COUNTING DECOMPOSABLE UNIVARIATE POLYNOMIALS

Joachim von zur Gathen

November 22, 2013

Abstract. A univariate polynomial f over a field is *decomposable* if it is the composition $f = g \circ h$ of two polynomials g and h whose degree is at least 2. We determine an approximation to the number of decomposables over a finite field. The tame case, where the field characteristic p does not divide the degree n of f, is reasonably well understood, and we obtain exponentially decreasing relative error bounds. The wild case, where p divides n, is more challenging and our error bounds are weaker.

Keywords. computer algebra, polynomial decomposition, multivariate polynomials, finite fields, combinatorics on polynomials

Subject classification. 68W30, 11T06, 12E10

1. Introduction

It is intuitively clear that the decomposable polynomials form a small minority among all polynomials (univariate over a field). The goal in this work is to give a quantitative version of this intuition, namely to approximate the number of decomposables over a finite field, together with a good relative error bound.

For a given integer n, we consider a factorization $n = em$ and polynomials $f, g, h \in \mathbb{F}_q[x]$ of degrees n, e, m, respectively, with $f = g \circ h$. All polynomials may be taken monic and with constant coefficient zero; then their graph contains the origin and we call them *original*. We denote the set of all these f as $D_{n,e}$, and D_n is the union of all $D_{n,e}$ as e runs through the nontrivial divisors of n. One readily sees that the major contributions to D_n arise when either e or m equals the smallest prime divisor ℓ of n. The number of all (g, h) in these two cases together is denoted as α_n. We then face four tasks:

- ○ lower bound: $\#D_{n,\ell} \geq \alpha_n(1/2 - \varepsilon)$,
- ○ lower bound: $\#D_{n,n/\ell} \geq \alpha_n(1/2 - \varepsilon)$,

- upper bound: $\#(D_{n,\ell} \cap D_{n,n/\ell}) \leq \varepsilon\alpha_n$,
- upper bound: $\#D_n \leq \alpha_n(1+\varepsilon)$,

with various small ε. (The case $n/\ell = \ell$ needs special consideration.) Then

$$\begin{aligned}\alpha_n(1-3\varepsilon) &\leq \#D_{n,\ell} + \#D_{n,n/\ell} - \#(D_{n,\ell} \cap D_{n,n/\ell}) \\ &= \#(D_{n,\ell} \cup D_{n,n/\ell}) \leq \#D_n \leq \alpha_n(1+\varepsilon).\end{aligned}$$

For most n and q, we achieve this with exponentially vanishing ε, and then have a high-quality approximation α_n of $\#D_n$.

We denote as *tame* the case where the field characteristic p does not divide the degree of the left component, and as *wild* the complementary case. (See von zur Gathen (1990a,b); Schinzel (2000), § 1.5, uses *tame* in a different sense.) Algorithmically, the tame case is well understood since the breakthrough result of Kozen & Landau (1986); see also von zur Gathen, Kozen & Landau (1987); Kozen & Landau (1989); Kozen, Landau & Zippel (1996); Gutierrez & Sevilla (2006), and the survey articles of von zur Gathen (2002) and Gutierrez & Kozen (2003) with further references.

Already Dorey & Whaples (1974) and Schinzel (1982, 2000) had shown that the composition is injective in the tame case, so that in the first two tasks equality holds with $\varepsilon = 0$. In the wild case, various lower bounds, depending on division relations between n and p, are shown in von zur Gathen (2013), which we use here for the first two tasks.

For the third task, the famous Second Theorem of Ritt (1922) plays a central role. Von zur Gathen (2012) provides a normal form for the polynomials occurring in such a "collision". When $\gcd(q, n) = 1$, one can then calculate the ε in the third task exactly; otherwise, we have approximations of varying quality. The fourth task is solved by Theorem 3.2 below.

An advantage of the present approach are the rather precise bounds obtained. A clear disadvantage is the rather large number of case distinctions. Each of the nine leaves of the tree in Figure 4.1 requires a slightly different argument. It is not clear whether this is the nature of the problem or an artifact of our approach. Can a simpler method yield results of similar precision?

The following is proved at the very end of the paper and provides a précis of our results—by necessity less precise than the individual bounds, in particular when $q \leq 4$ or n is (close to) ℓ^2. The basic statement is that α_n is an approximation to the number of decomposable polynomials of degree n, with relative error bounds of varying quality.

MAIN THEOREM. *Let $\mathbb{F}_q$ be a finite field with q elements and characteristic p, let ℓ be the smallest prime divisor of the composite positive integer n, D_n the set of decomposable monic original polynomials in $\mathbb{F}_q[x]$ of degree n, and*

$$\alpha_n = \begin{cases} 2q^{\ell+n/\ell-2} & \text{if } n \neq \ell^2, \\ q^{2\ell-2} & \text{if } n = \ell^2. \end{cases}$$

Then the following hold.

(i) $q^{2\sqrt{n}-2} \leq \alpha_n < 2q^{n/2}$.

(ii) $\alpha_n/2 \leq \#D_n \leq \alpha_n(1+q^{-n/3\ell^2}) < 2\alpha_n < 4q^{n/2}$.

(iii) *If $n \neq p^2$ and $q > 5$, then $\#D_n \geq (3-2q^{-1})\alpha_n/4 \geq q^{2\sqrt{n}-2}/2$.*

(iv) *Unless $p = \ell$ and p divides n exactly twice, we have $\#D_n \geq \alpha_n(1 - 2q^{-1})$.*

(v) *If $p \nmid n$, then $|\#D_n - \alpha_n| \leq \alpha_n \cdot \min\{q^{-1}, q^{-n/3\ell^2}\}$.*

In (v), the relative error in $\#D_n \approx \alpha_n(1+\varepsilon)$ essentially has ε exponentially decreasing in the input size $n \log q$, in the tame case and for growing $n/3\ell^2$. The precise upper bound is always valid, by (ii). But in the lower bound of (iii), when p is the smallest prime divisor of n and divides n exactly twice, then ε is only in $O(1)$, but Blankertz *et al.* (2013) give an exact count for $n = p^2$, using function field theoretic methods. In all other cases, ε is in $O(q^{-1})$ over $\mathbb{F}_q$. It remains a challenge whether these gaps can be reduced. An attentive reader may have observed that for some sequences of n, the value of $n/3\ell^2$ is not unbounded. However, this expression is only chosen as an easily stated and generally valid bound. For special cases we provide special upper bounds. Figure 1.1 presents an illustration for degree $n = 30$.

Giesbrecht (1988) was the first to consider our counting problem. He showed that the decomposable polynomials form an exponentially small fraction of all univariate polynomials. My interest, dating back to the supervision of this thesis, was rekindled by a study of similar (but multivariate) counting problems (von zur Gathen 2008) and during a visit to Pierre Dèbes' group at Lille, where I received a preliminary version of Bodin, Dèbes & Najib (2009). Multivariate decomposable polynomials are counted in von zur Gathen (2010).

The structure of this paper is as follows. Section 2 presents basic notation concerning (de)compositions and their collisions, and collects results from previous work to be used here. Section 3 presents a general upper bound for the decomposables, and a lower bound in the tame case. Section 4 struggles

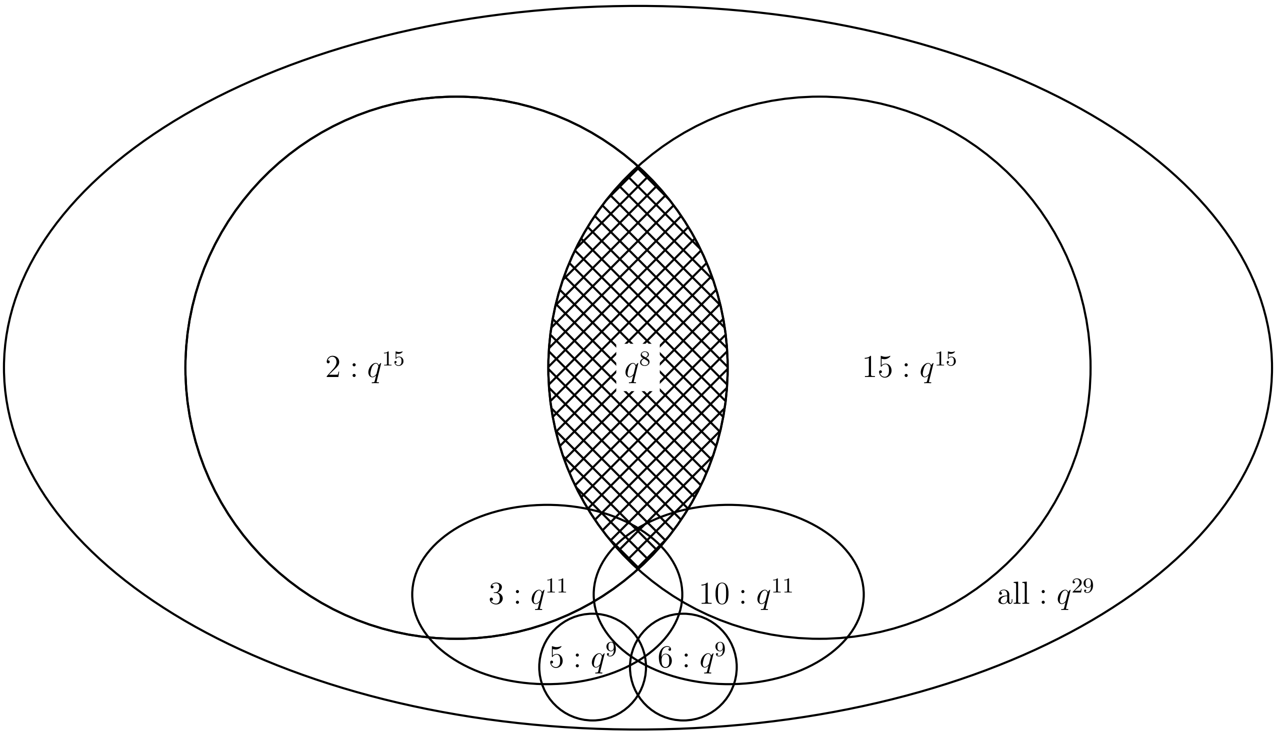

Figure 1.1: There are q^{29} monic original polynomials of degree 30. The six proper divisors of 30 come in pairs $\{m, 30/m\}$. Ignoring lower order terms and assuming $p > 5$, we have $\#D_{30,m} = \#D_{30,30/m} \approx q^{m+30/m-2}$. The hashed region illustrates $\#D_{30,2} \cap D_{30,15} \approx q^8$. The drawing is "not to scale", and x^{30} lies in the intersection of all sets that are shown.

with many special cases in deriving lower bounds, and Section 5 proves the Main Theorem stated above. All inequalities so far are explicit, without unspecified constants, but then Section 6 derives asymptotic results. They illuminate, in particular, the most immediate questions that remain open.

2. Decompositions and collisions

A nonzero polynomial $f \in F[x]$ over a field F is *monic* if its leading coefficient $\mathrm{lc}(f)$ equals 1. We call f *original* if its graph contains the origin, that is, $f(0) = 0$.

Definition 2.1. *For $g, h \in F[x]$,*

$$f = g \circ h = g(h) \in F[x]$$

is their composition. *If $\deg g, \deg h \geq 2$, then (g, h) is a* decomposition *of f. A polynomial $f \in F[x]$ is* decomposable *if there exist such g and h, otherwise f is* indecomposable.

Multiplication by a unit or addition of a constant does not change decomposability, since

$$f = g \circ h \Longleftrightarrow af + b = (ag + b) \circ h$$

for all f, g, h as above and $a, b \in F$ with $a \neq 0$. In other words, the set of decomposable polynomials is invariant under this action of $F^\times \times F$ on $F[x]$. In particular, if we have a set M of monic original decomposable polynomials and let M^* be the set of all their compositions with a linear factor on the left, then

$$\#M^* = q^2(1 - q^{-1}) \cdot \#M. \tag{2.2}$$

Furthermore, any decomposition (g, h) can be normalized by this action, by taking $a = \mathrm{lc}(h)^{-1} \in F^\times$, $b = -a \cdot h(0) \in F$, $g^* = g((x - b)a^{-1}) \in F[x]$, and $h^* = ah + b$. Then $g \circ h = g^* \circ h^*$ and h^* is monic original. If $g \circ h$ and h^* are monic original, then so is g^*.

It is therefore sufficient to consider compositions $f = g \circ h$ where all three polynomials are monic and original. We then call (g, h) monic original. If $F = \mathbb{F}_q$ and D_n is the set of such f of degree n, then the number of all decomposable polynomials of degree n, not restricted to monic original, is

$$q^2(1 - q^{-1}) \cdot \#D_n. \tag{2.3}$$

We fix some notation for the remainder of this paper. F is a field of characteristic $p \geq 0$. For $n \geq 1$, we write

$$P_n = \{f \in F[x] \colon \deg f = n, f \text{ monic and original}\}.$$

For any divisor e of n, we have the composition map for monic original polynomials

$$\gamma_{n,e} \colon \begin{array}{rcl} P_e \times P_{n/e} & \longrightarrow & P_n, \\ (g,h) & \longmapsto & g \circ h, \end{array}$$

corresponding to Definition 2.1, and set

$$D_{n,e} = \operatorname{im} \gamma_{n,e}. \tag{2.4}$$

The set D_n of all decomposable polynomials in P_n satisfies

$$D_n = \bigcup_{\substack{e \mid n \\ 1<e<n}} D_{n,e}. \tag{2.5}$$

In particular, $D_n = \varnothing$ if n is prime. Over a finite field $\mathbb{F}_q$ with q elements, we have

$$\begin{aligned} \# P_n &= q^{n-1}, \\ \# D_{n,e} &\leq q^{n/e+e-2}. \end{aligned} \tag{2.6}$$

A decomposition (g, h) of $f = g \circ h$ over a field of characteristic p is called *tame* if $p \nmid \deg g$, and *wild* otherwise, in analogy with ramification indices. The polynomial f itself is *tame* if $p \nmid \deg f$, and *wild* otherwise. The tame case is well understood, both theoretically and algorithmically. The wild case is more difficult and less well understood; there are polynomials with superpolynomially many "inequivalent" complete decompositions into indecomposable components (Giesbrecht 1988).

For $u, v \in F[x]$ and $j \in \mathbb{N}$, we write

$$u = v + O(x^j)$$

if $\deg(u-v) \leq j$. We start with a well-known result concerning the injectivity of the composition map, see e.g., von zur Gathen (1990a) and the references therein.

Fact 2.7. *Let F be a field of characteristic p, and let e be a nontrivial divisor of $n \geq 2$, not divisible by p. Then $\gamma_{n,e}$ is injective, and*

$$\# D_{n,e} = q^{e+n/e-2}.$$

In the wild case, when $p \mid n$, von zur Gathen (1990b) defines a polynomial $f = x^n + f_i x^i + O(x^{i-1})$ with $f_i \neq 0$ to be *simple* if $i \neq n - p$. If p divides n exactly d times and $f \in F[x]$ is simple, then f has at most $s < 2p^d \leq 2n$ monic original decompositions, where $s = (p^{d+1}-1)/(p-1) = 1+p+\cdots+p^d$. This bound is insufficient for our purposes and replaced by the stronger estimates in Fact 2.12.

In Section 3, we find an upper bound α_n on $\#D_n$, up to some small relative error. When the exact size of the error term is not a concern, then this is quite easy. Furthermore, Fact 2.7 immediately yields a lower bound of $\alpha_n/2$ if p is not the smallest prime divisor ℓ of n, and the remark above yields about $\alpha_n/4n$ in general, since "most" polynomials are simple.

Our goal in this paper is to improve these estimates. Clearly $\#D_n$ equals the number of possible decompositions minus the ambiguities arising from the nonuniqueness of monic original compositions of the form

$$g \circ h = g^* \circ h^*. \tag{2.8}$$

These come in two flavors. We call $\{(g,h),(g^*,h^*)\}$ satisfying (2.8) with $h \neq h^*$ an *equal-degree collision* if $\deg g = \deg g^*$ (and hence $\deg h = \deg h^*$), and a *distinct-degree collision* if $\deg g = \deg h^* \neq \deg h$ (and hence $\deg h = \deg g^*$).

By Fact 2.7, there are no equal-degree collisions when $p \nmid \deg g$. In the more interesting case $p \mid \deg g$, collisions are well-known to exist; von zur Gathen (2013) shows algorithmically that there are few of them, so that the decomposable polynomials are still numerous. For many, but not all, (g,h) that algorithm reconstructs (g,h) from $g \circ h$.

Distinct-degree collisions are classically taken care of by Ritt's Second Theorem. Some versions put a restriction on p that would make our task difficult, but Umberto Zannier (1993) has cut this restriction down to the bare minimum. The additional common restriction that $\gcd(\deg g, \deg h) = 1$ has essentially been removed by Tortrat (1988) in the case that p does not divide the degree. If, in addition, the composition is wild, then a look at derivatives provides a reasonable bound. It is useful to single out a special case of wild compositions.

Definition 2.9. *We assume $n > p \geq 2$ and call* Frobenius composition *any monic original $f \in F[x^p]$, since then $f = g \circ x^p$ for some $g \in P_{n/p}$. For any integer j, we denote by $\varphi_j \colon F \longrightarrow F$ the jth power of the Frobenius map, with $\varphi_j(a) = a^{p^j}$ for all $a \in F$, and extend it to an $\mathbb{F}_p$-linear map $\varphi_j \colon F[x] \longrightarrow F[x]$ with $\varphi_j(x) = x$. Then if $h \in F[x]$, we have*

$$x^{p^j} \circ h = \varphi_j(h) \circ x^{p^j}. \tag{2.10}$$

The Frobenius compositions are easily counted and it is useful to separate them from the others. If $p \mid n$ and ℓ is a proper divisor of n, we set

$$\begin{aligned} D_n^{\varphi} &= D_n \cap F[x^p] = F[x^p], \\ D_n^{+} &= D_n \smallsetminus D_n^{\varphi}, \\ D_{n,\ell}^{+} &= D_{n,\ell} \cap D_n^{+}, \end{aligned} \tag{2.11}$$

so that D_n^{φ} comprises exactly the Frobenius compositions of degree n.

The algorithm in von zur Gathen (2013) provides the following lower bounds on the number of decomposable polynomials; see Theorem 6.1 of that paper.

FACT 2.12. *Let $\mathbb{F}_q$ have characteristic p with $q = p^e$, and take integers $d \geq 1$, $r = p^d$, $k = ar$ with $p \nmid a$, $m \geq 2$, $n = km$, $c = \gcd(d, e)$, $z = p^c$, $\mu = \gcd(r-1, m)$, $\mu^* = \lfloor (\mu-1)/p \rfloor$, $r^* = (r-1)/\mu$. Then the set $D_{n,k}^{+}$ of non-Frobenius monic original compositions has at least the following size.*

(i) If $r \neq m$ and $\mu = 1$:

$$q^{k+m-2}(1-q^{-k})\big(1 - q^{-1}(1 + q^{-p+2}\frac{(1-q^{-1})^2}{1-q^{-p}})\big),$$

(ii) If $r \neq m$:

$$\begin{aligned} & q^{k+m-2}\big((1 - q^{-1}(1 + q^{-p+2}\frac{(1-q^{-1})^2}{1-q^{-p}}))(1-q^{-k}) \\ & \qquad - q^{-r^*-c/e+1}\frac{(1-q^{-1})^2(1-q^{-r^*(\mu-1)})}{(1-q^{-c/e})(1-q^{-r^*})} \\ & \qquad \cdot (1 - q^{-r^*(p-1)}\frac{(1-q^{-r^*})(1-q^{-pr^*\mu^*})}{(1-q^{-r^*(\mu-1)})(1-q^{-pr^*})})\big) \\ \geq {} & q^{k+m-2}\big((1 - q^{-1}(1 + q^{-p+2}\frac{(1-q^{-1})^2}{1-q^{-p}}))(1-q^{-k}) \\ & \qquad - q^{-r^*+1}\frac{(1-q^{-1})^2(1-q^{-r^*(\mu-1)})}{1-q^{-r^*}})\big) \\ \geq {} & q^{k+m-2}\big((1 - q^{-1}(1 + q^{-p+2}\frac{(1-q^{-1})^2}{1-q^{-p}}))(1-q^{-k}) \\ & \qquad - 2q^{-r^*+1}(1-q^{-1})^2\big). \end{aligned}$$

(iii) If $r = m$:

$$q^{k+m-2}(1-q^{-1})(\frac{1}{2} + \frac{1+q^{-1}}{2z+2} + \frac{q^{-1}}{2} - q^{-k}\frac{1-q^{-p+1}}{1-q^{-p}} - q^{-p+1}\frac{1-q^{-1}}{1-q^{-p}}).$$

Von zur Gathen (2012), Table 1.1 and Corollary 7.4, provides the following estimates on the number of distinct-degree collisions. We use Kronecker's δ in the statement. An integer is $(p+1)$-rough if any divisor $d \geq 2$ of it is larger than p.

FACT 2.13. *Let $\mathbb{F}_q$ be a finite field of characteristic p, let ℓ and m be integers with $m > \ell \geq 2$, $n = \ell m$, $s = \lfloor m/\ell \rfloor$, and $t = \#(D_{n,\ell} \cap D_{n,m} \cap D_n^+)$. Then the following bounds hold.*

	conditions	*bounds on t*
(i)	$p \nmid n,\ \gcd(\ell, m) = 1$	$t = q^{s+1} + (1-\delta_{\ell,2})(q^2 - q)$ $q^{s+1} \leq t \leq q^{s+1} + q^2 \leq 2q^{s+1}$
(ii)	$p \mid \ell,\ \gcd(\ell, m) = 1$	$t = 0$
(iii)	$p \mid m,\ \gcd(\ell, m) = 1$	$t \leq q^{s+1} - q^{\lfloor s/p \rfloor + 1}$
(iv)	$p \nmid n,\ \ell \mid m$	$t = q^{2\ell+s-3}$
(v)	$p \nmid n,\ \ell \nmid m,\ \gcd(\ell, m) = i$	$t = q^{2i}(q^{s-1} + (1-\delta_{\ell,2})(1-q^{-1}))$
(vi)	$p \nmid n$	$t \leq q^{2\ell+s-3}$
(vii)	$p \nmid \ell,\ p \mid m$	$t \leq q^{m+\lceil \ell/p \rceil - 2}$
(viii)	$p \mid \ell,\ c = \lceil (m-\ell+1)/\ell \rceil$	$t \leq q^{m+\ell-c+\lceil c/p \rceil - 2}$
(ix)	$p = \ell \mid m,\ m/p\ \ (p+1)$*-rough*	$t \geq q^{2p+m/p-3}(1-q^{-1})(1-q^{-p+1})$

(x) If $p \nmid \ell$ and p divides m exactly $d \geq 1$ times, then

$$t \geq q^{2\ell+m/\ell-3}(1-q^{-m/\ell})\big(1 - q^{-1}(1 + q^{-p+2}\frac{(1-q^{-1})^2}{1-q^{-p}})\big)$$

if $\ell \nmid p^d - 1$. Otherwise we set $\mu = \gcd(p^d-1, \ell)$, $r^* = (p^d-1)/\mu$ and have

$$\begin{aligned} t \geq q^{2\ell+m/\ell-3}\big(& (1 - q^{-1}(1 + q^{-p+2}\frac{(1-q^{-1})^2}{1-q^{-p}}))(1-q^{-m/\ell}) \\ & - q^{-m/\ell-r^*+2}\frac{(1-q^{-1})^2(1-q^{-r^*(\mu-1)})}{1-q^{-r^*}}(1+q^{-r^*(p-2)})\big). \end{aligned}$$

(i) is an important special case of (v). The Frobenius compositions are counted in von zur Gathen (2012), Lemma 4.1, which we restate next.

FACT 2.14. *Let $\mathbb{F}_q$ have characteristic p, let ℓ, $m \geq 2$ be integers for which p divides $n = \ell m$, and let g and h in $F[x]$ have degrees ℓ and m, respectively. Then the following hold.*

(i) $g \circ h \in D_n^\varphi \Longleftrightarrow g'h' = 0 \Longleftrightarrow g \in D_\ell^\varphi$ or $h \in D_m^\varphi$,

(ii) $$\#D_n^{\varphi} = \begin{cases} q^{n/p-1} & \text{if } n \neq p^2, \\ q^{n/p-1} - 1 & \text{if } n = p^2, \end{cases}$$

(iii)

$$\#D_{n,\ell}^{\varphi} \begin{cases} = \#D_{n/p,\ell} & \text{if } p \nmid \ell, \\ = \#D_{n/p,\ell/p} & \text{if } p \nmid m, \\ \leq \#D_{n/p,\ell} + \#D_{n/p,\ell/p} & \text{always.} \end{cases}$$

If $n = p^2$, the methods of this paper do not yield satisfactory bounds. However, this has been completely resolved by Blankertz *et al.* (2013), as follows.

FACT 2.15. *Let $\mathbb{F}_q$ be a finite field of characteristic p and τ the number of positive divisors of $p-1$. Then*

$$\#D_{p^2}(\mathbb{F}_q) = q^{2p-2} - q^{p-1} + 1 - \frac{(\tau q - q + 1)(q-1)(qp - p - 2)}{2(p+1)} - \delta_{p\neq 2} \frac{q(q-1)(q-2)(p-3)}{4}.$$

3. Counting tame decomposable polynomials

This section estimates the dimension and number of decomposable monic original univariate polynomials. We start with the dimension of decomposables over an algebraically closed field. Next, over a finite field, Theorem 3.2 below provides a general upper bound on the number of decomposables, and an almost matching lower bound. The latter applies only to the tame case, where $p \nmid n$, and both bounds carry a relative error term. Lower bounds in the more difficult wild case are the subject of Section 4.

Giesbrecht (1988) was the first work on our counting problem. He proves (in his Section 1.G and translated to our notation) an upper bound of $d(n)q^{n/2}$ on the number of decomposable monic original polynomials, where $d(n)$ is the number of divisors of n. This is mildly larger than our bound of about $2q^{\ell+n/\ell-2}$, in Theorem 3.2(i), with its dependence on ℓ replaced by the "worst case" $\ell = 2$, as in the Main Theorem (i). With the same replacement, Giesbrecht's thesis contains the upper bound in the following result.

THEOREM 3.1. *Let F be an algebraically closed field of characteristic $p \geq 0$, suppose that $n \geq 2$ is not a multiple of p, and let ℓ be the smallest prime divisor of n. Then $D_n = \varnothing$ if n is prime, and otherwise*

$$\dim D_n = \ell + n/\ell - 2.$$

PROOF. We may assume that n is composite. By Fact 2.7, the fibers of $\gamma_{n,\ell}$ are finite, and hence

$$\dim D_n \geq \dim D_{n,\ell} = \dim(P_\ell \times P_{n/\ell}) = \ell + n/\ell - 2.$$

Now $D_{n,n/\ell}$ has the same dimension, and $D_{n,e}$ has smaller dimension for all other divisors e of n. □

The argument used in von zur Gathen (2012) for Fact 2.13(i) shows that if n is composite, $p \nmid n$, and $\ell^2 \nmid n$, then $\dim(D_{n,\ell} \cap D_{n,n/\ell}) \leq \lfloor n/\ell^2 \rfloor + 1 < \ell + n/\ell - 2$. Thus $\gamma_{n,\ell}$ and $\gamma_{n,n/\ell}$ describe two different irreducible components of D_n, both of dimension $\ell + n/\ell - 2$.

Zannier (2008) studies a different but related question, namely compositions $f = g \circ h$ in $\mathbb{C}[x]$ with a *sparse* polynomial f, having t terms. The degree is not bounded. He gives bounds, depending only on t, on the degree of g and the number of terms in h. Furthermore, he gives a parametrization of all such f, g, h in terms of varieties (for the coefficients) and lattices (for the exponents).

We now present a generally valid upper bound on the number of decomposables, and a lower bound in the tame case $p \nmid n$. $I_n = P_n \smallsetminus D_n$ consists of the indecomposable polynomials in P_n.

THEOREM 3.2. *Let $\mathbb{F}_q$ be a field of characteristic p and with q elements, and $n \geq 2$. Let ℓ and ℓ_2 be the smallest and second smallest nontrivial divisors of n, respectively (with $\ell_2 = 1$ if $n \in \{\ell, \ell^2\}$), $s = \lfloor n/\ell^2 \rfloor$, and*

$$\alpha_n = \begin{cases} 0 & \text{if } n = \ell, \\ q^{2\ell-2} & \text{if } n = \ell^2, \\ 2q^{n/\ell+\ell-2} & \text{otherwise}, \end{cases} \tag{3.3}$$

$$c = \frac{(n - \ell\ell_2)(\ell_2 - \ell)}{\ell\ell_2},$$

$$\beta_n = \begin{cases} 0 & \text{if } n \in \{\ell, \ell^2, \ell^3, \ell\ell_2\}, \\ \dfrac{q^{-c}}{1-q^{-1}} & \text{otherwise}, \end{cases} \tag{3.4}$$

$$\beta_n^* = q^{-n/\ell-\ell+s+3}, \tag{3.5}$$

$$t = \begin{cases} 0 & \text{if } n \in \{\ell, \ell^2\}, \\ \#(D_{n,\ell} \cap D_{n,n/\ell}) & \text{otherwise}. \end{cases} \tag{3.6}$$

Then the following hold.

(i) $\#D_n \leq \alpha_n(1 - \alpha_n^{-1} t + \beta_n) \leq \alpha_n(1 + \beta_n)$.

(ii) $\#I_n \geq \#P_n - 2\alpha_n$.

(iii) If $p \nmid n$ *and* $\ell^2 \nmid n$*, then*

$$\alpha_n(1 - q^{-n/\ell+\ell+s-1}) \leq \alpha_n(1 - \beta_n^*) \leq \#D_n \leq \alpha_n(1 - \frac{\beta_n^*}{2} + \beta_n).$$

(iv) If $p \nmid n$ *and* $\ell^2 \mid n$*, then*

$$\alpha_n(1 - \frac{1}{2}q^{-n/\ell+\ell+s-1}) \leq \#D_n \leq \alpha_n(1 - \frac{\beta_n^*}{2} + \beta_n).$$

(v) If $p \neq \ell$*, then* $\#D_{\ell^2} = \alpha_{\ell^2}$ *and* $\#D_{\ell^3} = \alpha_{\ell^3}(1 - q^{-(\ell-1)^2}/2)$.

(vi) If $p \nmid n \neq \ell^2$ *and* n/ℓ *is prime, then*

$$\#D_n = \alpha_n\big(1 - \frac{1}{2}q^{-n/\ell-\ell+3}(q^s + (1 - \delta_{\ell,2})(q-1))\big).$$

PROOF. When $n = \ell$ is prime, then $D_n = \varnothing$ and all claims are clear (reading $\alpha_n \cdot \alpha_n^{-1}t$ as 0). We may now assume that n is composite.

It is convenient to start with the proof of (v). For $n = \ell^2$, we have $D_n = D_{n,\ell}$ and

$$\#D_n = q^{n/\ell+\ell-2} = \alpha_n,$$

using the injectivity of $\gamma_{\ell^2,\ell}$ (Fact 2.7). When $n = \ell^3$, then Fact 2.13(iv) says that

$$t = q^{3\ell-3},$$
$$\#D_{\ell^3} = \alpha_{\ell^3}(1 - \frac{t}{\alpha_{\ell^3}}) = \alpha_n(1 - \frac{q^{-(\ell-1)^2}}{2}).$$

This shows (v), and we now proceed with the other claims.

(i) The claim for $n \in \{\ell^2, \ell^3\}$ follows from (v) proven above, and we now exclude these cases. We write $u(e) = n/e + e - 2$ for the exponent in (2.6). We have the two largest subsets $D_{n,\ell}$ and $D_{n,n/\ell}$ of D_n, both of size at most

$$\frac{\alpha_n}{2} = q^{u(\ell)} = q^{n/\ell+\ell-2} = \#(P_\ell \times P_{n/\ell}). \tag{3.7}$$

Their joint contribution to $\#D_n$ is at most

$$\alpha_n - t. \tag{3.8}$$

Since n is not ℓ or ℓ^2, we have $\ell < \ell_2 \leq n/\ell$, and ℓ_2 is either ℓ^2 or a prime number larger than ℓ. The index set E in (2.5) consists of all proper divisors of n. If $n = \ell\ell_2$, then $E = \{\ell, \ell_2\}$, and from (3.8) we have

$$\#D_n \leq \alpha_n - t,$$

from which the claims of (i) follow. We may now assume that $n \neq \ell\ell_2$. For any $e \in E$, we have $u(e) = e + n/e - 2 = u(n/e)$. Furthermore

$$u(e) - u(e') = \frac{(n - ee')(e' - e)}{ee'} \tag{3.9}$$

holds for $e, e' \in E$, and in particular

$$u(\ell) - u(\ell_2) = \frac{(n - \ell\ell_2)(\ell_2 - \ell)}{\ell\ell_2} = c. \tag{3.10}$$

Considered as a function of a real variable e, u is convex on the interval $[1..n]$, since $\partial^2 u/\partial e^2 = 2n/e^3 > 0$. Thus $u(\ell) - u(e) \geq c$ for all $e \in E_2 = E \smallsetminus \{\ell, n/\ell\}$. Then

$$\begin{aligned} \sum_{e \in E_2} q^{u(e)-u(\ell)} &= q^{-c} \sum_{e \in E_2} q^{u(e)-u(\ell)+c} \\ &< q^{-c} \cdot 2 \sum_{i \geq 0} q^{-i} = \frac{2q^{-c}}{1 - q^{-1}}, \end{aligned} \tag{3.11}$$

since each value $u(e)$ is assumed at most twice, namely for e and n/e, according to (3.9) (or by the convexity of u). Using (3.8), it follows for $n \neq \ell^2$ that

$$\begin{aligned} \#D_n + t &\leq \sum_{e \in E} \#D_{n,e} \leq \sum_{e \in E} q^{u(e)} \\ &\leq q^{\ell + n/\ell - 2}(2 + \sum_{e \in E_2} q^{u(e)-u(\ell)}) \\ &< q^{\ell + n/\ell - 2}(2 + \frac{2q^{-c}}{1 - q^{-1}}) = \alpha_n(1 + \beta_n). \end{aligned} \tag{3.12}$$

This implies the claim in (i).

(ii) follows from $\beta_n \leq 1$.

For (iii), we have $D_{n,\ell} \cup D_{n,n/\ell} \subseteq D_n$. Since $p \nmid n$, both $\gamma_{n,\ell}$ and $\gamma_{n,n/\ell}$ are injective, by Fact 2.7. From (i) above and Fact 2.13(i), we find

$$\begin{aligned}\#D_n &\geq \#D_{n,\ell} + \#D_{n,n/\ell} - \#(D_{n,\ell} \cap D_{n,n/\ell}) \\ &\geq 2q^{\ell+n/\ell-2} - 2q^{s+1} \\ &= \alpha_n(1 - \frac{2q^{s+1}}{2q^{\ell+n/\ell-2}}) = \alpha_n(1-\beta_n^*), \\ \#D_n &\leq \alpha_n(1 - \frac{q^{s+1}}{\alpha_n} + \beta_n) = \alpha_n(1 - \frac{\beta_n^*}{2} + \beta_n).\end{aligned}$$

Furthermore, we have $\ell \geq 2$ and hence

$$-\ell - \frac{n}{\ell} + s + 3 \leq -\frac{n}{\ell} + \ell + s - 1.$$

It follows that

$$\beta^* \leq q^{-n/\ell+\ell+s-1}.$$

(iv) For the lower bound if $\ell^2 \mid n$, we replace the upper bound $2q^{s+1}$ on t in the previous estimate by the one from Fact 2.13(vi).

For (vi), we replace the bound on $\#(D_{n,\ell} \cap D_{n,n/\ell})$ by its exact value from Fact 2.13(i). □

Bodin *et al.* (2009) state an upper bound as in Theorem 3.2(i), with an error term which is worse than β_n by a factor of $O(n)$.

Remark 3.13. *How often does it happen that the smallest prime factor ℓ of n actually divides n at least twice? The answer: almost a third of the time.*

For a prime ℓ, let

$$S_\ell = \{n \in \mathbb{N} \colon \ell^2 \mid n, \forall \text{primes } r < \ell \quad r \nmid n\},$$

so that $\bigcup_\ell S_\ell$ is the set in question. The union is disjoint, and its density is

$$\sigma = \sum_\ell \frac{1}{\ell^2} \prod_{r<\ell} (1 - \frac{1}{r}) \approx 0.330098.$$

If we take a prime p and further ask that $p \nmid n$, then we have the density

$$\sigma_p = \sigma - \frac{1}{p^2} \prod_{r<p} (1 - \frac{1}{r}) - \frac{1}{p} \sum_{\ell<p} \frac{1}{\ell^2} \prod_{r<\ell} (1 - \frac{1}{r}).$$

The correction terms $\sigma - \sigma_p$ are $\approx$ 0.25, 0.13889, 0.07444 for $p = 2, 3, 5$, respectively.

The upper and lower bounds in Theorem 3.2(i) and (iii) have distinct relative error estimates. We now compare the two.

PROPOSITION 3.14. *In the notation of Theorem 3.2, assume that* $n \notin \{\ell, \ell^2, \ell^3, \ell\ell_2\}$.

(i) If $\ell_2 \leq \ell^2$, *then* $\beta_n > \beta_n^*$. *If furthermore* $\ell^2 \nmid n$ *and* $p \nmid n$, *then*

$$|\#D_n - \alpha_n| \leq \alpha_n \beta_n.$$

(ii) If $\ell_2 \geq \ell^2 + \ell$, *then* $\beta_n \leq \beta_n^*$. *If furthermore* $\ell^2 \nmid n$ *and* $p \nmid n$, *then*

$$|\#D_n - \alpha_n| \leq \alpha_n \beta_n^*.$$

PROOF. We let $\mu = -\log_q(1 - q^{-1})$ and $\sigma = n/\ell^2 - s$, so that $0 < \mu \leq 1$, $0 \leq \sigma \leq 1 - 1/\ell < 1$, and

$$\begin{aligned}\beta_n &= q^{-c+\mu},\\ \beta_n^* &= q^{-\ell - n/\ell + n/\ell^2 - \sigma + 3}.\end{aligned}$$

Furthermore,

$$\begin{aligned}\beta_n \leq \beta_n^* &\Longleftrightarrow \ell\ell_2(\ell + \frac{n}{\ell} - \frac{n}{\ell^2} + \sigma + \mu - 3) \leq (n - \ell\ell_2)(\ell_2 - \ell)\\ &\Longleftrightarrow \ell\ell_2(\ell_2 + \sigma + \mu - 3) \leq \frac{n}{\ell}(\ell_2 - \ell^2).\end{aligned} \tag{3.15}$$

We note that $\ell_2 \geq 3$ and $\ell_2 + \sigma + \mu - 3 > 0$. If $\ell_2 \leq \ell^2$, it follows that $\beta_n > \beta_n^*$. If $\ell_2 \geq \ell^2 + \ell$, then $a = n/\ell\ell_2$ is a proper divisor of n, since $n \neq \ell\ell_2$. It follows that $a \geq \ell_2$, since $a = \ell$ would mean that ℓ^2 is a divisor of n with $\ell < \ell^2 < \ell_2$, contradicting the minimality of ℓ_2. Then

$$\frac{n}{\ell}(\ell_2 - \ell^2) \geq \ell_2^2 \cdot \ell > \ell\ell_2(\ell_2 + \sigma + \mu - 3),$$

and $\beta_n \leq \beta_n^*$.

The claims about $\#D_n$ follow from Theorem 3.2. □

We have $\ell_2 \leq \ell^2$ and $\beta_n = 0 < \beta_n^*$ in the three exceptional cases $n \in \{\ell, \ell^2, \ell^3\}$. There remains the "gray area" of $\ell^2 < \ell_2 < \ell^2 + \ell$, where (3.15) has to be evaluated. The three equivalent properties in (3.15) hold when n has at least four prime factors, and do not hold when $n = \ell\ell_2$.

We can simplify the bounds of Theorem 3.2, at the price of a slightly larger relative error.

COROLLARY 3.16. *We assume the notation q, p, n, ℓ, and α_n of Theorem 3.2.*

(i) If n is prime, then $D_n = \varnothing$.

(ii) For all n, we have

$$\#D_n \leq \alpha_n(1 + q^{-n/3\ell^2}). \tag{3.17}$$

(iii) If $p \nmid n$, then

$$|\#D_n - \alpha_n| \leq \alpha_n \cdot \min\{q^{-n/3\ell^2}, q^{-1}\}.$$

PROOF. (i) follows from Theorem 3.2(i), since $\alpha_n = 0$. In the remainder of this proof, we assume n to be composite. For (ii), we claim that $\beta_n \leq q^{-n/3\ell^2}$. The cases where $n \in \{\ell, \ell^2, \ell^3, \ell\ell_2\}$ follow from Theorem 3.2(i) with $\beta_n = 0$, and we may now assume that $a = n/\ell\ell_2 \geq 2$. We set $\mu = -\log_q(1 - q^{-1})$, so that $0 < \mu \leq 1$ and $\beta_n = q^{-c+\mu}$.

We have

$$\frac{3\ell^3 + 3\ell}{3\ell - 2} \geq \frac{3\ell^2}{3\ell - 1}.$$

If

$$\ell_2 \geq \frac{3\ell^2 + 3\ell}{3\ell - 2} = \ell + \frac{5}{3} + \frac{10}{9\ell - 6}, \tag{3.18}$$

then $\ell_2 - \ell - \ell_2/3\ell \geq 0$ and

$$a(\ell_2 - \ell - \frac{\ell_2}{3\ell}) \geq 2(\ell_2 - \ell - \frac{\ell_2}{3\ell}) \geq \ell_2 - \ell + 1,$$

$$c - \mu \geq (a-1)(\ell_2 - \ell) - 1 \geq \frac{a\ell_2}{3\ell} = \frac{n}{3\ell^2}, \tag{3.19}$$

from which the claim follows. (3.18) is satisfied except when (ℓ, ℓ_2) is $(2, 3)$, $(2, 4)$ or $(3, 5)$.

In the first exceptional case, (3.19) is satisfied for $a \geq 4$, and in the other two for $a \geq 3$. The latter always holds in the case $(3, 5)$, and we are left with $n \in \{12, 16, 18\}$. For these values of n, we use a direct bound on the sum in (3.12), namely

$$\sum_{e \in E_2} q^{u(e)-u(\ell)} \leq \#E_2 \cdot q^{-c} = 2\gamma q^{-c},$$

where $\gamma = \#E_2/2$, so that

$$\#D_n \leq \alpha_n(1 + \gamma q^{-c}) - t < \alpha_n(1 + \gamma q^{-c}).$$

n:	12	16	18
γ	1	1/2	1
c	1	2	2
$n/3\ell^2$	1	4/3	3/2

Table 3.1: Parameters for three values of n.

The required values are given in Table 3.1. In all cases, we conclude from Theorem 3.2(i) that $\#D_n \leq \alpha_n(1+q^{-n/3\ell^2})$.

(iii) We call $q^{-n/3\ell^2}$ the first and q^{-1} the second bound, and distinguish between the upper and lower bounds on $\#D_n - \alpha_n$ claimed in (iii). For the first upper bound

$$\#D_n \leq \alpha_n(1+q^{-n/3\ell^2}),$$

we claim that

$$c = \frac{(n-\ell\ell_2)(\ell_2-\ell)}{\ell\ell_2} \geq \frac{n}{3\ell^2}+1 \tag{3.20}$$

The claim implies, as above, that

$$(1-q^{-1})\beta_n = q^{-c} \leq q^{-1}\cdot q^{-n/3\ell^2} \leq (1-q^{-1})q^{-n/3\ell},$$

from which the bound follows by Theorem 3.2(iv). We may again assume that $n \notin \{\ell, \ell^2, \ell^3, \ell\ell_2\}$ and let $a = n/\ell\ell_2$, so that $a \geq \ell_2 > \ell \geq 2$ and $a \geq 3$. We first assume that $a \geq 4$. Then

$$\begin{aligned} a \geq 4 \geq \frac{6\ell}{2\ell-1}&, \\ (3\ell(a-1)-a)\ell_2 \geq \big(3\ell(a-1)-a\big)(\ell+1) &\geq 3\ell^2(a-1)+3\ell, \\ c = (a-1)(\ell_2-\ell) &\geq \frac{a\ell_2+3\ell}{3\ell} = \frac{n}{3\ell^2}+1, \end{aligned}$$

and (3.20) follows. If $a = 3$, then $\ell_2 = 3$, $\ell = 2$, $n = 18$, $\alpha_{18} = 2q^9$, and by (2.5)

$$\begin{aligned} \#D_{18} &\leq \#D_{18,2} + \#D_{18,3} + \#D_{18,6} + \#D_{18,9} \\ &\leq 2\cdot q^9 + 2\cdot q^7 = \alpha_{18}(1+q^{-2}) \\ &\leq \alpha_{18}\cdot(1+q^{-3/2}) = \alpha_{18}\cdot(1+q^{-n/3\ell^2}). \end{aligned}$$

This shows the first upper bound in (iii). For the first lower bound, we start by assuming that $\ell^2 \nmid n$. If $\ell \geq 3$, then

$$\frac{4}{3}\cdot\frac{n}{\ell^2}+3 \leq \frac{n}{\ell}+\ell,$$

and this is also true for $\ell = 2$, since then $n \geq 6$. It follows that

$$\begin{aligned} -\ell - \frac{n}{\ell} + s + 3 \leq -\ell - \frac{n}{\ell} + \frac{n}{\ell^2} + 3 \leq -\frac{n}{3\ell^2}, \\ \#D_n \geq \alpha_n(1 - \beta_n^*) \geq \alpha_n(1 - q^{-n/3\ell^2}). \end{aligned}$$

Now suppose that $\ell^2 \mid n$, and set $a = n/\ell^2$. For $a = 1$, Theorem 3.2(v) shows the claim in (iii). Thus we may assume $a \geq 2$, and then $a \geq \ell$. For $\ell \geq 3$, we have, using Theorem 3.2(iv),

$$\begin{aligned} \ell \leq \ell(\ell - \frac{4}{3}) \leq a(\ell - \frac{4}{3}) + 1, \\ \frac{n}{3\ell^2} + \ell + s \leq \frac{n}{3\ell^2} + \ell + \frac{n}{\ell^2} \leq \frac{n}{\ell} + 1, \\ \#D_n \geq \alpha_n(1 - \frac{1}{2}q^{-n/\ell+\ell+s-1}) \geq \alpha_n(1 - q^{-n/3\ell^2}). \end{aligned}$$

For $\ell = 2$, we have $n \geq 8$ and the last inequality holds again.

The second upper bound claims that

$$\#D_n \leq \alpha_n(1 + q^{-1}).$$

Theorem 3.2(iv) implies that $\#D_n \leq \alpha_n(1+\beta_n)$, and we claim that $\beta_n \leq q^{-1}$. According to (3.4), we may assume that $n \notin \{\ell, \ell^2, \ell^3, \ell\ell_2\}$. Now $a = n/\ell\ell_2$ is an integer with $a \geq 2$ and all its prime divisors at least ℓ_2, hence $a \geq \ell_2 > \ell \geq 2$. It follows that

$$\begin{aligned} \ell_2 &\leq \ell_2(\ell_2 - \ell) \leq a(\ell_2 - \ell), \\ \ell\ell_2^2 &\leq n(\ell_2 - \ell), \\ 2\ell\ell_2 &\leq \ell^2\ell_2 \leq \ell^2\ell_2 + n(\ell_2 - \ell) - \ell\ell_2^2 = (n - \ell\ell_2)(\ell_2 - \ell), \\ 2 &\leq \frac{(n - \ell\ell_2)(\ell_2 - \ell)}{\ell\ell_2} = c, \\ q^{-c} &\leq q^{-2} \leq (1 - q^{-1})q^{-1}, \\ \beta_n &= \frac{q^{-c}}{1 - q^{-1}} \leq q^{-1}, \end{aligned}$$

as claimed. The second lower bound

$$\#D_n \geq \alpha_n(1 - q^{-1})$$

is satisfied by the previous argument if $n \geq 3\ell^2$. So we now assume that $n < 3\ell^2$. Then $n/\ell < 3\ell$, and all prime factors of n/ℓ are at least ℓ. It follows that either $n = 8$ or $n/\ell = \ell_2$ is prime. If $\ell_2 = \ell$, then $\#D_n = \alpha_n$, by

Theorem 3.2(v). Otherwise we have $s = \lfloor n/\ell^2 \rfloor = \lfloor \ell_2/\ell \rfloor \leq \lfloor (3\ell - 1)/\ell \rfloor \leq 2$ and from Theorem 3.2(iii) that

$$\#D_n \geq \alpha_n(1 - \beta_n^*) \geq \alpha_n(1 - q^{-\ell-\ell_2+5}).$$

It is now sufficient to show

$$\ell + \ell_2 \geq 6.$$

This holds unless $n \in \{4, 6, 9\}$, so that only $n = 6$ needs to be further considered. We have $\beta_6^* = q^{-2-3+1+3} = q^{-1}$, and the claim follows from Theorem 3.2(iii). □

4. Counting general decomposable polynomials

Theorem 3.2 provides a satisfactory result in the tame case, where $p \nmid n$. Most of the preparatory work cited in Section 2 is geared towards the wild case. The upper bound of Theorem 3.2(i) still holds, and we now present the resulting lower bounds.

We have to deal with an annoyingly large jungle of case distinctions. To keep an overview, we reduce it to the single tree of Figure 4.1. Its branches correspond to the various bounds on equal-degree collisions (Fact 2.12) and on distinct-degree collisions (Fact 2.13). Since at each internal vertex, the two branches are complementary, the leaves cover all possibilities. We use a top down numbering of the vertices according to the branches; as an example, II.B.ii.b.β is the rightmost leaf at the lowest level. Furthermore, if a branching is left out, as in II.B, then a bound at that vertex holds for all descendants, which comprise three internal vertices and five leaves in this example.

One of the two difficult cases without a lower bound $1-\varepsilon$ is $n = p^2$ (I.B). This is completely resolved by Blankertz *et al.* (2013), where the exact size of D_{p^2} is determined. We include the weaker result that follows in that case from the present method, but forego a proof.

Theorem 4.1. *Let $\mathbb{F}_q$ be a finite field of characteristic p with q elements, ℓ the smallest prime divisor of the composite integer $n \geq 2$, and α_n as in (3.3). Then we have the following bounds on $\#D_n$ over $\mathbb{F}_q$.*

(i) The lower bounds in Table 4.1 hold.

(ii) If the "upper" column in Table 4.1 contains a 1, then $\#D_n \leq \alpha_n$.

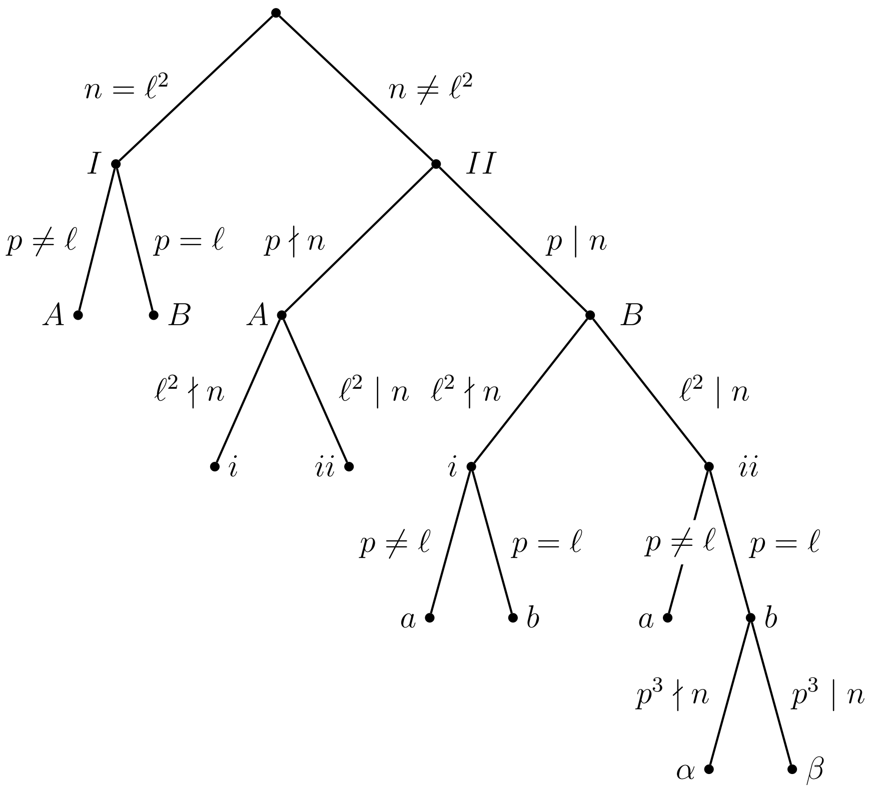

Figure 4.1: The tree of case distinctions for estimating $\#D_n$.

leaf in Figure 4.1	lower bound on $\#D_n/\alpha_n$	up- per
I.A	1	1
I.B	$\frac{1}{2}(1+\frac{1}{p+1})(1-q^{-2})+q^{-p+1}+q^{-p} > 1/2$	1
II.A.i	$1-\beta_n^* \geq 1-q^{-n/\ell-\ell+n/\ell^2+3}$	
II.A.ii	$1-q^{-n/\ell+\ell+n/\ell^2-1}/2$	
II.B.i.a	$1-(q^{-1}+q^{-p+1}+q^{-n/\ell-\ell+n/\ell^2+3})/2$	
II.B.i.b	$1-(q^{-1}-q^{-p})/2$	1
II.B.ii.a	$1-(q^{-1}+q^{-p+1}-q^{-p}+q^{-\ell+1})/2$	
II.B.ii.b.α	$\frac{1}{2}(\frac{3}{2}+\frac{1}{2p+2}-q^{-1}-\frac{q^{-2}}{2}(1+\frac{1}{p+1})-q^{-p+1})$	
II.B.ii.b.β	$1-q^{-1}-q^{-p+1}$	1

Table 4.1: The bounds at the leaves of Figure 4.1.

PROOF. We recall $D_{n,e}$ from (2.4), β_n from (3.4), the superscript $+$ for non-Frobenius from (2.11), and set at each vertex in Figure 4.1

$$\nu = \frac{\# D_n}{\alpha_n},\ \nu_0 = \frac{\# D^+_{n,\ell}}{\alpha_n},\ \nu_1 = \frac{\# D^+_{n,n/\ell}}{\alpha_n},\ \nu_2 = \frac{\#(D^+_{n,\ell} \cap D^+_{n,n/\ell})}{\alpha_n},\ \nu_3 = \frac{\# D^{\varphi}_n}{\alpha_n}.$$

Then $\nu = \nu_0 + \nu_3$ if $n = \ell^2$, and otherwise

$$\nu_0 + \nu_1 - \nu_2 + \nu_3 \leq \nu \leq 1 + \beta_n - \nu_2 - \nu_3. \tag{4.2}$$

In the lower bound, $\nu_0 + \nu_1 - \nu_2$ counts the non-Frobenius compositions of the dominant contributions $D_{n,\ell}$ and $D_{n,n/\ell}$, and ν_3 adds the Frobenius compositions. Theorem 3.2(i) yields the upper bound $1 + \beta_n - \nu_2$. We may subtract ν_3 since the Frobenius compositions have been counted twice, in $D_{n,p}$ and $D_{n,n/p}$; of course, ν_3 is nonzero only if $p \mid n$.

The proof proceeds in two stages. In the first one, we indicate for some vertices V bounds $\lambda_i(V)$ with the following properties:

$$\nu_0 \geq \lambda_0,\ \nu_1 \geq \lambda_1,\ \lambda_2 \geq \nu_2 \geq \lambda_4.$$

Such a bound at V applies to all descendants of V. The value λ_4 only intervenes in the upper bound on ν, and we sometimes forego its detailed calculation and simply use $\lambda_4 = 0$. In the second stage, we assemble those bounds for each leaf, according to (4.2).

Throughout the proof, $d \geq 0$ denotes the multiplicity of p in n, and $s = \lfloor n/\ell^2 \rfloor$. In the first stage, we use Theorem 3.2(v) at I.A:

$$\nu(\text{I.A}) = 1.$$

At II.A, we have from Fact 2.7

$$\lambda_0(\text{II.A}) = \lambda_1(\text{II.A}) = \frac{1}{2},$$

and since $p \nmid n$,

$$\nu_3(\text{II.A}) = 0.$$

Vertex II.A.i is dealt with in Fact 2.13(i):

$$\begin{aligned} \lambda_2(\text{II.A.i}) &= \beta^*_n = q^{-n/\ell - \ell + s + 3}, \\ \lambda_4(\text{II.A.i}) &= \frac{1}{2} q^{-n/\ell - \ell + s + 3}. \end{aligned}$$

Since $\ell \mid n/\ell$ at II.A.ii, Fact 2.13(iv) yields

$$\lambda_2(\text{II.A.ii}) = \lambda_4(\text{II.A.ii}) = \frac{1}{2} q^{-n/\ell + \ell + s - 1}.$$

Since $p \mid n$ at II.B, Fact 2.14(ii) implies that

$$\nu_3(\text{II.B}) = \frac{1}{2} q^{-n/\ell - \ell + n/p + 1}.$$

We now let V be one of II.B.i.a or II.B.ii.a. Then we have

$$\lambda_0(V) = \frac{1}{2},$$

by Fact 2.7. Applying Fact 2.12 to $D_{n,n/\ell}$ at V, we have $d \geq 1$, $r = p^d \neq \ell = m$, $k = n/\ell$, and

$$\mu = \gcd(p^d - 1, \ell) \text{ is either 1 or } \ell. \tag{4.3}$$

In the first case, where $\mu = 1$, we have

$$\nu_1(V) \geq \frac{1}{2}\big(1 - q^{-1}(1 + q^{-p+2}\frac{(1-q^{-1})^2}{1-q^{-p}})\big)(1 - q^{-n/\ell})$$

from Fact 2.12(i). In the second case, where $\mu = \ell$, we have $p > \ell = \mu \geq 2$. We first assume that $r \neq 3$. Then $r - 1 = p^d - 1$ is not a prime number, and $r^* = (r-1)/\ell \geq 2$, so that the last bound in Fact 2.12(ii) applies and

$$\nu_1(V) \geq \frac{1}{2}\big((1 - q^{-1}(1 + q^{-p+2}\frac{(1-q^{-1})^2}{1-q^{-p}})\big)(1 - q^{-n/\ell}) - \frac{2}{3} q^{-n/\ell}(1 - q^{-1})^2. \tag{4.4}$$

If $r = 3$, then $p = 3$, $\mu = \ell = 2$, $r^* = 1$, and according to the second bound in Fact 2.12(ii), we have to replace the last summand in (4.4) by

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

Since $2/3 < q(1 + q^{-1})/2$, the latter term dominates in absolute value the one in (4.4). Its value is at least $-q^{-n/\ell+1}/2$, and we find for $\mu = \ell$ that

$$\begin{aligned} \nu_1(V) &\geq \frac{1}{2} - \frac{q^{-1}}{2}\big(1 + q^{-p+2}(1 - q^{-1})\big) \\ &\quad - \frac{q^{-n/\ell}}{2}(1 - q^{-1} - q^{-p+1}\frac{(1-q^{-1})^2}{1-q^{-p}} + q) \\ &> \frac{1}{2}\big(1 - q^{-1} - q^{-p+2} + q^{-p} - q^{-n/\ell}(q+1)\big). \end{aligned}$$

Thus we may take the last value as λ_1(II.B.i.a) and λ_1(II.B.ii.a). Furthermore, Fact 2.13(iii) yields

$$\lambda_2(\text{II.B.i.a}) = \frac{1}{2} q^{-n/\ell - \ell + 3}(q^s - q^{\lfloor s/p \rfloor}).$$

When V is II.B.i.b or II.B.ii.b, we have for λ_0 in the notation of Fact 2.12 that $k = r = p \neq n/p = m$ and $\mu = \gcd(p-1, n/p) = 1$, since all proper divisors of n/p are at least $\ell = p$. Thus we may apply Fact 2.12(i) to find

$$\begin{aligned}\lambda_0(V) &= \frac{1}{2}(1-q^{-p})\big(1-q^{-1}(1+q^{-p+2}\frac{(1-q^{-1})^2}{1-q^{-p}})\big)\\ &= \frac{1}{2}(1-q^{-1}-q^{-p+1}+q^{-p}).\end{aligned}$$

At II.B.i.b, we have $p \nmid n/p$, so that Fact 2.7 for $D_{n,n/p}$ implies

$$\lambda_1(\text{II.B.i.b}) = \frac{1}{2},$$

and Fact 2.13(ii) yields

$$\lambda_2(\text{II.B.i.b}) = \lambda_4(\text{II.B.i.b}) = 0.$$

At II.B.ii.a, we have $\ell < p$, and Fact 2.13(vii) allows

$$\lambda_2(\text{II.B.ii.a}) = \frac{1}{2}q^{-\ell+\lceil \ell/p \rceil} = \frac{1}{2}q^{-\ell+1}.$$

At II.B.ii.b.α, we have $k = n/p$ and $r = p = z = m$ in the notation of Fact 2.12(iii) for $D_{n,n/p}$, so that

$$\begin{aligned}\lambda_1(\text{II.B.ii.b.}\alpha) = \frac{1}{2}(1-q^{-1})(&\frac{1}{2}+\frac{1+q^{-1}}{2p+2}+\frac{q^{-1}}{2}\\ &-q^{-n/p}\frac{1-q^{-p+1}}{1-q^{-p}}-q^{-p+1}\frac{1-q^{-1}}{1-q^{-p}}).\end{aligned}$$

Furthermore, from Fact 2.13(viii) we take

$$\lambda_2(\text{II.B.ii.b}) = \frac{1}{2}q^{-n/p^2+\lceil n/p^3 \rceil}.$$

At II.B.ii.b.β, we have for $D_{n,n/p}$ that $k = n/p$, $r = p^{d-1} \neq p = m$, since $d \geq 3$, and $\mu = \gcd(r-1, m) = \gcd(p^{d-1}-1, p) = 1$, so that Fact 2.12(i) yields

$$\begin{aligned}\lambda_1(\text{II.B.ii.b.}\beta) &= \frac{1}{2}\big(1-q^{-1}(1+q^{-p+2}\frac{(1-q^{-1})^2}{1-q^{-p}})\big)(1-q^{-n/p})\\ &= \frac{(1-q^{-1})(1-q^{-p+1})(1-q^{-n/p})}{2(1-q^{-p})}.\end{aligned}$$

Fact 2.13(ix) says that

$$\lambda_4(\text{II.B.ii.b.}\alpha) = \frac{1}{2} q^{-n/p+p+n/p^2-1}(1-q^{-1})(1-q^{-p+1}).$$

In the second stage of the proof, we now find bounds on ν at the leaves according to (4.2), using the values determined above.

I.A:

$$\nu = \lambda_0(\text{I.A}) = 1,$$

II.A.i:

$$\begin{aligned} \nu &\le 1 + \beta_n - \lambda_4(\text{II.A.i}) = 1 + \beta_n - \frac{1}{2} q^{-n/\ell-\ell+s+3} \le 1 + \beta_n, \\ \nu &\ge \lambda_0(\text{II.A}) + \lambda_1(\text{II.A}) - \lambda_2(\text{II.A.i}) = 1 - \beta_n^*. \end{aligned}$$

A calculation similar to the one in Proposition 3.14 provides conditions under which the upper bound is at most 1. We do not pursue this here.

II.A.ii:

$$\begin{aligned} \nu &\ge \lambda_0(\text{II.A}) + \lambda_1(\text{II.A}) - \lambda_2(\text{II.A.ii}) \\ &= \frac{1}{2} + \frac{1}{2} - \frac{1}{2} q^{-n/\ell+\ell+s-1} = 1 - \frac{1}{2} q^{-n/\ell+\ell+s-1}. \end{aligned}$$

II.B.i.a:

For the lower bound, we find

$$\begin{aligned} \nu &\ge \lambda_0(\text{II.B.i.a}) + \lambda_1(\text{II.B.i.a}) - \lambda_2(\text{II.B.i.a}) + \nu_3(\text{II.B}) \\ &= \frac{1}{2} + \frac{1}{2}(1 - q^{-1}(1+q^{-p+2}) + q^{-p} - q^{-n/\ell}(q+1)) \\ &\quad - \frac{1}{2} q^{-n/\ell-\ell}(q^{s+3} - q^{\lfloor s/p \rfloor+3}) + \frac{1}{2} q^{-\ell-n/\ell+n/p+1} \\ &\ge 1 - \frac{1}{2}(q^{-1} + q^{-p+1}) + \frac{q^{-p}}{2} - \frac{q^{-n/\ell}}{2}(q+1+q^{s-\ell+3} - q^{n/p-\ell+1}). \end{aligned} \tag{4.5}$$

At the present leaf, we have $n = a\ell p$ with $p > \ell \ge 2$ and $a \ge 1$. Thus $n/\ell \ge p$ and

$$q^{-p} \ge q^{-n/\ell}.$$

Furthermore, $n/p \ge \ell$ and

$$q^{n/p-\ell+1} \ge q.$$

It follows that

$$\nu \ge 1 - \frac{1}{2}(q^{-1} + q^{-p+1} + q^{-n/\ell-\ell+s+3}). \tag{4.6}$$

II.B.i.b:

$$\nu \leq 1 + \beta_n - \lambda_4(\text{II.B.i.b}) - \nu_3(\text{II.B}) = 1 + \beta_n - 0 - \frac{1}{2}q^{-p+1}.$$

We claim that $\beta_n \leq \frac{1}{2}q^{-p+1}$, so that $\nu \leq 1$. We may assume that $n \notin \{\ell^2, \ell\ell_2\}$, since otherwise $\beta_n = 0$. Setting $\mu = \log_q(2/(1-q^{-1}))$, we have $0 < \mu \leq 2$ and $2\beta_n = q^{-c+\mu} \leq q^{-c+2}$, so that it suffices to show

$$\ell - 1 = p - 1 \leq c - 2 = \frac{(n - \ell\ell_2)(\ell_2 - \ell)}{\ell\ell_2} - 2.$$

Abbreviating $a = n/\ell\ell_2$, this is equivalent to

$$\frac{\ell + 1}{\ell_2 - \ell} + 1 \leq a. \tag{4.7}$$

Since $p = \ell$ and $p^2 \nmid n$, we have $\ell \nmid a$ and $a \geq \ell_2 > \ell$, by the minimality conditions on ℓ and ℓ_2. If $\ell_2 \geq \ell + 2$, then (4.7) holds. If $\ell_2 = \ell + 1$, then $\ell = 2$ and $a \geq 4$ is required for (4.7). Since $2 \nmid a$, this holds except in the case $a = 3$, corresponding to $n = 18$ and $p = 2$. One checks that $\beta_{18} \leq \frac{1}{2}q^{-1}$ for $q \geq 4$. For $q = 2$, we have to go back to (3.12) and check that $\#D_{18}^{\varphi} = q^8$ and

$$\#D_{18} \leq \alpha_{18} + 2q^7 - \#D_{18}^{\varphi} = \alpha_{18}.$$

For the lower bound, we have

$$\begin{aligned}\nu &\geq \lambda_0(\text{II.B.i.b}) + \lambda_1(\text{II.B.i.b}) - \lambda_2(\text{II.B.i.b}) + \nu_3(\text{II.B}) \\ &= \frac{1}{2}(1 - q^{-1} - q^{-p+1} + q^{-p}) + \frac{1}{2} - 0 + \frac{1}{2}q^{-p+1} \\ &= 1 - \frac{1}{2}(q^{-1} - q^{-p}).\end{aligned}$$

At II.B.ii.a, we have

$$\begin{aligned}\nu &\geq \lambda_0\big(\text{II.B.ii.a}\big) + \lambda_1\big(\text{II.B.ii.a}\big) - \lambda_2\big(\text{II.B.ii.a}\big) + \nu_3\big(\text{II.B}\big) \\ &= \frac{1}{2} + \frac{1}{2} - \frac{q^{-1}}{2}(1 + q^{-p+2}) + \frac{q^{-p}}{2} - \frac{q^{-n/\ell}(q+1)}{2} \\ &\quad - \frac{q^{-\ell+1}}{2} + \frac{q^{-n/\ell-\ell+n/p+1}}{2} \\ &= 1 - \frac{1}{2}(q^{-1} + q^{-p+1}) + \frac{q^{-p}}{2} - \frac{q^{-\ell+1}}{2} + \frac{q^{-n/\ell}}{2}(q^{n/p-\ell+1} - q - 1).\end{aligned}$$

Since $n = a\ell^2 p$ with $a \geq 1$, we have $n/p \geq \ell^2 > \ell + 1$, and

$$\begin{aligned} q^{n/p-\ell+1} &> q^2 > q+1, \\ \nu &> 1 - \frac{1}{2}(q^{-1} + q^{-p+1} - q^{-p} + q^{-\ell+1}). \end{aligned}$$

II.B.ii.b.α:

$$\begin{aligned} \nu &\geq \lambda_0(\text{II.B.ii.b}) + \lambda_1(\text{II.B.ii.b.}\alpha) - \lambda_2(\text{II.B.ii.b}) + \nu_3(\text{II.B}) \\ &= \frac{1}{2}(1 - q^{-1} - q^{-p+1} + q^{-p}) + \frac{1}{2}(1-q^{-1})(\frac{1}{2} + \frac{1+q^{-1}}{2p+2} + \frac{q^{-1}}{2} \\ &\quad - q^{-n/p}\frac{1-q^{-p+1}}{1-q^{-p}} - q^{-p+1}\frac{1-q^{-1}}{1-q^{-p}}) - \frac{1}{2}q^{-n/p^2+\lceil n/p^3 \rceil} + \frac{1}{2}q^{-p+1} \\ &= \frac{1}{2}(\frac{3}{2} + \frac{1-(p+2)q^{-2}}{2p+2} - q^{-1} - \frac{q^{-p}(q-3+q^{-1}+q^{-p})}{1-q^{-p}} \\ &\quad - q^{-n/p^2+\lceil n/p^3 \rceil} - q^{-n/p}\frac{(1-q^{-1})(1-q^{-p+1})}{1-q^{-p}}). \end{aligned} \tag{4.8}$$

We have $n = ap^2$ with $a > p$ and all prime divisors of a larger than p. If $p \geq 3$, then $a \geq p+2$ and

$$\begin{aligned} a &\geq p + 2 > p + 1 + \frac{1}{p-1} = \frac{p^2}{p-1}, \\ a &\geq p + \frac{a}{p}, \\ a &\geq p + \left\lceil \frac{a}{p} \right\rceil, \\ q^{-p} &\geq q^{-n/p^2+\lceil n/p^3 \rceil}. \end{aligned} \tag{4.9}$$

We may now assume that $p = 2$. If $a \geq 5$, then

$$a - \frac{a}{2} = \frac{a}{2} \geq 2 = p,$$

and (4.9) again holds. In the remaining case $p = 2$ and $a = 3$, we have $n = 12$ and (4.9) is false. Furthermore, we have $p < n/p$ for all n and bound the sum of the three last terms in (4.8) as follows for $n \neq 12$.

$$\begin{aligned} &\frac{q^{-p}(q-3+q^{-1}+q^{-p})}{1-q^{-p}} + q^{-n/p^2+\lceil n/p^3 \rceil} + q^{-n/p}\frac{(1-q^{-1})(1-q^{-p+1})}{1-q^{-p}}) \\ &< \frac{q^{-p+1} - 3q^{-p} + q^{-p-1} + q^{-2p} + q^{-p}(1-q^{-p}) + q^{-p}(1-q^{-1}-q^{-p+1}+q^{-p})}{1-q^{-p}} \\ &= q^{-p+1}(1-q^{-1}) < q^{-p+1}. \end{aligned}$$

Thus for $n \neq 12$ the following holds:

$$\nu \geq \frac{1}{2}\big(\frac{3}{2} + \frac{1-(p+2)q^{-2}}{2p+2} - q^{-1} - q^{-p+1}\big).$$

For $n = 12$, Example 7.7 of von zur Gathen (2012) shows that $\lambda_2(\text{II.B.ii.b}) = t/\alpha_{12} \leq q^{-2} = q^{-p}$, and we may substitute this to the same effect as (4.9), so that the last inequality also holds for $n = 12$.

II.B.ii.b.β:

$$\begin{aligned}
\nu &\geq \lambda_0(\text{II.B.ii.b}) + \lambda_1(\text{II.B.ii.b.}\beta) - \lambda_2(\text{II.B.ii.b}) + \nu_3(\text{II.B})\\
&= \frac{1}{2}(1 - q^{-1} - q^{-p+1} + q^{-p}) + \frac{1}{2}\frac{(1-q^{-1})(1-q^{-p+1})(1-q^{-n/p})}{1-q^{-p}}\\
&\quad - \frac{1}{2}q^{-n/p^2+\lceil n/p^3\rceil} + \frac{1}{2}q^{-p+1}\\
&= 1 - q^{-1} - \frac{q^{-p+1}}{2}\cdot\frac{(1-q^{-1})^2}{1-q^{-p}} + \frac{q^{-p}}{2}\\
&\quad - \frac{q^{-n/p}(1-q^{-1}-q^{-p+1}+q^{-p})}{2(1-q^{-p})} - \frac{1}{2}q^{-n/p^2+n/p^3}.
\end{aligned} \tag{4.10}$$

Since $n \geq p^3$, we have

$$\begin{aligned}
n/p &\geq p^2 > p,\\
q^{-p} &> q^{-n/p},\\
n(p-1) &\geq p^3(p-1),\\
-p+1 &\geq -\frac{n}{p^2} + \frac{n}{p^3},
\end{aligned}$$

$$\nu \geq 1 - q^{-1} - \frac{q^{-p+1}}{2} - \frac{1}{2}q^{-n/p^2+n/p^3} \geq 1 - q^{-1} - q^{-p+1}. \tag{4.11}$$

□

At I.B and II.B.ii.b.α, $p = \ell$ divides n exactly twice, for which we write $p^2 \| n$. Except at these two leaves, the lower bounds are of the satisfactory form $1 - O(q^{-1})$. For small values of q, the entry in Table 4.1 at II.B.ii.b.α provides the lower bounds in Table 4.2.

5. Proof of Main Theorem

The multitude of bounds, driven by the estimates of Section 2, is quite confusing. The Main Theorem in the introduction provides simple and universally applicable estimates. Before we come to its proof, we note that for special values, in particular for small ones, of our parameters one may find better bounds in other parts of this paper.

q	$\#D_n/\alpha_n \geq$
2	$1/6 > 0.1666$
3	$259/468 > 0.5534$
4	$133/240 > 0.5541$
5	$106091/156200 > 0.6791$
7	$56824055/80707116 > 0.7040$
8	$2831/4032 > 0.7021$
9	$88087/117936 > 0.7469$

Table 4.2: The lower bounds of Table 4.1 at the leaf II.B.ii.b.α, where $\ell^2 = p^2 \parallel n \neq p^2$.

Proof (Main Theorem). (i) follows from $2 \leq \ell \leq \sqrt{n} \leq n/2$ and $0 \leq (\ell - \sqrt{n})^2 = \ell^2 - 2\ell\sqrt{n} + n$. The first upper bound on $\#D_n$ in (ii) is Corollary 3.16(ii). It remains to deduce the lower bounds. Starting with the last claim, we note that (v) is Corollary 3.16(iii). In the assumption of (iv), only the leaves I.B and II.B.ii.b.α are disallowed. We claim that Theorem 4.1 implies

$$\nu \geq 1 - 2q^{-1} \tag{5.1}$$

at all leaves but these two. Leaf I.A is clear. At II.A.i, we have $n = a\ell$, where $a > \ell$ and all prime factors of a are larger than ℓ. When $a \geq \ell + 2$, then

$$\begin{aligned} \frac{n}{\ell} - \frac{n}{\ell^2} = a(1 - \frac{1}{\ell}) \geq (\ell+2)(1 - \frac{1}{\ell}) &= \ell + 1 - \frac{2}{\ell} \geq \ell, \\ \beta_n^* \leq q^{-n/\ell - \ell + n/\ell^2 + 3} &\leq q^{3-2\ell} \leq q^{-1}, \\ \nu \geq 1 - \beta_n^* &\geq 1 - q^{-1}. \end{aligned}$$

When $a = \ell + 1$, then $\ell = 2$, $a = 3$, $n = 6$, and by Theorem 3.2(iii) we have again

$$\frac{\#D_6}{\alpha_6} \geq 1 - \beta_6^* = 1 - q^{-1}.$$

At II.A.ii, we have $n = a\ell^2$ with $a \geq \ell$. When $a = \ell = 2$, hence $n = 8$, then Table 4.1 shows $\nu \geq 1 - q^{-1}/2 > 1 - 2q^{-1}$. When $a \geq 3$, then $n/3\ell^2 \geq 1$ and the bound in (iv) follows from the one in (v).

At II.B.i.a, we consider the inequality

$$-\frac{n}{\ell} - \ell + s + 3 \leq -1, \tag{5.2}$$

with $s = \lfloor n/\ell^2 \rfloor \le n/\ell^2$. It holds for $\ell \ge 3$. When $\ell = 2$, it holds for $n \ge 8$, and one checks it for $n = 6$. Now $n = 4$ is case I and excepted here. Thus (5.2) holds in all cases at II.B.i.a, and (4.6) implies that $\nu \ge 1 - 3q^{-1}/2 > 1 - 2q^{-1}$.

(5.1) is clear for II.B.i.b and II.B.ii.b.β. At II.B.ii.a, we have $q^{-1} + q^{-p+1} + q^{-\ell+1} < 3q^{-1}$, and (5.1) follows from Table 4.1. This concludes the proof of (iv).

In (iii), the second inequality follows from (i) and $(3 - 2q^{-1})/4 \ge 1/2$. For the first inequality, we have $1 - 2q^{-1} \ge (3 - 2q^{-1})/4$ when $q > 5$. Thus the lower bound in (iv) implies the one in (iii) and it remains to prove (iii) at II.B.ii.b.α.

We have for $p \ge 3$ and $q \ge 4$ that

$$\begin{aligned} 1 \ge q^{-2}(3q+4) \ge q^{-2}(3p+4) &= q^{-2}(p+2) + q^{-2}(2p+2), \\ \frac{1}{2p+2} > \frac{q^{-2}(p+2)}{2p+2} + q^{-2} &\ge \frac{q^{-2}}{2}(1 + \frac{1}{p+1}) + q^{-p+1}. \end{aligned}$$

From Table 4.1 we find

$$\begin{aligned} \nu &\ge \frac{1}{2}(\frac{3}{2} + \frac{1}{2p+2} - q^{-1} - \frac{q^{-2}}{2}(1 + \frac{1}{p+1}) - q^{-p+1}) \\ &> \frac{3}{4} - \frac{q^{-1}}{2} = \frac{3 - 2q^{-1}}{4}. \end{aligned} \tag{5.3}$$

For $q = 3$, there is no claim in (iii). When $p = 2$, then

$$\nu \ge \frac{5}{6} - q^{-1} - \frac{q^{-2}}{3} \tag{5.4}$$

by (5.3). It follows that $\nu \ge (3 - 2q^{-1})/4$ when $q \ge 8$. For $q \in \{2, 4\}$, we use the bound (4.8). At the current leaf, we can write $n = ap^2 > p^2$ with all prime divisors of a greater than p, and split the lower bound into two summands:

$$\begin{aligned} \nu_q &= \frac{1}{2}(\frac{3}{2} + \frac{1 - (p+2)q^{-2}}{2p+2} - q^{-1} - \frac{q^{-p+1}(1 - 3q^{-1} + q^{-2} + q^{-p-1})}{1 - q^{-p}}), \\ \varepsilon_{q,n} &= \frac{1}{2}(q^{-a+\lceil a/p \rceil} + q^{-ap}\frac{(1 - q^{-1})(1 - q^{-p+1})}{1 - q^{-p}}), \end{aligned}$$

so that $\nu \ge \nu_q - \varepsilon_{q,n}$, and $\varepsilon_{q,n}$ is monotonically decreasing in a.

For $q = 3$, we have $a \geq 5$,

$$\begin{aligned}
\nu_3 &= \frac{203}{27 \cdot 13} > 0.5783, \\
\varepsilon_{3,n} &\leq \frac{1}{2}(3^{-a+\lceil a/3 \rceil} + \frac{8}{13} \cdot 3^{-3a}) \leq \varepsilon_{3,45} = \frac{1}{2}(3^{-5+2} + \frac{8}{13} \cdot 3^{-15}) \\
&= \frac{1}{54} + \frac{4}{13} \cdot 3^{-15} < 0.0186, \\
\nu &\geq \nu_3 - \varepsilon_{3,n} > 0.5598 > 1/2.
\end{aligned}$$

For $p = 2$, we find

$$\begin{aligned}
\nu_q &= \frac{5}{6} - q^{-1} + q^{-2}(\frac{1}{6} + \frac{1}{1+q^{-1}}) \\
\varepsilon_{q,n} &= \frac{1}{2}(q^{-(a-1)/2} + q^{-2a} \cdot \frac{1-q^{-1}}{1+q^{-1}}).
\end{aligned}$$

For $q \geq 8$ and $n \geq 20$, we have

$$\begin{aligned}
\nu_q - \frac{3-2q^{-1}}{4} &= \frac{1 - 5q^{-1} + 8q^{-2} + 2q^{-3}}{12(1+q^{-1})} \\
&> \frac{1}{2}(q^{-2} + q^{-10} \frac{1-q^{-1}}{1+q^{-1}}) = \varepsilon_{q,20} \geq \varepsilon_{q,n}.
\end{aligned}$$

This shows (iii) except for $n = 12$, where

$$\nu_q - \frac{3-2q^{-1}}{4} > \frac{q^{-1} + q^{-2} + q^{-6} - q^{-7}}{2(1+q^{-1})} = \varepsilon_{q,12}$$

for $q \geq 16$. The last remaining case $q = 8$ and $n = 12$ is settled by Table 5.1. This finishes the proof of (iii).

For (ii), we have $1-2q^{-1} \geq 1/2$ for $q \geq 4$, $1-q^{-1} \geq 1/2$ and $(3-2q^{-1})/4 \geq 1/2$ for all q, so that (iii) or (iv) imply the lower bound in (ii). It remains to check $\nu \geq 1/2$ in three cases:

- $q \in \{2, 3\}$ at all leaves,
- leaf I.B,
- leaf II.B.ii.b.α for $q \leq 5$.

We go through the leaves in order. I.A is clear and I.B is shown elsewhere. At II.B.i, we have $2\ell^2/(\ell-1) \leq n^2$ when $\ell \geq 3$, which implies $-n/\ell - \ell + \lfloor n/\ell^2 \rfloor + 3 \leq 1$ and $\nu \geq 1 - q^{-1}$. This also holds for $\ell = 2$ except when $n = 4$, but that is leaf I.B.

For the remaining values $q \in \{2, 4\}$ or $n \in \{12, 20\}$, we note the values

$$\begin{aligned}
\nu_2 &= \frac{13}{24} > 0.54166, \\
\nu_4 &= \frac{103}{160} = 0.64375, \\
\varepsilon_{q,12} &= \frac{1}{2}(q^{-1} + q^{-6} \cdot \frac{1 - q^{-1}}{1 + q^{-1}}), \\
\varepsilon_{q,20} &= \frac{1}{2}(q^{-2} + q^{-10} \cdot \frac{1 - q^{-1}}{1 + q^{-1}}).
\end{aligned}$$

We find that $\nu \geq (3 - 2q^{-1})/4$ for $q \geq 8$ and $n = 20$, and for $q \geq 16$ and $n = 12$. Table 5.1 shows that this also holds for $(q, n) = (8, 12)$. When $q = 4$, we have $\nu \geq 1/2$ for $n \geq 20$ by the above, and according to Table 5.1 also for $n = 12$.

q, n	$\#D_n$	α_n	$\#D_n/\alpha_n \geq$
$2, 4$	3	4	0.7500
$2, 8$	18	32	0.5625
$2, 12$	118	128	0.9218
$2, 16$	381	512	0.7441
$2, 20$	1632	2048	0.7968
$2, 24$	7132	8192	0.8706
$2, 28$	24960	32768	0.7617
$2, 36$	410800	524288	0.7835
$4, 4$	11	16	0.6875
$4, 12$	8404	8192	1.0258
$8, 4$	43	64	0.6718
$8, 12$	542536	524288	1.0348
$16, 4$	171	256	0.6679
$32, 4$	683	1024	0.6669
$64, 4$	2731	4096	0.6667
$128, 4$	10923	16384	0.6666
$256, 4$	43691	65536	0.6666
$3, 9$	69	81	0.8518
$9, 9$	6261	6561	0.9542
$5, 25$	389905	390625	0.9981

Table 5.1: Decomposable polynomials of degree n over $\mathbb{F}_q$.

When $q = 2$, the general bounds above only show that $\nu \geq 1/4$ for $n \geq 28$. However, a different and simple approach gives a better bound for $n = 4a$

with an odd $a \geq 3$ over $\mathbb{F}_2$, as needed for (ii). We exploit the special fact that $x^2 + x \in \mathbb{F}_2[x]$ is the only quadratic original polynomial that is not a square.

Any $g \in \mathbb{F}_2[x]$ is uniquely determined by $f = g \circ (x^2 + x)$, due to the uniqueness of the Taylor expansion. The number of original g of degree $2a$ and that are not a square is $2^{2a-1} - 2^{a-1}$, so that $\#D^+_{n,n/2} = 2^{n/2-1} - 2^{n/4-1}$. Similarly, $(x^2 + x) \circ h = (x^2 + x) \circ h^*$ with $h \neq h^*$ implies that $-1 = h^* - h$, so that one of the two polynomials is not original. Thus $\gamma_{n,2}$ is injective on the original polynomials, and $\#D^+_{n,2} = 2^{n/2-1} - 2^{n/4-1}$. Furthermore, Fact 2.13(viii) says that

$$t = \#(D^+_{n,2} \cap D^+_{n,n/2}) \leq 2^{n/4+\lceil n/8 \rceil} = 2^{3n/8+1/2}.$$

The number of Frobenius compositions (that is, squares) of degree n equals $\#D^{\varphi}_n = 2^{2a-1}$, and $\alpha_n = 2^{n/2+1}$. It follows that

$$\begin{aligned} \#D_n &\geq \#D^+_{n,2} + \#D^+_{n,n/2} - t + \#D^{\varphi}_n \\ &\geq 2 \cdot 2^{n/2-1}(1 - 2^{-n/4}) - 2^{3n/8+1/2} + 2^{n/2-1} \\ &= (\frac{3}{4} - 2^{-n/8-3/2} - 2^{-n/4-1})\alpha_n, \qquad (5.5) \\ \nu &\geq \frac{3}{4} - 2^{-5/2-3/2} - 2^{-5-1} = \frac{43}{64} > 0.67187 > 1/2 \end{aligned}$$

for $n \geq 20$. Using Table 5.1 for $n = 12$, we find $\nu > 1/2$ also for $q = 2$, and hence for all values at leaf II.B.ii.b.α. Now it only remains to prove $\nu \geq 1/2$ in (ii). The leaf II.B.ii.b.α has just been dealt with. Since $(3-2q^{-1})/4 \geq 1/2$ for all q, the claim follows from the bound in (iii) at the leaves I.A, II.A.i, II.A.ii, and II.B.i.b. At II.B.i.a, we have shown $\nu \geq 1 - 3q^{-1}/2 \geq 1/2$ for $q \geq 3$; since $p \neq \ell$ and hence $p \geq 3$ at this leaf, the claim follows. Similarly, we have at II.B.ii.a that $q \geq p \geq 3$ and $\nu \geq 1 - \frac{1}{2}(q^{-1} + q^{-\ell+1} + q^{-p+1} - q^{-p}) \geq 1 - q^{-1} - q^{-2} \geq 1/2$. We do not treat I.B, and only leaf II.b.ii.b.β remains.

We have $\ell = p$ and $p^3 \mid n$. The lower bound in Table 4.1 implies $\nu \geq 1/2$ for $q \geq 4$. When $q = 3$, (4.11) yields

$$\nu \geq 1 - \frac{1}{3} - \frac{1}{9} = \frac{5}{9} > \frac{1}{2}.$$

For $q = 2$, we have from (4.10)

$$\nu \geq \frac{1}{2} + \frac{1}{24} - \frac{2^{-n/2-1}}{3} - 2^{-n/8-1}.$$

When $n \geq 32$, this shows $\nu \geq 1/2$. For the smaller values $8, 16$, and 24 of n, the data in Table 5.1 are sufficient. □

Two features are worth noting. Firstly, our lower bounds are rather pessimistic when $q = 2$, yielding for $n = 12$ that $\nu \geq 47/384 > 0.1223$ by (4.8), $\nu \geq 3/16 = 0.1875$ from the special argument, compared to $\nu = 59/64 > 0.9218$ from our experiments in Table 5.1. Secondly, our lower bounds are strictly increasing in n, while the experiments show a decrease in ν from $n = 12$ to $n = 20$. Both features show that more work is needed to understand the case where $p = \ell$ and $p^2 \parallel n$.

6. Asymptotic bounds

Much effort has been spent here in arriving at explicit bounds, without asymptotics or unspecified constants. We now derive some conclusions about the asymptotic behavior. There are three parameters: the field size q, the characteristic p, and the degree n. When n is prime, then $\#D_n = \alpha_n = 0$, and prime values of n are excepted in the following. We consider the asymptotics in one parameter, where the other one is fixed, and also the special situations where $\gcd(q, n) = 1$. Furthermore, we denote as "$q, n \longrightarrow \infty$" the set of all infinite sequences of pairwise distinct (q, n). The cases $p^2 \parallel n$ are the only ones where Table 4.1 does not show that $\nu \longrightarrow 1$.

THEOREM 6.1. *Let $\nu_{q,n} = \#D_n/\alpha_n$ over $\mathbb{F}_q$. We only consider composite n.*

(i) For any q, we have

$$\limsup_{n\to\infty} \nu_{q,n} = 1,$$

$$\lim_{\substack{n\to\infty \\ \gcd(q,n)=1}} \nu_{q,n} = 1,$$

$$\frac{1}{2} \leq \nu_{q,n} \text{ for any } n,$$

$$\frac{3-2q^{-1}}{4} \leq \nu_{q,n} \text{ for any } n, \text{ if } n \neq p^2 \text{ and } q \geq 5.$$

(ii) Let n be a composite integer and ℓ its smallest prime divisor. Then

$$\limsup_{q\to\infty} \nu_{q,n} = 1,$$

$$\liminf_{q\to\infty} \nu_{q,n} \begin{cases} \geq \frac{1}{2}(1 + \frac{1}{\ell+1}) & \text{if } n = \ell^2, \\ \geq \frac{1}{4}(3 + \frac{1}{\ell+1}) & \text{if } \ell^2 \parallel n \text{ and } n \neq \ell^2, \\ = 1 & \text{otherwise,} \end{cases}$$

$$\lim_{\substack{q\to\infty \\ \gcd(q,n)=1}} \nu_{q,n} = 1.$$

(iii) For any sequence $q, n \to \infty$, we have

$$\frac{1}{2} \le \liminf_{q,n\to\infty} \nu_{q,n} \le \limsup_{q,n\to\infty} \nu_{q,n} = 1,$$

$$\lim_{\substack{q,n\to\infty \\ \gcd(q,n)=1}} \nu_{q,n} = 1.$$

Proof. (i) We start with an upper bound. The conclusions of the Main Theorem are too weak for our current purpose, and we have to resort to Theorem 3.2. For the special n which are a square or a cube of a prime, or a product of two distinct primes, Theorem 3.2(i) says that $\nu_{q,n} \le 1$. For the other values, we set $d = n/\ell\ell_2$, and the upper bound on the lim sup follows if we show that $c = (d-1)(\ell_2 - \ell)$ is unbounded as n grows, since then $\beta_n = q^{-c}/(1-q^{-1})$ tends to zero, and $\nu_{q,n} \le 1 + \beta_n$. Since $\ell_2 - \ell \ge 1$, it is sufficient to show the unboundedness of d. When $n = \ell^\lambda$ is a power of a prime, we may assume by the above that $\lambda \ge 4$. Then $\ell_2 = \ell^2$, $\ell \le n^{1/4}$ and $d = \ell^{\lambda-3} \ge \ell^{\lambda/4} = n^{1/4}$ is unbounded.

If $n = \ell^\lambda r^\rho$ has exactly two prime factors $\ell < r$, we may assume that $\lambda + \rho \ge 3$. If $\lambda = 1$, then $\ell_2 = r$, $\rho \ge 2$, and $d = r^{\rho-1} \ge r^{(\rho+1)/3} > n^{1/3}$. We now assume that $\lambda \ge 2$. Then

$$\ell_2 = \begin{cases} \ell^2 & \text{if } \ell^2 < r, \\ r & \text{otherwise,} \end{cases}$$

$$d = \begin{cases} n/\ell^3 & \text{if } \ell^2 < r, \\ n/\ell r & \text{otherwise.} \end{cases} \tag{6.2}$$

We first treat the case where $\ell^2 < r$. If $\lambda = 2$, then

$$d = r^\rho/\ell > r^{\rho-1/2} \ge r^{(\rho+1)/4} > n^{1/4}.$$

If $\lambda = 3$, then

$$d = r^\rho > r^{(\rho+3/2)/3} > (\ell^2)^{1/2} r^{\rho/3} = n^{1/3}.$$

If $\lambda \ge 4$, then $d = \ell^{\lambda-3} r^\rho \ge \ell^{\lambda/4} r^\rho > n^{1/4}$. Next we deal with $r < \ell^2$. If $\rho = 1$, then we have $\lambda \ge 2$, and

$$d = \ell^{\lambda-1} \ge \ell^{(\lambda+2)/4} > \ell^{\lambda/4} r^{1/4} = n^{1/4}.$$

Finally, when λ, $\rho \ge 2$, we have

$$d = \ell^{\lambda-1} r^{\rho-1} \ge \ell^{\lambda/2} r^{\rho/2} = n^{1/2}.$$

In the last case, $n = \ell^{\lambda} r_2^{\rho_2} r_3^{\rho_3} \cdots$ has at least three distinct prime factors $\ell < r_2 < r_3 < \cdots$, and

$$d = \begin{cases} n/\ell^3 & \text{if } \lambda \geq 2 \text{ and } \ell^2 < r_2, \\ n/\ell r_2 & \text{otherwise.} \end{cases}$$

If $\lambda = \rho_2 = 1$, then $\ell r_2 < n^{2/3}$ and $d \geq n^{1/3}$. Otherwise, we apply the previous argument to $n^* = \ell^{\lambda} r_2^{\rho_2} = n/m$ and $d^* = d/m$, where $m = r_3^{\rho_3} \cdots = n\ell^{-\lambda} r_2^{-\rho_2}$. Then d^* equals the value d defined above for n^*, and

$$d = d^* m \geq (n^*)^{1/4} m > n^{1/4}.$$

In all cases, d is unbounded if n is. Thus $\limsup_{n\to\infty} \nu_{q,n} \leq 1$, and Theorem 3.2(v) for $n = \ell^2$ implies that $\limsup_{n\to\infty} \geq 1$.

If we only consider n with $\gcd(q, n) = 1$, then Theorem 3.2(iv) says that

$$\nu_{q,n} \geq 1 - \frac{1}{2} q^{-n/\ell + \ell + n/\ell^2 - 1} \geq 1 - q^{-n/\ell + \ell + n/\ell^2}.$$

When n is the product of two prime numbers, then $\nu_{q,n}$ tends to 1 for these special n by Theorem 3.2(iv). We may now assume that n has at least three prime factors. Then $n \geq \ell^3$, and

$$\begin{aligned} -\frac{n}{\ell} + \ell + \frac{n}{\ell^2} &= -\frac{n}{\ell}(1 - \frac{1}{\ell}) + \ell \leq -\frac{n}{2\ell} + \ell \leq -\frac{n}{2n^{1/3}} + n^{1/3} \\ &= -\frac{n^{2/3}}{2} + n^{1/3} \leq -n^{1/3} \end{aligned}$$

for $n \geq 64$. The second claim in (i) follows. The other two inequalities are in the Main Theorem.

(ii) The first claim follows from Corollary 3.16(ii), since $n \geq \ell^2$ and hence $\nu_{q,n} \leq 1 + q^{-1/3}$. For the other claims, we consider two subsequences of q: $q = \ell^e$ with $e \to \infty$, and q with $\gcd(q, \ell) = 1$; we denote the latter as q'. For $n = \ell^2$, the lower bound follows from the entries at I.A and I.B in Table 4.1, and for $\ell^2 \parallel n \neq \ell^2$ from the entry at II.B.ii.b.α. In all other cases, the Main Theorem guarantees that $\nu_{\ell^e,n}$ and $\nu_{q',n}$ tend to 1; see also (5.1).

(iii) We take some infinite sequence of (q, n) for which $\nu_{q,n}$ tends to $s = \limsup$. If all q occurring in the sequence are bounded, then (i) implies that $s \leq 1$. Otherwise, $\nu_{q,n} \leq 1 + q^{-1/3}$ is sufficient. The same case distinction yields the lower bound on the limit, using the Main Theorem (v). The lower bound on $\liminf$ follows from (i). □

Example 6.3. Let $n = ap^2$ with all prime factors of $a \geq 2$ larger than p, corresponding to leaf II.B.ii.b.α in Figure 4.1. We study D_n over $\mathbb{F}_q$, using the notation of (the proof of) Theorem 3.2. We have $\ell = p < \ell_2 \leq p^2 < n$,

$$c = \frac{(n - \ell\ell_2)(\ell_2 - \ell)}{\ell\ell_2} > \frac{n}{2\ell^2}.$$

With

$$E_2 = \{e \in \mathbb{N} \colon e \mid n, \ell_2 \leq e \leq n/\ell_2\},$$

we have, as in (3.11)

$$\sum_{e \in E_2} \#D_{n,e} \leq \sum_{e \in E_2} q^{u(e)} \leq q^{u(\ell)} \frac{2q^{-c}}{1 - q^{-1}} = \frac{q^{-c}}{1 - q^{-1}} \cdot \alpha_n \leq 2q^{-n/2\ell^2} \cdot \alpha_n.$$

We let

$$\begin{aligned} \lambda_{q,n} &= \frac{\#D^+_{n,p} + \#D^+_{n,n/p}}{\alpha_n}, \\ t &= \#(D^+_{n,p} \cap D^+_{n,n/p}). \end{aligned}$$

Then

$$\begin{aligned} \nu_{q,n} = \frac{\#D_n}{\alpha_n} &\leq \lambda_{q,n} - \frac{t}{\alpha_n} + \frac{\#D^\varphi_n}{\alpha_n} + \frac{\sum_{e \in E_2} \#D_{n,e}}{\alpha_n} \\ &\leq \lambda_{q,n} + \frac{q^{n/p-1}}{\alpha_n} + 2q^{-n/2\ell^2} = \lambda_{q,n} + \frac{q^{-p+1}}{2} + 2q^{-n/2p^2}. \end{aligned}$$

On the other hand, Fact 2.13(viii) says that

$$\begin{aligned} t &\leq q^{n/p+p-n/p^2+\lceil n/p^3 \rceil - 2}, \\ \nu_{q,n} &\geq \lambda_{q,n} - \frac{t}{\alpha_n} + \frac{\#D^\varphi_n}{\alpha_n} \geq \lambda_{q,n} - \frac{1}{2} q^{-n/p^2+\lceil n/p^3 \rceil - 2} + \frac{q^{-p+1}}{2}. \end{aligned}$$

Furthermore, we have

$$\begin{gathered} -\frac{n}{p^2} + \frac{n}{p^3} + 1 - 2 \leq -\frac{n}{2p^2}, \\ \big| \nu_{q,n} - (\lambda_{q,n} + \frac{q^{-p+1}}{2}) \big| \leq 2q^{-n/2p^2}. \end{gathered}$$

We have presented some bounds on $\lambda_{q,n}$, but they are not sufficient to determine its value in general, not even asymptotically. However, for $q = 2$ we have from (5.5)

$$\lambda_{q,n} = \frac{2^{n/2+1}(1 - 2^{-n/4})}{2 \cdot 2^{n/2+1}} = \frac{1 - 2^{-n/4}}{2},$$

$$\frac{3}{4} - 2^{-n/8-1/2} - 2^{n/4-1} \leq \nu_{2,n} \leq \frac{3}{4} + 2^{-n/8+1} - 2^{-n/4-1}. \tag{6.4}$$

◇

We have seen that $\nu_{q,n}$ tends to 1 unless $p^2 \parallel n$. Blankertz *et al.* (2013) show that

$$\lim_{e \longrightarrow \infty} \nu_{p^e,p^2} = \begin{cases} 2/3 & \text{if } p = 2, \\ 1 & \text{otherwise.} \end{cases}$$

Example 6.3 suggests to use a correction factor γ so that $\nu_{q,n}/\gamma$ tends to 1 also in the remaining case $p^2 \parallel n \neq p^2$.

Conjecture 6.5. *For any prime p and power q of p there exists $\gamma_q \in \mathbb{R}$ so that*

$$\lim_{\substack{n \longrightarrow \infty \\ p^2 \parallel n}} \nu_{q,n} = \gamma_q,$$

where the limit is only over those n whose smallest prime divisor is p.

If true, this would imply that $\#D_n \sim \gamma_q \alpha_n$ for these growing n. The inequalities (6.4) show that the conjecture holds for $q = 2$ with $\gamma_2 = 3/4$. Can we take $\gamma_q = 1$ for all other q?

Bodin *et al.* (2009) state without proof that $\#D_n \approx \frac{3}{4}\alpha_n$ over $\mathbb{F}_2$ for even $n \geq 6$. Assuming a standard meaning of the $\approx$ symbol, this is false unless $4 \parallel n$, in which case it is proven by (6.4).

Example 6.6. Theorem 4.1(ii) exhibits several situations where $\#D_n \leq \alpha_n$. One might wonder whether this always happens. We show that this is not the case. Table 5.1 presents two specific examples. For an infinite family, we take three primes $2 < \ell_1 < \ell_2 < \ell_3$, $n = \ell_1\ell_2\ell_3$, and an odd q with $\gcd(n, q) = 1$. For $i \leq 3$, we set

$$\begin{aligned} B_i &= D_{n,\ell_i} \cup D_{n,n/\ell_i}, \\ s_i &= \left\lfloor \frac{n}{\ell_i^2} \right\rfloor, \\ t_i &= \frac{1}{2}(2q^{s_i+3} + q^4 - q^3)(1 - q^{-1}). \end{aligned}$$

Then

$$\begin{aligned} D_n &= B_1 \cup B_2 \cup B_3, \\ \#B_i &= 2q^{n/\ell_i+\ell_i}(1 - q^{-1}) - t_i. \end{aligned}$$

For a permutation $\pi \in S_3$, we set

$$\begin{aligned} C_\pi &= \gamma_\pi(P^{=}_{\ell_{\pi 1}} \times P^0_{\ell_{\pi 2}} \times P^0_{\ell_{\pi 3}}), \\ C &= \bigcup_{\pi \in S_3} C_\pi, \end{aligned}$$

where γ_π is the composition map for three components. Then for any $\pi \in S_3$

$$\#C_\pi = q^{\ell_1+\ell_2+\ell_3-1}(1-q^{-1}).$$

Now let $i \neq j$ and $f = g \circ h = g^* \circ h^* \in B_i \cap B_j$, with $\{\deg g, \deg h\} = \{\ell_i, n/\ell_i\}$ and $\{\deg g^*, \deg h^*\} = \{\ell_j, n/\ell_j\}$. To simplify notation, suppose that $i = 1$ and $j = 2$. We refine both decompositions into complete ones. Then for $g \circ h$, the set of degrees is either $\{\ell_1, \ell_2\ell_3\}$ or $\{\ell_1, \ell_2, \ell_3\}$, and for $g^* \circ h^*$ it is either $\{\ell_2, \ell_1\ell_3\}$ or $\{\ell_1, \ell_2, \ell_3\}$. Ritt's First Theorem (see Schinzel (2000), Theorem 1.3.7) says that this set of degrees is unique, so that it equals $\{\ell_1, \ell_2, \ell_3\}$. It follows that $f \in C$ and $B_i \cap B_j \subseteq C$. Thus

$$\begin{aligned}
\#D_n &\geq \sum_{1\leq i\leq 3} \#B_i - \#C \\
&\geq (1-q^{-1}) \sum_{1\leq i\leq 3} \left(2q^{n/\ell_i+\ell_i} - \frac{1}{2}(2q^{s_i+3} + q^4)\right) - 6q^{\ell_1+\ell_2+\ell_3-1} \\
&= (1-q^{-1}) \left(2\sum_{1\leq i\leq 3} q^{n/\ell_i+\ell_i} - \sum_{1\leq i\leq 3} q^{s_i+3} - \frac{3}{2}q^4 - 6q^{\ell_1+\ell_2+\ell_3-1}\right). \qquad (6.7)
\end{aligned}$$

Now suppose further that

$$\ell_3 \leq 2 + (\ell_1-1)(\ell_2-1), \quad 5 \leq \ell_2 \leq \ell_1^2, \quad q \geq 7.$$

Then

$$\begin{aligned}
\ell_1+\ell_2+\ell_3-1 &\leq \ell_1+\ell_2+1+(\ell_1-1)(\ell_2-1) \\
&= \ell_1\ell_2+2, \\
6q^{\ell_1+\ell_2+\ell_3-1} &\leq 6q^{\ell_1\ell_2+2} \leq q^{\ell_1\ell_2+3}, \\
4\ell_3 &\leq 10(\ell_3-1) \leq \ell_1\ell_2(\ell_3-1), \\
\frac{\ell_1\ell_2}{\ell_3} + 4 &\leq \ell_1\ell_2 < \ell_1\ell_2+\ell_3, \\
q^{\ell_1\ell_2/\ell_3+3} + \frac{3}{2}q^4 + 6q^{\ell_1+\ell_2+\ell_3-1} &< q^{\ell_1\ell_2+\ell_3}\left(q^{-1} + \frac{3}{2}q^{4-\ell_3} + q^{3-\ell_3}\right) \\
&< 2q^{\ell_1\ell_2+\ell_3}, \\
\frac{\ell_2\ell_3}{\ell_1} &\leq \ell_1\ell_3, \\
\frac{\ell_1\ell_3}{\ell_2} &< \ell_1\ell_3, \\
q^{\ell_2\ell_3/\ell_1+3} + q^{\ell_1\ell_3/\ell_2+3} &< (q^{3-\ell_2} + q^{3-\ell_2})q^{\ell_1\ell_3+\ell_2} < q^{\ell_1\ell_3+\ell_2}.
\end{aligned}$$

Finally, (6.7) implies that

$$\frac{\#D_n}{1-q^{-1}} \geq \frac{\alpha_n}{1-q^{-1}} + 2q^{\ell_1\ell_3+\ell_2} + 2q^{\ell_1\ell_2+\ell_3} - \sum_{1\leq i\leq 3} q^{\lfloor n/\ell_i^2\rfloor+3} - \frac{3}{2}q^4 - 6q^{\ell_1+\ell_2+\ell_3-1}$$
$$> \frac{\alpha_n}{1-q^{-1}}.$$

As a small example, we take $\ell_1 = 3$, $\ell_2 = 5$, $\ell_3 = 7$, $q = 11$, so that $n = 105$ and $\alpha_{105} = 2q^{38}(1-q^{-1})$. The lower bound in (6.7) evaluates to

$$\#D_{105} \geq \alpha_{105} + (1-q^{-1})(2(q^{26}+q^{22}) - (q^{14}+q^7+q^5+\frac{3}{2}q^4+6q^{15}))$$
$$> \alpha_{105} + 2q^{26}(1-q^{-1}).$$

The general bounds of Theorem 3.2(i) and Fact 2.13(i) specialize to

$$\#D_{105} \leq \alpha_{105}(1+\frac{q^{-12}}{1-q^{-1}}) = \alpha_{105} + 2q^{26}.$$

The closeness of these two estimates indicates a certain precision in our bounds. ♢

Open Question 6.8. ∘ *In the case where $p = \ell$ and $p^2 \parallel n \neq p^2$, can one tighten the gap between upper and lower bounds in the Main Theorem (ii), maybe to within a factor $1 + O(q^{-1})$? We would then have $\lim_{q\longrightarrow\infty} \nu_{q,n} = 1$ as q runs through the powers of p.*

∘ *Can one simplify the arguments and reduce the number of cases, yet obtain results of a quality as in the Main Theorem? The bounds in Theorem 4.1 are based on "low level" coefficient comparisons. Can these results be (im)proved by "higher level" methods?*

7. Acknowledgments

Many thanks go to Jaime Gutiérrez for alerting me to Umberto Zannier's paper, to Henning Stichtenoth for discussions and for pointing out Antonia Bluher's work, to Laila El Aimani for some computations, and to Konstantin Ziegler for drawing the tree. I appreciate Igor Shparlinski's comments on Remark 3.13, pointing out a notational infelicity, and thank Umberto Zannier for correcting a misunderstanding. I appreciate the discussions with Arnaud Bodin, Pierre Dèbes, and Salah Najib about the topic, and in particular the challenges that their work Bodin *et al.* (2009) posed.

An Extended Abstract of this work has appeared as part of von zur Gathen (2009). It was supported by the B-IT Foundation and the Land Nordrhein-Westfalen.

References

RAOUL BLANKERTZ, JOACHIM VON ZUR GATHEN & KONSTANTIN ZIEGLER (2013). Compositions and collisions at degree p^2. *Journal of Symbolic Computation* URL http://dx.doi.org/10.1016/j.jsc.2013.06.001. In Press. Extended abstract in *Proceedings of the 2012 International Symposium on Symbolic and Algebraic Computation ISSAC2012,* Grenoble, France (2012), 91–98.

ARNAUD BODIN, PIERRE DÈBES & SALAH NAJIB (2009). Indecomposable polynomials and their spectrum. *Acta Arithmetica* **139(1)**, 79–100.

F. DOREY & G. WHAPLES (1974). Prime and Composite Polynomials. *Journal of Algebra* **28**, 88–101. URL http://dx.doi.org/10.1016/0021-8693(74)90023-4.

JOACHIM VON ZUR GATHEN (1990a). Functional Decomposition of Polynomials: the Tame Case. *Journal of Symbolic Computation* **9**, 281–299. URL http://dx.doi.org/10.1016/S0747-7171(08)80014-4.

JOACHIM VON ZUR GATHEN (1990b). Functional Decomposition of Polynomials: the Wild Case. *Journal of Symbolic Computation* **10**, 437–452. URL http://dx.doi.org/10.1016/S0747-7171(08)80054-5.

JOACHIM VON ZUR GATHEN (2002). Factorization and Decomposition of Polynomials. In *The Concise Handbook of Algebra*, ALEXANDER V. MIKHALEV & GÜNTER F. PILZ, editors, 159–161. Kluwer Academic Publishers. ISBN 0-7923-7072-4.

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 (2009). The Number of Decomposable Univariate Polynomials — Extended Abstract. In *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation ISSAC2009,* Seoul, Korea, JOHN P. MAY, editor, 359–366. ACM Press. ISBN 978-1-60558-609-0. Preprint (2008) available at http://arxiv.org/abs/0901.0054.

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 (2012). Normal form for Ritt's Second Theorem. *Submitted,* 39 pages. Preprint at http://arxiv.org/abs/1308.1135.

Joachim von zur Gathen (2013). Lower bounds for decomposable univariate wild polynomials. *Journal of Symbolic Computation* **50**, 409–430. URL http://dx.doi.org/10.1016/j.jsc.2011.01.008.

Joachim von zur Gathen, Dexter Kozen & Susan Landau (1987). Functional Decomposition of Polynomials. In *Proceedings of the 28th Annual IEEE Symposium on Foundations of Computer Science,* Los Angeles CA, 127–131. IEEE Computer Society Press, Washington DC. URL http://dx.doi.org/10.1109/SFCS.1987.29. Final version in Journal of Symbolic Computation.

Mark William Giesbrecht (1988). Complexity Results on the Functional Decomposition of Polynomials. Technical Report 209/88, University of Toronto, Department of Computer Science, Toronto, Ontario, Canada. Available as http://arxiv.org/abs/1004.5433.

Johannes Grabmeier, Erich Kaltofen & Volker Weispfenning (editors) (2003). *Computer Algebra Handbook – Foundations, Applications, Systems.* Springer-Verlag, Berlin, Heidelberg, New York. ISBN 3-540-65466-6. URL http://www.springer.com/978-3-540-65466-7.

Jaime Gutierrez & Dexter Kozen (2003). Polynomial Decomposition. In Grabmeier *et al.* (2003), section 2.2.4 (pages 26–28). URL http://www.springer.com/978-3-540-65466-7.

Jaime Gutierrez & David Sevilla (2006). On Ritt's decomposition theorem in the case of finite fields. *Finite Fields and Their Applications* **12**(3), 403–412. URL http://dx.doi.org/10.1016/j.ffa.2005.08.004.

Dexter Kozen & Susan Landau (1986). Polynomial Decomposition Algorithms. Technical Report 86-773, Department of Computer Science, Cornell University, Ithaca NY, 1986.

Dexter Kozen & Susan Landau (1989). Polynomial Decomposition Algorithms. *Journal of Symbolic Computation* **7**, 445–456. An earlier version was published as Technical Report 86-773, Cornell University, Department of Computer Science, Ithaca, New York, 1986.

Dexter Kozen, Susan Landau & Richard Zippel (1996). Decomposition of Algebraic Functions. *Journal of Symbolic Computation* **22**, 235–246.

J. F. Ritt (1922). Prime and Composite Polynomials. *Transactions of the American Mathematical Society* **23**, 51–66. URL http://www.jstor.org/stable/1988911.

ANDRZEJ SCHINZEL (1982). *Selected Topics on Polynomials.* Ann Arbor; The University of Michigan Press. ISBN 0-472-08026-1.

ANDRZEJ SCHINZEL (2000). *Polynomials with special regard to reducibility.* Cambridge University Press, Cambridge, UK. ISBN 0521662257.

PIERRE TORTRAT (1988). Sur la composition des polynômes. *Colloquium Mathematicum* **55**(2), 329–353.

U. ZANNIER (1993). Ritt's Second Theorem in arbitrary characteristic. *Journal für die reine und angewandte Mathematik* **445**, 175–203.

UMBERTO ZANNIER (2008). On composite lacunary polynomials and the proof of a conjecture of Schinzel. *Inventiones mathematicae* **174**, 127–138. ISSN 0020-9910 (Print) 1432-1297 (Online). URL http://dx.doi.org/10.1007/s00222-008-0136-8.

JOACHIM VON ZUR GATHEN
B-IT
Universität Bonn
D-53113 Bonn
gathen@bit.uni-bonn.de
http://cosec.bit.uni-bonn.de/