Counting reducible, powerful, and relatively irreducible multivariate polynomials over finite fields

Joachim von zur Gathen[†] Alfredo Viola[‡]

Konstantin Ziegler[†]

April 23, 2013

Dedicated to the memory of Philippe Flajolet

Abstract

We present counting methods for some special classes of multivariate polynomials over a finite field, namely the reducible ones, the s-powerful ones (divisible by the sth power of a nonconstant polynomial), and the relatively irreducible ones (irreducible but reducible over an extension field). One approach employs generating functions, another one uses a combinatorial method. They yield exact formulas and approximations with relative errors that essentially decrease exponentially in the input size.

Keywords. multivariate polynomials, finite fields, combinatorics on polynomials, counting problems, generating functions, analytic combinatorics

2010 Mathematics Subject Classification. 11T06, 12Y05, 05A15

1 Introduction

Most integers are composite and most univariate polynomials over a finite field are reducible. The classical results of the Prime Number Theorem and a theorem of Gauß present approximations saying that randomly chosen integers up to x or polynomials of degree up to n are prime or irreducible with probability about $1/\ln x$ or $1/n$, respectively.

Concerning special classes of univariate polynomials over a finite field, Zsigmondy (1894) counts those with a given number of distinct roots or without irreducible factors of a given degree. In the same situation, Artin (1924) counts the irreducible ones in an arithmetic progression and Hayes (1965) generalizes these results. Cohen (1969) and Car (1987) count polynomials with certain

An Extended Abstract of this paper appeared as von zur Gathen, Viola & Ziegler (2010) and the full version is to appear in *SIAM Journal of Discrete Mathematics*.

[†]B-IT, Universität Bonn, D-53113 Bonn, Germany, {gathen,zieglerk}@bit.uni-bonn.de

[‡]Instituto de Computación, Universidad de la República, Montevideo, Uruguay, viola@fing.edu.uy

factorization patterns and Williams (1969) those with irreducible factors of given degree. Polynomials that occur as a norm in field extensions are studied by Gogia & Luthar (1981).

In two or more variables, the situation changes dramatically. Most multivariate polynomials are irreducible. Carlitz (1963) provides the first count of irreducible multivariate polynomials. In Carlitz (1965), he goes on to study the fraction of irreducibles when bounds on the degrees in each variable are prescribed; see also Cohen (1968). In this paper, we opt for bounding the total degree because it has the charm of being invariant under invertible linear transformations. Gao & Lauder (2002) consider our problem in yet another model, namely where one variable occurs with maximal degree. The natural generating function (or zeta function) for the irreducible polynomials in two or more variables does not converge anywhere outside of the origin. Wan (1992) notes that this explains the lack of a simple combinatorial formula for the number of irreducible polynomials. But he gives a p-adic formula, and also a (somewhat complicated) combinatorial formula. For further references, see Mullen & Panario (2013, Section 3.6).

In the bivariate case, von zur Gathen (2008) proves precise approximations with an exponentially decreasing relative error. Bodin (2008) gives a recursive formula for the number of irreducible bivariate polynomials and remarks on a generalization for more than two variables; he follows up with Bodin (2010). Some further types of multivariate polynomials are examined from a counting perspective: decomposable ones (von zur Gathen (2010), Bodin, Dèbes & Najib (2009)), singular ones (von zur Gathen (2008)), and pairs of coprime polynomials (Hou & Mullen (2009)).

This paper provides exact formulas for the numbers of reducible, s-powerful, and relatively irreducible polynomials. The latter also yields the number of absolutely reducible polynomials. Of these, only reducible polynomials have been treated in the literature, usually with much larger error terms. The formulas yield simple, yet precise, approximations to these numbers, with rapidly decaying relative errors.

We use two different methodologies to obtain such bounds: generating functions and combinatorial counting. The usual approach, see Flajolet & Sedgewick (2009), of analytic combinatorics on series with integer coefficients leads, in our case, to power series that diverge everywhere (except at 0). We have not found a way to make this work. Instead, we use power series with symbolic coefficients, namely rational functions in a variable representing the field size. Several useful relations from standard analytic combinatorics carry over to this new scenario. In a first step, this yields in a straightforward manner exact formulas for the numbers under consideration (Theorems 3.5, 5.2, and 6.11). These formulas are, however, not very transparent. Even the leading term is not immediately visible.

In a second step, coefficient comparisons yield easy-to-use approximations to our numbers (Theorems 3.14, 5.6, and 6.23). The relative error is exponentially decreasing in the bit size of the data. As an example, Theorem 3.14 gives a "third order" approximation for the number of reducible polynomials, and thus a "fourth order" approximation for the irreducible ones. The error term is in the big-Oh form and thus contains an unspecified constant.

In a third step, a different method, namely some combinatorial counting, yields "second order" approximations with explicit constants in the error term

(Theorems 4.3, 5.17, and 6.28).

Geometrically, a single polynomial corresponds to a hypersurface, that is, to a cycle in affine or projective space, of codimension 1. This correspondence preserves the respective notions of reducibility. Thus, Sections 3 and 4 can also be viewed as counting reducible hypersurfaces, in particular, planar curves, and Section 5 those with an s-fold component. Reducible curves embedded in higher-dimensional spaces, parametrized by the appropriate Chow variety, are counted in Cesaratto, von zur Gathen & Matera (2013).

2 Notation

We work in the polynomial ring $F[x_1, \ldots, x_r]$ in $r \geq 1$ variables over a field F and consider polynomials with total degree equal to some nonnegative integer n:

$$P_{r,n}^{\text{all}}(F) = \{f \in F[x_1, \ldots, x_r] \colon \deg f = n\}.$$

The polynomials of degree at most n form an F-vector space of dimension

$$b_{r,n} = \binom{r+n}{r} = \frac{(r+n)^{\underline{r}}}{r!},$$

where the *falling factorial* or *Pochhammer symbol* is

$$(r+x)^{\underline{r}} = (r+x) \cdot (r-1+x) \cdots (1+x), \tag{2.1}$$

for any real x and any nonnegative integer r, see e.g. Knuth (1992). Over a finite field $\mathbb{F}_q$ with q elements, we have

$$\#P_{r,n}^{\text{all}}(\mathbb{F}_q) = q^{b_{r,n}} - q^{b_{r,n-1}} = q^{b_{r,n}}(1 - q^{-b_{r-1,n}}).$$

The property of a certain polynomial to be reducible, squareful or relatively irreducible is shared with all polynomials associated to the given one. For counting them, it is sufficient to take one representative. We choose an arbitrary monomial order, say, the degree-lexicographic one, so that the monic polynomials are those with leading coefficient 1, and write

$$P_{r,n}(F) = \{f \in P_{r,n}^{\text{all}}(F) \colon f \text{ is monic}\}.$$

Then

$$\#P_{r,n}(\mathbb{F}_q) = \frac{\#P_{r,n}^{\text{all}}(\mathbb{F}_q)}{q-1} = q^{b_{r,n}-1} \frac{1 - q^{-b_{r-1,n}}}{1 - q^{-1}}. \tag{2.2}$$

The product of two monic polynomials is again monic.

Our exact formulas are derived using a generating series, the standard tool in analytic combinatorics as presented in Flajolet & Sedgewick (2009) by two experts who created large parts of the theory. We first recall a few general primitives from this theory that enable one to set up symbolic equations for generating functions starting from combinatorial specifications. A countable set $\mathcal{C}$ with a "size" function $|\cdot| \colon \mathcal{C} \to \mathbb{Z}_{\geq 0}$ is called a *combinatorial class* if the preimage of any $n \in \mathbb{Z}_{\geq 0}$ is finite. The number of elements of size n is denoted by C_n and these numbers are encoded in the *generating function* $\mathrm{C}(z)$ of the sequence C_n:

$$\mathrm{C}(z) = \sum_{n \geq 0} \mathrm{C}_n z^n \in \mathbb{Z}_{\geq 0} [\![z]\!].$$

We sometimes omit the argument z. Before we tackle the task of counting polynomials, let us recall some basics about power series. An element in the ring of univariate power series over a ring is invertible if and only if its constant term is invertible. We call a power series *original* if its constant term vanishes, so that its graph passes through the origin. The power series

$$\log(1-z) = -\sum_{n\geq 1} \frac{z^n}{n} \in \mathbb{Q}[\![z]\!] \tag{2.3}$$

is original and substituting a power series f in another power series g is well-defined if f is original.

Two combinatorial classes $\mathcal{A}$ and $\mathcal{B}$ are *isomorphic* if there is a size-preserving bijection $\mathcal{A} \to \mathcal{B}$ or equivalently if $\mathrm{A} = \mathrm{B}$. We recall three basic constructions of new combinatorial classes from given ones; see Flajolet & Sedgewick (2009, Section I. 2.).

Let $\mathcal{A}$ and $\mathcal{B}$ be two combinatorial classes. We define the *disjoint union*

$$\mathcal{A} \dot\cup \mathcal{B} = \{\{0\} \times \mathcal{A}\} \cup \{\{1\} \times \mathcal{B}\}.$$

The size of an element $(0, a)$ or $(1, b)$ is defined as the size of a or b, respectively. We also define the *sequence class*

$$\mathcal{SEQ}(\mathcal{A}) = \{(\alpha_1, \ldots, \alpha_\ell) \colon \ell \geq 0, \alpha_i \in \mathcal{A}\},$$

where $|(\alpha_1, \ldots, \alpha_\ell)| = \sum_i |\alpha_i|$. This is a combinatorial class, if $\mathcal{A}$ contains no element of size 0. Finally, we derive the *multiset class*

$$\mathcal{MSET}(\mathcal{A}) = \mathcal{SEQ}(\mathcal{A})/\!\sim,$$

where $(\alpha_1, \ldots, \alpha_\ell) \sim (\beta_1, \ldots, \beta_\ell)$ if there is a permutation σ of $\{1, \ldots, \ell\}$ such that $\alpha_i = \beta_{\sigma(i)}$ for all i. This class contains all finite sequences of elements from $\mathcal{A}$ where repetition is allowed, but ordering ignored. The generating functions for these constructions are classic applications of combinatorics.

Fact 2.4 (see Flajolet & Sedgewick (2009, Theorems I.1 and I.5))**.** *Let $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ be combinatorial classes.*

(i) If $\mathcal{A} = \mathcal{B} \dot\cup \mathcal{C}$, then $\mathrm{A} = \mathrm{B} + \mathrm{C}$.

(ii) If $\mathcal{A} = \mathcal{MSET}(\mathcal{B})$ and $\mathrm{B}_0 = 0$, then

$$\mathrm{B} = \sum_{k\geq 1} \frac{\mu(k)}{k} \log(\mathrm{A}(z^k)),$$

where μ is the number-theoretic Möbius-function, defined as

$$\mu(k) = \begin{cases} 1 & \text{if } k = 1, \\ (-1)^\ell & \text{if } k \text{ is the product of } \ell \text{ distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

3 Generating functions for reducible polynomials

To study reducible polynomials, we consider the following subsets of $P_{r,n}(F)$:

$$I_{r,n}(F) = \{f \in P_{r,n}(F) \colon f \text{ irreducible}\},$$
$$R_{r,n}(F) = P_{r,n}(F) \setminus I_{r,n}(F).$$

In the usual notions, the polynomial 1 is neither reducible nor irreducible. In our context, it is natural to have $R_{r,0}(F) = \{1\}$ and $I_{r,0}(F) = \varnothing$.

The sets of polynomials

$$\mathcal{P} = \bigcup_{n \geq 0} P_{r,n}(\mathbb{F}_q),$$
$$\mathcal{I} = \bigcup_{n \geq 0} I_{r,n}(\mathbb{F}_q),$$
$$\mathcal{R} = \mathcal{P} \setminus \mathcal{I},$$

are combinatorial classes with the total degree as size functions and we denote the corresponding generating functions by $\mathrm{P}, \mathrm{I}, \mathrm{R} \in \mathbb{Z}_{\geq 0}[\![z]\!]$, respectively. Their coefficients are

$$\mathrm{P}_n = \mathrm{P}_{r,n}(\mathbb{F}_q) = \#P_{r,n}(\mathbb{F}_q) = q^{b_{r,n}-1}\frac{1-q^{-b_{r-1,n}}}{1-q^{-1}}, \tag{3.1}$$
$$\mathrm{R}_n = \mathrm{R}_{r,n}(\mathbb{F}_q) = \#R_{r,n}(\mathbb{F}_q),$$
$$\mathrm{I}_n = \mathrm{I}_{r,n}(\mathbb{F}_q) = \#I_{r,n}(\mathbb{F}_q),$$

respectively, dropping $\mathbb{F}_q$ and r from the notation. By definition, $\mathcal{P}$ is isomorphic to the disjoint union of $\mathcal{R}$ and $\mathcal{I}$, and therefore

$$\mathrm{R} = \mathrm{P} - \mathrm{I} \tag{3.2}$$

by Fact 2.4 (i). By unique factorization, every element in $\mathcal{P}$ corresponds to an unordered finite sequence of irreducible polynomials, where repetition is allowed. Hence $\mathcal{P}$ is isomorphic to $\mathcal{MSET}(\mathcal{I})$ and by Fact 2.4 (ii),

$$\mathrm{I} = \sum_{k \geq 1} \frac{\mu(k)}{k} \log \mathrm{P}(z^k). \tag{3.3}$$

A Maple implementation of the resulting algorithm to compute the number of reducible polynomials is described in Figure 1. It is easy to program and execute and was used to calculate the number of bivariate reducible polynomials in von zur Gathen (2008, Table 2.1). We extend these exact results in Table 1.

This approach quickly leads to explicit formulas. For a positive integer n, a *composition* of n is a sequence $j = (j_1, j_2, \ldots, j_{|j|})$ of positive integers $j_1, j_2, \ldots, j_{|j|}$ with $j_1 + j_2 + \cdots + j_{|j|} = n$, where $|j|$ denotes the length of the sequence. We define the set

$$M_n = \{\text{compositions of } n\}. \tag{3.4}$$

This standard combinatorial notion is not to be confused with the composition of polynomials, for which also counting results are available.

n	$\#R_{3,n}(\mathbb{F}_q)$
1	0
2	$(q^6+2\,q^5+3\,q^4+3\,q^3+2\,q^2+q)/2$
3	$(3\,q^{12}+6\,q^{11}+9\,q^{10}+8\,q^9+6\,q^8+3\,q^7-q^6-3\,q^5-3\,q^4+q^2+q)/3$
4	$(4\,q^{22}+8\,q^{21}+12\,q^{20}+12\,q^{19}+14\,q^{18}+16\,q^{17}+18\,q^{16}+16\,q^{15}+10\,q^{14}-13\,q^{12}-20\,q^{11}-20\,q^{10}-10\,q^9-q^8+6\,q^7+7\,q^6+4\,q^5-2\,q^3-q^2)/4$
5	$(5\,q^{37}+10\,q^{36}+15\,q^{35}+15\,q^{34}+15\,q^{33}+15\,q^{32}+15\,q^{31}+15\,q^{30}+15\,q^{29}+20\,q^{28}+25\,q^{27}+30\,q^{26}+30\,q^{25}+25\,q^{24}+15\,q^{23}-15\,q^{21}-30\,q^{20}-45\,q^{19}-60\,q^{18}-65\,q^{17}-55\,q^{16}-26\,q^{15}+10\,q^{14}+40\,q^{13}+50\,q^{12}+40\,q^{11}+19\,q^{10}-10\,q^8-10\,q^7-5\,q^6-q^5+q^3+q^2+q)/5$
6	$(6\,q^{58}+12\,q^{57}+18\,q^{56}+18\,q^{55}+18\,q^{54}+18\,q^{53}+18\,q^{52}+18\,q^{51}+18\,q^{50}+18\,q^{49}+18\,q^{48}+18\,q^{47}+18\,q^{46}+18\,q^{45}+18\,q^{44}+24\,q^{43}+30\,q^{42}+36\,q^{41}+36\,q^{40}+30\,q^{39}+21\,q^{38}+6\,q^{37}-3\,q^{36}-6\,q^{35}-3\,q^{34}+3\,q^{32}-6\,q^{31}-27\,q^{30}-60\,q^{29}-99\,q^{28}-128\,q^{27}-141\,q^{26}-132\,q^{25}-104\,q^{24}-60\,q^{23}-3\,q^{22}+70\,q^{21}+144\,q^{20}+201\,q^{19}+203\,q^{18}+147\,q^{17}+51\,q^{16}-45\,q^{15}-102\,q^{14}-105\,q^{13}-71\,q^{12}-27\,q^{11}+3\,q^{10}+14\,q^9+11\,q^8+5\,q^7+3\,q^6+3\,q^5+2\,q^4-2\,q^3-2\,q^2-q)/6$

n	$\#R_{4,n}(\mathbb{F}_q)$
1	0
2	$(q^8+2\,q^7+3\,q^6+4\,q^5+4\,q^4+3\,q^3+2\,q^2+q)/2$
3	$(3\,q^{18}+6\,q^{17}+9\,q^{16}+12\,q^{15}+12\,q^{14}+12\,q^{13}+11\,q^{12}+9\,q^{11}+6\,q^{10}+2\,q^9-3\,q^8-6\,q^7-7\,q^6-6\,q^5-2\,q^4+q^2+q)/3$
4	$(4\,q^{38}+8\,q^{37}+12\,q^{36}+16\,q^{35}+16\,q^{34}+16\,q^{33}+16\,q^{32}+16\,q^{31}+16\,q^{30}+16\,q^{29}+18\,q^{28}+20\,q^{27}+22\,q^{26}+24\,q^{25}+26\,q^{24}+28\,q^{23}+26\,q^{22}+20\,q^{21}+10\,q^{20}-4\,q^{19}-22\,q^{18}-36\,q^{17}-45\,q^{16}-48\,q^{15}-42\,q^{14}-34\,q^{13}-21\,q^{12}-6\,q^{11}+8\,q^{10}+18\,q^9+20\,q^8+16\,q^7+9\,q^6+2\,q^5-2\,q^4-2\,q^3-q^2)/4$

n	$\#R_{5,n}(\mathbb{F}_q)$
1	0
2	$(q^{10}+2\,q^9+3\,q^8+4\,q^7+5\,q^6+5\,q^5+4\,q^4+3\,q^3+2\,q^2+q)/2$
3	$(3\,q^{25}+6\,q^{24}+9\,q^{23}+12\,q^{22}+15\,q^{21}+15\,q^{20}+15\,q^{19}+15\,q^{18}+15\,q^{17}+15\,q^{16}+14\,q^{15}+12\,q^{14}+9\,q^{13}+5\,q^{12}-6\,q^{10}-10\,q^9-12\,q^8-12\,q^7-10\,q^6-5\,q^5-2\,q^4+q^2+q)/3$
4	$(4\,q^{60}+8\,q^{59}+12\,q^{58}+16\,q^{57}+20\,q^{56}+20\,q^{55}+20\,q^{54}+20\,q^{53}+20\,q^{52}+20\,q^{51}+20\,q^{50}+20\,q^{49}+20\,q^{48}+20\,q^{47}+20\,q^{46}+20\,q^{45}+20\,q^{44}+20\,q^{43}+20\,q^{42}+20\,q^{41}+22\,q^{40}+24\,q^{39}+26\,q^{38}+28\,q^{37}+30\,q^{36}+32\,q^{35}+34\,q^{34}+36\,q^{33}+38\,q^{32}+40\,q^{31}+38\,q^{30}+32\,q^{29}+22\,q^{28}+8\,q^{27}-10\,q^{26}-32\,q^{25}-50\,q^{24}-64\,q^{23}-74\,q^{22}-80\,q^{21}-79\,q^{20}-78\,q^{19}-74\,q^{18}-66\,q^{17}-53\,q^{16}-34\,q^{15}-12\,q^{14}+10\,q^{13}+29\,q^{12}+42\,q^{11}+45\,q^{10}+40\,q^9+30\,q^8+18\,q^7+7\,q^6-2\,q^4-2\,q^3-q^2)/4$

Table 1: Exact values of $\#R_{r,n}(\mathbb{F}_q)$ for small values of r and n. For $n<4$, these are the numbers given in Theorem 3.14.

```
allpolysGF:=proc(z,N,r) local i: option remember:
    sum('simplify((q^binomial(r+i,r)-q^binomial(r+i-1,r))/
        (q-1))*z^i',i = 0..N):
end:

irreduciblesGF:=proc(z,N,r) local k: option remember:
    convert(taylor((sum('mobius(k)/k*log(allpolysGF(z^k,N,r))',
        k=1..N)), z, N+1), polynom):
end:

reduciblesGF:=proc(z,N,r) option remember:
    allpolysGF(z,N,r)-irreduciblesGF(z,N,r):
end:

reducibles:=proc(n,r)
coeff(sort(expand(reduciblesGF(z,n,r))),z^n):
end:
```

Figure 1: Maple program to compute the number of monic reducible polynomials in r variables of degree n.

Theorem 3.5. *For $r \geq 1$, $q \geq 2$, and P_n as in (3.1), we have*

$$\begin{aligned} \mathrm{I}_0 &= 0, \\ \mathrm{I}_n &= -\sum_{k \mid n} \frac{\mu(k)}{k} \sum_{j \in M_{n/k}} \frac{(-1)^{|j|}}{|j|} \mathrm{P}_{j_1} \mathrm{P}_{j_2} \cdots \mathrm{P}_{j_{|j|}}, \end{aligned}$$

for $n \geq 1$, and therefore

$$\begin{aligned} \mathrm{R}_0 &= 1, \\ \mathrm{R}_n &= \mathrm{P}_n + \sum_{k \mid n} \frac{\mu(k)}{k} \sum_{j \in M_{n/k}} \frac{(-1)^{|j|}}{|j|} \mathrm{P}_{j_1} \mathrm{P}_{j_2} \cdots \mathrm{P}_{j_{|j|}}, \end{aligned}$$

for $n \geq 1$.

Proof. We consider the original power series $\mathrm{F} = 1 - \mathsf{P} = -\sum_{i \geq 1} \mathrm{P}_i z^i$. The Taylor expansion (2.3) of $\log(1 - \mathrm{F}(z^k))$ in (3.3) yields

$$\begin{aligned} \mathrm{I} &= -\sum_{k \geq 1} \frac{\mu(k)}{k} \sum_{i \geq 1} \frac{\mathrm{F}(z^k)^i}{i} = -\sum_{k \geq 1} \frac{\mu(k)}{k} \sum_{i \geq 1} \frac{(-1)^i}{i} \Big(\sum_{j \geq 1} \mathrm{P}_j z^{jk} \Big)^i \\ &= -\sum_{k \geq 1} \frac{\mu(k)}{k} \sum_{i \geq 1} \frac{(-1)^i}{i} (\mathrm{P}_1 z^k + \mathrm{P}_2 z^{2k} + \mathrm{P}_3 z^{3k} + \dots)^i, \end{aligned}$$

$$\begin{aligned} \mathrm{I}_0 &= 0, \\ \mathrm{I}_n &= -\sum_{k \mid n} \frac{\mu(k)}{k} \sum_{i \geq 1} \frac{(-1)^i}{i} \sum_{\substack{j \in M_{n/k} \\ |j| = i}} \mathrm{P}_{j_1} \mathrm{P}_{j_2} \cdots \mathrm{P}_{j_i}, \end{aligned}$$

for $n \geq 1$, which proves the claimed formulas for I. The results for R follow by (3.2). □

We check that the formula yields the well-known one, see Lidl & Niederreiter (1997, Theorem 3.25), in the univariate case, where $r = 1$. We then have $\mathrm{P}_j = q^j$ and so $\mathrm{P}_{j_1}\mathrm{P}_{j_2}\cdots\mathrm{P}_{j_i} = q^{n/k}$ for any composition $j_1 + j_2 + \cdots + j_i = n/k$. Moreover, the number of compositions of m with i components is $\binom{m-1}{i-1}$, see Flajolet & Sedgewick (2009, Section I.3.1). As a consequence we have for k dividing n

$$\begin{aligned}\sum_{\substack{j\in M_{n/k}\\ |j|=i}} \frac{(-1)^i}{i}\mathrm{P}_{j_1}\mathrm{P}_{j_2}\cdots\mathrm{P}_{j_i} &= q^{n/k}\sum_{i\geq 1}\frac{(-1)^i}{i}\binom{n/k-1}{i-1}\\ &= \frac{kq^{n/k}}{n}\sum_{i\geq 1}(-1)^i\binom{n/k}{i} = -\frac{kq^{n/k}}{n},\\ \mathrm{I}_n &= \frac{1}{n}\sum_{k\,|\,n}\mu(k)q^{n/k}. \end{aligned} \tag{3.6}$$

Cohen (1968) notes that, compared to the univariate case, "the situation is different and much more difficult. In this case, no explicit formula [...] is available."

For $r \geq 2$, the power series P, I, and R do not converge anywhere except at 0, and the standard asymptotic arguments of analytic combinatorics are inapplicable. We now deviate from this approach and move from power series in $\mathbb{Q}[\![z]\!]$ to power series in $\mathbb{Q}(\mathbf{q})[\![z]\!]$, where $\mathbf{q}$ is a symbolic variable representing the field size. For $r \geq 2$ and $n \geq 0$ we let

$$\mathsf{P}_n(\mathbf{q}) = \mathsf{P}_{r,n}(\mathbf{q}) = \mathbf{q}^{b_{r,n}-1}\frac{1-\mathbf{q}^{-b_{r-1,n}}}{1-\mathbf{q}^{-1}} \in \mathbb{Z}[\mathbf{q}], \tag{3.7}$$

where we usually omit r from the notation. As examples, we have

$$\mathsf{P}_0(\mathbf{q}) = 1, \mathsf{P}_1(\mathbf{q}) = \mathbf{q}^r\frac{1-\mathbf{q}^{-r}}{1-\mathbf{q}^{-1}}, \text{ and } \mathsf{P}_2(\mathbf{q}) = \mathbf{q}^{r(r+3)/2}\frac{1-\mathbf{q}^{-r(r+1)/2}}{1-\mathbf{q}^{-1}}. \tag{3.8}$$

We define the power series $\mathsf{P}, \mathsf{I}, \mathsf{R} \in \mathbb{Q}(\mathbf{q})[\![z]\!]$ by

$$\mathsf{P}(\mathbf{q}, z) = \sum_{n\geq 0}\mathsf{P}_n(\mathbf{q})z^n, \tag{3.9}$$

$$\mathsf{I}(\mathbf{q}, z) = \sum_{k\geq 1}\frac{\mu(k)}{k}\log\mathsf{P}(\mathbf{q}, z^k), \tag{3.10}$$

$$\mathsf{R}(\mathbf{q}, z) = \mathsf{P}(\mathbf{q}, z) - \mathsf{I}(\mathbf{q}, z).$$

Now $1 - \mathsf{P}(\mathbf{q}, z^k)$ is an original power series, and $\log\mathsf{P}(\mathbf{q}, z^k)$ and I are well-defined, with $\mathsf{I}(\mathbf{q}, 0) = 0$. For $q \in \mathbb{Q}$, the rational functions in $\mathbb{Q}(\mathbf{q})$ without pole at $\mathbf{q} \leftarrow q$ form a ring, the localization $\mathbb{Q}[\mathbf{q}]_{(\mathbf{q}-q)}$. If we restrict the power series coefficients to this ring, the evaluation map which substitutes an integer q for $\mathbf{q}$ is a ring homomorphism. Since P_n is actually a polynomial in $\mathbf{q}$, this poses no

restriction in our case, and evaluating $\mathbf{q} \leftarrow q$ maps $\mathsf{P}(\mathbf{q}, z)$ to $\mathrm{P}(z)$ coefficientwise. In other words, the coefficient of z^n equals

$$[z^n]\mathsf{P}(q, z) = \mathrm{P}_n$$

by (2.2). Furthermore, I and R relate to P in the same way as I and R do to P, so that

$$[z^n]\mathsf{I}(q, z) = \mathrm{I}_n,$$
$$[z^n]\mathsf{R}(q, z) = \mathrm{R}_n.$$

The formula of Theorem 3.5 is exact but somewhat cumbersome. A main goal in this work is to find simple yet precise approximations, with rapidly decaying error terms. We fix some notation. For nonzero $f \in \mathbb{Q}(\mathbf{q})$, $\deg_{\mathbf{q}} f$ is the degree of f, that is, the numerator degree minus the denominator degree. Thus $\deg_{\mathbf{q}} \mathsf{P}_n = b_{r,n} - 1$ and $\deg_{\mathbf{q}}(f + g) \le \max\{\deg_{\mathbf{q}} f, \deg_{\mathbf{q}} g\}$. The appearance of $O(\mathbf{q}^{-m})$ with a positive integer m in an equation means the existence of some f with degree at most $-m$ that makes the equation valid. The charm of our approach is that we obtain results for any "fixed" r and n. If a term $O(\mathbf{q}^{-m})$ appears, then we may conclude a numerical asymptotic result for growing prime powers q.

We start with a degree comparison for certain products of the $\mathsf{P}_i(\mathbf{q})$ and sometimes omit the argument $\mathbf{q}$.

Lemma 3.11. *Let $r \ge 2$ and $n \ge 0$.*

(i) For $i, j \ge 0$, we have $\deg_{\mathbf{q}}(\mathsf{P}_i \cdot \mathsf{P}_j) \le \deg_{\mathbf{q}} \mathsf{P}_{i+j}$, with equality if and only if $ij = 0$.

(ii) For $1 \le k \le n/2$, the sequence of integers $\deg_{\mathbf{q}}(\mathsf{P}_k \cdot \mathsf{P}_{n-k})$ is strictly decreasing in k.

(iii) For $3 \le k \le n/2$, we have $\deg_{\mathbf{q}} \mathsf{P}_1^2 \mathsf{P}_{n-2} \ge \deg_{\mathbf{q}} \mathsf{P}_k \mathsf{P}_{n-k}$, with equality only for $(r, n, k) = (2, 6, 3)$.

Proof. (i) The claimed inequality is equivalent to

$$\binom{r+i}{r} + \binom{r+j}{r} - 1 \le \binom{r+i+j}{r},$$

which follows by considering the choices of r-element subsets from a set with $r + i + j$ elements. Since $r \ge 2$, this inequality is strict if and only if both i and j are nonzero.

(ii) Using (3.7), we define a function u as

$$u(k) = \deg_{\mathbf{q}}(\mathsf{P}_k \cdot \mathsf{P}_{n-k}) = \binom{r+k}{r} + \binom{r+n-k}{r} - 2. \tag{3.12}$$

We extend the domain of $u(k)$ to real numbers k between 1 and $n/2$ by means of falling factorials as in (2.1)

$$u(k) = \frac{(r+k)^{\underline{r}}}{r!} + \frac{(r+n-k)^{\underline{r}}}{r!} - 2.$$

It is sufficient to show that the affine transformation $\bar{u}$ with

$$\bar{u}(k) = r! \cdot (u(k) + 2) = (r+k)^{\underline{r}} + (r+n-k)^{\underline{r}}$$

is strictly decreasing. The first derivative with respect to k is

$$\bar{u}'(k) = \sum_{1 \le i \le r} \Big(\frac{(r+k)^{\underline{r}}}{i+k} - \frac{(r+n-k)^{\underline{r}}}{i+n-k} \Big).$$

Since $0 < i+k < i+n-k$ for $1 < k < n/2$, each difference is negative, and so is $\bar{u}'(k)$.

(iii) Since $r \ge 2$ we have

$$\begin{aligned} (r-2)(r-1)(r+5) &\ge 0, \\ b_{r-1,4} &\ge b_{r,3} - 2r - 1, \\ 2r + b_{r,4} - 1 &\ge 2b_{r,3} - 2, \\ \deg_{\mathbf{q}} \mathsf{P}_1^2 \mathsf{P}_4 &\ge \deg_{\mathbf{q}} \mathsf{P}_3 \mathsf{P}_3, \end{aligned} \tag{3.13}$$

and equality if and only if $r = 2$. This proves the claimed inequality for $n = 6$.

For $n > 6$ we have $b_{r-1,n-2} > b_{r-1,4}$ and with (3.13) follows

$$\begin{aligned} b_{r-1,n-2} &> b_{r,3} - 2r - 1, \\ 2r + b_{r,n-2} - 1 &> b_{r,3} + b_{r,n-3} - 2, \\ \deg_{\mathbf{q}} \mathsf{P}_1^2 \mathsf{P}_{n-2} &> \deg_{\mathbf{q}} \mathsf{P}_3 \mathsf{P}_{n-3}, \end{aligned}$$

which proves (iii) for $k = 3$ and by the monotonicity proven in (ii) also for all larger k. □

Theorem 3.14. *Let $r \ge 2$ and*

$$\rho_{r,n}(\mathbf{q}) = \mathbf{q}^{\binom{r+n-1}{r}+r-1} \frac{1-\mathbf{q}^{-r}}{(1-\mathbf{q}^{-1})^2} \in \mathbb{Q}(\mathbf{q}). \tag{3.15}$$

Then

$$\begin{aligned} \mathsf{R}_0 &= 1, \\ \mathsf{R}_1 &= 0, \\ \mathsf{R}_2 &= \frac{\rho_{r,2}(\mathbf{q})}{2} \cdot (1 - \mathbf{q}^{-r-1}), \\ \mathsf{R}_3 &= \rho_{r,3}(\mathbf{q}) \Big(1 - \mathbf{q}^{-r(r+1)/2} + \mathbf{q}^{-r(r-1)/2} \frac{1 - 2\mathbf{q}^{-r} + 2\mathbf{q}^{-2r-1} - \mathbf{q}^{-2r-2}}{3(1-\mathbf{q}^{-1})} \Big), \\ \mathsf{R}_4 &= \rho_{r,4}(\mathbf{q}) \cdot \Big(1 + \mathbf{q}^{-\binom{r+1}{3}} \cdot \frac{1 + O(\mathbf{q}^{-r(r-1)/2})}{2(1-\mathbf{q}^{-r})} \Big), \end{aligned} \tag{3.16}$$

and for $n \ge 5$

$$\mathsf{R}_n = \rho_{r,n}(\mathbf{q}) \cdot \Big(1 + \mathbf{q}^{-\binom{r+n-2}{r-1}+r(r+1)/2} \cdot \frac{1 + O(\mathbf{q}^{-r(r-1)/2})}{1-\mathbf{q}^{-r}} \Big). \tag{3.17}$$

Proof. We start the symbolic analog of our approach in the proof of Theorem 3.5 with the original power series $\mathsf{F} = 1 - \mathsf{P} = -\sum_{i\geq 1} \mathsf{P}_i z^i$. The Taylor expansion of $\log(1 - \mathsf{F}(z^k))$ in (3.10) yields

$$\mathsf{R} = \mathsf{P} - \mathsf{I} = 1 + \sum_{i\geq 2} \frac{\mathsf{F}^i}{i} + \sum_{k\geq 2} \frac{\mu(k)}{k} \sum_{i\geq 1} \frac{\mathsf{F}(z^k)^i}{i}. \tag{3.18}$$

Since $\mathsf{R}_n = [z^n]\mathsf{R}$, we find $\mathsf{R}_0 = 1$, $\mathsf{R}_1 = 0$, $\mathsf{R}_2 = (\mathsf{P}_1^2 + \mathsf{P}_1)/2$, and $\mathsf{R}_3 = \mathsf{P}_2\mathsf{P}_1 - (\mathsf{P}_1^3 - \mathsf{P}_1)/3$. Together with (3.8), these imply the claims for $n < 4$.

	i	summands	summands with largest degree in $\mathbf{q}$
$[z^n]\mathsf{F}^i$	2	$\mathsf{P}_j\mathsf{P}_{n-j}$, $1 \leq j \leq n/2$	$\mathsf{P}_1\mathsf{P}_{n-1}, \mathsf{P}_2\mathsf{P}_{n-2}$, $\mathsf{P}_3\mathsf{P}_{n-3}$ (for $n \geq 6$)
	≥ 3	$\mathsf{P}_{j_1}\mathsf{P}_{j_2}\cdots\mathsf{P}_{j_i}$, $1 \leq j_1 \leq j_2 \leq \cdots \leq j_i \leq n$, $j_1 + j_2 + \cdots + j_i = n$,	$\mathsf{P}_1^2\mathsf{P}_{n-2}$
$[z^n]\mathsf{F}(z^k)^i$	1	$\mathsf{P}_{n/k}$	$\mathsf{P}_{n/k}$
	≥ 2	$\mathsf{P}_{j_1}\mathsf{P}_{j_2}\cdots\mathsf{P}_{j_i}$, $1 \leq j_1 \leq j_2 \leq \cdots \leq j_i \leq n/k$, $j_1 + j_2 \cdots + j_i = n/k$,	$\mathsf{P}_1\mathsf{P}_{n/k-1}$

Table 2: Summands of R and bounds on their degrees in $\mathbf{q}$.

When $n \geq 4$, the contributions to $[z^n]\mathsf{R}$ from both sums in (3.18) are displayed in Table 2, distinguishing the smallest possible value for i from the remaining larger ones. The third column lists all summands. We first show that the last column displays the terms of largest degree in their row, and then compare the summands in the last column. The terms of $[z^n]\mathsf{F}^i$ are products of i factors

$$\mathsf{P}_{j_1}\mathsf{P}_{j_2}\cdots\mathsf{P}_{j_i}, \quad 1 \leq j_1 \leq j_2 \leq \cdots \leq j_i \leq n,$$

with $j_1 + j_2 + \cdots + j_i = n$. For $i = 2$, we find

$$\deg_{\mathbf{q}} \mathsf{P}_1\mathsf{P}_{n-1} > \deg_{\mathbf{q}} \mathsf{P}_2\mathsf{P}_{n-2} > \deg_{\mathbf{q}} \mathsf{P}_j\mathsf{P}_{n-j} \tag{3.19}$$

for all j with $3 \leq j \leq n/2$ by Lemma 3.11 (ii). For $i \geq 3$,

$$\deg_{\mathbf{q}} \mathsf{P}_1^2\mathsf{P}_{n-2} \geq \deg_{\mathbf{q}} \mathsf{P}_{j_1}\mathsf{P}_{j_2}\cdots\mathsf{P}_{j_i}$$

for all admissible values of $j_1, \ldots, j_i$ by repeated application of Lemma 3.11 (i) and a single instance of (ii). Let k divide n. Then $[z^n]\mathsf{F}(z^k) = -\mathsf{P}_{n/k}$ and $[z^n]\sum_{i\geq 2} \mathsf{F}(z^k)^i$ has degree $\deg_{\mathbf{q}} \mathsf{P}_1\mathsf{P}_{n/k-1}$ as shown above for $k = 1$.

We continue the comparison started in (3.19) by noting that $\deg_{\mathbf{q}} \mathsf{P}_2\mathsf{P}_{n-2} > \deg_{\mathbf{q}} \mathsf{P}_1^2\mathsf{P}_{n-2}$ by Lemma 3.11 (i), and also $\deg_{\mathbf{q}} \mathsf{P}_1^2\mathsf{P}_{n-2} \geq \deg_{\mathbf{q}} \mathsf{P}_j\mathsf{P}_{n-j}$ for all $3 \leq j \leq n/2$ with equality only for $(r, n, j) = (2, 6, 3)$ by Lemma 3.11 (iii). Furthermore, since $\deg_{\mathbf{q}} \mathsf{P}_1 \geq 1$, we have for $k \geq 2$

$$\deg_{\mathbf{q}} \mathsf{P}_1^2\mathsf{P}_{n-2} > \deg_{\mathbf{q}} \mathsf{P}_{n-2} \geq \deg_{\mathbf{q}} \mathsf{P}_{n/k} > \deg_{\mathbf{q}} \mathsf{P}_1\mathsf{P}_{n/k-1},$$

by Lemma 3.11 (i). Therefore, the summands of largest degree in $\mathbf{q}$ are in decreasing order $\mathsf{P}_1\mathsf{P}_{n-1}$, $\mathsf{P}_2\mathsf{P}_{n-2}$, and $\mathsf{P}_1^2\mathsf{P}_{n-2}$. For $n = 4$, this leads to

$$\begin{aligned}\mathsf{R}_4 &= \mathsf{P}_1\mathsf{P}_3 + \mathsf{P}_2^2/2 - \mathsf{P}_1^2\mathsf{P}_2(1 + O(\mathbf{q}^{-1})) \\ &= \mathsf{P}_1\mathsf{P}_3\bigg(1 + \frac{\mathsf{P}_2^2}{2\mathsf{P}_1\mathsf{P}_3} \cdot \Big(1 - \frac{\mathsf{P}_1^2}{\mathsf{P}_2} \cdot (1 + O(\mathbf{q}^{-1}))\Big)\bigg),\end{aligned}$$

while for $n \geq 5$, $(r,n) \neq (2,6)$ we have

$$\begin{aligned}\mathsf{R}_n &= \mathsf{P}_1\mathsf{P}_{n-1} + \mathsf{P}_2\mathsf{P}_{n-2} - \mathsf{P}_1^2\mathsf{P}_{n-2}(1+O(\mathbf{q}^{-1})) \\ &= \mathsf{P}_1\mathsf{P}_{n-1}\left(1 + \frac{\mathsf{P}_2\mathsf{P}_{n-2}}{\mathsf{P}_1\mathsf{P}_{n-1}} \cdot \left(1 - \frac{\mathsf{P}_1^2}{\mathsf{P}_2}(1+O(\mathbf{q}^{-1}))\right)\right). \qquad (3.20)\end{aligned}$$

For $(r,n) = (2,6)$, we have (3.20) with $(1/2 + O(\mathbf{q}^{-1}))$ instead of $(1+O(\mathbf{q}^{-1}))$.

The estimates (3.16) and (3.17) follow from

$$\begin{aligned}\mathsf{P}_1\mathsf{P}_{n-1} &= \rho_{r,n}(\mathbf{q})(1-q^{-b_{r-1,n-1}}), \\ \frac{\mathsf{P}_2\mathsf{P}_{n-2}}{\mathsf{P}_1\mathsf{P}_{n-1}} &= q^{-b_{r-1,n-1}+b_{r-1,2}}\frac{1+O(\mathbf{q}^{-r(r-1)/2})}{1-q^{-r}}, \text{ and} \\ \frac{\mathsf{P}_1^2}{\mathsf{P}_2} &= O(\mathbf{q}^{-r(r-1)/2}).\end{aligned}$$

□

Alekseyev (2006) lists $(\#I_{r,n}(\mathbb{F}_q))_{n\geq 0}$ as A115457–A115472 in The On-Line Encyclopedia of Integer Sequences, for $2 \leq r \leq 6$ and prime $q \leq 7$.

Bodin (2008, Theorem 7) states (in our notation)

$$1 - \frac{\#I_{r,n}}{\#P_{r,n}} \sim q^{-b_{r-1,n}-r}\frac{1-q^{-r}}{1-q^{-1}}.$$

Hou & Mullen (2009) provide results for $\#I_{r,n}(\mathbb{F}_q)$. These do not yield error bounds for the approximation of $\#R_{r,n}(\mathbb{F}_q)$. Bodin (2010) also uses (3.3). Without proving the required bounds on the various terms, as in Lemma 3.11, he claims a result similar to (3.17), but only for values of n that tend to infinity and with an unspecified multiplicative factor $O(1)$ in the place of our $(1+O(\mathbf{q}^{-r(r-1)/2}))/(1-\mathbf{q}^{-r})$ in the error term; the latter is independent of n.

Our approach can be described as follows. We start in the usual framework of algebraic combinatorics with a power series, $\mathrm{P} = \sum_{n\geq 0}\mathrm{P}_n z^n$ in our case, with well-known integer coefficients. Then we consider a well-defined series, $\mathrm{I} = \sum_{n\geq 0}\mathrm{I}_n z^n$ in our case, whose coefficients we want to determine. We find a description of P as $f(\mathrm{I})$ and turn this around to get $\mathrm{I} = g(\mathrm{P})$, usually by Möbius inversion. For convergent series, we can then apply powerful tools from calculus, such as singularity analysis, to analyze the asymptotic behavior of the coefficients.

Since our series are not convergent, we deviate from the standard approach. The coefficients P_n are rational functions of the field size q. We introduce a variable $\mathbf{q}$ and define a power series $\mathsf{P} \in \mathbb{Q}(\mathbf{q})[\![z]\!]$, whose coefficients are rational functions in a variable $\mathbf{q}$, such that $\mathsf{P}(q,z) = \mathrm{P}$. Then $g(\mathsf{P})$ is well-defined, and we set $\mathsf{I} = g(\mathsf{P}) \in \mathbb{Q}(\mathbf{q})[\![z]\!]$. Then $[z^n]\,\mathsf{I}(q,z) = \mathrm{I}_n$. We now estimate the degrees of the terms in $g(\mathsf{P})$. This yields $\mathsf{I} = h(\mathbf{q})(1+O(\mathbf{q}^{-m}))$, with a main contribution $h(\mathbf{q}) \in \mathbb{Q}(\mathbf{q})$ and a relative error $O(\mathbf{q}^{-m})$, which is an unspecified rational function of degree at most $-m$.

Overall, we first have to determine $\mathrm{P}, \mathrm{I}, f$, and g, which is often a substantial part of the labor in the standard framework. From then on, our derivation enjoys three advantages.

- No convergence of the power series is required.
- A clean concentration on the degrees of the various contributions, as embodied in Lemmas 3.11, 5.5, and 6.17.

- The degree of a sum of rational functions is bounded by the degree of the summands.

In the standard approach, the bound for a sum as in the third point has to be multiplied by the number of summands. As to the second point, one sometimes sees in the literature a simple claim of what the main contribution is, without argument. It is not clear whether this constitutes a mathematical proof in the usual sense. Since our series are not convergent, the first point is a definitive requirement.

4 Explicit bounds for reducible polynomials

We now describe a third approach to counting the reducible polynomials. The derivation is somewhat more involved. The payoff of this additional effort is an explicit relative error bound in Theorem 4.3. However, the calculations are sufficiently complicated for us to stop at the first error term. Thus we replace the asymptotic $1 + O(\mathbf{q}^{-r(r-1)/2})$ in Theorem 3.14 by $1/(1-q^{-1})$.

We consider, for integers $1 \leq k < n$, the sets

$$R_{r,n,k}(F) = \{g \cdot h \colon g \in P_{r,k}(F), h \in P_{r,n-k}(F)\} \subseteq P_{r,n}(F).$$

For the remainder of this section we restrict ourselves to finite fields $\mathbb{F}_q$, which we omit from the notation. Then

$$\#R_{r,n,k} \leq \#P_{r,k} \cdot \#P_{r,n-k} = q^{u(k)} \frac{(1-q^{-b_{r-1,k}})(1-q^{-b_{r-1,n-k}})}{(1-q^{-1})^2}, \tag{4.1}$$

with $u(k) = b_{r,k} + b_{r,n-k} - 2$ as in (3.12). The asymptotic behavior of this upper bound is dominated by the behavior of $u(k)$. Since $R_{r,n,k} = R_{r,n,n-k}$, we assume without loss of generality $k \leq n/2$. From Lemma 3.11 (ii), we know that, for any $r, n \geq 2$, $u(k)$ is strictly decreasing for $1 \leq k \leq n/2$. As $u(k)$ takes only integral values for integers k we conclude that

$$\sum_{2 \leq k \leq n/2} q^{u(k)} < q^{u(2)} \sum_{k \geq 0} q^{-k} = \frac{q^{u(2)}}{1-q^{-1}}. \tag{4.2}$$

Theorem 4.3. *Let $r, q \geq 2$, and $\rho_{r,n}$ as in Theorem 3.14. We have*

$$\begin{aligned}
\#R_{r,0}(\mathbb{F}_q) &= 1, \\
\#R_{r,1}(\mathbb{F}_q) &= 0, \\
\#R_{r,2}(\mathbb{F}_q) &= \frac{\rho_{r,2}(q)}{2} \cdot (1 - q^{-r-1}), \\
|\#R_{r,3}(\mathbb{F}_q) - \rho_{r,3}(q)| &= \rho_{r,3}(q) \cdot q^{-r(r-1)/2} \frac{1 - 2q^{-r} + 2q^{-2r-1} - q^{-2r-2}}{3(1-q^{-1})} \qquad (4.4) \\
&\leq \rho_{r,3}(q) \cdot q^{-r(r-1)/2},
\end{aligned}$$

and for $n \geq 4$

$$\begin{aligned}
|\#R_{r,n}(\mathbb{F}_q) - \rho_{r,n}(q)| &\leq \rho_{r,n}(q) \cdot \frac{q^{-\binom{r+n-2}{r-1} + r(r+1)/2}}{(1-q^{-1})(1-q^{-r})} \qquad (4.5) \\
&\leq \rho_{r,n}(q) \cdot 3q^{-\binom{r+n-2}{r-1} + r(r+1)/2}.
\end{aligned}$$

Proof. For $n < 4$, the claims follow from Theorem 3.14. We remark that the fraction on the right-hand side of (4.4) is actually bounded by $2/3$. For $n \geq 4$, the proof proceeds in three steps. We claim

$$\#R_{r,n} \leq \rho_{r,n}(q)\Big(1 + \frac{q^{-b_{r-1,n-1}+b_{r-1,2}}}{(1-q^{-1})(1-q^{-r})}\Big), \tag{4.6}$$

$$\#I_{r,n} \geq \#P_{r,n}\Big(1 - 3q^{-b_{r-1,n}+r}\frac{1-q^{-r}}{1-q^{-1}}\Big), \tag{4.7}$$

$$\#R_{r,n} \geq \rho_{r,n}(q)\Big(1 - 3q^{-b_{r-1,n-1}+r}\frac{1-q^{-r-1}}{1-q^{-1}}\Big). \tag{4.8}$$

We start with the proof of (4.6). Using $R_{r,n} = \bigcup_{1\leq k\leq n/2} R_{r,n,k}$ and inequality (4.1), we have

$$\begin{aligned}
\#R_{r,n} &\leq \sum_{1\leq k\leq n/2} \#R_{r,n,k} \\
&\leq \frac{1}{(1-q^{-1})^2} \sum_{1\leq k\leq n/2} q^{u(k)}(1-q^{-b_{r-1,k}})(1-q^{-b_{r-1,n-k}}) \\
&< \frac{1}{(1-q^{-1})^2} \sum_{1\leq k\leq n/2} q^{u(k)}(1-q^{-b_{r-1,k}}).
\end{aligned}$$

For the sum, (4.2) shows

$$\begin{aligned}
\sum_{1\leq k\leq n/2} q^{u(k)}(1-q^{-b_{r-1,k}}) &< q^{u(1)}(1-q^{-r}) + \sum_{2\leq k\leq n/2} q^{u(k)} \\
&< q^{u(1)}(1-q^{-r}) + \frac{q^{u(2)}}{1-q^{-1}} \\
&= q^{u(1)}(1-q^{-r})\Big(1 + \frac{q^{-u(1)+u(2)}}{(1-q^{-1})(1-q^{-r})}\Big).
\end{aligned} \tag{4.9}$$

Since $u(1) = b_{r,n-1} + r - 1$ and $-u(1) + u(2) = -b_{r-1,n-1} + b_{r-1,2}$, we conclude that

$$\begin{aligned}
\#R_{r,n} &\leq \frac{q^{b_{r,n-1}+r-1}(1-q^{-r})}{(1-q^{-1})^2}\Big(1 + \frac{q^{-b_{r-1,n-1}+b_{r-1,2}}}{(1-q^{-1})(1-q^{-r})}\Big) \\
&= \rho_{r,n}(q)\Big(1 + \frac{q^{-b_{r-1,n-1}+b_{r-1,2}}}{(1-q^{-1})(1-q^{-r})}\Big) \\
&< \rho_{r,n}(q)(1 + 3q^{-b_{r-1,n-1}+b_{r-1,2}}).
\end{aligned} \tag{4.10}$$

This proves (4.6) and we proceed with (4.7). Using (4.10), we have

$$\begin{aligned}
\#I_{r,n} &= \#P_{r,n} - \#R_{r,n} \\
&\geq \#P_{r,n}\Big(1 - \rho_{r,n}(q)\frac{1 + 3q^{-b_{r-1,n-1}+b_{r-1,2}}}{\#P_{r,n}}\Big) \\
&= \#P_{r,n}\Big(1 - q^{-b_{r-1,n}+r}\frac{(1 + 3q^{-b_{r-1,n-1}+b_{r-1,2}})(1-q^{-r})}{(1-q^{-1})(1-q^{-b_{r-1,n}})}\Big).
\end{aligned}$$

We observe that the exponent $-b_{r-1,n-1} + b_{r-1,2}$ is decreasing in r and n for $n \geq 4$. It is furthermore always negative and hence the fraction $(1 + 3q^{-b_{r-1,n-1}+b_{r-1,2}})/(1 - q^{-b_{r-1,n}})$ is also decreasing in q. Therefore it achieves its maximal value for $n = 4$, $r = 2$ and $q = 2$, yielding $80/31 < 3$ as upper bound and proving (4.7). For the last argument, we need (4.7) also for $n = 3$; this follows from Theorem 3.14.

We conclude with the proof of (4.8). The subset $\{g \cdot h \colon g \in P_{r,1}, h \in I_{r,n-1}\} \subset R_{r,n,k}$ has size $\#P_{r,1} \cdot \#I_{r,n-1}$. With (4.7), we find

$$\begin{aligned}
\#R_{r,n} &\geq \#P_{r,1} \cdot \#I_{r,n-1} \\
&\geq q^{b_{r,1}-1} \frac{1-q^{-r}}{1-q^{-1}} \cdot \#P_{r,n-1} \Big(1 - 3q^{-b_{r-1,n-1}+r} \frac{1-q^{-r}}{1-q^{-1}}\Big) \\
&= \rho_{r,n}(q)(1-q^{-b_{r-1,n-1}}) \Big(1 - 3q^{-b_{r-1,n-1}+r} \frac{1-q^{-r}}{1-q^{-1}}\Big) \\
&\geq \rho_{r,n}(q) \Big(1 - 3q^{-b_{r-1,n-1}+r} \frac{1-q^{-r-1}}{1-q^{-1}}\Big).
\end{aligned}$$

We combine the upper and lower bounds (4.6) and (4.8). The maximum of the bounds on the relative error term is

$$\max\Big(3q^{-r(r-1)/2}(1-q^{-r-1}), \frac{1}{1-q^{-r}}\Big) \cdot \frac{q^{-b_{r-1,n-1}+b_{r-1,2}}}{1-q^{-1}} = \frac{q^{-\binom{r+n-2}{r-1}+r(r+1)/2}}{(1-q^{-1})(1-q^{-r})}$$

and the observation $(1 - q^{-1})(1 - q^{-r}) \leq 8/3$ concludes the proof. □

The approach of this section also works, with minor modifications, for $n < 4$ and can provide a stand-alone proof of Theorem 4.3, without recourse to Theorem 3.14.

Figure 2 shows plots of $(\mathsf{R}_n(\mathbf{q}) - \rho_{r,n}(\mathbf{q}))/(\rho_{r,n}(\mathbf{q})\mathbf{q}^{-\binom{r+n-2}{r-1}+r(r+1)/2})$ for $r = 2$ and $n = 4, 5, 20$ as we substitute for $\mathbf{q}$ real numbers from 2 to 20. Theorem 4.3 says that the values are absolutely at most $1/((1 - \mathbf{q}^{-r})(1 - \mathbf{q}^{-1}))$. Theorem 3.14 indicates a bound of $1/2 + o(1)$ for $n = 4$ and $1 + o(1)$ for $n > 4$, but without explicit error estimate.

According to (4.5), the bound on the absolute value of the relative error for $n \geq 4$ is

$$\frac{q^{-b_{r-1,n-1}+b_{r-1,2}}}{(1-q^{-1})(1-q^{-r})}.$$

For $n > 4$, this is at most $2/3$. For $n = 4$, we can drop the factor $1 - q^{-1}$, since the sum in (4.9) consists only of a single summand and the estimate by a geometric sum is not necessary. This shows that also for $n = 4$, the relative error is at most $2/3$.

Remark 4.11. How close is our relative error estimate to being exponentially decaying in the input size? The usual dense representation of a polynomial in r variables and of degree n requires $b_{r,n} = \binom{r+n}{r}$ monomials, each of them equipped with a coefficient from $\mathbb{F}_q$, using about $\log_2 q$ bits. Thus the total input size is about $\log_2 q \cdot b_{r,n}$ bits. This differs from $\log_2 q \cdot (b_{r-1,n-1} - b_{r-1,2})$ by a factor of

$$\frac{b_{r,n}}{b_{r-1,n-1} - b_{r-1,2}} < \frac{b_{r,n}}{\frac{1}{2} b_{r-1,n-1}} = \frac{2(n+r)(n+r-1)}{nr}.$$

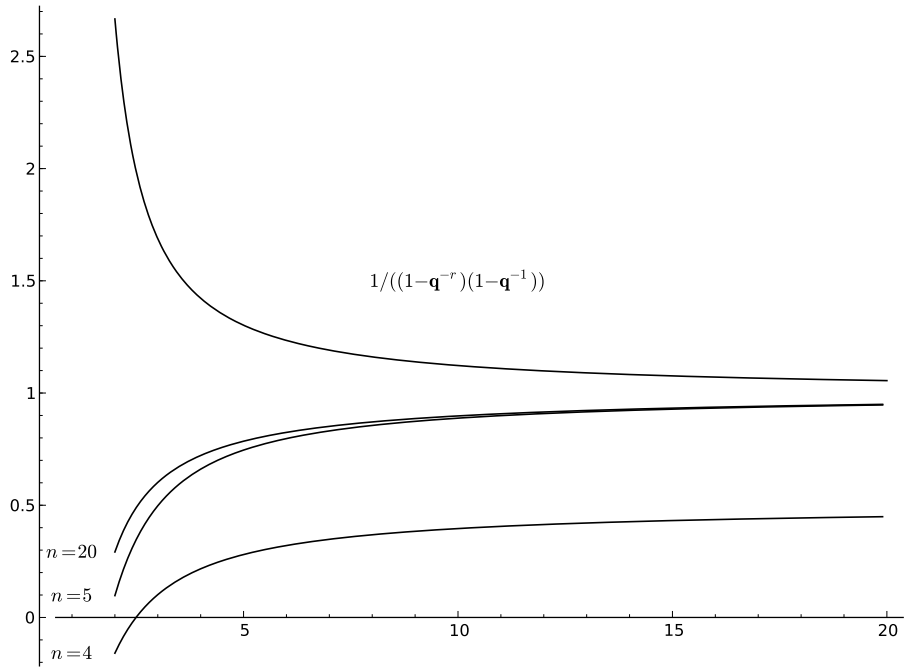

Figure 2: The normalized relative error in Theorem 3.14 for $r = 2$.

Up to this polynomial difference (in the exponent), the relative error is exponentially decaying in the bit size of the input, that is, $(\log q)$ times the number of coefficients in the usual dense representation. In particular, it is exponentially decaying in any of the parameters r, n, and $\log_2 q$, when the other two are fixed.

These bounds fit well into the picture described in Section 2 of von zur Gathen (2008) for $r = 2$. The family of functions described there approximates the quotient $\#R_{2,n}/\#P_{2,n}$ (using our notation). If we compare them to $\rho_{r,2}(q)/\#P_{2,n}$ we find that they differ only by the factor $1 - q^{-n-1}$, which tends to 1 as n and q increase. Our bound $3q^{-n+3}$ on the relative error for $r = 2$ and $n \geq 4$ is only slightly larger than the bound $2q^{-n+3}$ in Theorem 2.1(ii) of the paper cited.

The following provides some handy bounds.

Corollary 4.12. *For $r, q \geq 2$, and $n \geq 5$, we have*

$$\frac{1}{4}q^{\binom{r+n-1}{r}+r-1} \leq \#R_{r,n}(\mathbb{F}_q) \leq 6q^{\binom{r+n-1}{r}+r-1},$$
$$\frac{1}{4}q^{-\binom{r+n-1}{r-1}+r} \leq \frac{\#R_{r,n}(\mathbb{F}_q)}{\#P_{r,n}(\mathbb{F}_q)} \leq 3q^{-\binom{r+n-1}{r-1}+r}.$$

We conclude this section with bounds for the number of irreducible polynomials.

Corollary 4.13. *Let $r, q \geq 2$, and $\rho_{r,n}$ as in Theorem 3.14. We have*

$$\#P_{r,n}(\mathbb{F}_q) - 2\rho_{r,n}(q) \leq \#I_{r,n}(\mathbb{F}_q) \leq \#P_{r,n}(\mathbb{F}_q), \tag{4.14}$$

and more precisely

$$\#I_{r,1}(\mathbb{F}_q) = \#P_{r,1}(\mathbb{F}_q),$$
$$\#I_{r,2}(\mathbb{F}_q) = \#P_{r,2}(\mathbb{F}_q) - \frac{\rho_{r,2}(q)}{2} \cdot (1 - q^{-r-1}),$$
$$|\#I_{r,3}(\mathbb{F}_q) - (\#P_{r,3}(\mathbb{F}_q) - \rho_{r,3}(q))| \le \rho_{r,3}(q) \cdot q^{-(r-1)r/2},$$

and for $n \ge 4$

$$|\#I_{r,n}(\mathbb{F}_q) - (\#P_{r,n}(\mathbb{F}_q) - \rho_{r,n}(q))| \le \rho_{r,n}(q) \cdot 3q^{-\binom{r+n-2}{r-1}+r(r+1)/2}.$$

Proof. The more precise statements follow directly from Theorem 4.3 by application of $\#P_{r,n}(\mathbb{F}_q) = \#R_{r,n}(\mathbb{F}_q) + \#I_{r,n}(\mathbb{F}_q)$. These imply the first claim for $n < 4$. For $n \ge 4$, the relative error in (4.5) is at most $2/3 < 1$ as remarked after the proof of Theorem 4.3 and this concludes the proof of (4.14). □

5 Powerful polynomials

For an integer $s \ge 2$, a polynomial is called *s-powerful* if it is divisible by the sth power of some nonconstant polynomial, and *s-powerfree* otherwise; it is *squarefree* if $s = 2$. Let

$$Q_{r,n,s}(F) = \{f \in P_{r,n}(F) \colon f \text{ is } s\text{-powerful}\},$$
$$S_{r,n,s}(F) = P_{r,n}(F) \setminus Q_{r,n,s}(F).$$

As in the previous section, we restrict our attention to a finite field $F = \mathbb{F}_q$, which we omit from the notation.

For the approach by generating functions, we consider the combinatorial classes $\mathcal{Q} = \bigcup_{n\ge 0} Q_{r,n,s}$ and $\mathcal{S} = \mathcal{P} \setminus \mathcal{Q}$, where the explicit reference to r and s is omitted. Any monic polynomial f factors uniquely as $f = g \cdot h^s$ where g is a monic s-powerfree polynomial and h an arbitrary monic polynomial, hence

$$\mathrm{P} = \mathrm{S} \cdot \mathrm{P}(z^s) \tag{5.1}$$

and by definition $\mathrm{Q} = \mathrm{P} - \mathrm{S}$ for the generating functions of $\mathcal{S}$ and $\mathcal{Q}$, respectively. For univariate polynomials, Carlitz (1932) derives (5.1) directly from generating functions to prove the counting formula which we reproduce in (5.4). Flajolet, Gourdon & Panario (2001, Section 1.1) use (5.1) for $s = 2$ to count univariate squarefree polynomials, see also Flajolet & Sedgewick (2009, Note I.66). A corresponding Maple program to compute the coefficients of Q is shown in Figure 3. It was used to compute $\#Q_{2,n,2}(\mathbb{F}_q)$ for $n \le 6$ in von zur Gathen (2008, Table 3.1). We extend this in Table 3.

As in Theorem 3.5, this approach quickly leads to explicit formulas.

Theorem 5.2. *For* $r \ge 1$, $q, s \ge 2$, P_n *as in* (3.1), *and* M_n *as in* (3.4), *we have*

$$\mathrm{S}_n = \sum_{\substack{0\le i\le n/s \\ j\in M_i}} (-1)^{|j|} \mathrm{P}_{j_1}\mathrm{P}_{j_2}\cdots\mathrm{P}_{j_{|j|}}\mathrm{P}_{n-is},$$
$$\mathrm{Q}_n = -\sum_{\substack{1\le i\le n/s \\ j\in M_i}} (-1)^{|j|} \mathrm{P}_{j_1}\mathrm{P}_{j_2}\cdots\mathrm{P}_{j_{|j|}}\mathrm{P}_{n-is}. \tag{5.3}$$

```
spowerfreesGF:=proc(z,N,r,s) local i: option remember:
    convert(taylor(allpolysGF(z,N,r)/allpolysGF(z^s,N,r),
        z,N+1),polynom):
end:

spowerfulsGF:=proc(z,N,r,s) option remember:
    allpolysGF(z,N,r)-spowerfreesGF(z,N,r,s):
end:

spowerfuls:=proc(n,r,s)
    coeff(sort(expand(spowerfulsGF(z,n,r,s))),z^n):
end:
```

Figure 3: Maple program to compute the number of monic s-powerful polynomials in r variables of degree n.

n	$\#Q_{2,n,3}(\mathbb{F}_q)$
0, 1, 2	0
3	q^2+q
4	$q^4+2\,q^3+q^2$
5	$q^7+2\,q^6+2\,q^5+q^4$
6	$q^{11}+2\,q^{10}+2\,q^9+2\,q^8+q^7+q^5-q^3-q^2$
7	$q^{16}+2\,q^{15}+2\,q^{14}+2\,q^{13}+2\,q^{12}+q^{11}+q^7+q^6-q^5-2\,q^4-q^3$
8	$q^{22}+2\,q^{21}+2\,q^{20}+2\,q^{19}+2\,q^{18}+2\,q^{17}+q^{16}+q^{10}+q^9-2\,q^7-2\,q^6-q^5$
9	$q^{29}+2\,q^{28}+2\,q^{27}+2\,q^{26}+2\,q^{25}+2\,q^{24}+2\,q^{23}+q^{22}+q^{14}+q^{13}-q^{11}-2\,q^{10}-q^9-q^7-2\,q^6-q^5+q^4+q^3$

n	$\#Q_{3,n,2}(\mathbb{F}_q)$
0, 1	0
2	q^3+q^2+q
3	$q^6+2\,q^5+3\,q^4+2\,q^3+q^2$
4	$q^{12}+2\,q^{11}+3\,q^{10}+4\,q^9+4\,q^8+4\,q^7+2\,q^6-2\,q^4-2\,q^3-q^2$
5	$q^{22}+2\,q^{21}+3\,q^{20}+3\,q^{19}+3\,q^{18}+3\,q^{17}+3\,q^{16}+3\,q^{15}+3\,q^{14}+3\,q^{13}+3\,q^{12}+3\,q^{11}+3\,q^{10}+2\,q^9-3\,q^7-5\,q^6-5\,q^5-3\,q^4-q^3$
6	$q^{37}+2\,q^{36}+3\,q^{35}+3\,q^{34}+3\,q^{33}+3\,q^{32}+3\,q^{31}+3\,q^{30}+3\,q^{29}+3\,q^{28}+3\,q^{27}+3\,q^{26}+3\,q^{25}+3\,q^{24}+3\,q^{23}+2\,q^{22}+q^{21}+q^{19}+2\,q^{18}+3\,q^{17}+4\,q^{16}+4\,q^{15}+3\,q^{14}+q^{13}-4\,q^{12}-8\,q^{11}-11\,q^{10}-11\,q^9-8\,q^8-3\,q^7+2\,q^6+4\,q^5+3\,q^4+q^3$

n	$\#Q_{3,n,3}(\mathbb{F}_q)$
0, 1, 2	0
3	q^3+q^2+q
4	$q^6+2\,q^5+3\,q^4+2\,q^3+q^2$
5	$q^{12}+2\,q^{11}+3\,q^{10}+3\,q^9+3\,q^8+3\,q^7+2\,q^6+q^5$
6	$q^{22}+2\,q^{21}+3\,q^{20}+3\,q^{19}+3\,q^{18}+3\,q^{17}+3\,q^{16}+3\,q^{15}+3\,q^{14}+3\,q^{13}+2\,q^{12}+q^{11}+q^9+q^8+q^7-q^5-2\,q^4-2\,q^3-q^2$
7	$q^{37}+2\,q^{36}+3\,q^{35}+3\,q^{34}+3\,q^{33}+3\,q^{32}+3\,q^{31}+3\,q^{30}+3\,q^{29}+3\,q^{28}+3\,q^{27}+3\,q^{26}+3\,q^{25}+3\,q^{24}+3\,q^{23}+2\,q^{22}+q^{21}+q^{12}+2\,q^{11}+3\,q^{10}+2\,q^9-3\,q^7-5\,q^6-5\,q^5-3\,q^4-q^3$

Table 3: Exact values of $\#Q_{r,n,s}(\mathbb{F}_q)$ for small values of r, n, s.

Proof. We consider the original power series $\mathrm{F} = 1 - \mathrm{P} = -\sum_{i\geq 1} \mathrm{P}_i z^i$ and express (5.1) as

$$\begin{aligned}\mathrm{S} &= \mathrm{P} \cdot \sum_{i\geq 0} \mathrm{F}(z^s)^i \\ &= \sum_{k\geq 0} \mathrm{P}_k z^k \cdot \sum_{i\geq 0} \Big(-\sum_{j\geq 1} \mathrm{P}_j z^{js}\Big)^i.\end{aligned}$$

Comparison of coefficients provides us with

$$\mathrm{S}_n = \sum_{\substack{0\leq i\leq n/s \\ j\in M_i}} (-1)^{|j|} \mathrm{P}_{j_1} \mathrm{P}_{j_2} \cdots \mathrm{P}_{j_{|j|}} \mathrm{P}_{n-is},$$

and the claim for $\mathrm{Q}_n = \mathrm{P}_n - \mathrm{S}_n$ follows. □

For $r = 1$, we have $\mathrm{P}_j = q^j$ and for any composition $j_1 + j_2 + \cdots + j_k$ of i in (5.3)

$$\mathrm{P}_{j_1} \mathrm{P}_{j_2} \cdots \mathrm{P}_{j_k} \mathrm{P}_{n-is} = q^{n-(s-1)i}.$$

Moreover, since

$$\sum_{k\geq 1} (-1)^k \binom{i-1}{k-1} = -\binom{0}{i-1} = \begin{cases} -1 & \text{if } i = 1, \\ 0 & \text{if } i \geq 2, \end{cases}$$

see Graham, Knuth & Patashnik (1989, p. 167), we have in the univariate case

$$\mathrm{Q}_n = -\sum_{\substack{1\leq i\leq n/s \\ k\geq 1}} (-1)^k \binom{i-1}{k-1} q^{n-(s-1)i} = \begin{cases} 0 & \text{if } n < s, \\ q^{n-s+1} & \text{if } n \geq s, \end{cases} \tag{5.4}$$

as shown by Carlitz (1932, Section 6).

To study the asymptotic behavior of S_n and Q_n for $r \geq 2$ we again deviate from the standard approach and move to power series in $\mathbb{Q}(\mathbf{q})[\![z]\!]$. With P from (3.9), we define $\mathsf{S}, \mathsf{Q} \in \mathbb{Q}(\mathbf{q})[\![z]\!]$ by

$$\begin{aligned}\mathsf{P} &= \mathsf{S} \cdot \mathsf{P}(z^s), \\ \mathsf{Q} &= \mathsf{P} - \mathsf{S}.\end{aligned}$$

This is well-defined, since $\mathsf{P}(z^s)$ has constant term 1 and is therefore invertible. By construction, we have

$$\begin{aligned}\mathsf{S}_n(q) &= \#S_{r,n,s}(\mathbb{F}_q), \\ \mathsf{Q}_n(q) &= \#Q_{r,n,s}(\mathbb{F}_q).\end{aligned}$$

To study the asymptotic behavior, we examine $\mathsf{P}_k \cdot \mathsf{P}_{n-sk}$. Let

$$\begin{aligned}v_{r,n,s}(k) &= \deg_{\mathbf{q}}(\mathsf{P}_k \cdot \mathsf{P}_{n-sk}) \\ &= (r+k)^{\underline{r}}/r! + (r+n-sk)^{\underline{r}}/r! - 2\end{aligned}$$

and consider $v_{r,n,s}(k)$ as a function of a real variable k (Figure 4). In contrast to $u(k)$ from Section 3, this function is not monotone in k.

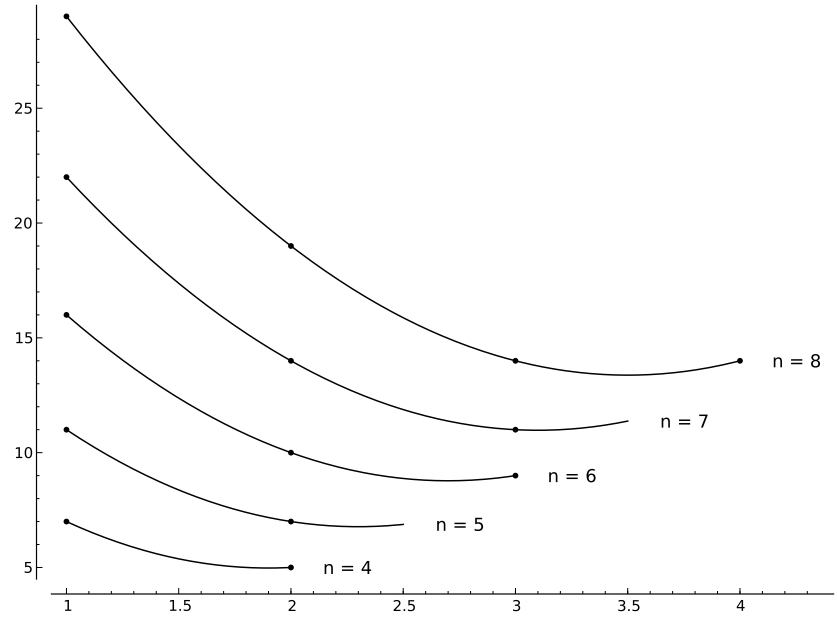

Figure 4: Graphs of $v_{2,n,2}(k)$ on $[1, n/2]$ as n runs from 4 to 8. The dots represent the values at integer arguments.

Lemma 5.5. *Let $r, n, s, q \geq 2$.*

(i) The function $v_{r,n,s}(k)$ is convex for $1 \leq k \leq n/s$.

(ii) For all integers k with $2 \leq k \leq n/s$, we have

$$v_{r,n,s}(1) > v_{r,n,s}(k).$$

(iii) For all integers k with $3 \leq k \leq n/s$, we have

$$v_{r,n,s}(2) > v_{r,n,s}(k) \qquad \text{if } (n,s) \neq (6,2).$$

Furthermore,

$$\begin{aligned} &v_{r,6,2}(2) < v_{r,6,2}(3) && \text{if } r \geq 3, \\ &v_{2,6,2}(2) = v_{2,6,2}(3) + 1. \end{aligned}$$

(iv) If $(n,s) \neq (6,2)$, then

$$\sum_{2 \leq k \leq n/s} q^{v_{r,n,s}(k)} \leq \frac{2q^{v_{r,n,s}(2)}}{1 - q^{-1}}.$$

Proof. We switch to the affine transformation

$$\begin{aligned} \bar{v}(k) &= r! \cdot \Big(v_{r,n,s}(k) + 2 \Big) \\ &= (r+k)^{\underline{r}} + (r+n-sk)^{\underline{r}}, \end{aligned}$$

which exhibits the same behavior as $v_{r,n,s}$ concerning convexity and maximality.

(i) We have

$$\bar{v}''(k) = \sum_{\substack{1\le i,j\le r\\ i\ne j}} \Big(\frac{(r+k)^{\underline{r}}}{(i+k)(j+k)} + \frac{s^2(r+n-sk)^{\underline{r}}}{(i+n-sk)(j+n-sk)} \Big) > 0.$$

(ii) For $n < 2s$, there is nothing to prove. For $n \ge 2s$, we find $n \ge s+2 \ge s+1+1/(s-1)$ and for all i

$$\begin{aligned} (i+n-s) - (i+n/s) &\ge 0,\\ (r+n-s)^{\underline{r}} - (r+n/s)^{\underline{r}} &\ge 0,\\ \bar{v}(1) - \bar{v}(n/s) = (r+1)! + (r+n-s)^{\underline{r}} - (r+n/s)^{\underline{r}} - r!&\\ = (r+n-s)^{\underline{r}} - (r+n/s)^{\underline{r}} + r\cdot r! > 0.& \end{aligned}$$

With the convexity of $\bar{v}$, this suffices.

(iii) Analogously to (ii), it is sufficient to prove $\bar{v}(2) > \bar{v}(n/s)$ for $(n,s) \ne (6,2)$. If $n \ge 2s^2/(s-1)$, then $n - 2s \ge n/s$, so that for all i

$$(i+n-2s) - (i+n/s) \ge 0$$

and hence

$$\begin{aligned} \bar{v}(2) - \bar{v}(n/s) &= (r+2)!/2 + (r+n-2s)^{\underline{r}} - (r+n/s)^{\underline{r}} - r!\\ &> (r+n-2s)^{\underline{r}} - (r+n/s)^{\underline{r}} \ge 0. \end{aligned}$$

If $n < 2s^2/(s-1)$, then $n/s < 3$ for $s \ge 3$ or $n < 6$ and there is nothing to prove. Finally, the three conditions $n < 2s^2/(s-1)$, $s = 2$, and $n \ge 6$ enforce $6 \le n < 8$, and we compute directly

$$v_{r,7,2}(2) - v_{r,7,2}(3) = \frac{1}{2} r(r+1) > 0,$$

$$v_{r,6,2}(2) - v_{r,6,2}(3) = -\frac{1}{6}(r-3)(r+1)(r+2) - 1 \begin{cases} = 1 & \text{if } r = 2,\\ < 0 & \text{if } r \ge 3. \end{cases}$$

(iv) The maximal value of the integer sequence $v_{r,n,s}(k)$ for $2 \le k \le n/s$ is $v_{r,n,s}(2)$ by (iii). Each value is taken at most twice, due to (i), and we can bound the sum by twice a geometric sum as

$$\sum_{2\le k\le n/s} q^{v_{r,n,s}(k)} \le 2q^{v_{r,n,s}(2)} \sum_{k\ge 0} q^{-k} = \frac{2q^{v_{r,n,s}(2)}}{1-q^{-1}}. \quad \square$$

The approach by generating functions now yields the following result. Its "general" case is (iv). We give exact expressions in special cases, namely for $n < 3s$ in (ii) and for $(n,s) = (6,2)$ in (iii), which also apply when we substitute the size q of a finite field $\mathbb{F}_q$ for $\mathbf{q}$.

Theorem 5.6. *Let $r, s \ge 2$, $n \ge 0$, and*

$$\eta_{r,n,s}(\mathbf{q}) = \mathbf{q}^{\binom{r+n-s}{r}+r-1} \frac{(1-\mathbf{q}^{-r})(1-\mathbf{q}^{-\binom{r+n-s-1}{r-1}})}{(1-\mathbf{q}^{-1})^2} \in \mathbb{Q}(\mathbf{q}),$$

$$\delta = \binom{r+n-s}{r} - \binom{r+n-2s}{r} - \frac{r(r+1)}{2}.$$

(i) If $n \ge 2s$, then $\delta \ge r$.

(ii)

$$\mathsf{Q}_n = \begin{cases} 0 & \text{for } n < s, \\ \eta_{r,n,s}(\mathbf{q}) & \text{for } s \le n < 2s, \\ \eta_{r,n,s}(\mathbf{q})\Big(1 + \mathbf{q}^{-\delta} \cdot \frac{1-\mathbf{q}^{-\binom{n+r-2s-1}{r-1}}}{1-\mathbf{q}^{-\binom{n+r-s-1}{r-1}}} & \\ \quad \cdot \Big(\frac{1-\mathbf{q}^{-r(r+1)/2}}{1-\mathbf{q}^{-r}} - \mathbf{q}^{-r(r-1)/2}\frac{1-\mathbf{q}^{-r}}{1-\mathbf{q}^{-1}}\Big)\Big) & \text{for } 2s \le n < 3s. \end{cases} \tag{5.7}$$

(iii) For $(n,s) = (6,2)$ and $r \ge 2$, we have

$$\begin{aligned} \mathsf{Q}_6 = \eta_{r,6,2}(\mathbf{q})\Big(1 + \mathbf{q}^{-\binom{r+3}{4}-r+1} \cdot \Big(\mathbf{q}^{-1}\frac{(1-\mathbf{q}^{-1})\big(1-\mathbf{q}^{-\binom{r+2}{3}}\big)}{(1-\mathbf{q}^{-r})\big(1-\mathbf{q}^{-\binom{r+3}{4}}\big)} \\ + \mathbf{q}^{-(r^3-7r+6)/6}\frac{(1-\mathbf{q}^{-r(r+1)/2})^2}{(1-\mathbf{q}^{-r})\big(1-\mathbf{q}^{-\binom{r+3}{4}}\big)} \\ - \mathbf{q}^{-(r^3+3r^2-10r+6)/6}\frac{(1-\mathbf{q}^{-r})(1-\mathbf{q}^{-r(r+1)/2})}{(1-\mathbf{q}^{-1})\big(1-\mathbf{q}^{-\binom{r+3}{4}}\big)} \\ - 2\mathbf{q}^{-(r^3+3r^2+4r-6)/6}\frac{1-\mathbf{q}^{-r(r+1)/2}}{1-\mathbf{q}^{-\binom{r+3}{4}}} \\ + \mathbf{q}^{-(r^3+6r^2-7r+6)/6}\frac{(1-\mathbf{q}^{-r})^2}{(1-\mathbf{q}^{-1})\big(1-\mathbf{q}^{-\binom{r+3}{4}}\big)}\Big)\Big) \\ = \eta_{r,6,2}(\mathbf{q})\big(1 + \mathbf{q}^{-\delta+(r-2)(r-1)(r+3)/6}(1+O(\mathbf{q}^{-1}))\big). \end{aligned} \tag{5.8}$$

(iv) For $n \ge 2s$ and $(n,s) \ne (6,2)$, we have

$$\mathsf{Q}_n = \eta_{r,n,s}(\mathbf{q})\big(1 + \mathbf{q}^{-\delta}(1+O(\mathbf{q}^{-1}))\big). \tag{5.9}$$

Proof. (i) If $n \ge 2s$, then

$$\delta \ge \binom{r+s}{r} - 1 - \frac{r(r+1)}{2} \ge \binom{r+2}{r} - 1 - \frac{r(r+1)}{2} = r.$$

(ii) The exact formulas of Theorem 5.2 yield

$$\begin{aligned} &\mathsf{Q}_n = 0 && \text{for } n < s, \\ &\mathsf{Q}_n = \mathsf{P}_1\mathsf{P}_{n-s} = \eta_{r,n,s}(\mathbf{q}) && \text{for } s \le n < 2s, \end{aligned}$$

and for $2s \le n < 3s$,

$$\begin{aligned} \mathsf{S}_n &= \mathsf{P}_n - \mathsf{P}_1\mathsf{P}_{n-s} - (\mathsf{P}_2 - \mathsf{P}_1^2)\mathsf{P}_{n-2s}, \\ \mathsf{Q}_n &= \mathsf{P}_1\mathsf{P}_{n-s} + (\mathsf{P}_2 - \mathsf{P}_1^2)\mathsf{P}_{n-2s} \\ &= \eta_{r,n,s}(\mathbf{q})\Big(1 + \frac{\mathsf{P}_2\mathsf{P}_{n-2s}}{\mathsf{P}_1\mathsf{P}_{n-s}}\Big(1 - \frac{\mathsf{P}_1^2}{\mathsf{P}_2}\Big)\Big) \\ &= \eta_{r,n,s}(\mathbf{q})\Big(1 + \mathbf{q}^{-\delta}\frac{1-\mathbf{q}^{-\binom{n+r-2s-1}{r-1}}}{1-\mathbf{q}^{-\binom{n+r-s-1}{r-1}}} \\ &\qquad \cdot \Big(\frac{1-\mathbf{q}^{-r(r+1)/2}}{1-\mathbf{q}^{-r}} - \mathbf{q}^{-r(r-1)/2}\frac{1-\mathbf{q}^{-r}}{1-\mathbf{q}^{-1}}\Big)\Big), \end{aligned} \tag{5.10}$$

where $\delta = -\deg_{\mathbf{q}}(\mathsf{P}_2\mathsf{P}_{n-2s}/(\mathsf{P}_1\mathsf{P}_{n-s}))$.

(iii) For $s=2$, we evaluate (5.3) for

$$\begin{aligned}
\mathsf{Q}_6 &= \mathsf{P}_1\mathsf{P}_4 + \mathsf{P}_3 + \mathsf{P}_2^2 - \mathsf{P}_1^2\mathsf{P}_2 - 2\mathsf{P}_1\mathsf{P}_2 + \mathsf{P}_1^3 \\
&= \eta_{r,6,2}(\mathbf{q})(1 + (\mathsf{P}_3 + \mathsf{P}_2^2 - \mathsf{P}_1^2\mathsf{P}_2 - 2\mathsf{P}_1\mathsf{P}_2 + \mathsf{P}_1^3)/(\mathsf{P}_1\mathsf{P}_4)) \\
&= \eta_{r,6,2}(\mathbf{q})\Big(1 + \mathbf{q}^{-v_{r,6,2}(1)+v_{r,6,2}(3)+1} \\
&\quad \cdot \Big(\mathbf{q}^{-1}\tfrac{(1-\mathbf{q}^{-1})(1-\mathbf{q}^{-b_{r-1,3}})}{(1-\mathbf{q}^{-r})(1-\mathbf{q}^{-b_{r-1,4}})} \qquad (5.11) \\
&\quad + \mathbf{q}^{-(r^3-7r+6)/6}\tfrac{(1-\mathbf{q}^{-r(r+1)/2})^2}{(1-\mathbf{q}^{-r})(1-\mathbf{q}^{-b_{r-1,4}})} \\
&\quad - \mathbf{q}^{-(r^3+3r^2-10r+6)/6}\tfrac{(1-\mathbf{q}^{-r})(1-\mathbf{q}^{-r(r+1)/2})}{(1-\mathbf{q}^{-1})(1-\mathbf{q}^{-b_{r-1,4}})} \\
&\quad - 2\mathbf{q}^{-(r^3+3r^2+4r-6)/6}\tfrac{1-\mathbf{q}^{-r(r+1)/2}}{1-\mathbf{q}^{-b_{r-1,4}}} \\
&\quad + \mathbf{q}^{-(r^3+6r^2-7r+6)/6}\tfrac{(1-\mathbf{q}^{-r})^2}{(1-\mathbf{q}^{-1})(1-\mathbf{q}^{-b_{r-1,4}})}\Big)\Big) \qquad (5.12) \\
&= \eta_{r,6,2}(\mathbf{q})\big(1 + \mathbf{q}^{-\delta+(r-2)(r-1)(r+3)/6}(1+O(\mathbf{q}^{-1}))\big), \qquad (5.13)
\end{aligned}$$

since the sum (5.11)–(5.12) has nonpositive degree in $\mathbf{q}$ and $-v_{r,6,2}(1) + v_{r,6,2}(3) + 1 = -\binom{r+3}{4} - r + 1 = -\delta + (r-2)(r-1)(r+3)/6$.

(iv) Finally, for $n \geq 2s$ and $(n,s) \neq (6,2)$, we claim

$$\mathsf{S}_n = \mathsf{P}_n - \mathsf{P}_1\mathsf{P}_{n-s} - \mathsf{P}_2\mathsf{P}_{n-2s}(1+O(\mathbf{q}^{-1})). \qquad (5.14)$$

This implies immediately

$$\begin{aligned}
\mathsf{S}_n &= \mathsf{P}_n - \mathsf{P}_1\mathsf{P}_{n-s}(1+O(\mathbf{q}^{-1})) \\
&= \mathsf{P}_n(1+O(\mathbf{q}^{-1})),
\end{aligned} \qquad (5.15)$$

by Lemmas 5.5 (ii) and 3.11 (i), respectively. We already have (5.14) for $2s \leq n < 3s$ from (5.10) by Lemma 3.11 (i). We also have (5.15) for $(n,s) = (6,2)$ from (5.13). This is enough to obtain inductively

$$\begin{aligned}
\mathsf{S}_n &= \mathsf{P}_n - \sum_{1\leq i\leq n/s} \mathsf{S}_{n-is}\mathsf{P}_i \\
&= \mathsf{P}_n - \mathsf{P}_1\mathsf{S}_{n-s} - \sum_{2\leq i\leq n/s} \mathsf{P}_i\mathsf{S}_{n-is} \\
&= \mathsf{P}_n - \mathsf{P}_1\big(\mathsf{P}_{n-s} - \mathsf{P}_1\mathsf{P}_{n-2s}(1+O(\mathbf{q}^{-1}))\big) - \sum_{2\leq i\leq n/s} \mathsf{P}_i\mathsf{P}_{n-is}(1+O(\mathbf{q}^{-1})) \\
&= \mathsf{P}_n - \mathsf{P}_1\mathsf{P}_{n-s} + \mathsf{P}_1^2\mathsf{P}_{n-2s}(1+O(\mathbf{q}^{-1})) - \mathsf{P}_2\mathsf{P}_{n-2s}(1+O(\mathbf{q}^{-1})) \\
&= \mathsf{P}_n - \mathsf{P}_1\mathsf{P}_{n-s} - \mathsf{P}_2\mathsf{P}_{n-2s}(1+O(\mathbf{q}^{-1})),
\end{aligned}$$

using Lemma 5.5 (iii) for $(n,s) \neq (6,2)$ and Lemma 3.11 (i). We conclude with

$$\begin{aligned}
\mathsf{Q}_n &= \mathsf{P}_1\mathsf{P}_{n-s} + \mathsf{P}_2\mathsf{P}_{n-2s}(1+O(\mathbf{q}^{-1})) \\
&= \eta_{r,n,s}(\mathbf{q})(1 + \mathbf{q}^{-\delta}(1+O(\mathbf{q}^{-1})))
\end{aligned}$$

by the definition of $\eta_{r,n,s}(\mathbf{q}) = \mathsf{P}_1\mathsf{P}_{n-s}$ and $\delta = -\deg_{\mathbf{q}}(\mathsf{P}_2\mathsf{P}_{n-2s}/(\mathsf{P}_1\mathsf{P}_{n-s}))$, respectively. □

For $r \geq 3$, we can replace $1 + O(\mathbf{q}^{-1})$ in (5.8) by $\mathbf{q}^{-1} + O(\mathbf{q}^{-2})$.

In the following, the combinatorial approach replaces the asymptotic $1 + O(\mathbf{q}^{-1})$ of (5.9) with an explicit bound of 6 in (5.19). We consider for integers $1 \leq k \leq n/s$ the sets

$$Q_{r,n,s,k}(F) = \{g \cdot h^s \colon g \in P_{r,n-sk}, h \in P_{r,k}\} \in P_{r,n}(F)$$

and have

$$Q_{r,n,s}(F) = \bigcup_{1 \leq k \leq n/s} Q_{r,n,s,k}(F). \tag{5.16}$$

For $n < 3s$ the exact formula (5.7) of Theorem 5.6 (ii) applies. We provide explicit bounds for $n \geq 3s$.

Theorem 5.17. *Let $r, s, q \geq 2$, $n \geq 0$, and*

$$\eta_{r,n,s}(\mathbf{q}) = \mathbf{q}^{\binom{r+n-s}{r}+r-1} \frac{(1-\mathbf{q}^{-r})\big(1-\mathbf{q}^{-\binom{r+n-s-1}{r-1}}\big)}{(1-\mathbf{q}^{-1})^2} \in \mathbb{Q}(\mathbf{q}),$$
$$\delta = \binom{r+n-s}{r} - \binom{r+n-2s}{r} - \frac{r(r+1)}{2}$$

as in Theorem 5.6.

(i) For $(n,s) = (6,2)$, we have $\delta = r(r+1)(r^2+9r+2)/24$ and

$$|\#Q_{r,6,2}(\mathbb{F}_q) - \eta_{r,6,2}(q)| \leq \eta_{r,6,2}(q) \cdot 2q^{-\delta+(r-2)(r-1)(r+3)/6}. \tag{5.18}$$

(ii) For $n \geq 3s$ and $(n,s) \neq (6,2)$, we have

$$|\#Q_{r,n,s}(\mathbb{F}_q) - \eta_{r,n,s}(q)| \leq \eta_{r,n,s}(q) \cdot 6q^{-\delta}. \tag{5.19}$$

Proof. We omit the argument $\mathbb{F}_q$ from the notation. Considering only the positive and negative summands of (5.12), respectively, we find

$$\begin{aligned} \#Q_{r,6,2} &\leq \eta_{r,6,2}(q)(1 + 2q^{-\delta+(r-2)(r-1)(r+3)/6}), \\ \#Q_{r,6,2} &\geq \eta_{r,6,2}(q)(1 - q^{-\delta+(r-2)(r-1)(r+3)/6}), \end{aligned} \tag{5.20}$$

which proves (i).

For the general case (ii), we claim

$$\#Q_{r,n,s} \leq \eta_{r,n,s}(q)\Big(1 + \frac{16}{3}q^{-\delta}\Big) \qquad \text{for } (n,s) \neq (6,2), \tag{5.21}$$

$$\#Q_{r,n,s} \geq \eta_{r,n,s}(q)\Big(1 - \frac{7}{2}q^{-\delta-r(r-1)/2}\Big) \qquad \text{for } n \geq 3s. \tag{5.22}$$

For (5.21), we find from (5.16)

$$\begin{aligned}
\#Q_{r,n,s} &\le \sum_{1\le k\le n/s} \#Q_{r,n,s,k} \le \sum_{1\le k\le n/s} \#P_{r,n-sk}\cdot\#P_{r,k} \\
&= \sum_{1\le k\le n/s} q^{v_{r,n,s}(k)}\frac{(1-q^{-b_{r-1,n-sk}})(1-q^{-b_{r-1,k}})}{(1-q^{-1})^2} \\
&= \eta_{r,n,s}(q)\Big(1+q^{-v_{r,n,s}(1)}\cdot\sum_{2\le k\le n/s} q^{v_{r,n,s}(k)}\frac{(1-q^{-b_{r-1,k}})(1-q^{-b_{r-1,n-sk}})}{(1-q^{-r})(1-q^{-b_{r-1,n-s}})}\Big) \\
&\le \eta_{r,n,s}(q)\Big(1+q^{-v_{r,n,s}(1)}\cdot\sum_{2\le k\le n/s} q^{v_{r,n,s}(k)}\frac{(1-q^{-b_{r-1,k}})}{(1-q^{-r})}\Big) \\
&\le \eta_{r,n,s}(q)\Big(1+\frac{2q^{-v_{r,n,s}(1)+v_{r,n,s}(2)}}{(1-q^{-r})(1-q^{-1})}\Big) \le \eta_{r,n,s}(q)\Big(1+\frac{16}{3}q^{-\delta}\Big),
\end{aligned}$$

using the bound of Lemma 5.5 (iv).

To prove (5.22), we observe that $Q_{r,n,s,1}$ contains an injective image of $(P_{r,n-s}\setminus Q_{r,n-s,s})\times I_{r,1}$ by $(g,h)\mapsto g\cdot h^s$. For $n\ge 3s$, we get from $I_{r,1}=P_{r,1}$

$$\begin{aligned}
\#Q_{r,n,s} &\ge \#Q_{r,n,s,1} \\
&\ge \#I_{r,1}\cdot\#(P_{r,n-s}\setminus Q_{r,n-s,s}) \\
&\ge \#P_{r,1}\cdot(\#P_{r,n-s}-\#Q_{r,n-s,s}) \\
&\ge \eta_{r,n,s}(q)\cdot\Big(1-\frac{\eta_{r,n-s,s}(q)(1+\frac{16}{3}q^{-r})}{\#P_{r,n-s}}\Big) \\
&\ge \eta_{r,n,s}(q)\cdot\Big(1-q^{b_{r,n-2s}-b_{r,n-s}+r}\frac{(1-q^{-r})(1-q^{-b_{r-1,n-2s}})(1+\frac{16}{3}q^{-r})}{(1-q^{-1})(1-q^{-b_{r-1,n-s}})}\Big) \qquad (5.23)\\
&\ge \eta_{r,n,s}(q)\Big(1-\frac{7}{2}q^{-\delta-r(r-1)/2}\Big),
\end{aligned}$$

if $(n,s)\ne(8,2)$ using (5.21) for $Q_{r,n-s,s}$ with exponent $\delta\ge r$ by Theorem 5.6 (i).

If $(n,s)=(8,2)$, we modify (5.23) according to (5.20) and get

$$\begin{aligned}
\#Q_{r,8,2} &\ge \eta_{r,8,2}(q)\Big(1-\frac{3}{2}\big(1+2q^{-\binom{r+3}{4}-r+1}\big)q^{-\delta-r(r-1)/2}\Big) \\
&\ge \eta_{r,8,2}(q)(1-2q^{-\delta-r(r-1)/2}).
\end{aligned}$$

Combining (5.21) and (5.22) proves (ii). □

We note that for $(n,s)=(6,2)$, inequality (5.19) follows from (5.18) if $r=2$ and is false for sufficiently large q if $r\ge 3$.

Figure 5 shows plots of $(\mathsf{Q}_{r,n,s}(\mathbf{q})-\eta_{r,n,s}(\mathbf{q}))/(\eta_{r,n,s}(\mathbf{q})\mathbf{q}^{-\delta})$ for $r=2$, $s=2$ and $n=4,6,10$, as we substitute for $\mathbf{q}$ real numbers from 2 to 20.

Remark 5.24. As noted in Remark 4.11 for reducible polynomials, the relative error term is (essentially) exponentially decreasing in the input size, and exponentially decaying in any of the parameters r, n, s, and $\log_2 q$, when the other three are fixed.

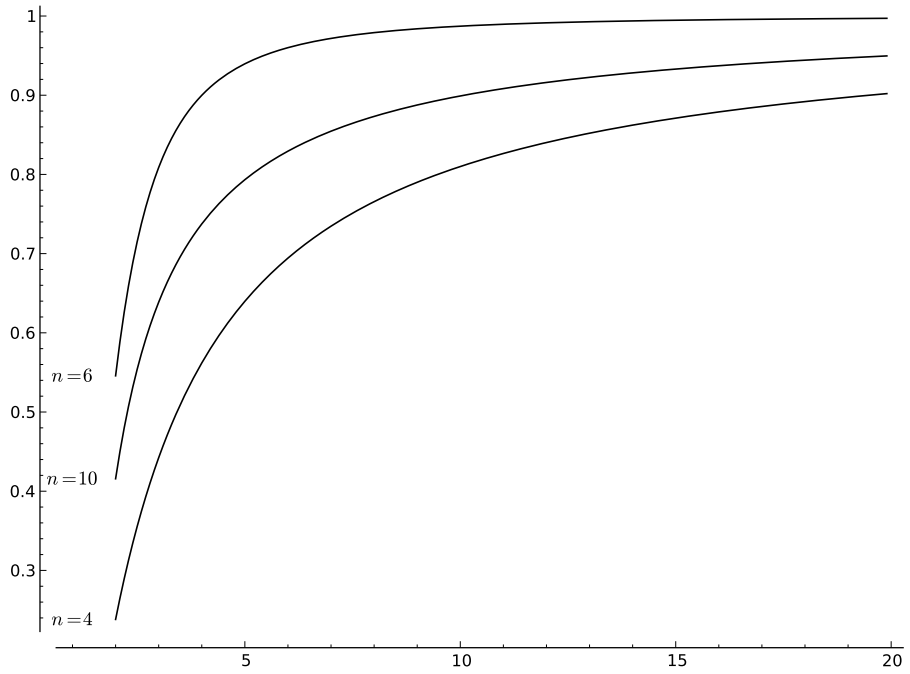

Figure 5: The normalized relative error in Theorem 5.6 (iii)–(iv) for $(r, s) = (2, 2)$.

In the bivariate case, von zur Gathen (2008, Theorem 3.1) approximates the quotient $\#Q_{2,n,s}(\mathbb{F}_q)/\#P_{2,n}(\mathbb{F}_q)$ (using our notation) by

$$q^{-(2ns-s^2+3s-4)/2}\frac{(1+q^{-1})(1-q^{-n+s-1})}{1-q^{-n-1}},$$

which equals the term $\eta_{2,n,s}(q)/\#P_{2,n}(\mathbb{F}_q)$ derived from our analysis above.

We append handy bounds using Corollary 4.12.

Corollary 5.25. *For $r, s, q \geq 2$, and $n \geq s$, we have*

$$\begin{aligned}
\frac{1}{2}q^{\binom{r+n-s}{r}+r-1} &\leq \#Q_{r,n,s}(\mathbb{F}_q) \leq 10q^{\binom{r+n-s}{r}+r-1},\\
\frac{1}{2}q^{-\binom{r+n}{r}+\binom{r+n-s}{r}+r} &\leq \frac{\#Q_{r,n,s}(\mathbb{F}_q)}{\#P_{r,n}(\mathbb{F}_q)} \leq 5q^{-\binom{r+n}{r}+\binom{r+n-s}{r}+r},\\
\frac{1}{6}q^{-\binom{r+n-1}{r}+\binom{r+n-s}{r}} &\leq \frac{\#Q_{r,n,s}(\mathbb{F}_q)}{\#R_{r,n}(\mathbb{F}_q)} \leq 19q^{-\binom{r+n-1}{r}+\binom{r+n-s}{r}}.
\end{aligned}$$

We conclude this section with bounds for the number of s-powerfree polynomials.

Corollary 5.26. *Let $r, s, q \geq 2$, $n \geq 0$, and $\eta_{r,n,s}$ and δ as in Theorem 5.6. We have*

$$\#P_{r,n}(\mathbb{F}_q) - 3\eta_{r,n,s}(q) \leq \#S_{r,n,s}(\mathbb{F}_q) \leq \#P_{r,n}(\mathbb{F}_q),$$

and more precisely

$$\#S_{r,n,s}(\mathbb{F}_q) = \begin{cases} \#P_{r,n}(\mathbb{F}_q) & \text{for } n < s, \\ \#P_{r,n}(\mathbb{F}_q) - \eta_{r,n,s}(q) & \text{for } s \le n < 2s, \\ \#P_{r,n}(\mathbb{F}_q) - \eta_{r,n,s}(q)\Bigg(1 + q^{-\delta} \cdot \frac{1-q^{-\binom{n+r-2s-1}{r-1}}}{1-q^{-\binom{n+r-s-1}{r-1}}} & \\ \quad \cdot \Big(\frac{1-q^{-r(r+1)/2}}{1-q^{-r}} - q^{-r(r-1)/2}\frac{1-q^{-r}}{1-q^{-1}}\Big)\Bigg) & \text{for } 2s \le n < 3s, \end{cases}$$

$$|\#S_{r,6,2}(\mathbb{F}_q) - (\#P_{r,n}(\mathbb{F}_q) - \eta_{r,6,2}(q))| \le \eta_{r,6,2}(q) \cdot 2q^{-\delta+(r-2)(r-1)(r+3)/6},$$

and for $n \ge 3s$ *with* $(n,s) \ne (6,2)$

$$|\#S_{r,n,s}(\mathbb{F}_q) - (\#P_{r,n}(\mathbb{F}_q) - \eta_{r,n,s}(q))| \le \eta_{r,n,s}(q) \cdot 6q^{-\delta}.$$

6 Relatively irreducible polynomials

A polynomial over F is *absolutely irreducible* if it is irreducible over an algebraic closure of F, and *relatively irreducible* if it is irreducible over F but factors over some extension field of F. We define

$$\begin{aligned} A_{r,n}(F) &= \{f \in P_{r,n}(F) \colon f \text{ is absolutely irreducible}\} \subseteq I_{r,n}(F), \\ E_{r,n}(F) &= I_{r,n}(F) \setminus A_{r,n}(F). \end{aligned} \tag{6.1}$$

As before, we restrict ourselves to finite fields and recall that all our polynomials are monic. For a field extension $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ of degree k, we consider the Galois group $G_k = \mathrm{Gal}(\mathbb{F}_{q^k} : \mathbb{F}_q) \cong \mathbb{Z}_k$. It acts on $\mathbb{F}_{q^k}[x]$ coefficientwise and we have the "norm" map

$$\begin{aligned} \varphi_{r,n,k} \colon P_{r,n/k}(\mathbb{F}_{q^k}) &\to P_{r,n}(\mathbb{F}_q), \\ g &\mapsto \prod_{\sigma \in G_k} g^\sigma, \end{aligned}$$

for each k dividing n. Since $(\varphi_{r,n,k}(g))^\tau = \varphi_{r,n,k}(g)$ for any $\tau \in G_k$ and therefore $\varphi_{r,n,k}(g) \in P_{r,n}(\mathbb{F}_q)$, this map is well-defined.

Relatively irreducible polynomials in $P_{r,n}(\mathbb{F}_q)$ are the product of all conjugates of an irreducible polynomial g defined over some extension field $\mathbb{F}_{q^k}$. If g itself is relatively irreducible over $\mathbb{F}_{q^k}$, then there exists an appropriate multiple j of k and $h \in P_{r,n/j}(\mathbb{F}_{q^j})$ with the same image $\varphi_{r,n,k}(g) = \varphi_{r,n,j}(h)$ in $P_{r,n}(\mathbb{F}_q)$ and the property that h is absolutely irreducible. So, every relatively irreducible polynomial is contained in $\varphi_{r,n,k}(A_{r,n/k}(\mathbb{F}_{q^k}))$ for a unique $k > 1$ dividing n. Furthermore, the absolutely irreducible polynomials in $P_{r,n}(\mathbb{F}_q)$ are exactly those in $\varphi_{r,n,1}(A_{r,n}(\mathbb{F}_q))$, and we summarize

$$A_{r,n}(\mathbb{F}_q) = \varphi_{r,n,1}(A_{r,n}(\mathbb{F}_q)), \tag{6.2}$$

$$E_{r,n}(\mathbb{F}_q) \subseteq \bigcup_{1<k \,|\, n} \varphi_{r,n,k}(A_{r,n/k}(\mathbb{F}_{q^k})). \tag{6.3}$$

In order to replace the latter by an equality, we let

$$A^+_{r,n/k}(\mathbb{F}_{q^k}) = A_{r,n/k}(\mathbb{F}_{q^k}) \setminus \bigcup_{s \,|\, k,\, s \ne k} A_{r,n/k}(\mathbb{F}_{q^s}) \tag{6.4}$$

be the set of absolutely irreducible polynomials over $\mathbb{F}_{q^k}$ that are not defined over a proper subfield containing $\mathbb{F}_q$, and

$$I_{r,n,k}(\mathbb{F}_q) = \varphi_{r,n,k}(A^+_{r,n/k}(\mathbb{F}_{q^k})).$$

Lemma 6.5. *(i) We have the disjoint union*

$$I_{r,n}(\mathbb{F}_q) = \dot{\bigcup_{k \mid n}} I_{r,n,k}(\mathbb{F}_q) \tag{6.6}$$

and more precisely

$$A_{r,n}(\mathbb{F}_q) = I_{r,n,1}(\mathbb{F}_q), \tag{6.7}$$

$$E_{r,n}(\mathbb{F}_q) = \dot{\bigcup_{1<k \mid n}} I_{r,n,k}(\mathbb{F}_q). \tag{6.8}$$

(ii) $$\#I_{r,n,k}(\mathbb{F}_q) = \tfrac{1}{k}\#A^+_{r,n/k}(\mathbb{F}_{q^k}).$$

Proof. (i) Let $g \in A_{r,n/k}(\mathbb{F}_{q^k})$. By definition, g is monic. The k conjugates g^σ, for $\sigma \in G_k$, are pairwise non-associate if and only if the coefficients are not contained in some proper subfield of $\mathbb{F}_{q^k}$. This shows

$$I_{r,n,k}(\mathbb{F}_q) \subseteq I_{r,n}(\mathbb{F}_q). \tag{6.9}$$

Let $f \in I_{r,n}(\mathbb{F}_q)$. Then $f = \varphi_{r,n,k}(g)$ for some $g \in A_{r,n/k}(\mathbb{F}_{q^k})$, with k dividing n as observed in (6.3). If g has coefficients from a subfield of $\mathbb{F}_{q^k}$, say $g \in A_{r,n/k}(\mathbb{F}_{q^s})$ for some $s < k$ dividing k, then g^σ equals g for some $\sigma \in G_k \setminus \{\mathrm{id}\}$. Taking the smallest such s and

$$h = \prod_{\tau \in G_s} g^\tau \in I_{r,n,k/s}(\mathbb{F}_q),$$

we have $h^{k/s} = \varphi_{r,n,k}(g)$. Hence $\varphi_{r,n,k}(g)$ is a (k/s)-th power and therefore reducible, in contradiction to the choice of f. This shows that $g \in A^+_{r,n/k}(\mathbb{F}_{q^k})$ and a fortiori

$$I_{r,n}(\mathbb{F}_q) \subseteq \bigcup_{k \mid n} I_{r,n,k}(\mathbb{F}_q).$$

The disjointness follows from the fact that the factorization of $\varphi_{r,n,k}(g)$ for any $g \in A^+_{r,n/k}(\mathbb{F}_{q^k})$ has exactly k irreducible factors over $\mathbb{F}_{q^n}$, and (6.6) follows with (6.9).

Finally, (6.7) and (6.8) follow from (6.2) and (6.1), respectively.

(ii) Let $g, h \in I_{r,n/k}(\mathbb{F}_{q^k})$. Then $\varphi_{r,n,k}(g) = \varphi_{r,n,k}(h)$ if and only if $h = g^\sigma$ for some automorphism $\sigma \in G_k$. Sufficiency is a direct computation and necessity follows from the unique factorization of $\varphi_{r,n,k}(g)$ and $\varphi_{r,n,k}(h)$ over $\mathbb{F}_{q^k}$. Therefore, the size of each fibre of $\varphi_{r,n,k}$ on $A^+_{r,n/k}(\mathbb{F}_{q^k})$ is $\#G_k = k$. □

```
absirreds:=proc(n,r) local k,s: option remember:
    add(1/k*add(mobius(s)*subs(q=q^s,coeff(irreduciblesGF(
        z,n/k,r),z^(n/k))),s=divisors(k)),k=divisors(n))
end:

absirredsGF:=proc(z,N,r) local k,s: option remember:
    sum('absirreds(k,r)*z^k',k=1..N)
end:

relirredsGF:=proc(z,N,r) option remember:
    irreduciblesGF(z,N,r)-absirredsGF(z,N,r);
end:

relirreds:=proc(n,r)
    coeff(sort(expand(relirredsGF(z,n,r))),z^n):
end:
```

Figure 6: Maple program to compute the number of relatively irreducible polynomials in r variables of degree n.

We omit the parameter r from the notation of the generating functions and their coefficients. The generating function $\mathrm{A}^+(\mathbb{F}_{q^k})$ of $\#A^+_{r,n}(\mathbb{F}_{q^k})$ is related to the generating function $\mathrm{A}(\mathbb{F}_q)$ of $\#A_{r,n}(\mathbb{F}_q)$ by definition (6.4) and we find by inclusion-exclusion

$$\mathrm{A}^+(\mathbb{F}_{q^k}) = \sum_{s \mid k} \mu(k/s)\mathrm{A}(\mathbb{F}_{q^s}).$$

With (6.6) and Lemma 6.5 (ii), we relate this to the generating function $\mathrm{I}(\mathbb{F}_q)$ of irreducible polynomials as introduced in Section 3 and obtain

$$\begin{aligned}[z^n]\mathrm{I}(\mathbb{F}_q) &= \sum_{k \mid n} \frac{1}{k} \sum_{s \mid k} \mu(k/s) \cdot [z^{n/k}]\mathrm{A}(\mathbb{F}_{q^s}),\\ [z^n]\mathrm{A}(\mathbb{F}_q) &= \sum_{k \mid n} \frac{1}{k} \sum_{s \mid k} \mu(s) \cdot [z^{n/k}]\mathrm{I}(\mathbb{F}_{q^s}) \qquad (6.10)\end{aligned}$$

with Möbius inversion.

A Maple program to compute the latter is shown in Figure 6. Exact values for $\#E_{2,n}(\mathbb{F}_q)$ with $n \leq 6$ are given in von zur Gathen (2008, Table 4.1). We extend this in Table 4.

For an explicit formula, we combine the expression for $\mathrm{I}_n(\mathbb{F}_q) = \mathrm{I}_n$ from Theorem 3.5 with (6.10).

Theorem 6.11. *For $r, n \geq 1$, $q \geq 2$, M_n as in (3.4), and $\mathrm{P}_n(\mathbb{F}_q) = \mathrm{P}_n$ as in (3.1), we have*

$$\mathrm{A}_0(\mathbb{F}_q) = 0,$$

$$\mathrm{A}_n(\mathbb{F}_q) = -\sum_{s \mid k \mid n} \frac{\mu(s)}{k} \sum_{m \mid n/k} \frac{\mu(m)}{m} \sum_{j \in M_{n/(km)}} \frac{(-1)^{|j|}}{|j|} \mathrm{P}_{j_1}(\mathbb{F}_{q^s})\mathrm{P}_{j_2}(\mathbb{F}_{q^s}) \cdots \mathrm{P}_{j_{|j|}}(\mathbb{F}_{q^s}),$$

n	$\#E_{2,n}(\mathbb{F}_q)$
1	0
2	$(q^4-q)/2$
3	$(q^6+q^3-q^2-q)/3$
4	$(2\,q^{10}+q^8-2\,q^5-2\,q^4+q^2)/4$
5	$(q^{10}+q^5-q^2-q)/5$
6	$(3\,q^{18}+3\,q^{16}+2\,q^{15}-2\,q^{12}-3\,q^{10}-3\,q^9-3\,q^8+q^6+q^5-q^4-q^3+2\,q^2+q)/6$
7	$(q^{14}+q^7-q^2-q)/7$
8	$(4\,q^{28}+4\,q^{26}+4\,q^{24}-6\,q^{20}-8\,q^{18}-3\,q^{16}-4\,q^{13}+6\,q^{10}+8\,q^9+2\,q^8-4\,q^7-4\,q^6+q^4)/8$

n	$\#E_{3,n}(\mathbb{F}_q)$
1	0
2	$(q^6+q^4-q^3-q)/2$
3	$(q^9+q^6-q^2-q)/3$
4	$(2\,q^{18}+2\,q^{16}+2\,q^{14}+q^{12}-2\,q^9-3\,q^8-2\,q^7-3\,q^6+2\,q^3+q^2)/4$
5	$(q^{15}+q^{10}+q^5-q^3-q^2-q)/5$
6	$(3\,q^{38}+3\,q^{36}+3\,q^{34}+3\,q^{32}+3\,q^{30}+3\,q^{28}+2\,q^{27}+3\,q^{26}+2\,q^{24}-3\,q^{22}+2\,q^{21}-6\,q^{20}-3\,q^{19}-11\,q^{18}-3\,q^{17}-9\,q^{16}-3\,q^{15}-6\,q^{14}-3\,q^{13}-q^{12}+3\,q^{11}+9\,q^{10}+4\,q^9+7\,q^8+q^7-3\,q^6-3\,q^5-2\,q^4+2\,q^3+2\,q^2+q)/6$
7	$(q^{21}+q^{14}+q^7-q^3-q^2-q)/7$

n	$\#E_{4,n}(\mathbb{F}_q)$
1	0
2	$(q^8+q^6-q^3-q)/2$
3	$(q^{12}+q^9+q^6-q^4-q^2-q)/3$
4	$(2\,q^{28}+2\,q^{26}+2\,q^{24}+2\,q^{22}+2\,q^{20}+2\,q^{18}+q^{16}-2\,q^{14}-2\,q^{13}-3\,q^{12}-2\,q^{11}-4\,q^{10}-2\,q^9-4\,q^8-q^6+2\,q^5+2\,q^4+2\,q^3+q^2)/4$
5	$(q^{20}+q^{15}+q^{10}+q^5-q^4-q^3-q^2-q)/5$
6	$(3\,q^{68}+3\,q^{66}+3\,q^{64}+3\,q^{62}+3\,q^{60}+3\,q^{58}+3\,q^{56}+3\,q^{54}+3\,q^{52}+3\,q^{50}+3\,q^{48}+3\,q^{46}+3\,q^{44}+5\,q^{42}+3\,q^{40}+2\,q^{39}+3\,q^{38}+2\,q^{36}-6\,q^{34}-q^{33}-9\,q^{32}-3\,q^{31}-10\,q^{30}-3\,q^{29}-15\,q^{28}-q^{27}-15\,q^{26}-3\,q^{25}-14\,q^{24}-3\,q^{23}-12\,q^{22}-3\,q^{21}-9\,q^{20}-3\,q^{19}-4\,q^{18}+3\,q^{17}+9\,q^{16}+7\,q^{15}+16\,q^{14}+10\,q^{13}+12\,q^{12}+7\,q^{11}+10\,q^{10}-2\,q^9-q^8-6\,q^7-7\,q^6-4\,q^5+q^4+2\,q^3+2\,q^2+q)/6$

Table 4: Exact values of $\#E_{r,n}(\mathbb{F}_q)$ for small values of r and n.

$$
\begin{aligned}
&\mathrm{E}_0(\mathbb{F}_q) = 0,\\
&\mathrm{E}_n(\mathbb{F}_q) = -\sum_{1<k\,|\,n} \frac{1}{k} \sum_{s\,|\,k} \mu(s) \mathrm{I}_{n/k}(\mathbb{F}_{q^s}) \qquad (6.12)\\
&\qquad = \sum_{1<k\,|\,n} \frac{1}{k} \sum_{\substack{s\,|\,k\\ m\,|\,n/k}} \frac{\mu(s)\mu(m)}{m} \sum_{j\in M_{n/(km)}} \frac{(-1)^{|j|}}{|j|} \mathrm{P}_{j_1}(\mathbb{F}_{q^s}) \mathrm{P}_{j_2}(\mathbb{F}_{q^s}) \cdots \mathrm{P}_{j_{|j|}}(\mathbb{F}_{q^s}).
\end{aligned}
$$

We check that for $r = 1$ we obtain the expected result

$$
\mathrm{A}_n(\mathbb{F}_q) = \begin{cases} q & \text{if } n = 1,\\ 0 & \text{if } n > 1. \end{cases}
$$

To this end, we use the well-known fact that

$$
\sum_{s\,|\,n} \mu(s) = \begin{cases} 1 & \text{if } n = 1,\\ 0 & \text{if } n > 1. \end{cases}
$$

From (6.13) and (3.6) we have

$$
\begin{aligned}
n\mathrm{A}_n(\mathbb{F}_q) &= \sum_{\substack{s\,|\,k\,|\,n\\ t\,|\,n/k}} \mu(s)\mu(t) q^{\frac{ns}{kt}} = \sum_{\substack{s\,|\,k\,|\,n\\ a\,|\,n/k}} \mu(s)\mu(n/(ka)) q^{sa}\\
&= \sum_{m\,|\,n} q^m \sum_{\substack{s\,|\,k\,|\,n\\ m=sa,\, a\,|\,n/k}} \mu(s)\mu(n/(ka)) = \sum_{m\,|\,n} q^m \sum_{s\,|\,m} \mu(s) \sum_{\substack{s\,|\,k\,|\,n\\ m/s\,|\,n/k}} \mu(ns/(mk))\\
&= \sum_{m\,|\,n} q^m \sum_{s\,|\,m} \mu(s) \sum_{j\,|\,n/m} \mu(n/(mj))\\
&= \sum_{m\,|\,n} q^m \sum_{s\,|\,m} \mu(s) \sum_{i\,|\,n/m} \mu(i) = \begin{cases} q & \text{if } n = 1,\\ 0 & \text{if } n > 1, \end{cases}
\end{aligned}
$$

where $a = n/(kt)$, $m = as$, $j = k/s$, and $i = n/(mj)$.

The remainder of this section deals with the case $r \geq 2$. For the approach by symbolic generating functions, we define, with $\mathsf{I}(\mathbf{q}, z)$ as in (3.10), the two power series $\mathsf{A}, \mathsf{E} \in \mathbb{Q}(\mathbf{q})\,[\![z]\!]$ by

$$
\begin{aligned}
\mathsf{A}_0(\mathbf{q}) &= \mathsf{I}_0(\mathbf{q}) = 0,\\
\mathsf{A}_n(\mathbf{q}) &= \sum_{k\,|\,n} \frac{1}{k} \sum_{s\,|\,k} \mu(s) \mathsf{I}_{n/k}(\mathbf{q}^s) \in \mathbb{Z}[\mathbf{q}] \text{ for } n > 0, \qquad (6.13)\\
\mathsf{A}(\mathbf{q}, z) &= \sum_{n\geq 0} \mathsf{A}_n(\mathbf{q}) z^n \in \mathbb{Z}[\mathbf{q}]\,[\![z]\!]\,,\\
\mathsf{E}(\mathbf{q}, z) &= \mathsf{I}(\mathbf{q}, z) - \mathsf{A}(\mathbf{q}, z)\\
&= -\sum_{1<k\,|\,n} \frac{1}{k} \sum_{s\,|\,k} \mu(s) \mathsf{I}_{n/k}(\mathbf{q}^s) \in \mathbb{Z}[\mathbf{q}]\,[\![z]\!]\,. \qquad (6.14)
\end{aligned}
$$

summand	$\deg_{\mathbf{q}}$
$\mathsf{P}_{n/\ell}(\mathbf{q}^\ell)$	$\ell(b_{r,n/\ell}-1) = w_{r,n}(\ell)$
$\mathsf{R}_{n/\ell}(\mathbf{q}^\ell)$	$\ell(b_{r,n/\ell-1}+r-1) = w_{r,n}(\ell) - \ell(b_{r-1,n/\ell}-r)$
$\mathsf{I}_{n/\ell}(\mathbf{q})$	$b_{r,n/\ell}-1 = \frac{1}{\ell}w_{r,n}(\ell)$
$\sum_{\ell<k\,\mid\,n}\mathsf{I}_{n/k}(\mathbf{q}^k)$	$\le \max_{\ell<k\,\mid\,n} w_{r,n}(k)$

Table 5: Summands of E and their degrees in $\mathbf{q}$.

Then

$$\mathsf{A}_n(q) = \#A_{r,n}(\mathbb{F}_q),$$
$$\mathsf{E}_n(q) = \#E_{r,n}(\mathbb{F}_q).$$

The inner sum of (6.14) has degree $\deg_{\mathbf{q}}\mathsf{I}_{n/k}(\mathbf{q}^k)$ in $\mathbf{q}$. Let n be composite and ℓ its smallest prime divisor. For $k=\ell$, this inner sum consists of only two terms and we find

$$\begin{aligned}\mathsf{E}_n(\mathbf{q}) &= \frac{1}{\ell}(\mathsf{I}_{n/\ell}(\mathbf{q}^\ell) - \mathsf{I}_{n/\ell}(\mathbf{q})) - \sum_{\ell<k\,\mid\,n}\frac{1}{k}\sum_{s\mid k}\mu(s)\mathsf{I}_{n/k}(\mathbf{q}^s)\\ &= \frac{1}{\ell}(\mathsf{P}_{n/\ell}(\mathbf{q}^\ell) - \mathsf{R}_{n/\ell}(\mathbf{q}^\ell) - \mathsf{I}_{n/\ell}(\mathbf{q})) + O(\mathbf{q}^{\max_{\ell<k\mid n} w_{r,n}(k)}), \quad (6.15)\end{aligned}$$

with

$$w_{r,n}(k) = \deg_{\mathbf{q}}(\mathsf{I}_{n/k}(\mathbf{q}^k)) = \deg_{\mathbf{q}}(\mathsf{P}_{n/k}(\mathbf{q}^k)) = k((r+n/k)^{\underline{r}}/r! - 1) \quad (6.16)$$

for any divisor k of n. Table 5 lists the degree in $\mathbf{q}$ for all summands in (6.15). We consider $w_{r,n}$ as a function on the real interval $[1,n]$, see Figure 7.

Lemma 6.17. *Let $r \ge 2$, n be composite, ℓ the smallest and k_2 the second smallest divisor of n greater than 1.*

(i) The function $w_{r,n}(k)$ is strictly decreasing in k on $[1,n]$.

(ii) For composite $n \ne 4, 6$, we have

$$w_{r,n}(\ell) - w_{r,n}(k_2) - w_{r-1,n}(\ell) \ge 0. \quad (6.18)$$

(iii) For composite $n > \ell k_2$ different from 12, we have

$$w_{r,n}(\ell) - w_{r,n}(k_2) - w_{r-1,n}(\ell) \ge \log_2 n - 2. \quad (6.19)$$

This also holds if $n = 12$ and $r \ge 3$.

The inequality (6.18) is false when n is 4 or 6, and (6.19) is false for $n = 12$, $r = 2$.

Proof. (i) We compute

$$\begin{aligned}w'_{r,n}(k) &= \frac{(r+n/k)^{\underline{r}}}{r!} - \frac{n}{r!k}\sum_{1\le i\le r}\frac{(r+n/k)^{\underline{r}}}{i+n/k} - 1\\ &= \frac{(r+n/k)^{\underline{r}}}{r!}\Big(1 - \sum_{1\le i\le r}\frac{1}{1+i\frac{k}{n}}\Big) - 1. \quad (6.20)\end{aligned}$$

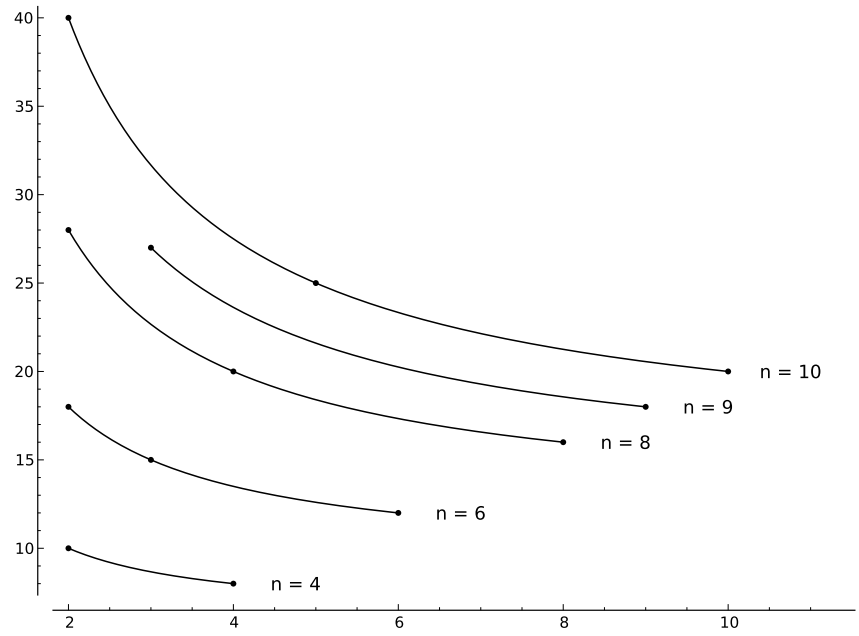

Figure 7: Graphs for $w_{2,n}(k)$ on $[\ell, n]$ for composite n in the range from 4 to 10, where ℓ denotes the smallest prime divisor of n. The dots represent the values at divisors of n.

If $r \geq 3$, then

$$\sum_{1 \leq i \leq r} \frac{1}{1 + i\frac{k}{n}} \geq \sum_{1 \leq i \leq 3} \frac{1}{1+i} > 1$$

for all $1 \leq k \leq n$, which proves $w'_{r,n}(k) < 0$.

If $r = 2$, we evaluate (6.20) as

$$w'_{2,n}(k) = \frac{(1+n/k)(2+n/k)}{2}\Big(1 - \frac{1}{1+k/n} - \frac{1}{1+2k/n}\Big) - 1 = -\frac{n^2}{2k^2}$$

to find $w'_{2,n}(k) < 0$ for all k.

For (ii) and (iii), we first show that the sequence $a_{r,n} = w_{r,n}(\ell) - w_{r-1,n}(\ell) - w_{r,n}(k_2) = \ell b_{r,n/l-1} - k_2(b_{r,n/k_2} - 1)$ is monotonically increasing in r. We have

$$a_{r,n} - a_{r-1,n} = \ell b_{r,n/\ell-2} - k_2 b_{r,n/k_2-1} \geq 0$$

if and only if

$$A_{r,n} = \frac{\ell(r+n/\ell-2)^{\underline{r}}}{k_2(r+n/k_2-1)^{\underline{r}}} \geq 1$$

and prove the latter by induction on $r \geq 2$.

For $r = 2$, we have to prove

$$n(k_2 - \ell) \geq 2\ell k_2. \tag{6.21}$$

If $k_2 = \ell + 1$, then $\ell = 2$, $k_2 = 3$ and since we exclude $n = 6$, we have $n \geq 12$ to show (6.21). If $k_2 \geq \ell + 2$, we distinguish two cases. Now, $k_2 = n$ if and only if $n = \ell^2$. Since we exclude $n = 4$, we then have $\ell \geq 3$ and (6.21) follows. If $k_2 \neq n$, then $k_2 \leq \sqrt{n} < n$ and therefore $2\ell k_2 < 2\sqrt{n}\sqrt{n} \leq (k_2 - \ell)n$.

For the induction step, we have

$$A_{r,n} = A_{r-1,n}\frac{n/\ell - 2 + r}{n/k_2 - 1 + r} \geq \frac{n/\ell - 2 + r}{n/k_2 - 1 + r} \geq 1,$$

where the last inequality is equivalent to $n(k_2 - \ell) \geq \ell k_2$, which follows from (6.21).

With this monotonicity of $a_{r,n}$ in r, it is sufficient to check (ii) and (iii) for the smallest admissible value of r.

(ii) We have

$$a_{2,n} = \frac{n}{2}\Big(\frac{n}{\ell} - \frac{n}{k_2} - 2\Big). \tag{6.22}$$

For

- $n = \ell^2$, $\ell \neq 4$,
- $n = \ell k_2$, $n \neq 6$, or
- $n = 12$,

this is non-negative by direct computation, and in the remaining case, $n > \ell k_2$ different from 12, by (iii).

(iii) For $n > \ell k_2$ different from 12, we have $n/\ell - n/k_2 \geq 3$ and find with (6.22)

$$a_{2,n} \geq \frac{n}{2} > \log_2 n - 2.$$

For $n = 12$ and $r \geq 3$, we compute directly $a_{3,12} = 10 > \log_2 12 - 2$. □

This lemma allows us to order the summands in (6.15) by $\deg_{\mathbf{q}}$, and the approach by generating functions gives the following result.

Theorem 6.23. *Let $r, n \geq 2$, let ℓ be the smallest prime divisor of n, and*

$$\epsilon_{r,n}(\mathbf{q}) = \frac{\mathbf{q}^{\ell(\binom{r+n/\ell}{r}-1)}}{\ell(1-\mathbf{q}^{-\ell})} \in \mathbb{Q}(\mathbf{q}),$$
$$\kappa = (\ell-1)(\binom{r-1+n/\ell}{r-1} - r) + 1.$$

Then the following hold.

(i) $\mathsf{E}_1(\mathbf{q}) = 0$.

(ii) If n is prime, then

$$\mathsf{E}_n(\mathbf{q}) = \epsilon_{r,n}(\mathbf{q})(1-\mathbf{q}^{-nr})\Big(1 - \mathbf{q}^{-r(n-1)}\frac{(1-\mathbf{q}^{-r})(1-\mathbf{q}^{-n})}{(1-\mathbf{q}^{-1})(1-\mathbf{q}^{-nr})}\Big).$$

(iii) If n is composite, then $\kappa \geq 2$ and

$$\mathsf{E}_n(\mathbf{q}) = \epsilon_{r,n}(\mathbf{q})(1 + O(\mathbf{q}^{-\kappa})).$$

Proof. For $n = 1$, the sum (6.12) is empty and this shows (i). For $n = \ell$ prime, (6.12) simplifies to $\mathsf{E}_n(\mathbf{q}) = (\mathsf{I}_1(\mathbf{q}^\ell) - \mathsf{I}_1(\mathbf{q}))/\ell = (\mathsf{P}_1(\mathbf{q}^\ell) - \mathsf{P}_1(\mathbf{q}))/\ell$, since $\mathsf{I}_1 = \mathsf{P}_1$ by Theorem 3.14 and (ii) follows.

For composite n, the product $(\ell-1)(b_{r-1,n/\ell} - r)$ is positive and therefore $\kappa \geq 2$. We recall the summands of (6.15) in Table 5. Lemma 6.17 (i) shows that $\max_{\ell<k\,|\,n} w_{r,n}(k) = w_{r,n}(k_2)$ and we find

$$\mathsf{E}_n(\mathbf{q}) = \frac{1}{\ell}(\mathsf{P}_{n/\ell}(\mathbf{q}^\ell) - \mathsf{R}_{n/\ell}(\mathbf{q}^\ell) - \mathsf{I}_{n/\ell}(\mathbf{q})) + O(\mathbf{q}^{w_{r,n}(k_2)}).$$

Since $b_{r-1,n/\ell} - r > 0$ for composite n, we identify with Lemma 6.17 (i) as main term $\mathsf{P}_{n/\ell}(\mathbf{q}^\ell)/\ell = \epsilon_{r,n}(\mathbf{q})(1-\mathbf{q}^{-\ell b_{r-1,n/\ell}})$. For the summands of

$$\mathsf{E}_n(\mathbf{q})/\epsilon_{r,n}(\mathbf{q}) = (1-\mathbf{q}^{-\ell b_{r-1,n/\ell}})\Big(1 - \frac{\mathsf{R}_{n/\ell}(\mathbf{q}^\ell)}{\mathsf{P}_{n/\ell}(\mathbf{q}^\ell)} - \frac{\mathsf{I}_{n/\ell}(\mathbf{q})}{\mathsf{P}_{n/\ell}(\mathbf{q}^\ell)}\Big) + O(\mathbf{q}^{w_{r,n}(k_2) - \deg_{\mathbf{q}} \mathsf{P}_{n/\ell}(\mathbf{q}^\ell)})$$

we find as degrees in $\mathbf{q}$

$$-\ell b_{r-1,n/\ell} \leq -\kappa,$$
$$\deg_{\mathbf{q}} \mathsf{R}_{n/\ell}(\mathbf{q}^\ell) - \deg_{\mathbf{q}} \mathsf{P}_{n/\ell}(\mathbf{q}^\ell) = -\ell(b_{r-1,n/\ell} - r) \leq -\kappa, \tag{6.24}$$
$$\deg_{\mathbf{q}} \mathsf{I}_{n/\ell}(\mathbf{q}) - \deg_{\mathbf{q}} \mathsf{P}_{n/\ell}(\mathbf{q}^\ell) = -(\ell-1)(b_{r,n/\ell} - 1) \leq -\kappa, \tag{6.25}$$
$$w_{r,n}(k_2) - \deg_{\mathbf{q}} \mathsf{P}_{n/\ell}(\mathbf{q}^\ell) \leq -\ell(b_{r-1,n/\ell} - 1) \leq -\kappa \tag{6.26}$$

for $n \neq 4, 6$ by Lemma 6.17 (ii). When n is 4 or 6, the last inequality in (6.26) is false, but still

$$w_{r,n}(k_2) - \deg_{\mathbf{q}} \mathsf{P}_{n/\ell}(\mathbf{q}^\ell) \leq -\kappa. \quad \square \tag{6.27}$$

On closer inspection, it is possible to partition for each composite n the range for r into two non-empty intervals, where either the difference in (6.24) or the difference in (6.25) dominates all others. This provides tighter bounds at the cost of further case distinctions.

The combinatorial approach yields the following result.

Theorem 6.28. *Let $r, q \geq 2$, and $\epsilon_{r,n}$ and κ as in Theorem 6.23.*

(i) $\#E_{r,1}(\mathbb{F}_q) = 0$.

(ii) If n is prime, then

$$\#E_{r,n}(\mathbb{F}_q) = \epsilon_{r,n}(q)(1-q^{-nr})\Big(1 - q^{-r(n-1)}\frac{(1-q^{-r})(1-q^{-n})}{(1-q^{-1})(1-q^{-nr})}\Big), \tag{6.29}$$
$$0 \leq \epsilon_{r,n}(q) - \#E_{r,n}(\mathbb{F}_q) \leq 3q^{-r(n-1)}.$$

(iii) If n is composite, then

$$|\#E_{r,n}(\mathbb{F}_q) - \epsilon_{r,n}(q)| \leq \epsilon_{r,n}(q) \cdot 3q^{-\kappa}.$$

Proof. The exact statements of (i) and (ii) were already shown in Theorem 6.23 and in (6.29) we have $q^{-r(n-1)}/16$ as upper bound for q^{-nr} and $32q^{-r(n-1)}/15$ as upper bound for the last subtracted term.

For (iii), let ℓ be the smallest and k_2 the second smallest divisor of n greater than 1. We prove that

$$\#E_{r,n}(\mathbb{F}_q) \geq \epsilon_{r,n}(q)(1-3q^{-\kappa}), \tag{6.30}$$
$$\#E_{r,n}(\mathbb{F}_q) \leq \epsilon_{r,n}(q)(1+2q^{-\ell(b_{r-1,n/\ell}-1)}) \quad \text{for } n \neq 4,6, \tag{6.31}$$
$$\#E_{r,n}(\mathbb{F}_q) \leq \epsilon_{r,n}(q)(1+q^{-\kappa}) \quad \text{for } n = 4,6. \tag{6.32}$$

We begin with (6.30) and have from Lemma 6.5 (ii)

$$\begin{aligned}\#E_{r,n}(\mathbb{F}_q) &\geq \#I_{r,n,\ell}(\mathbb{F}_q) = \frac{1}{\ell}\#A^+_{r,n/\ell}(\mathbb{F}_{q^\ell}) \\ &= \frac{1}{\ell}(\#I_{r,n/\ell}(\mathbb{F}_{q^\ell}) - \#I_{r,n/\ell}(\mathbb{F}_q)),\end{aligned}$$

since ℓ is prime and there are no proper intermediate fields between $\mathbb{F}_q$ and $\mathbb{F}_{q^\ell}$. With the lower bound on the number of irreducible polynomials from Corollary 4.13 this yields

$$\begin{aligned}\#E_{r,n}(\mathbb{F}_q) &\geq \frac{1}{\ell}(\#P_{r,n/\ell}(\mathbb{F}_{q^\ell}) - 2\rho_{r,n/\ell}(q^\ell) - \#P_{r,n/\ell}(\mathbb{F}_q)) \\ &= \epsilon_{r,n}(q)\Big(1 - q^{-\ell b_{r-1,n/\ell}} - 2q^{-\ell(b_{r-1,n/\ell}-r)}\frac{1-q^{-\ell r}}{1-q^{-\ell}} \\ &\quad - q^{-(\ell-1)(b_{r,n/\ell}-1)}\frac{(1-q^{-b_{r-1,n/\ell}})(1-q^{-\ell})}{1-q^{-1}}\Big) \\ &= \epsilon_{r,n}(q)\Bigg(1 - q^{-\kappa}\Big(q^{-b_{r-1,n/\ell}-\ell r+1} + 2q^{-b_{r-1,n/\ell}+r+1}\frac{1-q^{-\ell r}}{1-q^{-\ell}} \\ &\quad + q^{-(\ell-1)b_{r,n/\ell-1}-\ell r+\ell+r}\frac{(1-q^{-b_{r-1,n/\ell}})(1-q^{-\ell})}{1-q^{-1}}\Big)\Bigg) \\ &\geq \epsilon_{r,n}(q)(1-q^{-\kappa}(1/16+8/3+1/4)) \\ &\geq \epsilon_{r,n}(q)(1-3q^{-\kappa}).\end{aligned}$$

For the lower bounds (6.31) and (6.32), we have from Lemma 6.5 (ii)

$$\begin{aligned}\#I_{r,n,k}(\mathbb{F}_q) &= \frac{1}{k}\#A^+_{r,n/k}(\mathbb{F}_{q^k})\\ &\le \frac{1}{k}\#P_{r,n/k}(\mathbb{F}_{q^k})\\ &= q^{w_{r,n}(k)}\frac{1-q^{-k\binom{n/k+r-1}{r-1}}}{k(1-q^{-k})},\end{aligned}$$

with $w_{r,n}(k)$ as defined in (6.16). We obtain with (6.8)

$$\begin{aligned}\#E_{r,n}(\mathbb{F}_q) &\le \sum_{1<k|n}\#I_{r,n,k}(\mathbb{F}_q)\\ &\le \sum_{1<k\,|\,n} q^{w_{r,n}(k)}\cdot\frac{1-q^{-kb_{r-1,n/k}}}{k(1-q^{-k})}\\ &= q^{w_{r,n}(\ell)}\frac{1-q^{-\ell b_{r-1,n/\ell}}}{\ell(1-q^{-\ell})}+\sum_{\ell<k\,|\,n} q^{w_{r,n}(k)}\frac{1-q^{-kb_{r-1,n/k}}}{k(1-q^{-k})}\\ &= \epsilon_{r,n}(q)(1-q^{-\ell b_{r-1,n/\ell}})\\ &\quad\cdot\Big(1+q^{-w_{r,n}(\ell)}\sum_{\ell<k\,|\,n} q^{w_{r,n}(k)}\frac{\ell(1-q^{-\ell})(1-q^{-kb_{r-1,n/k}})}{k(1-q^{-k})(1-q^{-\ell b_{r-1,n/\ell}})}\Big)\\ &\le \epsilon_{r,n}(q)\Big(1+q^{-w_{r,n}(\ell)}\sum_{\ell<k\,|\,n}\frac{\ell}{k}q^{w_{r,n}(k)}\Big),\end{aligned}\tag{6.33}$$

since $(1-q^{-k})/(1-q^{-kb_{r-1,n/k}})$ is monotone increasing with k.

For $n=\ell^2$ or $n=\ell k_2$, we compute directly from (6.33)

$$\begin{aligned}\#E_{r,\ell^2}(\mathbb{F}_q) &\le \epsilon_{r,n}(q)\Big(1+\frac{1}{\ell}q^{-w_{r,n}(\ell)+w_{r,n}(n)}\Big),\\ \#E_{r,\ell k_2}(\mathbb{F}_q) &\le \epsilon_{r,n}(q)\Big(1+q^{-w_{r,n}(\ell)+w_{r,n}(k_2)}\Big(\frac{\ell}{k_2}+\frac{\ell}{n}\Big)\Big)\\ &\le \epsilon_{r,n}(q)(1+q^{-w_{r,n}(\ell)+w_{r,n}(k_2)}),\end{aligned}$$

respectively. These prove (6.31) for $n\ne 4,6$, since $-w_{r,n}(\ell)+w_{r,n}(k_2)\le -w_{r-1,n}(\ell)\le-\kappa$ by Lemma 6.17 (ii), and they also show (6.32) for $n=4,6$ with (6.27).

For $n>\ell k_2$, we show

$$q^{-w_{r,n}(\ell)}\sum_{\ell<k\,|\,n}\frac{\ell}{k}q^{w_{r,n}(k)}\le 2q^{-w_{r-1,n}(\ell)}.\tag{6.34}$$

We use the coarse bound $\#\{k\colon \ell<k\mid n\}\le n/2=2^{\log_2 n-1}\le 2q^{\log_2 n-2}$ and show the stronger

$$q^{-w_{r,n}(\ell)}2q^{\log_2 n-2}q^{w_{r,n}(k_2)}\le 2q^{-w_{r-1,n}(\ell)}$$

or equivalently

$$-w_{r,n}(\ell)+w_{r,n}(k_2)\le -w_{r-1,n}(\ell)-\log_2 n+2.$$

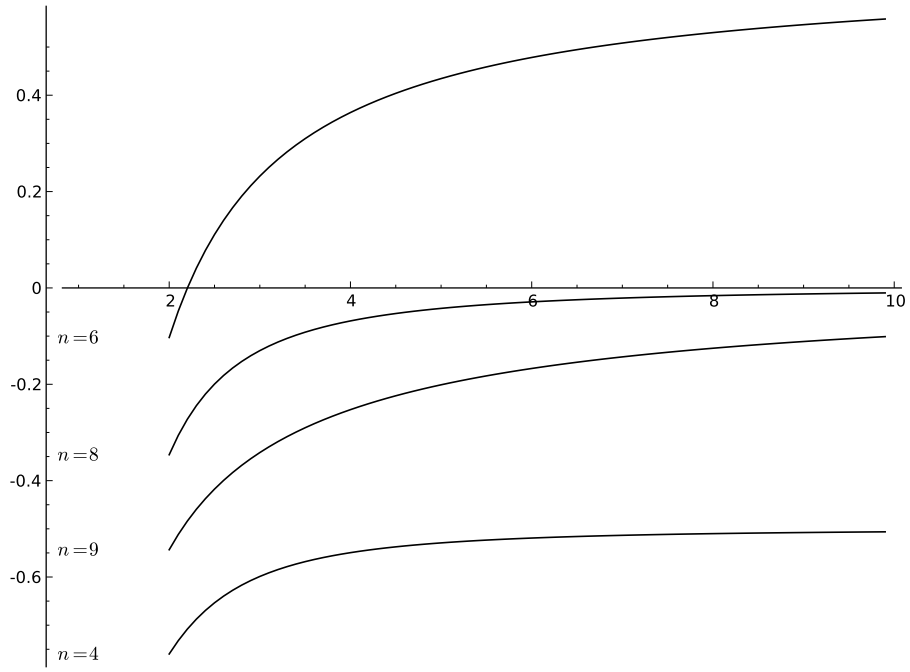

Figure 8: The normalized relative error in Theorem 6.23 (iii) for $r = 2$.

For $n \neq 12$ or $n = 12$ and $r \geq 3$, this follows from Lemma 6.17 (iii). For $r = 2$ and $n = 12$, it suffices to evaluate left- and right-hand side of (6.34) to find $5/6q^{-12} < 2q^{-12}$ as claimed.

Finally, we combine the bounds (6.30), (6.31), and (6.32) with $-w_{r-1,n}(\ell) \leq -\kappa$ from (6.26). □

Figure 8 shows plots of $(\mathsf{E}_{r,n}(\mathbf{q}) - \epsilon_{r,n}(\mathbf{q}))/(\epsilon_{r,n}(\mathbf{q})\mathbf{q}^{-\kappa})$ for $r = 2$ and $n = 4, 6, 8, 9$, as we substitute for $\mathbf{q}$ real numbers from 2 to 10.

Remark 6.35. The bivariate result of von zur Gathen (2008) approximates the ratio $\#E_{2,n}(\mathbb{F}_q)/\#P_{2,n}(\mathbb{F}_q)$ by

$$\frac{q^{-n^2(\ell-1)/(2\ell)}(1-q^{-1})}{\ell(1-q^{-\ell})(1-q^{-n-1})}.$$

This differs from the approximation by $\epsilon_{2,n}(q)/\#P_{2,n}(\mathbb{F}_q)$ in Theorem 6.28 by a factor of $1 - q^{-n-1}$.

We append some handy bounds.

Corollary 6.36. *Let $r, n, q \geq 2$, and ℓ be the smallest prime divisor of n, then*

$$\frac{1}{4\ell} q^{\ell\binom{r+n/\ell}{r}-\ell} \leq \#E_{r,n}(\mathbb{F}_q) \leq \frac{2}{\ell} q^{\ell\binom{l+n/\ell}{r}-\ell},$$

$$\frac{1}{8\ell} q^{-\binom{r+n}{r}+\ell\binom{r+n/\ell}{r}-\ell+1} \leq \frac{\#E_{r,n}(\mathbb{F}_q)}{\#P_{r,n}(\mathbb{F}_q)} \leq \frac{2}{\ell} q^{-\binom{r+n}{r}+\ell\binom{r+n/\ell}{r}-\ell+1},$$

$$\frac{1}{8\ell} q^{-\binom{r+n}{r}+\ell\binom{r+n/\ell}{r}-\ell+1} \leq \frac{\#E_{r,n}(\mathbb{F}_q)}{\#I_{r,n}(\mathbb{F}_q)} \leq \frac{2}{\ell} q^{-\binom{r+n}{r}+\ell\binom{r+n/\ell}{r}-\ell+1}.$$

The last inequalities follow with Corollary 4.12 for $n \geq 5$ and by computation with the exact expressions otherwise.

We conclude with bounds for the number of absolutely irreducible polynomials by combining Corollary 4.13 and Theorem 6.28.

Corollary 6.37. *Let $r, n, q \geq 2$, and $\rho_{r,n}(q)$ as in* (3.15)*. Then*

$$\#P_{r,n}(\mathbb{F}_q) - 4\rho_{r,n}(q) \leq \#A_{r,n}(\mathbb{F}_q) \leq \#I_{r,n}(\mathbb{F}_q) \leq \#P_{r,n}(\mathbb{F}_q),$$

where the 4 can be replaced by 3 for $n \geq 3$.

7 Acknowledgments

Joachim von zur Gathen and Alfredo Viola thank the late Philippe Flajolet for useful discussions about Bender's method in analytic combinatorics of divergent series in April 2008. The work of Joachim von zur Gathen and Konstantin Ziegler was supported by the B-IT Foundation and the Land Nordrhein-Westfalen. We thank the anonymous referees for their useful comments.

References

Max Alekseyev (2006). A115457–A115472. In *The On-Line Encyclopedia of Integer Sequences*. OEIS Foundation Inc. URL `http://oeis.org`. Last download 4 December 2012.

E. Artin (1924). Quadratische Körper im Gebiete der höheren Kongruenzen. II. (Analytischer Teil.). *Mathematische Zeitschrift* **19**(1), 207–246. URL `http://dx.doi.org/10.1007/BF01181075`.

Arnaud Bodin (2008). Number of irreducible polynomials in several variables over finite fields. *American Mathematical Monthly* **115**(7), 653–660. ISSN 0002-9890.

Arnaud Bodin (2010). Generating series for irreducible polynomials over finite fields. *Finite Fields and Their Applications* **16**(2), 116–125. URL `http://dx.doi.org/10.1016/j.ffa.2009.11.002`.

Arnaud Bodin, Pierre Dèbes & Salah Najib (2009). Indecomposable polynomials and their spectrum. *Acta Arithmetica* **139(1)**, 79–100.

M. Car (1987). Théorèmes de densité dans $\mathbb{F}_q[X]$. *Acta Arithmetica* **48**, 145–165.

Leonard Carlitz (1932). The arithmetic of polynomials in a Galois field. *American Journal of Mathematics* **54**, 39–50.

Leonard Carlitz (1963). The distribution of irreducible polynomials in several indeterminates. *Illinois Journal of Mathematics* **7**, 371–375.

Leonard Carlitz (1965). The distribution of irreducible polynomials in several indeterminates II. *Canadian Journal of Mathematics* **17**, 261–266.

Eda Cesaratto, Joachim von zur Gathen & Guillermo Matera (2013). The number of reducible space curves over a finite field. *Journal of Number Theory* **133**, 1409–1434. URL `http://dx.doi.org/10.1016/j.jnt.2012.08.027`.

Stephen Cohen (1968). The distribution of irreducible polynomials in several indeterminates over a finite field. *Proceedings of the Edinburgh Mathematical Society* **16**, 1–17.

Stephen Cohen (1969). Some arithmetical functions in finite fields. *Glasgow Mathematical Society* **11**, 21–36.

P. Flajolet, X. Gourdon & D. Panario (2001). The Complete Analysis of a Polynomial Factorization Algorithm over Finite Fields. *Journal of Algorithms* **40**(1), 37–81. Extended Abstract in *Proceedings of the 23rd International Colloquium on Automata, Languages and Programming ICALP 1996*, Paderborn, Germany, ed. F. Meyer auf der Heide and B. Monien, Lecture Notes in Computer Science **1099**, Springer-Verlag, 1996, 232–243.

Philippe Flajolet & Robert Sedgewick (2009). *Analytic Combinatorics*. Cambridge University Press. ISBN 0521898064, 824 pages.

Shuhong Gao & Alan G. B. Lauder (2002). Hensel Lifting and Bivariate Polynomial Factorisation over Finite Fields. *Mathematics of Computation* **71**(240), 1663–1676.

Joachim von zur Gathen (2008). Counting reducible and singular bivariate polynomials. *Finite Fields and Their Applications* **14**(4), 944–978. URL `http://dx.doi.org/10.1016/j.ffa.2008.05.005`. Extended abstract in *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation ISSAC2007,* Waterloo, Ontario, Canada (2007), 369-376.

Joachim von zur Gathen (2010). Counting decomposable multivariate polynomials. *Applicable Algebra in Engineering, Communication and Computing* **22**(3), 165–185. URL `http://dx.doi.org/10.1007/s00200-011-0141-9`. Abstract in *Abstracts of the Ninth International Conference on Finite Fields and their Applications*, pages 21–22, Dublin, July 2009, Claude Shannon Institute, `http://www.shannoninstitute.ie/fq9/AllFq9Abstracts.pdf`.

Joachim von zur Gathen, Alfredo Viola & Konstantin Ziegler (2010). Counting Reducible, Powerful, and Relatively Irreducible Multivariate Polynomials over Finite Fields (Extended Abstract). In *Proceedings of LATIN 2010,* Oaxaca, Mexico, Alejandro López-Ortiz, editor, volume 6034 of *Lecture Notes in Computer Science*, 243–254. Springer-Verlag, Berlin, Heidelberg. ISBN 978-3-642-12199-9. ISSN 0302-9743 (Print) 1611-3349 (Online). URL `http://dx.doi.org/10.1007/978-3-642-12200-2_23`.

Sudesh K. Gogia & Indar S. Luthar (1981). Norms from certain extensions of $F_q(T)$. *Acta Arithmetica* **38**(4), 325–340. ISSN 0065-1036.

R. L. Graham, D. E. Knuth & O. Patashnik (1989). *Concrete Mathematics*. Addison-Wesley, Reading MA.

David. R. Hayes (1965). The Distribution of Irreducibles in GF$[q, x]$. *Transactions of the American Mathematical Society* **117**, 101–127. URL `http://dx.doi.org/10.2307/1994199`.

Xiang-dong Hou & Gary L. Mullen (2009). Number of Irreducible Polynomials and Pairs of Relatively Prime Polynomials in Several Variables over Finite Fields. *Finite Fields and Their Applications* **15**(3), 304–331. URL `http://dx.doi.org/10.1016/j.ffa.2008.12.004`.

Donald E. Knuth (1992). Two notes on notation. *The American Mathematical Monthly* **99**(5), 403–422. URL `http://arxiv.org/abs/math/9205211`.

Rudolf Lidl & Harald Niederreiter (1997). *Finite Fields*. Number 20 in Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, UK, 2nd edition. First published by Addison-Wesley, Reading MA, 1983.

Gary L. Mullen & Daniel Panario (2013). *Handbook of Finite Fields*. Discrete Mathematics and Its Applications. CRC Press.

Daqing Wan (1992). Zeta Functions of Algebraic Cycles over Finite Fields. *Manuscripta Mathematica* **74**, 413–444.

Kenneth S. Williams (1969). Polynomials with irreducible factors of specified degree. *Canadian Mathematical Bulletin* **12**, 221–223. ISSN 0008-4395.

K. Zsigmondy (1894). Über die Anzahl derjenigen ganzzahligen Functionen n-ten Grades von x, welche in Bezug auf einen gegebenen Primzahlmodul eine vorgeschriebene Anzahl von Wurzeln besitzen. *Sitzungsberichte der Kaiserlichen Akademie der Wissenschaften, Abteilung II* **103**, 135–144.