^{d} I(\ell) \leq \sum_{\ell=1}^{d} \frac{q^\ell}{\ell} < \frac{4q^d}{d+1},
\]
(9)
We proceed to proving Prop. 1 through Thm. 5. Many of the proofs in this work follow a similar pattern: we assume that a polynomial s ∈ ℙm does not satisfy the property to be proved, and we construct from s a polynomial ˜s ∈ ℙm for which Φ(˜s) > Φ(s), thereby showing that s cannot be maximal. Due to space limitations, in most cases we will only indicate which ˜s is; the full details can be found in [2].

Proof of Prop. 1. Given d1 < d2, assume that s(x) ∈ ℙm is such that r1 ≥ rj + 1, and let pk(x) ∈ ℌ1 where k ≠ j. The polynomial
\[
\tilde{s}(x) = s(x) \cdot p_k(x) / p_k(x)^{d_1}
\]
is in ℙm and satisfies
\[
\Phi(\tilde{s}) = (r_k + 2) / r_k + 1 > (r_j + 1) \cdot \frac{r_j + 2}{r_j + 1} \cdot \frac{r_i - 1}{r_i} \cdot \frac{r_j}{r_i} \cdot \Phi(s) > \Phi(s).
\]
Thus, s cannot be maximal.

Proof sketch of Prop. 2. Assuming that s(x) does not satisfy the left inequality in (5), define
\[
\tilde{s}(x) = s(x) \cdot p_k(x) / p_k(x)^{d_1}
\]
where pk(x) ∈ ℌ1 is such that ρ = r_k. Then Φ(˜s) > Φ(s). The right inequality in (5) is proved in a similar manner, taking
\[
\tilde{s}(x) = s(x) \cdot p_k(x)^{\lceil d_1/2 \rceil} / p_l(x)^{\lceil d_1/2 \rceil}
\]
where pk(x) and pl(x) are distinct in ℌ1.

Lemma 12. Using the notation of Prop. 2,
\[
d_i < \rho \leq 2d_i + 1 - 1. \tag{10}
\]
Proof. Substituting i = t (resp., i = t + 1) in Prop. 2 yields the left (resp., right) inequality.

Proof of Prop. 3. The following chain of inequalities imply the leftmost inequality in (6):
\[
m = \deg s = \sum_{i=1}^{t} r_i d_i \leq (t + 1) \leq 2d_t + 1 \cdot t \leq 2d_t + 1 \cdot \sum_{\ell=1}^{d_t} I(\ell) < 8q^{d_t}.
\]
As for the rightmost inequality in (6), we recall from [5, Corollary 3.21] that q^d = \sum_{\ell = 1}^{d} \ell \cdot I(\ell); hence, by Prop. 1,
\[
m = \deg s \geq \sum_{\ell=1}^{d_t + 1} \ell \cdot I(\ell) \geq q^{d_t + 1} - 1.
\]

Proof of Thm. 4. Let s(x) ∈ ℙm be maximal, let ε ∈ (0,1), and consider first all the irreducible factors of s(x) of degree at most Δ = \lfloor (1 - \epsilon) \log_q m \rfloor. By Prop. 2 and Lemma 12, their total number, w1 (counting multiplicities), is bounded from above by
\[
w_1 = \sum_{i:d_i \leq \Delta} r_i \leq \Delta \cdot \sum_{d=1}^{\Delta} I(d) \leq 2d_t + 1 \cdot \sum_{d=1}^{\Delta} I(d) \leq 2d_t + 1 \cdot \Delta \cdot \frac{4q^\Delta}{\Delta + 1} \cdot \frac{1}{\Delta} \leq \mathcal{O} \left( m^{1-\epsilon} \right).
\]
Selecting ε = 2(\log_q \log_q m)/\log_q m, we readily get:
\[
w_1 = \mathcal{O} \left( m^{1-\epsilon} \right) = \mathcal{O} \left( m/\log_q m \right).
\]
Turning to the irreducible factors of s(x) whose degrees exceed Δ, their total number, w2 (counting multiplicities), is bounded from above by
\[
w_2 \leq \frac{m}{\log_q m} \cdot \left( 1 + \mathcal{O} \left( \frac{\log_q m}{\log_q m} \right) \right).
\]
We conclude that
\[
\log_q \Phi(s) \leq w_1 + w_2 \leq \frac{m}{\log_q m} \cdot \left( 1 + \mathcal{O} \left( \frac{\log_q m}{\log_q m} \right) \right).
\]

Proof of Thm. 5. Let d be the smallest integer such that d · I(d) ≥ 2n; by (8) we have d ∈ \{ \lceil \log_q n \rceil + 1, \lceil \log_q n \rceil + 2 \}. Let w = \lfloor n/d \rfloor, and let s(x) be a product of 2w distinct monic irreducible polynomials of degree d. Such a polynomial has degree ≤ 2n and \( (\frac{2n}{w}) \) distinct \((n,n)\)-factorizations. We have:
\[
\mathbb{T}_{n,n} \geq \Phi(s) = \left( \frac{2w}{w} \right) = \left( \frac{2n}{\log_q n} \right) \left( 1 - \mathcal{O} \left( \frac{1}{\log_q n} \right) \right),
\]
where the last equality follows from \( w = \lfloor n/\log_q n \rfloor \) and known approximations of the binomial coefficients [6, p. 309, Eq. (16)].

IV. Characterization of maximal polynomials
Prop. 6 and Thm. 7 are proved using the next two lemmas. Hereafter, we let \( \delta_q(m) \) be the smallest positive integer \( \delta \) such that \( I(d) > \left( \log_q m \right) + 1 \) for every \( d \geq \delta \). By (8), it follows that \( \delta_q(m) = \log_q \log_q(q^m) + o(\log \log_q m) \).

Lemma 13. Let s(x) ∈ ℌm be maximal and let \( i \in [1:t] \).
(a) If \( d_i \geq \delta_q(m) \) and \( r_i > 1 \) then
\[
d_i \leq \log_2 (r_i / (r_i - 1)) \cdot (d_i + 1). \tag{11}
\]
(b) If \( d_i \geq \delta_q(m) + 1 \) then
\[
d_i \leq \log_2 (r_i + 1) / r_i \cdot (d_i + 1) + 1.
\]

Proof. (a) Let \( \mathcal{U} \) be a set of \( d_i + 1 \) indexes \( j \) for which \( d_j = d_i \); from \( d_i \geq \delta_q(m) \) and Prop. 3 we have \( I(d_i) > \left( \log_q m \right) + 1 \geq d_i \) and, so, such a set indeed exists. Also, let \( \mathcal{V} \) be a set of \( d_i \) indexes \( k \) for which \( d_k = d_i + 1 \). Prop. 2 implies that \( r_j > r_i - 1 > 0 \) when \( j \in \mathcal{U} \). Define the polynomial
\[
\tilde{s}(x) = s(x) \cdot \left( \prod_{k \in \mathcal{V}} p_k(x) / \prod_{j \in \mathcal{U}} p_j(x) \right) \]
We have:
\[ \frac{\Phi(\tilde{s})}{\Phi(s)} = 2^n \prod_{j \in U} \frac{r_j}{r_j + 1} \geq 2^{d_i} \left( \frac{r_i - 1}{r_i} \right)^{d_i + 1}. \]  
(12)

Now, \( \deg \tilde{s} = \deg s = m \) and, so, \( \Phi(\tilde{s})/\Phi(s) \leq 1 \) (since \( s \) is maximal). The result follows from (12) by taking logarithms.

(b) The proof is similar to part (a), except that \( d_i \) is replaced by \( d_i - 1 \): now \( U \) is a set of \( d_i + 1 \) indexes \( j \) for which \( d_j = d_i - 1 \), and \( V \) is a set of \( d_i - 1 \) indexes \( k \) for which \( d_k = d_i + 1 \).

Lemma 14. Let \( s(x) \in \mathcal{M}_m \) be maximal and let \( i \in [1 : t] \).

(a) If \( d_i \geq \delta_q(m) \) then
\[ d_i \geq \log_2 \left( \frac{(r_i+3)/(r_i+2)}{(d_i+1)} \right) \cdot (d_i+1) - 1. \]

(b) If \( d_i \geq \delta_q(m) - 1 \) then
\[ d_i \geq \log_2 \left( \frac{(r_i+2)/(r_i+1)}{(d_i+1) - 1} \right). \]

Proof sketch. Here we take \( U \) to be a set of \( d_i + 1 \) indexes \( j \) for which \( d_j = d_i \) (resp., \( d_j = d_i + 1 \) for part (b)) and \( V \) to be set of \( d_i \) (resp., \( d_i + 1 \)) indexes \( k \) for which \( d_k = d_i - 1 \).

The polynomial \( \tilde{s} \) is defined by
\[ \tilde{s}(x) = s(x) \cdot \left( \prod_{j \in U} p_j(x) \right) / \prod_{k \in V} p_k(x). \]

Proof of Prop. 6. Let \( i \in [1 : t] \) be such that \( d_i = \delta_q(m) (= O(\log_q \log_q m)) \). By Lemma 13(a) we have
\[ \frac{1}{r_i} - 1 \geq d_i / (d_i + 1) \geq 1 + d_i \ln \frac{2}{d_i + 1} \]  
and, so, along with Prop. 2 we obtain:
\[ \frac{\rho}{d_i} - 1 \leq r_i \leq \frac{d_i + 1}{d_i \ln 2} + 1. \]

Hence,
\[ \rho < \frac{d_i + 1}{\ln 2} + 3d_i = \frac{\log_q m}{\ln 2} + O \left( \log_q \log_q m \right). \]  
(14)

The proof of the lower bound on \( \rho \) is similar, except that we use Lemma 14(a) instead.

Proof of Thm. 7. Combine Lemmas 13(b) and 14(b) with Prop. 3.

V. CHARACTERIZATION OF \( n \)-MAXIMAL POLYNOMIALS

Given \( n \in \mathbb{Z}^+ \) and \( s(x) \in \mathcal{P}_{2n} \), we extend the degree of \( s(x) \) to \( 2n \) by introducing a slack variable \( y \) and defining
\[ s(x, y) = y^n \cdot s(x), \]  
(15)
where \( r_0 = 2n - \deg s(x) \). Accordingly, we introduce the following notation:
\[ \mathcal{P}_m = \mathcal{P}_m(q) = \left\{ y^{m-\deg u} \cdot u(x) : u(x) \in \mathcal{P}_m \right\}. \]

Given \( b(x, y) \in \mathcal{P}_m \), we denote by \( \mathcal{D}_n(b) \) the set of divisors of \( b(x, y) \) in \( \mathcal{P}_k \). Thus \( s(x, y) \in \mathcal{P}_{2n} \), and there is a one-to-one correspondence between the \((n, n)\)-factorizations \((u(x), v(x)) \in \mathcal{P}_2^n \) of \( s(x) \) and divisors \( u(x, y) \in \mathcal{D}_n(s(x, y)) \).

In particular, \( \Phi_n(s) = |\mathcal{D}_n(s)| \).

Given a polynomial \( s(x, y) \in \mathcal{P}_{2n} \), fix a factorization
\[ s(x, y) = a(x) \cdot b(x, y), \]  
(16)
where \( \gcd(a, b) = 1 \) and \( b(x, y) \in \mathcal{P}_h \), for some \( h \in [r_0 : 2n] \) (we will determine \( a \) and \( b \) later). For every \( k \in [h-n : n] \) let
\[ A_k = A_k(n, a) = \{ f \in \mathcal{M}_{n-k} : f \mid a \}. \]  
(17)

We have:
\[ \Phi_n(s) = |\mathcal{D}_n(s)| = \sum_{k \in \{0 : h\}} |A_k| \cdot |D_k(b)|. \]  
(18)

A. Proof of Prop. 8

To prove Prop. 8 we first observe that (7) is equivalent to
\[ \rho_n - 2d_i < r_i d_i \leq \rho_n. \]

These two inequalities will follow from the next two lemmas.

Lemma 15. \( r_i d_i > \rho_n - 2d_i \) for every \( i \in [1 : t] \).

Lemma 16. \( r_i d_i < \rho_n + 1 \) for every \( i \in [1 : t] \).

Fix a polynomial \( s(x) = \prod_{i=1}^t p_i(x)^{r_i} \in \mathcal{P}_{2n} \) and let \( s(x, y) = y^{n-\deg s(x)} \cdot s(x) \) be as in (15). W.l.o.g. assume that \( \rho_n = \rho_n(s) = r_0 \).

Proof sketch of Lemma 15. Assuming \( r_i d_i \leq \rho_n - 2d_i \), we show that \( \Phi_n(s) > \Phi_n(s) \), where
\[ \tilde{s}(x) = s(x) \cdot p_i(x) / y^{n-\deg s(x)}. \]

This is done as follows. Write \( s(x, y) = a(x) \cdot b(x, y) \) (as in (16)) and \( \tilde{s}(x) = a(x) \cdot b(x, y) \), where \( b(x, y) = y^{n-\deg s(x)} \cdot p_i(x)^{r_i} \) and \( \tilde{b}(x, y) = y^{n-\deg s(x)} \cdot p_i(x)^{r_i+1} \). (And, so, \( \gcd(a, b) = \gcd(a, \tilde{b}) = 1 \), \( h = \deg b(x, y) = r_0 + r_i d_i \), and \( \deg a(x) = 2n - h \).

First, by combinatorial considerations (which we omit), it can be shown that for all \( k \in [0 : h] \):
\[ |D_k(b)| \leq |D_k(\tilde{b})|. \]

Then, by a knapsack-like algorithm, one can show that \( A_{\lfloor h/2 \rfloor} \neq 0 \). Finally, one shows that
\[ |D_{\lfloor h/2 \rfloor}(\tilde{b})| < |D_{\lfloor h/2 \rfloor}(\tilde{b})| \]
which, with (18) (when stated for \( s \) and \( \tilde{s} \)) yields \( \Phi_n(s) > \Phi_n(s) \).

Proof sketch of Lemma 16. Assuming first that \( r_i d_i > r_0 + 1 \), we show that \( \Phi_n(s) > \Phi_n(s) \) for
\[ \tilde{s}(x) = s(x) \cdot y^{d_i} / p_i(x), \]

similarly to the proof of Lemma 15. When \( r_i d_i = r_0 + 1 \), we only get the weak inequality \( \Phi_n(s) \geq \Phi_n(s) \), yet then \( s \) (and, therefore, \( s \)) cannot be \( n \)-maximal since it violates Lemma 15.

The counterparts of Lemma 12 and Prop. 3 for \( n \)-maximal polynomials, which are obtained by replacing \( m \) and \( \rho \) therein by \( 2n \) and \( \rho_n \), respectively, are proved similarly.
B. Proof of Prop. 6 and Thm. 7 for the $n$-maximal case

In this section, we show that Prop. 6 and Thm. 7 hold also for the $n$-maximal case.

Fix an $n$-maximal polynomial $s(x) = \prod_{i=1}^n p_i(x)^{r_i}$, let $s(x, y) = y^{r_0} \cdot s(x)$ where $r_0 = 2n - \deg s(x)$, and write $\rho_n = \rho_n(s)$. Fix a factorization (16) where $\gcd(a, b) = 1$ and $b(x, y) \in \mathcal{P}_n$, for some $h \in [r_0 : 2n]$. For every $k \in [h - n : n]$ let $\mathcal{A}_k = \mathcal{A}_k(n, a)$ be as in (17).

**Proposition 17.** Let $s(x, y) \in \mathcal{P}_{2n}$ be $n$-maximal and assume the factorization (16) with $h = \deg b(x, y) = \mathcal{O}(\log^2 n)$. For any $k, k' \in [0 : h]$: $|\mathcal{A}_{k'}|/|\mathcal{A}_k| \geq 1 - \mathcal{O}(\lambda_q(n))$, where $\lambda_q(n) = \sqrt{(q \ln n)/n \cdot \log^2 n}$.

We omit the proof of the proposition due to space limitations. Next, we sketch how it implies Lemma 13(a) (and, similarly, Lemma 13(b) and Lemma 14(a)–(b) and, consequently, Prop. 6 and Thm. 7) for the $n$-maximal case. Assuming that $s(x)$ is $n$-maximal, we define the sets $\mathcal{U}$ and $\mathcal{V}$ and the polynomial $\tilde{s}(x)$ as in the proof of Lemma 13(a). We write $s(x, y) = y^{r_0} \cdot s(x) = a(x) \cdot b(x, y)$, where

$$b(x, y) = y^{r_0} \cdot \prod_{j \in \mathcal{U}} p_j(x)^{r_j}.$$

Similarly, we write $\tilde{s}(x, y) = y^{r_0} \cdot \tilde{s}(x) = a(x) \cdot \tilde{b}(x, y)$, where

$$\tilde{b}(x, y) = y^{r_0} \cdot \prod_{k \in \mathcal{V}} p_k(x) \cdot \prod_{j \in \mathcal{U}} p_j(x)^{r_j - 1}.$$

The degree $h = \deg b(x, y) = \deg \tilde{b}(x, y)$ is given by

$$h = r_0 + \sum_{j \in \mathcal{U}} r_j d_j \leq r_0 + \rho_n(d_i + 1) = \mathcal{O}(\log^2 n).$$

Denoting

$$D(b) = \bigcup_{k \in [0 : h]} D_k(b) \quad \text{and} \quad D(\tilde{b}) = \bigcup_{k \in [0 : h]} D_k(\tilde{b}),$$

we recall that, by (4),

$$|D(b)| = (r_0 + 1) \cdot \prod_{j \in \mathcal{U}} (r_j + 1) \quad (19)$$

$$|D(\tilde{b})| = (r_0 + 1) \cdot 2d_i \cdot \prod_{j \in \mathcal{U}} r_j. \quad (20)$$

From (18) (when stated for $s$ and $\tilde{s}$), (19)–(20), and Prop. 17 we get:

$$\frac{\Phi_n(\tilde{s})}{\Phi_n(s)} \geq \frac{\min_{k \in [0 : h]} |A_k|}{\max_{k \in [0 : h]} |A_k|} \cdot \frac{\sum_{k \in [0 : h]} |D_k(\tilde{b})|}{\sum_{k \in [0 : h]} |D_k(b)|}
\geq (1 - \mathcal{O}(\lambda_q(n))) \cdot \frac{|D(\tilde{b})|}{|D(b)|}
\geq (1 - \mathcal{O}(\lambda_q(n))) \cdot 2d_i \cdot \left(\frac{r_i - 1}{r_i}\right)^{d_i + 1},$$

which is the same as (12) except for the multiplicative $1 - \mathcal{O}(\log^2 n)$ term. Taking logarithms, we will have an $\mathcal{O}(\lambda_q(n))$ term substracted from the left-hand side of (11) and, consequently, from each instance of $d_i$ in (13). Since this term goes to zero as $n \to \infty$ much faster than $d_i/d_i$, its contribution amounts to adding an $o_n(1)$ term to the upper bound (14).

VI. AVERAGE-CASE ANALYSIS

We start with two lemmas, the proofs of which we omit.

**Lemma 18.** For $m \in \mathbb{Z}^+$ define the set

$$S_m = \{(a, b, c, d) \in \mathcal{P}_m^4 : \gcd(b, c) = 1, \ abcd \in \mathcal{M}_m \}.$$ 

Then

$$|S_m| = q^m \cdot \left(\frac{q - 1}{q} \left(\frac{m + 1}{3}\right) + (m + 1)^2\right). \quad (21)$$

**Lemma 19.** For $n \in \mathbb{Z}^+$ define the set

$$S_n^* = \{(a, b, c, d) \in \mathcal{P}_n^4 : \gcd(b, c) = 1, \ ab, \\text{cd, ac, bd} \in \mathcal{P}_n \}.$$ 

Then

$$|S_n^*| = \frac{1}{(1 + 1/q)}.$$ 

**Proof of Thm. 9.** Starting with $\mathbb{E}\{\Phi_m\}$, for $s(x) \in \mathcal{M}_m$, let

$$J(s) = \{(u(x), v) \in \mathcal{P}_m^2 : s(x) = u(x)v(x)\}.$$ 

We have:

$$q^m \cdot \mathbb{E}\{\Phi_m\} = \sum_{s \in \mathcal{M}_m} |J(s)| = \sum_{k=0}^m |M_k| \cdot |M_{m-k}| = (m + 1) \cdot q^m.$$ 

Turning to $\text{Var}\{\Phi_m\}$, we define the set

$$Q_m = \{(u, v, \hat{u}, \hat{v}) \in \mathcal{P}_m^2 : u(x)v(x) = \hat{u}(x)\hat{v}(x) \in \mathcal{M}_m\}.$$ 

It is easy to see that

$$|M_m| \cdot \mathbb{E}\{\Phi_m^2\} = \sum_{s \in \mathcal{M}_m} |J(s)|^2 = |Q_m|. \quad (22)$$

Let $S_m$ be as in Lemma 18, and consider the mapping from $S_m$ to $Q_m$ that sends each quadruple $(a, b, c, d) \in S_m$ to a quadruple $(u, v, \hat{u}, \hat{v}) \in Q_m$ by

$$u = ab, \ v = cd, \ \hat{u} = ac, \ \hat{v} = bd.$$ 

Under this mapping, each quadruple $(u, v, \hat{u}, \hat{v}) \in Q_m$ is an image of a (unique) quadruple $(a, b, c, d) \in S_m$ given by

$$a = \gcd(u, \hat{u}), \ d = \gcd(v, \hat{v}), \ b = u/a, \ c = v/d,$$

i.e., (23) defines a bijection $S_m \to Q_m$ and, so, $|Q_m| = |S_m|$. Combining with (21) and (22) finally yields

$$\text{Var}\{\Phi_m\} = \mathbb{E}\{\Phi_m^2\} - (\mathbb{E}\{\Phi_m\})^2 = \frac{q - 1}{q} \cdot \left(\frac{m + 1}{3}\right).$$

The proof of Prop. 10 is omitted.

The proof of Thm. 11 is similar to the computation of the variance in the proof of Thm. 9: we use Lemma 19 and a refinement of it to compute (resp., bound) the expectation (resp., variance) of $\Phi_{n,n}$. 

5
REFERENCES

[1] L. Alaoglu, P. Erdős, “On highly composite and similar numbers,” Trans. Amer. Math. Soc., 56 (1944), 448–469.
[2] R.N. Berman, R.M. Roth “On the number of factorizations of polynomials over finite fields,” https://arxiv.org/abs/2004.03058
[3] Y. Ding, “On list-decodability of random rank metric codes and subspace codes,” IEEE Trans. Inf. Theory, 61 (2015), 51–59.
[4] R. Köter, F.R. Kschischang, “Coding for errors and erasures in random network coding,” IEEE Trans. Inf. Theory, 54 (2008), 3579–3591.
[5] R. Lidl, H. Niederreiter, Finite Fields, Second Edition, Cambridge University Press, Cambridge, 1997.
[6] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[7] J.-L. Nicolas, “Répartition des nombres hautement composés de Ramanujan,” Can. J. Math., 23 (1971), 116–130.
[8] Ph. Piret “On the number of divisors of a polynomial over GF(2)” Applied Algebra, Algorithmics and Error-Correcting Codes, Springer Berlin Heidelberg (1986), 161–168.
[9] S. Ramanujan, “Highly composite numbers,” Proc. Lond. Math. Soc. (2), 14 (1915), 347–409. See also the extension work annotated by J.-L. Nicolas and G. Robin in Ramanujan J., 1 (1997), 119–153.
[10] N. Raviv, A. Wachter-Zeh, “Some Gabidulin codes cannot be list decoded efficiently at any radius,” IEEE Trans. Inf. Theory, 62 (2016), 1605–1615.
[11] R.M. Roth, “On decoding rank-metric codes over large fields,” IEEE Trans. Inf. Theory, 64 (2018), 944–951.
[12] D. Silva, F.R. Kschischang, R. Köter, “A rank-metric approach to error control in random network coding,” IEEE Trans. Inf. Theory, 54 (2008), 3951–3967.