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 ISSAC'07. The *Local PDF* includes a single-page correction.
This document is provided as a means to ensure timely dissemination of scholarly and technical work on a non-commercial basis. Copyright and all rights therein are maintained by the authors or by other copyright holders, notwithstanding that these works are posted here electronically. It is understood that all persons copying any of these documents will adhere to the terms and constraints invoked by each copyright holder, and in particular use them only for noncommercial purposes. These works may not be posted elsewhere without the explicit written permission of the copyright holder. (Last update 2016/05/18 :14 :16.)

Counting reducible and singular bivariate polynomials

Joachim von zur Gathen

B-IT
Universität Bonn
D-53113 Bonn

Abstract

Among the bivariate polynomials over a finite field, most are irreducible. We count some classes of special polynomials, namely the reducible ones, those with a square factor, the "relatively irreducible" ones which are irreducible but factor over an extension field, and the singular ones, which have a root at which both partial derivatives vanish.

Key words: bivariate polynomials, finite fields, combinatorics on polynomials, counting problems

1 Introduction

We investigate four "accidents" that can happen to a bivariate polynomial over a finite field: it can have a nontrivial factor, or a square factor, or a factor over an extension field, or a singular root, where all partial derivatives also vanish. The main results are quantitative versions of the intuition that a random polynomial is unlikely to suffer an accident.

We have a ground field F. The accidents may occur at two places: in F ("rational") or in an algebraic closure of F ("absolute"). We then have four notions: rationally or absolutely reducible, and rationally or absolutely singular. We also consider squareful polynomials, where the rational and absolute notions coincide.

Email address: gathen@bit.uni-bonn.de (Joachim von zur Gathen).
URL: http://cosec.bit.uni-bonn.de/ (Joachim von zur Gathen).

We take the set $B_n(F) \subseteq F[x,y]$ of bivariate polynomials with total degree not exceeding some integer n, and certain natural sets $A_n(F) \subseteq B_n(F)$ of "accidents", as above. We phrase our results in two languages, a geometric and a combinatorial one. Namely, geometrically $B_n(F)$ is an affine or vector space over F, and our $A_n(F)$ will be a union of images of polynomial maps, and thus a (reducible) subvariety. It has Zariski-irreducible components of maximal dimension, and we take the codimension of $A_n(F)$ to be the codimension of these maximal components; the geometric goal is its determination. In order for the required algebraic geometry to work, it is usually easiest to assume F to be algebraically closed. For the combinatorial results, we take $F = \mathbb{F}_q$ to be a finite field with q elements, and our goal is to find functions $\alpha_n(q)$ and $\beta_n(q)$ so that

$$\left| \frac{\#A_n(\mathbb{F}_q)}{\#B_n(\mathbb{F}_q)} - \alpha_n(q) \right| \leq \alpha_n(q) \cdot \beta_n(q),$$

with $\beta_n(q)$ tending to zero as q and n grow. Thus a random element of $B_n(\mathbb{F}_q)$ is in $A_n(\mathbb{F}_q)$ with probability about $\alpha_n(q)$. We provide functions $\beta_n(q)$ that go to zero like q^{-n} exponentially both in $\log q$ and n. But when we simplify $\alpha_n(q)$ to a power q^{-m} of q, with an integer m, then the relative error estimate $\beta_n(q)$ becomes only $\mathrm{O}(q^{-1})$, since that is the quality with which q^{-m} approximates $\alpha_n(q)$. The Weil bound also gives an estimate based on the geometric result, but with an even larger relative error of $n^{\mathrm{O}(1)}q^{-1/2}$.

Figure 1.1 gives a picture of the combinatorial results. The ellipse in the top half represents all bivariate polynomials and shows the subsets that we study. In the bottom half, we have excised five pieces. A power $1/q^e$ of q attached to an edge means that the fraction of bivariate polynomials in the piece within all polynomials is $q^{-e}(1 + \mathrm{O}(q^{-1}))$. This is valid for sufficiently large n, and more precise statements are given in the paper. The ϵ at the right hand edge is given in Theorem 4.1.

For univariate polynomials, the fractions of irreducible and of non-squarefree (and non-r-powerfree) polynomials among the monic ones of degree n are well known:$\frac{1}{n}\sum_{k|n}\mu(k)q^{n/k-n} \approx 1/n$ and $\approx 1/q$, respectively.

When counting multivariate polynomials, one has two obvious options of defining the base set of all polynomials: by bounding the total degree or the individual degree in each variable. The first "triangular" approach may look more natural, but is complicated by the fact that the base dimension is a binomial coefficient. We take this route but simplify our task by concentrating on bivariate polynomials. The general case requires more involved calculations. The second "rectangular" approach is often taken in the literature. Now the base dimension is just the product of the individual degree bounds (augmented by 1), but even here Cohen (1968) comes to "a fairly long, complicated argument, which we shall omit", and warns the interested reader that "the derivation of the above results is increasingly complicated. Each further computation, using

this method, would require considerable calculation.".

Carlitz (1963) provided the first count of irreducible multivariate polynomials. His work is discussed after Corollary 2.14. In Carlitz (1965), he went on to study the fraction of irreducibles in the rectangular model. Gao & Lauder (2002) considered 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 (1992b) 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.

Cohen (1970) gave asymptotic estimates for various arithmetical functions, including the number of r–power–free multivariate polynomials, again with the individual degrees being bounded. Ragot (1997) estimated the number of reducible bivariate polynomials, and in Ragot (1997, 1999), he calculated exactly the number of polynomials in $B_n(\mathbb{F}_q)$ with a singular root in $\mathbb{F}_q^2$. An improved version of this result, due to Hendrik W. Lenstra, Jr., is presented in Section 5. Ragot derived his bounds for the general multivariate case.

This study originated from the desire to understand these "accidents" for algorithms in multivariate polynomial computation. As one example, in various methods for estimating the size of plane algebraic curves (see Huang & Ierardi (1993), von zur Gathen & Shparlinski (1995, 1998), Cafure & Matera (2002)) the relatively irreducible (or "exceptional") curves had to be treated as a special case. One desires error estimates that are relatively good with respect to the true size. By Weil's Theorem, this size can be challengingly small in and only in this special case. This difficulty can be overcome by applying methods that are quite different from those that work in the case of polynomials that are not relatively irreducible. The results of Section 4 present good estimates on how (in)frequent these special cases are. In fact, Guillermo Matera and Antonio Cafure asked the author for this frequency, thus triggering this investigation. No estimates for reducible polynomials of the precision needed seem to be in the literature; so they are included here as well. In his algorithms for multivariate absolute irreducibility testing, Ragot (1997) had been able to do with weaker bounds. Finally, the singular polynomials form the most general "accident". In applying results from algebraic geometry such as Weil's bounds, one often has to assume the variety to be nonsingular. The nice results of Ragot (1997, 1999) are improved, with the help of Hendrik Lenstra, and supplemented in areas that arise naturally from the approach of the present paper. Multivariate analogs of our results appear in von zur Gathen & Viola (2008).

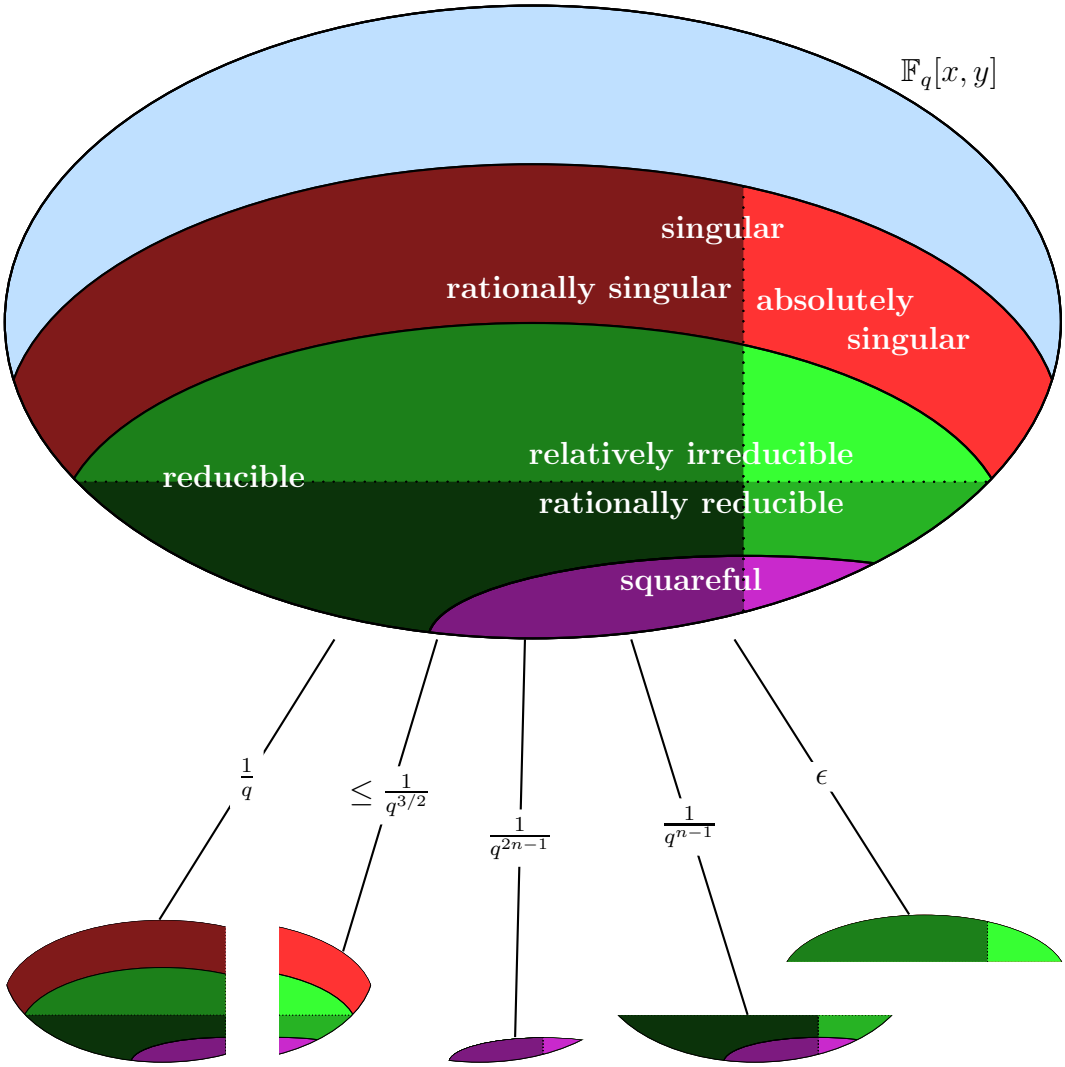


Figure 1.1. Special types of polynomials

2 Reducible polynomials

Let F be a field and $n \geq 0$. We set

$$\begin{aligned} B_n(F) &= \{f \in F[x,y] : \deg f \leq n\}, \\ I_n(F) &= \{f \in B_n(F) : f \text{ irreducible}\}, \\ R_n(F) &= B_n(F) \setminus (I_n(F) \cup F), \end{aligned}$$

where $\deg f$ is the total degree of f. Thus $R_n(F)$ consists of the reducible polynomials. The constants in $F = B_0(F)$ are neither irreducible nor reducible, and $R_1(F) = \varnothing$. $B_n(F)$ is a vector space over F of dimension

$$b_n = \binom{n+2}{2} = \frac{n^2+3n+2}{2}$$

n	$\#B_n^=(\mathbb{F}_q)$	$\#R_n^=(\mathbb{F}_q)$
1	q^3-q	0
2	q^6-q^3	$(q^5+q^4-q^2-q)/2$
3	$q^{10}-q^6$	$(3q^8+2q^7-2q^6-3q^5-q^4+2q^3-q)/3$
4	$q^{15}-q^{10}$	$(4q^{12}+6q^{11}-2q^{10}-5q^9-7q^8+6q^6$
		$-2q^4-q^3+q^2)/4$
5	$q^{21}-q^{15}$	$(5q^{17}+5q^{16}+5q^{15}-10q^{13}-15q^{12}-6q^{11}$
		$+11q^{10}+10q^9-5q^7-q^6+q^5+q^3-q)/5$
6	$q^{28}-q^{21}$	$(6q^{23}+6q^{22}+6q^{20}+3q^{19}-3q^{18}-21q^{17}$
		$-23q^{16}-10q^{15}+18q^{14}+32q^{13}+10q^{12}-15q^{11}$
		$-12q^{10}+3q^8-q^7+2q^5-3q^3+q^2+q)/6$

Table 2.1
The numbers of reducible polynomials of degrees up to 6.

for $n \geq 0$. We also consider the polynomials of degree exactly n:

$$\begin{aligned} B_n^=(F) &= B_n(F) \setminus B_{n-1}(F), \\ R_n^=(F) &= R_n(F) \cap B_n^=(F), \\ I_n^=(F) &= I_n(F) \cap B_n^=(F), \end{aligned}$$

with $B_{-1}(F) = \{0\}$ and

$$\#B_n^=(\mathbb{F}_q) = q^{b_n} - q^{b_{n-1}} = q^{b_n}(1-q^{-n-1}).$$

Our results transfer to the projective space of equivalence classes of associate polynomials, consisting of the multiples by a nonzero constant of one of them, and also to homogeneous (trivariate) polynomials.

The first "accident" we study is reducibility, in particular, the probability for a polynomial of degree n in $\mathbb{F}_q[x,y]$ to be reducible. For $n \leq 6$, Table 2.1 gives the exact value of $\#R_n^=(\mathbb{F}_q)$, calculated with the method of von zur Gathen & Viola (2008). These expressions are fairly complicated, and the goal of this section is to derive simple bounds that are generally valid.

THEOREM 2.1. *Let $n \geq 2$.*

(i) For an algebraically closed field F, $R_n(F)$ is a subvariety of codimension $n-1$ in $B_n(F)$.

(ii) Let $\rho_n(q) = (q+1)q^{-n}$. Then for $n \geq 3$ we have

$$\left| \frac{\#R_n^=(\mathbb{F}_q)}{\#B_n^=(\mathbb{F}_q)} - \rho_n(q) \right| \leq \rho_n(q) \cdot 2q^{-n+3},$$
$$\frac{\#R_2^=(\mathbb{F}_q)}{\#B_2^=(\mathbb{F}_q)} = \frac{\rho_2(q)}{2}.$$

(iii) For $n \geq 6$, we have

$$\left| \frac{\#R_n^=(\mathbb{F}_q)}{\#B_n^=(\mathbb{F}_q)} - q^{-n+1} \right| \leq 2q^{-n}.$$

PROOF. (i) For $1 \leq k < n$, we consider the multiplication map

$$\mu_{n,k}\colon \begin{array}{c} B_k^=(F) \times B_{n-k}^=(F) \longrightarrow B_n^=(F), \\ (g,h) \longmapsto g \cdot h, \end{array}$$

whose images form a stratification of $R_n^=(F)$:

$$R_n^=(F) = \bigcup_{1 \leq k \leq n/2} \operatorname{im} \mu_{n,k}. \tag{2.2}$$

For any $(g,h) \in B_k^=(F) \times B_{n-k}^=(F)$ and $a \in F^\times = F \setminus \{0\}$, we have

$$\mu_{n,k}(ag, a^{-1}h) = \mu_{n,k}(g,h). \tag{2.3}$$

Hence the fiber under $\mu_{n,k}$ of each polynomial in im $\mu_{n,k}$ includes a copy of $F^\times$ and thus has dimension at least 1. It follows that

$$\dim \operatorname{im} \mu_{n,k} \leq b_k + b_{n-k} - 1 = b_n - k(n-k) \leq b_n - n + 1 < b_n.$$

Thus the Zariski closure of im $\mu_{n,k}$ is a proper irreducible subvariety of $B_n(F)$, and its complement intersected with $B_n^=(F)$ is a dense open subset of $B_n^=(F)$ and contained in $I_n^=(F)$. (In fact, im $\mu_{n,k}$ is closed (von zur Gathen (1985), Lemma 4.1), but we do not need this here.) Let $1 \leq k \leq n/2$ and $(g,h) \in B_k^=(F) \times I_{n-k}^=(F)$. If $k < n/2$ or h is an associate of g, the fiber of $gh = \mu_{n,k}(g,h)$ under $\mu_{n,k}$ is isomorphic to $F^\times$. If $k = n/2$ and h is not an associate of g, the fiber

$$\mu_{n,k}(gh) = \{(ag, a^{-1}h), (ah, a^{-1}g)\colon a \in F^\times\} \tag{2.4}$$

has two one-dimensional components. Thus in all cases the generic fiber dimension is 1, and

$$\dim \operatorname{im} \mu_{n,k} = b_k + b_{n-k} - 1 = b_n - k(n-k). \tag{2.5}$$

The maximal dimension occurs at $k = 1$, where it equals $b_n - n + 1$. It follows that $\operatorname{codim}_{B_n^=(F)} R_n^=(F) = n - 1$. Since the complement of $B_n^=(F)$ in $B_n(F)$ has codimension $n + 1$, we also have $\operatorname{codim}_{B_n(F)} R_n(F) = n - 1$.

(ii) We start with the special case $n = 2$. When $g, h \in I_1^=(\mathbb{F}_q) = B_1^=(\mathbb{F}_q)$ are not associate, then the fiber (2.4) of $\mu_{2,1}$ at gh has $2(q-1)$ elements. Given an arbitrary g, there are $q^3 - q - (q-1) = (q-1)(q^2+q-1)$ choices for h. Furthermore, there are $q^3 - q$ polynomials bg^2 with $b \in \mathbb{F}_q^\times$ and $g \in I_1^=(\mathbb{F}_q)$; then $\mu_{2,1}^{-1}(bg^2) = \{(abg, a^{-1}g) \colon a \in \mathbb{F}_q^\times\}$. Together, these make up all of $\operatorname{im} \mu_{2,1} = \# R_2^=(\mathbb{F}_q)$. Therefore

$$\frac{\# R_2^=(\mathbb{F}_q)}{\# B_2^=(\mathbb{F}_q)} = \frac{(q^3-q)(q-1)(q^2+q-1)}{2(q-1)(q^6-q^3)} + \frac{q^3-q}{q^6-q^3} = \frac{\rho_2(q)}{2}. \tag{2.6}$$

We now may assume that $n \geq 3$. From (2.3), we know that each fiber of $\mu_{n,k}$ has at least $q - 1$ elements. Thus

$$\begin{aligned} \# \operatorname{im} \mu_{n,k} &\leq \frac{1}{q-1} \cdot \# B_k^=(\mathbb{F}_q) \cdot \# B_{n-k}^=(\mathbb{F}_q) && (2.7) \\ &< \frac{q^{b_k}(1-q^{-k-1}) \cdot q^{b_{n-k}}}{q-1} && (2.8) \\ &= \frac{\rho_n(q) \cdot \# B_n^=(\mathbb{F}_q) \cdot q^{n-1-k(n-k)}(1-q^{-k-1})}{(1-q^{-2})(1-q^{-n-1})}. \end{aligned}$$

Now the quadratic function $u(k) = -k(n-k)$ of k has the two roots 0 and n, and is monotonically strictly decreasing for $2 \leq k \leq n/2$, so that

$$\sum_{2 \leq k \leq n/2} q^{u(k)} < q^{u(2)} \sum_{k \geq 0} q^{-k} = \frac{q^{-2n+5}}{q-1}. \tag{2.9}$$

Thus

$$\begin{aligned} \frac{\# R_n^=(\mathbb{F}_q)}{\# B_n^=(\mathbb{F}_q)} &\leq \frac{1}{\# B_n^=(\mathbb{F}_q)} \sum_{1 \leq k \leq n/2} \# \operatorname{im} \mu_{n,k} && (2.10) \\ &< \frac{\rho_n(q)}{1-q^{-n-1}} \cdot \sum_{1 \leq k \leq n/2} \frac{q^{n-1-k(n-k)}(1-q^{-k-1})}{1-q^{-2}} \\ &\leq \frac{\rho_n(q)}{1-q^{-n-1}} \cdot \left(1 + q^{n-1} \sum_{2 \leq k \leq n/2} \frac{q^{-k(n-k)}}{1-q^{-2}}\right) && (2.11) \\ &< \frac{\rho_n(q)}{1-q^{-n-1}} \left(1 + \frac{q^{-n+4}}{(q-1)(1-q^{-2})}\right). \end{aligned}$$

Now we have

$$(q-1)(q^2-1)(2q^4 - 1 - 2q^{-n+3}) - q^7 \geq 0,$$

since the product is monotonically increasing with n, so that it is sufficient to check the case $n = 3$. The resulting expression increases monotonically with q, and is positive for $q = 3$ (and negative for $q = 2$). Thus for $q \geq 3$, we have

$$\begin{aligned} 1 + \frac{q^{-n+4}}{(q-1)(1-q^{-2})} &\leq (1-q^{-n-1})(1+2q^{-n+3}), \\ \frac{\#R_n^=(\mathbb{F}_q)}{\#B_n^=(\mathbb{F}_q)} &\leq \rho_n(q)(1+2q^{-n+3}). \end{aligned} \tag{2.12}$$

For $q = 2$, the estimate in (2.9) is too coarse for further usage. We refine it for $n \geq 8$ by observing that the summands $q^{-2(n-2)+i}$ for $i = 1, 2$ do not occur in the left hand sum, since $3(n-3) \geq 2(n-2)+3$. Thus

$$\sum_{2 \leq k \leq n/2} q^{-k(n-k)} \leq q^{-2n+4}\left(\frac{q}{q-1} - \frac{1}{q} - \frac{1}{q^2}\right).$$

Plugging this into (2.11) yields

$$\begin{aligned} \frac{\#R_n^=(\mathbb{F}_q)}{\#B_n^=(\mathbb{F}_q)} &\leq \frac{\rho_n(q)}{1-q^{-n-1}}\left(1 + \frac{q^{-n+3}(q^3-q^2+1)}{(q-1)(q^2-1)}\right) \\ &< \rho_n(q)(1+2q^{-n+3}), \end{aligned}$$

for any $q \geq 2$. For $q = 2$ and $3 \leq n \leq 7$, we take the exact value of the right hand sum in (2.11). (We may even ignore the factor $1-q^{-k-1}$ except for $n = 6$, $k = 2$.) This yields the upper bound (2.12) also for $q = 2$.

As a consequence, we have a lower bound on the number of irreducible polynomials for $n \geq 3$. First, we have from (2.12) that

$$\begin{aligned} \#I_n^=(\mathbb{F}_q) &= \#B_n^=(\mathbb{F}_q) - \#R_n^=(\mathbb{F}_q) \\ &\geq q^{b_n}(1-q^{-n-1})(1-\rho_n(q)(1+2q^{-n+3})) \\ &\geq q^{b_n}(1-(q+2)q^{-n}). \end{aligned} \tag{2.13}$$

The last inequality holds when $n \geq 5$, except when (n, q) is one of $(5, 2)$, $(5, 3)$, or $(6, 2)$. The remaining cases again require special consideration to show the lower bound (2.13). For $n = 2$, it follows from (2.6), and when $n = 3$ or $(n, q) = (5, 3)$, the bound in (2.11) is sufficient. For $n = 4$ and for (n, q) either $(5, 2)$ or $(6, 2)$, we use bounds that are easily derived from Table 2.1:

$$\begin{aligned} &\#R_4^=(\mathbb{F}_q) \leq q^{12} + 3q^{11}/2, \quad \#R_5^=(\mathbb{F}_q) \leq q^{17} + q^{16} + q^{15}, \\ &\#R_6^=(\mathbb{F}_q) \leq q^{23} + 3q^{22}/2. \end{aligned}$$

Corollary 4.9 will improve this by showing the lower bound (2.13) for the absolutely irreducible polynomials.

For a lower bound on $\#R_n(\mathbb{F}_q)$, we have the equalities in (2.3) under $\mu_{n,1}$. However, when $n \geq 3$ and h has no linear factor, in particular, when it is irreducible, then no other such equalities exist. It follows that for $n \geq 3$

$$\begin{aligned}\frac{\#R_n^=(\mathbb{F}_q)}{\#B_n^=(\mathbb{F}_q)} &\geq \frac{\#\operatorname{im}\,\mu_{n,1}}{\#B_n^=(\mathbb{F}_q)} \geq \frac{\#B_1^=(\mathbb{F}_q)\cdot\#I_{n-1}^=(\mathbb{F}_q)}{(q-1)\#B_n^=(\mathbb{F}_q)} \\ &\geq \frac{(q^3-q)\cdot q^{b_{n-1}}(1-(q+2)q^{-(n-1)})}{(q-1)q^{b_n}(1-q^{-n-1})} \\ &= \frac{\rho_n(q)(1-(q+2)q^{-n+1})}{1-q^{-n-1}} \\ &\geq \rho_n(q)(1-2q^{-n+2}) \\ &> \rho_n(q)(1-2q^{-n+3}).\end{aligned}$$

(iii) We have for $n \geq 6$, and for $n = 5$ if $q \geq 3$, the bound

$$\begin{aligned}\left|\frac{\#R_n^=(\mathbb{F}_q)}{\#B_n^=(\mathbb{F}_q)} - q^{-n+1}\right| &\leq \left|\frac{\#R_n^=(\mathbb{F}_q)}{\#B_n^=(\mathbb{F}_q)} - \rho_n(q)\right| + \left|\rho_n(q) - q^{-n+1}\right| \\ &\leq 2(q+1)q^{-2n+3} + q^{-n} \\ &\leq 2q^{-n}.\end{aligned}$$

□

For $n = 3$, the bound in (ii) needs to be strengthenend, and in fact we have

$$\frac{\#R_3^=(\mathbb{F}_q)}{\#B_3^=(\mathbb{F}_q)} - \rho_3(q) = \rho_3(q)\cdot\frac{-(3q^2+2q-2)}{q^2(q+1)(q^2+1)};$$

the last factor is absolutely not more than $3q^{-3}$.

We note two features that will recur in other sections. The constant 2 in the estimates is really $1+\varepsilon$ with ε going to 0 as q and n grow, but the bound would in general be invalid if one replaced 2 by 1. The thrust of the argument is as follows: obtain an upper bound on reducibility, yielding a lower bound on irreducibility, and then from this a lower bound on reducibility. This "self-reducibility" will be visible in other proofs as well.

Viewing $\#R_n^=(\mathbb{F}_q)$ as a polynomial in q, Theorem 2.1 (ii) says that its leading $n-3$ coefficients are $x^m + x^{m-1}$ with $m = b_n - n + 1$. Table 2.1 illustrates this for $n \geq 4$.

For later usage, we record from (2.13) the number of polynomials that are irreducible of degree exactly n.

COROLLARY 2.14. *We have $\#I_1^=(\mathbb{F}_q) = q^3 - q$, and for $n \geq 2$*

$$\#I_n^=(\mathbb{F}_q) \geq q^{b_n}\cdot(1-(q+2)q^{-n}).$$

Carlitz (1963) counts irreducible multivariate polynomials. His result (11) says, in the case of two variables and transformed to our notation, that

$$\frac{\#R_n^=(\mathbb{F}_q)}{\#B_n^=(\mathbb{F}_q)} = 1 - \frac{\#I_n^=(\mathbb{F}_q)}{\#B_n^=(\mathbb{F}_q)} = O((q-1)q^{-n-1}).$$

The reader might think that this conflicts with Theorem 2.1 (ii), which gives the bound $\Theta((q+1)q^{-n})$. However, Carlitz considers q as fixed, and thus factors like $(q-1)^{-1}$ or $q+1$ are absorbed by his O-notation. A few lines further on, Carlitz observes that "as the referee pointed out, [it] can be proved by a crude counting argument" that

$$1 - \frac{q^{-n+4}}{(q-1)^3} \le \frac{\#I_n^=(\mathbb{F}_q)}{\#B_n^=(\mathbb{F}_q)} \le 1.$$

The left hand bound is correct and has the same order of magnitude as Corollary 2.14, but is marginally worse in the second-order term.

Ragot (1997), Section 5.3, pages 91–97, shows the following:

$$q^{-n+1}(1 - \frac{5}{q}) \le \frac{\#R_n^=(\mathbb{F}_q)}{\#B_n^=(\mathbb{F}_q)} \le q^{-n+1}(1 + \frac{6}{q}).$$

Gao & Lauder (2002) consider the set of polynomials in $\mathbb{F}_q[x, y]$ that have total degree n and in which x^n has coefficient 1. They prove that the fraction of reducible polynomials is asymptotically q^{-n+1}, with a relative error bound of $(1 - q^{-n/2+1})^{-1}$. Wan (1992b) gives a p-adic zeta function, mentioned in the Introduction. In Wan (1992a) he considers a much more general situation, namely the irreducible ones within a family of polynomials whose coefficients are parametrized by an algebraic variety.

Bodin (2008) has the asymptotic approximation $(q+1)q^{-n}$ to

$$\frac{\#R_n^=(\mathbb{F}_q)}{\#B_n^=(\mathbb{F}_q)} = 1 - \frac{I_n^=(\mathbb{F}_q)}{B_n^=(\mathbb{F}_q)},$$

for large n, without an explicit error term, and includes experimental results for $q = 2$.

3 Powerful polynomials

For a positive integer s, a polynomial is called *s-power-ful* if it is divisible by the sth power of some nonconstant polynomial, and *s-power-free* otherwise; it

n	$\#Q^{=}_{n,2}(\mathbb{F}_q)$
1	0
2	$q^3 - q$
3	$q^5 + q^4 - q^3 - q^2$
4	$q^8 + q^7 + q^6 - 2q^5 - 2q^4 + q^2$
5	$q^{12} + q^{11} - q^7 - 2q^6 - q^5 + q^4 + q^3$
6	$q^{17} + q^{16} - q^{12} + q^{10} - q^9 - 4q^8 - q^7 + 2q^6 + 3q^5 - q^3$

Table 3.1
The number of squareful polynomials of degrees up to 6.

is *squarefree* if $s = 2$. We let

$$Q_{n,s}(F) = \{f \in B_n(F) : f \text{ is } s\text{-power-ful}\},$$
$$Q^{=}_{n,s}(F) = Q_{n,s}(F) \cap B^{=}_n(F).$$

For $n \le 6$, Table 3.1 gives the exact value of $\#Q^{=}_{n,2}(\mathbb{F}_q)$.

THEOREM 3.1. *Let $2 \le s \le n$.*

(i) For an algebraically closed field F, $Q_{n,s}(F)$ is a subvariety of codimension $d_{n,s} = (2ns - s^2 + 3s - 4)/2$ in $B_n(F)$.

(ii) Let

$$\eta_{n,s}(q) = \frac{q^{-d_{n,s}}(1 + q^{-1})(1 - q^{-n+s-1})}{1 - q^{-n-1}}.$$

Then

$$\left| \frac{\#Q^{=}_{n,s}(\mathbb{F}_q)}{\#B^{=}_n(\mathbb{F}_q)} - \eta_{n,s}(q) \right| \le \eta_{n,s}(q) \cdot 6q^{-2n+6}.$$

(iii) If $n \ge 8$, then

$$\left| \frac{\#Q^{=}_{n,s}(\mathbb{F}_q)}{\#B^{=}_n(\mathbb{F}_q)} - q^{-d_{n,s}} \right| \le q^{-d_{n,s}-1}.$$

PROOF. (i) For any positive integer $k \le n/s$, we consider the map

$$\sigma_{n,k} : B^{=}_k(F) \times B^{=}_{n-sk}(F) \to B^{=}_n(F)$$
$$(g, h) \mapsto g^s h.$$

Then

$$Q^{=}_{n,s}(F) = \bigcup_{1 \le k \le n/s} \operatorname{im} \sigma_{n,k},$$

and for nonzero $a \in F$ and (g, h) as above we have

$$\sigma_{n,k}(ag, a^{-s}h) = \sigma_{n,k}(g, h). \tag{3.2}$$

Thus each fiber of $\sigma_{n,k}$ includes a copy of $F^\times$, and im $\sigma_{n,k} \subseteq B_n^=(F)$ is an irreducible subvariety of dimension at most $b_k + b_{n-sk} - 1 < b_n$. We set

$$u(k) = b_k + b_{n-sk} - 1 - b_n = -k(2ns + 3s - 3 - s^2k - k)/2,$$

so that the codimension of $Q_{n,s}^=(F)$ is at least $-u(k)$. In particular, the Zariski closure of $Q_{n,s}^=(F)$ is a proper subvariety of $B_n(F)$. Now if

$$(g, h) \in B_k^=(F) \times (B_{n-sk}^=(F) \setminus Q_{n-sk,s}^=(F)), \tag{3.3}$$

so that h is s-power-free, then the fiber of $\sigma_{n,k}(g, h)$ is isomorphic to $F^\times$, since an irreducible polynomial dividing $g^s h$ with multiplicity e occurs $\lfloor e/s \rfloor$ many times in g and $e - s\lfloor e/s \rfloor$ many times in h, so that g and h are uniquely determined up to associates. Thus (3.2) describes the fiber exactly in this case, and since the set in (3.3) is dense in $B_k^=(F) \times B_{n-sk}^=(F)$, we have $\operatorname{codim}_{B_n(F)} Q_{n,s}(F) = -u(k)$. This quantity takes its minimal value in the admissible range for k at $k = 1$, where it equals $(2ns - s^2 + 3s - 4)/2 = d_{n,s}$.

(ii) Since each fiber of $\sigma_{n,k}$ (with $F = \mathbb{F}_q$) has at least $q - 1$ elements, we have

$$\begin{aligned}
\frac{\#Q_{n,s}^=(\mathbb{F}_q)}{\#B_n^=(\mathbb{F}_q)} &\le \sum_{1 \le k \le n/s} \frac{q^{b_k}(1 - q^{-k-1}) \cdot q^{b_{n-sk}}(1 - q^{-n+sk-1})}{(q-1) \cdot q^{b_n}(1 - q^{-n-1})} \\
&= \eta_{n,s}(q)\Big(1 + \frac{q^{d_{n,s}}}{1 - q^{-2}} \sum_{2 \le k \le n/s} \frac{q^{u(k)}(1 - q^{-k-1})(1 - q^{-n+sk-1})}{1 - q^{-n+s-1}}\Big) \\
&\le \eta_{n,s}(q)\Big(1 + \frac{q^{d_{n,s}}}{1 - q^{-2}} \sum_{2 \le k \le n/s} q^{u(k)}\Big).
\end{aligned} \tag{3.4}$$

The quadratic function $u(k)$ of k takes only integer values and has the two roots $k_0 = 0$ and

$$k_1 = \frac{2ns + 3s - 3}{s^2 + 1}.$$

For $2 \le k \le k_1 - 2$, we have $u(k) \le u(2)$. We let $t = s/n$, so that $2/n \le t \le 1$. In case that $t > 1/3$, we have $n/s < 3$ and the sum in (3.4) consists of the single term $q^{u(2)}$. In the other case we have $2/n \le t \le 1/3$, $1/3 \le 1 - 2t$, and

$$\frac{5t + 1}{t^2} \le \frac{n^2 + 9n}{3}.$$

This inequality holds for $t = 2/n$, and follows in general because the left hand side is monotonically decreasing for $t \ge 2/n$. It follows that

$$0 \le \frac{t^2 n(n + 9)}{3} - (5t + 1) \le (1 - 2t)t^2 n^2 + 3t^2 n - (5t + 1),$$

and multiplying by n we find

$$0 \le (n-2s)s^2 + 3s^2 - 5s - n,$$
$$\frac{n}{s} \le \frac{2ns + 3s - 5 - 2s^2}{s^2+1} = k_1 - 2.$$

Thus each k occurring in the sum in (3.4) lies in the interval from 2 to $k_1 - 2$, each value $u(k)$ occurs at most twice, and $u(k) \le u(2)$.

In either case, the sum in (3.4) is less than

$$q^{u(2)} \cdot 2 \sum_{k \ge 0} q^{-k} = \frac{2q^{u(2)}}{1-q^{-1}}.$$

In the range $2 \le s \le (2n-3)/3$, the quadratic function $u(2) + d_{n,s} = 3 + s(-2n+3s-3)/2$ of s takes its maximum $-2n+6$ at $s = 2$. If $s > (2n-3)/3$, then the index set for the sum in (3.4) is empty and hence the sum vanishes, with the exception of $(n,s) = (4,2)$, in which case the sum equals $q^{u(2)} = q^{-9}$ and $q^{d_{4,2}-9}(1-q^{-2})^{-1} \le \frac{4}{3}q^{-2} < 6q^{-2n+6}$. Furthermore, $2/(1-q^{-2})(1-q^{-1}) \le 6$. Thus in all cases,

$$\frac{\#Q^{=}_{n,s}(\mathbb{F}_q)}{\#B^{=}_n(\mathbb{F}_q)} \le \eta_{n,s}(q)\left(1 + \frac{2q^{u(2)+d_{n,s}}}{(1-q^{-2})(1-q^{-1})}\right) \le \eta_{n,s}(q)(1+6q^{-2n+6}).$$

As a lower bound, we have for $n \ge 2$ and $2 \le s \le n-s$

$$\begin{aligned}\frac{\#Q^{=}_{n,s}(\mathbb{F}_q)}{\#B^{=}_n(\mathbb{F}_q)} &\ge \frac{\#I^{=}_1(\mathbb{F}_q) \cdot \#(B^{=}_{n-s}(\mathbb{F}_q) \setminus Q^{=}_{n-s,s}(\mathbb{F}_q))}{(q-1)\#B^{=}_n(\mathbb{F}_q)} \\ &\ge \frac{(q^3-q)\cdot q^{b_{n-s}}(1-q^{-n+s-1})(1-\eta_{n-s,s}(q)(1+6q^{-2n+2s+6}))}{(q-1)\cdot q^{b_n}(1-q^{-n-1})} \\ &= \eta_{n,s}(q)(1-\eta_{n-s,s}(q)(1+6q^{-2n+2s+6})).\end{aligned} \tag{3.5}$$

The exponent

$$-d_{n-s,s} = 2 + s(-2n+3s-3)/2 = u(2) + d_{n,s} - 1$$

of q in $\eta_{n-s,s}$ is a quadratic function of s. As above, in the range $2 \le s \le (2n-3)/3$ it assumes its maximal value $-2n+5$ at $s = 2$. The only two exceptions where our assumption $s \le n-s$ does not imply $s \le (2n-3)/3$ are (n,s) equal to $(4,2)$ or $(5,2)$; but we may obviously again use the bound for $s = 2$. Furthermore we have

$$\frac{1-q^{-n+2s-1}}{1-q^{-n+s-1}} \le 1, \tag{3.6}$$
$$1 + q^{-1} \le 3/2,$$
$$1 + 6q^{-2n+2s+6} \le 8. \tag{3.7}$$

The last inequality holds for $s \le n-3$. When $s \ge n-2$, then $n \le 4$ since $s \le n-s$, and hence $(n,s) = (4,2)$. Thus we have, except for $(4,2)$,

$$\begin{aligned}(1+q^{-1})(1+6q^{-2n+2s+6}) &\le 6,\\ \eta_{n-s,s}(q)(1+6q^{-2n+2s+6}) &\le \frac{q^{-2n+5}(1+q^{-1})(1-q^{-n+2s-1})(1+6q^{-2n+2s+6})}{1-q^{-n+s-1}}\\ &\le 8q^{-2n+5} < 6q^{-2n+6},\end{aligned}$$

$$\frac{\#Q^{=}_{n,s}(\mathbb{F}_q)}{\#B^{=}_{n}(\mathbb{F}_q)} \ge \eta_{n,s}(q)(1-6q^{-2n+6}). \tag{3.8}$$

For $(n,s) = (4,2)$, one substitutes into (3.5), using $q^3 - q = \#Q^{=}_{2,2}(\mathbb{F}_q)$ from Table 3.1, and (3.8) again follows.

When $s > n-s$, then (3.5) holds with $Q^{=}_{n-s,s}(\mathbb{F}_q) = \varnothing$ and $\eta_{n-s,s} = 0$, and (3.8) is valid.

(iii) Abbreviating $w = (1+q^{-1})(1-q^{-n+s-1})$, we have for $n \ge 8$

$$\begin{aligned}\left|\frac{\#Q^{=}_{n,s}(\mathbb{F}_q)}{\#B^{=}_{n}(\mathbb{F}_q)} - q^{-d_{n,s}}\right| &\le \left|\frac{\#Q^{=}_{n,s}(\mathbb{F}_q)}{\#B^{=}_{n}(\mathbb{F}_q)} - \eta_{n,s}(q)\right| + \left|\eta_{n,s}(q) - q^{-d_{n,s}}\right|\\ &\le \frac{q^{-d_{n,s}}}{1-q^{-n-1}}(w\cdot 6q^{-2n+6} + |w-(1-q^{-n-1})|)\\ &= \frac{q^{-d_{n,s}-1}}{1-q^{-n-1}}(1-q^{-n+s}-q^{-n+s-1}+q^{-n}+6wq^{-2n+7})\\ &\le q^{-d_{n,s}-1}.\end{aligned}$$

□

From the proof it is clear that one can also get sharper error bounds that tend to zero with growing s, but we have preferred to state a bound that is independent of s.

For $2 \le s \le n \le 3$, we have in fact

$$\frac{\#Q^{=}_{n,s}(\mathbb{F}_q)}{\#B^{=}_{n}(\mathbb{F}_q)} = \eta_{n,s}(q).$$

We specialize the results of Theorem 3.1 to the case $s = 2$ of squareful polynomials.

THEOREM 3.9. *Let $n \ge 1$.*

(i) For $n \ge 2$, $Q_{n,2}(F)$ is a subvariety of codimension $2n-1$ in $B_n(F)$.

(ii) Let

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

Then

$$\left|\frac{\#Q^{=}_{n,2}(\mathbb{F}_q)}{\#B^{=}_{n}(\mathbb{F}_q)} - \eta_{n,2}(q)\right| \le \eta_{n,2}(q)\cdot 6q^{-2n+6},$$

and for $n \le 3$

$$\frac{\#Q^{=}_{n,2}(\mathbb{F}_q)}{\#B^{=}_{n}(\mathbb{F}_q)} = \eta_{n,2}(q).$$

(iii) If $n \ge 8$*, then*

$$\left|\frac{\#Q^{=}_{n,2}(\mathbb{F}_q)}{\#B^{=}_{n}(\mathbb{F}_q)} - q^{-2n+1}\right| \le q^{-2n}.$$

With the simpler value

$$\eta'_n(q) = q^{-2n+1}(1+q^{-1}),$$

we have

$$\left|\frac{\#Q^{=}_{n,2}(\mathbb{F}_q)}{\#B^{=}_{n}(\mathbb{F}_q)} - \eta'_n(q)\right| \le \eta'_n(q)\cdot q^{-n+1}$$

for $n \ge 9$, using the triangle inequality.

There is no need to consider the "absolute" problem here, because any "absolutely squareful" polynomial is also "rationally squareful". Namely, suppose that $f = g^2 h$ with $f \in B^{=}_{n}(\mathbb{F}_q)$, $g \in B^{=}_{m}(\mathbb{F}_{q^k})$ irreducible and normalized so that one of its coefficients equals 1, $h \in B^{=}_{n-2m}(\mathbb{F}_{q^k})$ and $g \notin B^{=}_{m}(\mathbb{F}_{q^\ell})$ for any $\ell < k$. Then for any $\sigma \in G = \mathrm{Gal}(\mathbb{F}_{q^k} : \mathbb{F}_q)$ with $\sigma \ne \mathrm{id}$, also $g^2 h = f = f^\sigma = (g^\sigma)^2 h^\sigma$, and g^σ does not divide g. Therefore $(g^\sigma)^2$ divides h, and $f = \prod_{\sigma\in G}(g^\sigma)^2 \cdot h^*$ with

$$h^* = h / \prod_{\substack{\sigma\in G\\ \sigma\ne\mathrm{id}}} (g^\sigma)^2 \in B^{=}_{n-2km}(\mathbb{F}_{q^k}) \cap \mathbb{F}_q(x,y) = B^{=}_{n-2km}(\mathbb{F}_q).$$

The last equality can be shown via multivariate division with remainder; see e.g. von zur Gathen & Gerhard (2003), Section 21.2. Since $\prod_{\sigma\in G} g^\sigma \in B^{=}_{km}(\mathbb{F}_q)$, it follows that $f \in Q^{=}_{n,2}(\mathbb{F}_q)$.

Cohen (1970), Theorem 7, shows that the fraction of s-power-free bivariate polynomials among the $q^{(m+1)(n+1)}$ many with the degree in each variable bounded by $m \le n$, respectively, is $(1 - q^{1-ms}) + O(nq^{-m-n-1})$.

Gao & Lauder (2002) show that in their model of bivariate polynomials in which x^n occurs, the squareful ones form a fraction of q^{-2n+1}, with a relative error bound of $(1 - q^{-3n/4+1})^{-1}$.

n	$\#E_n^=(\mathbb{F}_q)$
1	0
2	$(q^5-q^4-q^2+q)/2$
3	$(q^7-q^6+q^4-2q^3+q)/3$
4	$(2q^{11}-2q^{10}+q^9-q^8-2q^6+2q^4+q^3-q^2)/4$
5	$(q^{11}-q^{10}+q^6-q^5-q^3+q)/5$
6	$(3q^{19}-3q^{18}+3q^{17}-q^{16}-2q^{15}-2q^{13}+2q^{12}$
	$-3q^{11}+3q^8+q^7-2q^5+3q^3-q^2-q)/6$

Table 4.1
The numbers of relatively irreducible polynomials of degrees up to 6.

4 Relatively irreducible polynomials

Following the terminology of Hodge & Pedoe (1952), Section X.11, we call an irreducible polynomial *relatively irreducible* if it is not absolutely irreducible, that is, if it factors over some extension field. See (5.21) for an example. Over an algebraically closed field there are no relatively irreducible polynomials, and so we only consider the combinatorial problem in this section.

A univariate polynomial $f \in \mathbb{F}_q[x]$ is called *exceptional* if all irreducible factors of $(f(x)-f(y))/(x-y)$ are relatively irreducible. This property is equivalent to f being a permutation polynomial over infinitely many finite extension fields of $\mathbb{F}_q$. There is substantial literature about this topic; see e.g. Lidl & Niederreiter (1983), §7.4, Guralnick & Müller (1997) and the references therein. By slight abuse of notation, also relatively irreducible polynomials and their products have been called exceptional (von zur Gathen *et al.* (1996)).

A relatively irreducible polynomial is the product of all conjugates of an irreducible polynomial over some extension field. We denote as $E_n^=(\mathbb{F}_q) \subseteq I_n^=(\mathbb{F}_q)$ the set of all relatively irreducible polynomials, of degree exactly n.

THEOREM 4.1. *Let $n \geq 2$, let $\ell \geq 2$ be the smallest prime divisor of n, and*

$$\varepsilon_n(q) = \frac{q^{-n^2(\ell-1)/2\ell}(1-q^{-1})}{\ell(1-q^{-\ell})(1-q^{-n-1})},$$

$$\delta_n(q) = \begin{cases} 2q^{-2n+2} & \text{if } n \text{ is prime,} \\ 2q^{-n+\ell+1} & \text{if } n = 6, \\ 2q^{-n+\ell} & \text{otherwise.} \end{cases}$$

Then

(i) $\left|\dfrac{\#E_n^=(\mathbb{F}_q)}{\#B_n^=(\mathbb{F}_q)} - \varepsilon_n(q)\right| \le \varepsilon_n(q)\cdot\delta_n(q)$.

(ii) $\varepsilon_n(q) \le q^{-n^2(\ell-1)/2\ell}/\ell \le q^{-n^2/4}/2$ *and*

$$\#E_n^=(\mathbb{F}_q) < \#B_n^=(\mathbb{F}_q)\cdot q^{-n^2/4} \le q^{(n^2+6n+4)/4}.$$

(iii) If n is prime, then $\varepsilon_n(q) \le q^{-n(n-1)/2}/n$ and

$$\#E_n^=(\mathbb{F}_q) = (q-1)(q^{2n}+q^n-q^2-q)/n.$$

PROOF. For a positive integer divisor k of n, an automorphism $\sigma \in G_k = \mathrm{Gal}(\mathbb{F}_{q^k}\colon \mathbb{F}_q)$ and a polynomial g over $\mathbb{F}_{q^k}$, the application of σ to the coefficients of g yields a polynomial g^σ. We consider

$$\varphi_{n,k}\colon \begin{array}{c} B_{n/k}(\mathbb{F}_{q^k}) \longrightarrow B_n(\mathbb{F}_q), \\ g \longmapsto \prod_{\sigma\in G_k} g^\sigma. \end{array}$$

Then the restriction of $\varphi_{n,k}$ to constants is the norm of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, and indeed $\operatorname{im}\varphi_{n,k} \subseteq B_n(\mathbb{F}_q)$. The k conjugates g^σ, with $\sigma \in G_k$, are pairwise non-associate unless and only unless the coefficients of some nonzero constant multiple ag of g are contained in a proper subfield of $\mathbb{F}_{q^k}$, that is, $ag \in \mathbb{F}_{q^s}[x,y]$ with $a \in \mathbb{F}_{q^k}^\times$ and $s|k$, $s<k$. If $a=1$ and g is irreducible, then for the smallest such s,

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

is irreducible of degree ns/k, and $\varphi_{n,k}(g) = h^{k/s}$. If no such s exists, then $\varphi_{n,k}(g)$ is irreducible in $\mathbb{F}_q[x,y]$. Furthermore, if g (or one of its constant multiples) is relatively irreducible in $\mathbb{F}_{q^k}[x,y]$, then $\varphi_{n,k}(g) = \varphi_{n,j}(h)$ for an appropriate multiple j of k and $h \in I_{n/j}(\mathbb{F}_{q^j})$. Thus we set for any integer m

$$I_m^+(\mathbb{F}_{q^k}\colon\mathbb{F}_q) = I_m^=(\mathbb{F}_{q^k}) \setminus \Big(E_m^=(\mathbb{F}_{q^k}) \cup \bigcup_{1\ne s|k} \mathbb{F}_{q^k}^\times \cdot I_m^=(\mathbb{F}_{q^{k/s}})\Big) \subseteq B_m(\mathbb{F}_{q^k}), \quad (4.2)$$

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

where $A\cdot B = \{ab\colon a\in A, b\in B\}$. Then the $E_{n,k} \subseteq I_n^=(\mathbb{F}_q)$ are pairwise disjoint, and

$$E_n^=(\mathbb{F}_q) = \bigcup_{1\ne k|n} E_{n,k}. \quad (4.3)$$

What are the fibers in $I_{n/k}^+(\mathbb{F}_{q^k}\colon\mathbb{F}_q)$ of $\varphi_{n,k}$ over $E_{n,k}$? If $\varphi_{n,k}(g) = \varphi_{n,k}(h)$, then, since h is irreducible, it divides one of the factors in $\varphi_{n,k}(g)$. Since the degrees are equal, it follows that $h = ag^\sigma$ for some $\sigma\in G_k$ and $a\in\mathbb{F}_{q^k}$ with $\varphi_{n,k}(a)=1$. We denote as $N = \{a\in\mathbb{F}_{q^k}\colon \varphi_{n,k}(a)=1\}$ the set of elements of norm 1. Then we have seen that the fiber of $\varphi_{n,k}(g)$ is a subset of $\{ag^\sigma\colon (a,\sigma)\in$

$N \times G_k\}$. On the other hand, for $g \in I^+_{n/k}(\mathbb{F}_{q^k} \colon \mathbb{F}_q)$ the polynomials ag^σ, with $(a, \sigma) \in N \times G_k$, are pairwise distinct for the following reason. Suppose that $g = ag^\sigma$. If we let $g_0, ..., g_r \in \mathbb{F}_{q^k}$ be the nonzero coefficients of g, then $g_i = ag_i^\sigma$, $g_i/g_0 = (g_i/g_0)^\sigma$, and $g_i/g_0 \in F \subseteq \mathbb{F}_{q^k}$ for all i, where F is the fixed field of σ. Now for any $g \in I^+_{n/k}(\mathbb{F}_{q^k} \colon \mathbb{F}_q)$, F is not a proper subfield, so that $\sigma = \mathrm{id}$ and $a = 1$. It follows that each fiber of $\varphi_{n,k}$ has $\#(N \times G_k) = k(q^k - 1)/(q - 1)$ elements. Thus

$$\begin{aligned} \#E_{n,k} &= \frac{q-1}{k(q^k-1)} \#I^+_{n/k}(\mathbb{F}_{q^k} \colon \mathbb{F}_q) \\ &\leq \frac{(q-1)(q^k)^{b_{n/k}}(1-(q^k)^{-n/k-1})}{k(q^k-1)} \\ &= \frac{(q-1)(1-q^{-n-k})q^{3n/2+n^2/2k}}{k(1-q^{-k})}. \end{aligned} \tag{4.4}$$

If $\ell = n$, so that n is prime, then

$$\begin{aligned} I^+_1(\mathbb{F}_{q^n}) &= I^=_1(\mathbb{F}_{q^n}) \setminus \mathbb{F}^\times_{q^n} \cdot I^=_1(\mathbb{F}_q), \\ \#E^=_n(\mathbb{F}_q) = \#E_{n,n} &= \frac{(q-1)\Big(q^{3n} - q^n - \frac{q^n-1}{q-1}(q^3-q)\Big)}{n(q^n-1)} \\ &= (q-1)(q^{2n}+q^n-q^2-q)/n, \\ \frac{\#E^=_n(\mathbb{F}_q)}{\#B^=_n(\mathbb{F}_q)} - \varepsilon_n(q) &= -\varepsilon_n(q) \cdot q^{-2n+2}(1+q^{-1}+q^{-2}-q^{-n}-q^{-n-1}) \\ &> -\varepsilon_n(q) \cdot 2q^{-2n+2}, \\ \frac{\#E^=_n(\mathbb{F}_q)}{\#B^=_n(\mathbb{F}_q)} &< \varepsilon_n(q) \leq q^{-n(n-1)/2}/n < q^{-n^2/4}. \end{aligned} \tag{4.5}$$

This proves all claims in the case $\ell = n$. We may now assume that $n \geq 4$ and $\ell < n$, so that in fact $\ell \leq \sqrt{n}$. The quantity in (4.4) is monotonously decreasing in k, since k is a divisor of n and

$$1 - q^{-n-k} = (1-q^{-k})(1+q^{-k}+q^{-2k}+\cdots+q^{-n}).$$

Among the admissible values of k, its maximum is obtained at $k = \ell$, and all

other values are not more than that for $k = \ell + 1$. Thus

$$\begin{aligned}\frac{\#E_n(\mathbb{F}_q)}{\#B_n(\mathbb{F}_q)} &\leq \frac{1}{q^{b_n}(1-q^{-n-1})} \sum_{1\neq k|n} \#E_{n,k} \\ &\leq \frac{1}{q^{b_n}(1-q^{-n-1})} \sum_{1\neq k|n} \frac{(q-1)(1-q^{-n-k})q^{3n/2+n^2/2k}}{k(1-q^{-k})} \\ &= \varepsilon_n(q)\left(1-q^{-n-\ell} + \sum_{\ell<k|n} \frac{\ell(1-q^{-\ell})(1-q^{-n-k})q^{-(k-\ell)n^2/2k\ell}}{k(1-q^{-k})}\right) \\ &< \varepsilon_n(q)\left(1-q^{-n-\ell} + \sum_{\ell<k|n} q^{-(k-\ell)n^2/2k\ell}\right).\end{aligned}$$

We let $K = \{k \in \mathbb{N}\colon k|n, \ell < k\}$, so that $\#K = d(n) - 2 = n^{o(1)}$, where $d(n)$ is the number of divisors of n (Hardy & Wright (1985), Theorem 315), but only use the coarse estimate $\#K \leq n-2 \leq 2^{n/6} \leq q^{n/6}$; the middle inequality holds for $n \geq 29$, and one checks that $\#K \leq 2^{n/6}$ for $4 \leq n \leq 28$. Since n is composite, K is nonempty, and we let k_0 be its minimal element. Furthermore, we let $S = \sum_{k\in K} q^{-(k-\ell)n^2/2k\ell}$. When $n = 6$, we have $S = q^{-3} + q^{-30} < 2q^{-3} = 2q^{-n+\ell+1}$. For the upper bound in (i), it is now sufficient to show that for $n \neq 6$

$$S \leq 2q^{-n+\ell}. \tag{4.6}$$

The summands of S are monotonically decreasing with k, and therefore $S \leq \#K \cdot q^{-(k_0-\ell)n^2/2k_0\ell}$, so that it is sufficient to prove that

$$\frac{7n}{6} \leq \frac{(k_0-\ell)n^2}{2k_0\ell} + \ell. \tag{4.7}$$

We now distinguish three cases. The first case is where $k_0 = \ell+1$. If $\ell \geq 3$, then $\ell+1$ is even and 2 would also be a divisor of n, contradicting the minimality of ℓ. Thus $\ell = 2$, $k_0 = 3$, and (4.7) holds for all multiples $n \geq 12$ of 6. The exceptional case $n = 6$ has been dealt with above.

For the other cases, we may assume that $k_0 \geq \ell + 2$. Since the right hand side in (4.7) is monotonically increasing with k_0, we may substitute $k_0 = \ell+2$, and (4.7) will follow from the claim

$$\frac{7n}{6} \leq \frac{n^2}{\ell(\ell+2)} + \ell. \tag{4.8}$$

The second case is when $\ell \leq \sqrt{n/3}$. Then $n \geq 3\ell^2 \geq 12$, and we have

$$\frac{n^2}{\ell(\ell+2)} \geq \frac{n^2}{\sqrt{n/3}\cdot(\sqrt{n/3}+2)} = \frac{n^2}{n/3+2\sqrt{n/3}} \geq \frac{3n}{2} > \frac{7n}{6} - \ell.$$

The remaining case is $\ell > \sqrt{n/3}$. If n has three or more prime factors (not necessarily distinct), then $n \geq \ell^3 > 3^{-3/2} n^{3/2}$ and thus $n < 27$; all such numbers are even, and $2 = \ell > \sqrt{n/3}$ leaves only $n = 8$, in which case (4.6) is valid. Thus n now is either ℓ^2 or ℓk_0 with $\ell + 2 \leq k_0 < n$ and k_0 prime. If $n = \ell^2$, then $K = \{n\}$ and

$$S = q^{-(n-\ell)n/2\ell} \leq q^{-n+\ell},$$

since $n \geq 2\ell$ and $n - \ell \leq (n-\ell)n/2\ell$. If $n = \ell k_0$ with $\ell + 2 \leq k_0 < n$, then $K = \{k_0, n\}$ and

$$S \leq q^{-2n^2/2n} + q^{-(n-\ell)n^2/2n\ell} \leq 2q^{-n} < q^{-n+\ell},$$

since $3\ell < \ell k_0 = n$. Thus (4.6) is proved in all cases.

As a lower bound, we have for composite n

$$\#E_n^=(\mathbb{F}_q) \geq \#E_{n,\ell} \geq \frac{q-1}{\ell(q^\ell - 1)} \Big(\#I_{n/\ell}^=(\mathbb{F}_{q^\ell}) - \#(\mathbb{F}_{q^\ell}^\times \cdot I_{n/\ell}^=(\mathbb{F}_q)) \Big),$$

since ℓ is prime and there are no proper intermediate fields between $\mathbb{F}_q$ and $\mathbb{F}_{q^\ell}$. Corollary 2.14 implies that

$$\begin{aligned} \frac{\#E_n^=(\mathbb{F}_q)}{\#B_n^=(\mathbb{F}_q)} &\geq \frac{(q-1)\Big((q^\ell)^{b_{n/\ell}} (1 - (q^\ell+2)(q^\ell)^{-n/\ell}) - \frac{(q^\ell-1)q^{b_{n/\ell}}}{q-1} \Big)}{\ell(q^\ell-1)q^{b_n}(1-q^{-n-1})} \\ &= \varepsilon_n(q) \left(1 - (q^\ell+2)q^{-n} - \frac{(q^\ell-1)q^{-(\ell-1)b_{n/\ell}}}{q-1} \right). \end{aligned}$$

In order to estimate the last summand, we first note that

$$1 + \frac{2\ell}{n} \leq 1 + \frac{2}{\sqrt{n}} \leq 2 \leq \ell,$$

since $2 \leq \ell \leq \sqrt{n}$. It follows that $n + 2\ell \leq n\ell$ and

$$\begin{aligned} n^2 + 3n\ell + 2\ell^2 = (n+\ell)(n+2\ell) &\leq (n+\ell)n\ell = n^2\ell + n\ell^2, \\ n &\leq \frac{(\ell-1)(n^2+3n\ell+2\ell^2)}{2\ell^2} - \ell = (\ell-1)b_{n/\ell} - \ell, \\ \frac{(q^\ell-1)q^{-(\ell-1)b_{n/\ell}}}{q-1} &< q^{-(\ell-1)b_{n/\ell}+\ell} \leq q^{-n}, \\ \frac{\#E_n^=(\mathbb{F}_q)}{\#B_n^=(\mathbb{F}_q)} &\geq \varepsilon_n(q)(1-(q^\ell+3)q^{-n}) \geq \varepsilon_n(q)(1-2q^{-n+\ell}). \end{aligned}$$

The estimates in (ii) follow from the fact that $n, \ell \geq 2$ and

$$\begin{aligned} 1 - q^{-1} &\leq (1 - q^{-\ell})(1 - q^{-n-1}), \\ \varepsilon_n(q) &\leq q^{-n^2(\ell-1)/2\ell}/\ell \leq q^{-n^2/4}/2, \\ \delta_n(q) &\leq 1. \end{aligned}$$

□

We denote by

$$A_n^=(\mathbb{F}_q) = I_n^=(\mathbb{F}_q) \setminus E_n^=(\mathbb{F}_q)$$

the set of absolutely irreducible polynomials over $\mathbb{F}_q$ of degree n. Then the partition (4.3) with (4.2) leads to the exact formula

$$\#E_n^=(\mathbb{F}_q) = \sum_{\substack{1 \neq k \mid n \\ d \mid k}} \frac{\mu(d)(q-1)}{k(q^{k/d}-1)} \#A_{n/k}^=(\mathbb{F}_{q^{k/d}}),$$

where μ is the Möbius function. When n is prime, this is the formula in Theorem 4.1(iii). We also obtain a lower bound on the number of absolutely irreducible polynomials.

COROLLARY 4.9. *For $n \geq 2$, we have*

$$\#I_n^=(\mathbb{F}_q) \geq \#A_n^=(\mathbb{F}_q) > q^{b_n}(1 - (q+2)q^{-n}).$$

PROOF. We abbreviate

$$w_n = q^{-1} + q^{n-b_n}(\#R_n^=(\mathbb{F}_q) + \#E_n^=(\mathbb{F}_q)).$$

It is sufficient to show that

$$w_n \leq q + 2, \tag{4.10}$$

since then

$$\begin{aligned} \#A_n^=(\mathbb{F}_q) &= \#B_n^=(\mathbb{F}_q) - \#R_n^=(\mathbb{F}_q) - \#E_n^=(\mathbb{F}_q) \\ &= q^{b_n}(1 - q^{-n-1}) - q^{b_n-n}(w_n - q^{-1}) \\ &= q^{b_n}(1 - w_n q^{-n}) \\ &\geq q^{b_n}(1 - (q+2)q^{-n}). \end{aligned}$$

We have from (2.12) and Theorem 4.1 (ii) that

$$\begin{aligned} w_n &\leq q^{-1} + q^{n-b_n}(q^{b_n}(1 - q^{-n-1})(q+1)q^{-n}(1 + 2q^{-n+3}) + q^{b_n}(1 - q^{-n-1})q^{-n^2/4}) \\ &< q^{-1} + (q+1)(1 + 2q^{-n+3}) + q^{n-n^2/4} \leq q + 2 \end{aligned}$$

for $n \geq 7$. The last inequality also holds when $n \geq 5$ and $q \geq 4$, but we now have to consider the cases $n \leq 6$ separately. An alternative to the following

rather tedious calculations is to substitute upper bounds given by appropriate leading terms in Tables 2.1 and 4.1. Throughout the computations, we use Theorem 4.1 without explicit mention, and also $q^i \le 2^{-j} q^{i+j}$ for all i, j. For $n = 3, 5$, or 6, we examine the proof of Theorem 2.1 (ii) in detail. From (2.6) we find

$$\begin{aligned}
w_2 &< q^{-1} + q^{-4}\left(\frac{q^6(q+1)q^{-2}}{2} + \frac{(q-1)q^4}{2}\right) = q^{-1} + q < q + 2. \\
\#R_3^=(\mathbb{F}_q) &= \#\text{ im } \mu_{3,1} \le \frac{1}{q-1}(q^3 - q)q^6(1 - q^{-3}) < q^8(1 + q^{-1}), \\
\#E_3^=(\mathbb{F}_q) &< \frac{1}{3}q^6(q-1)(1+q^{-3}), \\
w_3 &< q^{-1} + q^{-7}\left(q^8 + q^7 + \frac{1}{3}(q^7 - q^6 + q^4 - q^3)\right) \\
&= q + \frac{4}{3} + \frac{2}{3}q^{-1} + \frac{1}{3}q^{-3} \le q + \frac{41}{24} < q + 2.
\end{aligned}$$

For $n = 4$, we have from Tables 2.1 and 4.1 that

$$\begin{aligned}
\#R_4^=(\mathbb{F}_q) &\le q^{12} + \frac{3}{2}q^{11} - \frac{1}{2}q^{10} - \frac{5}{4}q^9, \\
\#E_4^=(\mathbb{F}_q) &\le \frac{1}{2}q^{11} - \frac{1}{2}q^{10} + \frac{1}{4}q^9, \\
w_4 &\le q^{-1} + q^{-11}(q^{12} + 2q^{11} - q^{10} - q^9) = q + 2 - q^{-2} < q + 2.
\end{aligned}$$

For $n = 5$, we use

$$\begin{aligned}
\#\text{ im } \mu_{4,1} &\ge \frac{1}{q-1}(\#I_1^=(\mathbb{F}_q) \times I_3^=(\mathbb{F}_q)) \ge \frac{(q^3 - q)q^{10}(1 - (q+2)q^{-3})}{q-1} \\
&= q^{12}(1 + q^{-1})(1 - q^{-2} - 2q^{-3}), \\
R_5^=(\mathbb{F}_q) &= \mu_{5,1}(B_1^=(\mathbb{F}_q) \times (B_4^=(\mathbb{F}_q) \setminus \text{ im } \mu_{4,1})) \cup \mu_{5,2}(B_2^=(\mathbb{F}_q) \times B_3^=(\mathbb{F}_q)), \\
\#R_5^=(\mathbb{F}_q) &\le \frac{1}{q-1}\Bigg((q^3 - q) \cdot (q^{15}(1 - q^{-5}) - q^{12}(1 + q^{-1})(1 - q^{-2} - 2q^{-3})) \\
&\qquad + q^6(1 - q^{-3}) \cdot q^{10}(1 - q^{-4})\Bigg) \\
&= q^{17} + q^{16} + q^{15} - q^{13} - q^{12} + 2q^{11} + 4q^{10} + q^9 \\
&\le q^{17} + q^{16} + q^{15} - q^{13} + \frac{9}{8}q^{12}, \\
\#E_5^=(\mathbb{F}_q) &\le (q-1)(q^{10} + q^5)/5 < q^{11}/5. \\
w_5 &\le q^{-1} + q^{-16}(q^{17} + q^{16} + q^{15} - q^{13} + \frac{9}{8}q^{12} + \frac{1}{5}q^{11}) \\
&\le q + 2 - \frac{31}{80}q^{-3} < q + 2.
\end{aligned}$$

For $n = 6$, we use

$$R_6^=(\mathbb{F}_q) = \text{ im } \mu_{6,1} \cup \mu_{6,2}(I_2^=(\mathbb{F}_q) \times B_4^=(\mathbb{F}_q)) \cup \text{ im } \mu_{6,3}$$

and the fact that $\#\mu_{6,3}^{-1}(fg) \geq 2(q-1)$ if $f, g \in B_3^=(\mathbb{F}_q)$ are distinct. Thus

$$\begin{aligned}
\#R_6^=(\mathbb{F}_q) &\leq \frac{1}{q-1}\Bigg((q^3-q)\cdot q^{21}(1-q^{-6}) \\
&\quad + q^6(1-q^{-3})(1-\frac{(q+1)q^{-2}}{2})\cdot q^{15}(1-q^{-5}) \\
&\quad + \frac{1}{2}q^{10}(1-q^{-4})(q^{10}(1-q^{-4})+1)\Bigg) \\
&\leq q^{23}+q^{22}+q^{20}(1-q^{-3})(1+\frac{q^{-1}}{2})+\frac{1}{2}q^{19}(1+q^{-1}+q^{-2}+q^{-3}) \\
&= q^{23}+q^{22}+q^{20}+q^{19}+\frac{1}{2}q^{18}-\frac{1}{2}q^{17} < q^{23}+\frac{45}{32}q^{22}, \\
\#E_6^=(\mathbb{F}_q) &\leq \frac{q^{28}(1-q^{-7})\cdot q^{-9}(1-q^{-1})\cdot(1+2q^{-3})}{2(1-q^{-2})(1-q^{-7})} \\
&= \frac{q^{19}(1+2q^{-3})}{2(1+q^{-1})} \leq \frac{1}{2}q^{19} \leq \frac{1}{16}q^{22}, \\
w_6 &\leq q^{-1}+q^{-22}(q^{23}+\frac{47}{32}q^{22}) \leq q+\frac{1}{2}+\frac{47}{32} < q+2. \qquad \square
\end{aligned}$$

Carlitz (1936) considers the special case of irreducible bivariate polynomials over $\mathbb{F}_q$ that factor into linear polynomials over some extension field of $\mathbb{F}_q$. He calls these polynomials *factorable* and determines their number exactly as

$$\frac{1}{n}\sum_{k|n}\mu(\frac{n}{k})\frac{q^2(q^{2k}-1)}{q^k-1}.$$

Simply replacing 2 by r in Carlitz' formula yields the corresponding value for r variables.

Fredman (1972) determines the number of absolutely irreducible bivariate polynomials. He gives an exact formula and the fraction $1-q^{-m}$ as approximation, when $m = \deg_x f$ is fixed.

5 Singular polynomials

A plane algebraic curve is *nonsingular* (or smooth) *at a point* P on it if the tangent at P is well-defined, that is, the two partial derivatives of the defining equation do not vanish simultaneously; otherwise, it is *singular* at P. The

curve is *nonsingular* if it is nonsingular at all points on it, and *singular* otherwise.

Many useful properties of algebraic curves, for example the Weil bounds, take their simplest form for nonsingular curves. Singularities also complicate the analysis of some algorithms dealing with curves. The goal of this section is to show quantitatively that there are few singular curves. We only deal with affine curves.

Rather than speaking about plane curves, we consider bivariate polynomials $f \in F[x, y]$ over a field F. The (affine) curve $V(f)$ of f is the set

$$V(f) = \{(u, v) \in F^2 \colon f(u, v) = 0\} \subseteq F^2$$

of zeroes of f. A point $P \in F^2$ is *singular* on $V(f)$ if and only if

$$f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0. \tag{5.1}$$

When $P = (u, v)$ with $u, v \in F$, then $m_P = (x - u, y - v) \subseteq F[x, y]$ is the *maximal ideal* of P, and the *singularity ideal*

$$s_P = m_p^2 = (x - u, y - v)^2 \subseteq F[x, y]$$

contains precisely the polynomials satisfying (5.1). The quotient ring

$$F[x, y]/s_P = F + (x - u)F + (y - v)F \tag{5.2}$$

is a 3-dimensional vector space over F, and

$$S_n(F) = \{f \in B_n(F) \colon f \in s_P \text{ for some } P \in F^2\}$$

is the set of polynomials with a rational singularity.

This section presents the following material:

- an exact determination of $\#S_n(\mathbb{F}_q)$ for sufficiently large degree, due to Ragot and to Lenstra,
- an approximate count, valid also for small degree,
- bounds for absolutely but not rationally singular polynomials,
- some examples.

Ragot (1997), Proposition 5.4.6, page 105, and Ragot (1999), Propositions 4.1

and 5.5, show that

$$\frac{\#S_n(\mathbb{F}_q)}{\#B_n(\mathbb{F}_q)} = 1 - (1 - q^{-3})^{q^2} \tag{5.3}$$

for $n \geq 4q - 2$. Ragot derives his results for the general multivariate case. Hendrik Lenstra found the exact degree condition for (5.3) to hold.

THEOREM 5.4. *(Lenstra 2006) (5.3) holds if and only if $n \geq 3q - 2$.*

PROOF. For two distinct points P and Q in $\mathbb{F}_q^2$, the maximal ideals m_P and m_Q in $R = \mathbb{F}_q[x, y]$ are comaximal, so that $m_P + m_Q = 1$. Hence also $s_P = m_P^2$ and s_Q are comaximal. The Chinese Remainder Theorem says that

$$R/\prod_{P \in \mathbb{F}_q^2} s_P \cong \prod_{P \in \mathbb{F}_q^2} R/s_P.$$

We denote as

$$\varphi\colon R \longrightarrow \prod_{P \in \mathbb{F}_q^2} R/s_P$$

the product of the canonical ring homomorphisms, so that

$$\begin{gathered} f \text{ singular at } P \iff f \in s_P \iff (\varphi(f))_P = 0, \\ f \text{ rationally nonsingular} \iff (\varphi(f))_P \neq 0 \text{ for all } P \in \mathbb{F}_q^2. \end{gathered}$$

We write $\varphi_n = \varphi \restriction B_n(\mathbb{F}_q)$ for the restriction of φ to $B_n(\mathbb{F}_q) \subseteq R$. Then

$$B_n(\mathbb{F}_q) \setminus S_n(\mathbb{F}_q) = \varphi_n^{-1}\left(\prod_{P \in \mathbb{F}_q^2} ((R/s_P) \setminus \{0\})\right). \tag{5.5}$$

For each $P \in \mathbb{F}_q^2$, R/s_P has q^3 elements, and thus the product in (5.5) has $(q^3 - 1)^{q^2}$ elements.

Now φ_n is a linear map of vector spaces over $\mathbb{F}_q$. We claim that (5.3) holds if and only if φ_n is surjective. If it is, then each fiber of φ_n has $q^{b_n - 3q^2}$ elements, and

$$\begin{aligned} \frac{\#S_n(\mathbb{F}_q)}{\#B_n(\mathbb{F}_q)} &= q^{-b_n} \cdot (q^{b_n} - q^{b_n - 3q^2} \cdot (q^3 - 1)^{q^2}) \\ &= 1 - (1 - q^{-3})^{q^2}, \end{aligned}$$

so that (5.3) holds. On the other hand, $\varphi_n^{-1}(\varphi_n(f)) \subseteq S_n(\mathbb{F}_q)$ for all $f \in S_n(\mathbb{F}_q)$. Thus if we write

$$\frac{\#S_n(\mathbb{F}_q)}{\#B_n(\mathbb{F}_q)} = \frac{\#\varphi_n(S_n(\mathbb{F}_q))}{\#\varphi_n(B_n(\mathbb{F}_q))} = \frac{a}{b}$$

with $a, b \in \mathbb{N}$ coprime, then b divides $\#\varphi_n(B_n(\mathbb{F}_q))$. If (5.3) holds, then $b = q^{3q^2} = \#\prod_{P\in\mathbb{F}_q^2} R/s_P$, so that φ_n is surjective.

We have

$$\prod_{P\in\mathbb{F}_q^2} m_P = (x^q - x, y^q - y),$$

since the right hand ideal is included in the left hand one, and both have codimension q^2. It follows that

$$\begin{aligned}\prod_{P\in\mathbb{F}_q^2} s_P = \prod_{P\in\mathbb{F}_q^2} m_P^2 = (\prod_{P\in\mathbb{F}_q^2} m_P)^2 = (x^q - x, y^q - y)^2 \\ = \left((x^q - x)^2, (x^q - x)(y^q - y), (y^q - y)^2\right).\end{aligned}$$

We denote this ideal as I and have the following system U_I of $3q^2$ representatives for R/I as a vector space over $\mathbb{F}_q$:

$$\begin{aligned}U_I = \{x^i y^j \colon (0 \le i < 2q \text{ and } 0 \le j < q) \text{ or} \\ (0 \le i < q \text{ and } q \le j < 2q)\}.\end{aligned}$$

$B_n(\mathbb{F}_q)$ has an $\mathbb{F}_q$-basis

$$T_n = \{x^i y^j \colon i + j \le n\}$$

of size $(n+1)(n+2)/2$. Figure 5.1 gives a graphical representation of the two sets of exponents, in a case where $n \ge 3q - 2$.

We claim that im φ_n is the vector space spanned by $U_I \cap T_n$. For any $x^i y^j \in U_I \cap T_n$, we have $x^i y^j = \varphi_n(x^i y^j) \in$ im φ_n. On the other hand, for any $x^i y^j \in T_n$ with $i \ge 2q$, the left hand side in

$$x^i y^j - x^{i-2q}(x^q - x)^2 y^j \equiv x^i y^j \mod I$$

is a linear combination of monomials in T_n with degree in x at most $i-q+1 < i$. Continuing by induction on the degree, one finds that each element of T_n is congruent modulo I to a linear combination of monomials with degree in x less than $2q$. The corresponding reduction by $(y^q - y)^2$ makes the degree in y less than $2q$, and finally reduction by $(x^q - x)(y^q - y)$, if necessary, leads to monomials in $U_I \cap T_n$. Thus dim im $\varphi_n = \#(U_I \cap T_n)$, and we have

$$\begin{aligned}\varphi_n \text{ surjective} &\iff \#(U_I \cap T_n) = 3q^2 = \#U_I \\ &\iff U_I \subseteq T_n \iff n \ge 3q - 2.\end{aligned}$$ □

What can we say about $\#S_n(\mathbb{F}_q)$ when $n < 3q - 2$? The binomial expansion

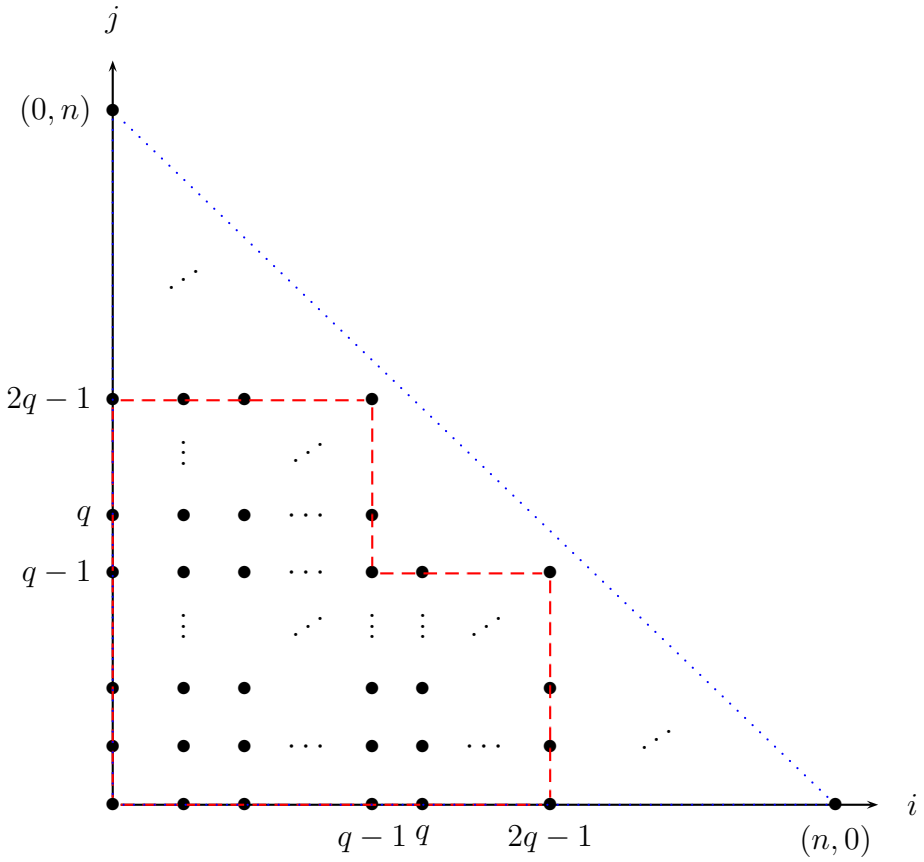


Figure 5.1. The exponents making up U_I and T_n.

of (5.3) yields

$$q^2 \cdot q^{-3} - \binom{q^2}{2} q^{-6} + - \cdots = q^{-1} - q^2/2 + - \cdots .$$

We now prove an estimate that is valid also for small n and consistent with the first two terms of this expansion.

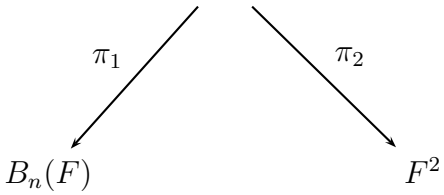
THEOREM 5.6. *Let $n \geq 2$.*

(i) Let F be algebraically closed. Then $S_n(F)$ is an irreducible subvariety of $B_n(F)$ with codimension 1 and degree at most $(n+1)n^2$.
(ii) For $n \geq 3$, we have

$$\frac{1}{q} - \frac{1}{2q^2} \leq \frac{\#S_n(\mathbb{F}_q)}{\#B_n(\mathbb{F}_q)} \leq \frac{1}{q}.$$

PROOF. (i) We consider the singularity correspondence

$$C = \{(f, P) \in B_n(F) \times F^2 \colon f \text{ singular at } P \in V(f)\}$$



(5.7)

with its two projections π_1 and π_2. For any $P \in F^2$, the fiber $\pi_2^{-1}(P) \cong s_P \subseteq B_n(F)$ is a linear subspace of codimension 3.

We want to use the theorem on the fiber dimension to show that C is irreducible of codimension 3. In order to apply this theorem, we have to consider the projective version of our situation. So we take $\mathbb{P}^2 \supset F^2$ with projective coordinates x, y, z. The projective version of some

$$f = \sum_{i+j \le n} f_{ij} x^i y^j \in B_n(F)$$

is the ternary form

$$\widetilde{f} = \sum_{i+j \le n} f_{ij} x^i y^j z^{n-i-j} \in F[x, y, z]_n$$

of degree n, and any form $g \in F[x, y, z]_n$ can be written in this way: $g = \widetilde{g(x, y, 1)}$. (Note that $\widetilde{\ }$ depends on n, not on the degree of f if that is less than n.)

$F[x, y, z]_n$ is a vector space of dimension b_n, and its projectivization $T-$ that is, the nonzero forms modulo multiplication by $F^\times-$ is a projective space of dimension $b_n - 1$ with coordinate functions f_{ij} for $i + j \le n$. Our notation will not distinguish between a form $\widetilde{f}$ and its class in T. We thus have a map $\widetilde{\ }\colon B_n(F)\backslash\{0\} \to T$ and $\widetilde{C} \subseteq \widetilde{B_n(F)} \times F^2 = T \times F^2 \subseteq T \times \mathbb{P}^2$. Denoting partial derivatives by subscripts, we have

$$(\widetilde{f})_x = \widetilde{f_x} = \sum_{i+j \le n} i f_{ij} x^{i-1} y^j z^{n-i-j},$$

and similarly for $(\widetilde{f})_y = \widetilde{f_y}$ and $(\widetilde{f})_z = \widetilde{f_z}$. For any $h \in T$, we have

$$nh = xh_x + yh_y + zh_z. \tag{5.8}$$

We define the subvariety

$$X = \{(h, P) \in T \times \mathbb{P}^2 : h(P) = h_x(P) = h_y(P) = h_z(P) = 0\}.$$

Then (5.8) shows that

$$\widetilde{C} = X \cap \{z \neq 0\}.$$

It was noted above that for $P \in F^2 = \{z \neq 0\} \subseteq \mathbb{P}^2$, the fiber $\pi_2^{-1}(P)$ is a linear subspace of $B_n(F)$ with codimension 3. If we denote as

$$\widetilde{\pi}_2 : X \to \mathbb{P}^2$$

the second projection, then for such P we have $\widetilde{\pi}_2^{-1}(P) = \widetilde{\pi_2^{-1}(P)\backslash\{0\}}$. Since both ambient space and fiber lose one dimension under projectivization, this is a projective linear subspace of T with codimension 3. Furthermore, the definition of X is symmetric in x, y, z, so that the latter statement is also true over the other two standard open sets $\{y \neq 0\}$ and $\{z \neq 0\}$, and each fiber of $\widetilde{\pi}_2$ is a $\mathbb{P}^{b_n-4}$. By the theorem on the fiber dimension (see Shafarevich (1974), Theorem I.6.8; Harris (1992), Theorem 11.14), X is an irreducible variety of dimension $2 + b_n - 4 = b_n - 2$, and so is its dense open subset $\widetilde{C}$. It follows that C is an irreducible affine variety of dimension $b_n - 1$ and codimension 3. Furthermore, the set

$$S_n(F) = \operatorname{im} \pi_1 \subseteq B_n(F)$$

of singular polynomials is an irreducible affine subvariety of codimension c with $1 \leq c \leq 3$, since its projectivization is the closed set $\operatorname{im} \widetilde{\pi}_1 \subseteq T$. Any squarefree $f \in S_n(F)$ has only a finite number of singularities, and these form an open subset of $S_n(F)$ by Theorem 3.9 (i). This subset contains for example $x^n + y$, hence is dense, the generic fiber of π_1 is zero-dimensional, and thus $c = 1$.

C is described by the three equations (5.1) in the coefficients of f and the coordinates of P. These equations have degrees $n + 1$, n, n, respectively, and thus $\deg C \leq (n+1)n^2$, where deg is the usual degree of an affine variety. Since the degree does not increase under a projection, it follows that $S_n(F) \subseteq B_n(F)$ is an irreducible hypersurface of degree at most $(n + 1)n^2$.

(ii) For $P \in \mathbb{F}_q^2$, we have

$$\#(B_n(\mathbb{F}_q) \cap s_P) = q^{b_n-3},$$

and thus

$$\#S_n(\mathbb{F}_q) \leq q^2 \cdot q^{b_n-3} = q^{-1} \cdot \#B_n(\mathbb{F}_q),$$

since $S_n(\mathbb{F}_q) = \bigcup_{P \in \mathbb{F}_q^2} (B_n(\mathbb{F}_q) \cap s_P)$. Furthermore

$$\begin{aligned} \#S_n(\mathbb{F}_q) &\geq \#\{f \in B_n(\mathbb{F}_q) \colon f \text{ has exactly one singularity in } \mathbb{F}_q^2\} \\ &\geq \sum_{P \in \mathbb{F}_q^2} \#(B_n(\mathbb{F}_q) \cap s_P) - \sum_{\substack{P, P' \in \mathbb{F}^2 \\ P \neq P'}} \#(B_n(\mathbb{F}_q) \cap s_P \cap s_{P'}). \end{aligned}$$

So let $P = (u, v)$, $P' = (u', v') \in \mathbb{F}_q^2$, $P \neq P'$, $n \geq 3$, and

$$f = \sum_{2 \leq i+j \leq n} f_{ij}(x-u)^i(y-v)^j \in B_n(\mathbb{F}_q) \cap s_P.$$

The condition that $f \in s_{P'}$ corresponds to three linear equations in the f_{ij}. When we just look at the coefficients of f_{20}, f_{11}, and f_{30}, we have the following 3×3 matrix of coefficients in the linear equations:

$$\begin{pmatrix} (u'-u)^2 & (u'-u)(v'-v) & (u'-u)^3 \\ 2(u'-u) & v'-v & 3(u'-u)^2 \\ 0 & u'-u & 0 \end{pmatrix}. \tag{5.9}$$

The second row, e.g., comes from

$$\begin{aligned} 0 = \frac{\partial f}{\partial x}(u', v') &= \sum i f_{ij}(u'-u)^{i-1}(v'-v)^j \\ &= 2(u'-u) \cdot f_{20} + (v'-v) \cdot f_{11} + 3(u'-u)^2 \cdot f_{30} + \cdots . \end{aligned}$$

The determinant of this matrix is $-(u'-u)^5$. If $u' \neq u$, then

$$\operatorname{codim}_{B_n(\mathbb{F}_q) \cap s_P}(B_n(\mathbb{F}_q) \cap s_P \cap s_{P'}) = 3,$$

and hence $\operatorname{codim}_{B_n(\mathbb{F}_q)}(B_n(\mathbb{F}_q) \cap s_P \cap s_{P'}) = 6$. If $u' = u$, then $v' \neq v$ and the codimension is again 6, by symmetry. Thus

$$\begin{aligned} \#S_n(\mathbb{F}_q) &\geq q^2 \cdot q^{b_n - 3} - q^2(q^2-1)/2 \cdot q^{b_n - 6} \\ &\geq q^{-1} \#B_n(\mathbb{F}_q) \cdot (1 - \frac{1}{2q}). \end{aligned}$$

□

In the case $n = 2$, we have $\dim B_2(\mathbb{F}_q) = 6$ and $f = ((v-v')(x-u) - (u-u')(y-v))^2 \in B_2(\mathbb{F}_q) \cap s_P \cap s_{P'}$ is nonzero, and hence the codimension of $s_P \cap s_{P'}$ in $B_2(\mathbb{F}_q)$ is at most 5. The inequalities used above would only yield a lower bound of $\#B_n(\mathbb{F}_q)/2q$. (In fact, the codimension equals 5, since the 2×2 matrix corresponding to f_{20} and f_{11} has determinant $-(u'-u)^2(v'-v)$, which implies this claim if $u \neq u'$ and $v \neq v'$, and one also verifies it if, say, $u = u'$.)

In fact, we can determine the number of singular quadratic polynomials f, that is, of those that are the product of two linear factors (over the field or a quadratic extension), as follows. Each of them is obtained by a linear shift of

condition	f	(u,v)	$\#(u,v)$	$\#(a,b,c)$	#shifts
$b^2 \neq 4ac$	f	$(0,0)$	1	q^3-q^2	$q^2\cdot(q^3-q^2)$
$b^2=4ac, a\neq 0$	$\frac{1}{4a}(2ax+by)^2$	$(-bv,2av)$	q	$q(q-1)$	$q\cdot q(q-1)$
$a=b=0, c\neq 0$	cy^2	$(u,0)$	q	$q-1$	$q\cdot(q-1)$
$a=b=c=0$	0	(u,v)	q^2	1	1

Table 5.1
The singular quadratics for odd q.

variables from a quadratic

$$f = ax^2 + bxy + cy^2$$

with a singularity at $(0,0)$. Two shifts of distinct such f are distinct, and for most f, two distinct shifts of f are distinct. The squareful f form an exception, where the q^2 shifts only generate q pairwise distinct polynomials. The total

$$\#S_2(\mathbb{F}_q) = q^5 - q^4 + q^3 - q + 1$$

is the sum of the last column in Table 5.1, for odd q. Thus

$$\frac{\#S_2(\mathbb{F}_q)}{\#B_2(\mathbb{F}_q)} = q^{-1} - q^{-2} + q^{-3} - q^{-5} + q^{-6}.$$

In this table, the column "(u,v)" is the set of singularities of f, where u and v denote arbitrary elements of $\mathbb{F}_q$, and "$\#(u,v)$" is their number. "$\#(a,b,c)$" is the number of choices for (a,b,c), and "#shifts" is the number $(q^2/\#(u,v))\cdot \#(a,b,c)$ of polynomials that are linear shifts of the f satisfying the "condition". For even q, in the second line we have $b=0, a\neq 0$, $f=(a^{q/2}x+c^{q/2}y)^2$, and $(u,v)=(c^{q/2}v, a^{q/2}v)$. The other entries and the final count do not change.

Next we study the question of absolute singularity, that is, of polynomials without rational singularity but with one in an algebraic closure. For a finite algebraic field extension $F\subseteq E$ of degree $k=[E:F]$ and $P\in E^2$, we let

$$\begin{aligned} \deg P &= \min\{[D:F]\colon D \text{ a field with } F\subseteq D\subseteq E \text{ and } P\in D^2\},\\ A &= \{P\in E^2\colon \deg P = k\}. \end{aligned} \tag{5.10}$$

If E is Galois over F, then A is the set of $P=(u,v)$ that are not fixed under any automorphism $\sigma\neq \mathrm{id}$ of E over F: $(u,v)\neq(\sigma u,\sigma v)$. If $F=\mathbb{F}_q$, then

$$q^{2k} = \sum_{d|k} \#\{P\in E^2\colon \deg P = d\},$$

and by Möbius inversion

$$\#A = \sum_{d|k} \mu(k/d) q^{2d} = q^{2k}(1-\varepsilon) < q^{2k},$$

with

$$\varepsilon = -\sum_{d|k, d\neq k} \mu(k/d) q^{2d-2k} \leq \sum_{\ell|k, \ell \text{ prime}} q^{-2k(\ell-1)/\ell}.$$

Furthermore, for any subset $C \subseteq E^2$ we set

$$S_n(C\colon F) = \{f \in B_n(F)\colon f \text{ is singular at some } P \in C\}.$$

We take some $P = (u, v) \in E^2$, the natural embedding $\varphi\colon F[x, y] \longrightarrow E[x, y]$, the singularity ideal $s_P \subseteq E[x, y]$, and

$$s_{P,F} = \varphi^{-1}(s_P). \tag{5.11}$$

We have a commutative diagram of F-linear maps:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & s_{P,F} & \longrightarrow & F[x,y] & \longrightarrow & F[x,y]/s_{P,F} & \longrightarrow & 0 \\ & & \downarrow \varphi & & \downarrow \varphi & & \downarrow & & \\ 0 & \longrightarrow & s_P & \longrightarrow & E[x,y] & \longrightarrow & E[x,y]/s_P & \longrightarrow & 0 \end{array}$$

Its rows are exact, the bottom row is E-linear, φ is injective and hence also the right hand downward arrow, and $\dim_E E[x, y]/s_P = 3$, so that $\dim_F E[x, y]/s_P = 3k$. It follows that $\dim_F F[x, y]/s_{P,F} \leq 3k$, and we only need to find a lower bound on this dimension.

LEMMA 5.12. *Let E be separable over F, $\#F \geq 1 + \log_2 k$, and $P \in A$. Then*

(i) $\operatorname{codim}_{F[x,y]} s_{P,F} = 3k$,

(ii) $\operatorname{codim}_{B_n(F)}(s_{P,F} \cap B_n(F)) \begin{cases} = 3k & \text{if } 2k-1 \leq n, \\ \geq 2n-k+2 & \text{if } k \leq n < 2k-1, \\ \geq n+1 & \text{if } n < k. \end{cases}$

PROOF. (i) Let $P = (u, v)$. We first assume that both u and v have degree k over F, and let $h_u, h_v \in F[t]$ be the minimal polynomials of u, v, respectively. Both have degree k. It is sufficient to prove that the following $3k$ polynomials in $F[x, y]$ are linearly independent modulo $s_{P,F}$ over F, since the lower bound $3k$ on the codimension follows:

$$x^i, h_u(x)x^i, h_v(y)y^i \text{ for } 0 \leq i < k. \tag{5.13}$$

So suppose that

$$f = \sum_{0\le i<k} \lambda_i x^i + h_u(x) \sum_{0\le i<k} \mu_i x^i + h_v(y) \sum_{0\le i<k} \nu_i y^i \in s_{P,F},$$

with all $\lambda_i, \mu_i, \nu_i \in F$. Now $h_u(u) = h_v(v) = 0$, and $0 = f(P) = \sum_{0\le i<k} \lambda_i u^i$ implies that all λ_i are zero, since u has degree k. Furthermore,

$$\begin{aligned} 0 = \frac{\partial f}{\partial x}(P) &= (h_u(x) \sum_{i<k} i\mu_i x^{i-1} + \frac{\partial h_u}{\partial t}(x) \sum_{i<k} \mu_i x^i)(P) \\ &= \frac{\partial h_u}{\partial t}(u) \cdot \sum_{i<k} \mu_i u^i. \end{aligned}$$

Since E is separable and hence the derivative of h_u does not vanish at u, the left hand factor is nonzero, and thus the right hand factor vanishes. Again from the degree of u we conclude that all μ_i are zero. Finally, the vanishing of $\partial f/\partial y$ at P implies in the same way that all ν_i are zero.

Now we come to the general case, where u and v together generate E, but not each of them individually. By the Theorem of the Primitive Element in Mihăilescu (2006), $u + tv$ generates E for nonzero $t \in F$ with at most $\omega(k)$ exceptions, at most $\omega(k')$ exceptions, where $k' = \gcd([F(u)\colon F], [F(v)\colon F])$ is a proper divisor of k, and $\omega(m)$ is the number of distinct prime divisors of an integer m. Thus $\omega(k') < \omega(k) < \log_2 k$ and hence $\#F \ge 3 + \omega(k')$. Therefore we can take two distinct values t_0 and t_1 in $F^\times$ with the above property. Now each coordinate of $P' = (u + t_0 v, u + t_1 v)$ generates E, and by the argument above we have $\operatorname{codim}_{F[x,y]} s_{P',F} = 3k$. Furthermore the linear transformation of variables in $E[x, y]$ mapping (x, y) to $(x + t_0 y, x + t_1 y)$, with inverse $(x, y) \mapsto (\frac{t_1 x - t_0 y}{t_1 - t_0}, \frac{x-y}{t_0 - t_1})$, maps s_P to $s_{P'}$ and leaves $F[x, y]$ invariant. Thus also $s_{P,F}$ has codimension $3k$.

For (ii), we note that the number of polynomials in (5.13) that lie in $B_n(F)$ equals $3k$, $2n - k + 2$, and $n + 1$, respectively, in the three cases, as stated. □

THEOREM 5.14. *Let $k \ge 2$, $q \ge 1 + \log_2 k$ be a prime power, $n \ge 2k - 1$, and A as in (5.10). Then*

$$\frac{\#S_n(A\colon \mathbb{F}_q)}{\#B_n(\mathbb{F}_q)} < q^{-k}.$$

PROOF. We have

$$\begin{aligned} \#S_n(A : \mathbb{F}_q) &\le \sum_{P\in A} \#(s_{P,\mathbb{F}_q} \cap B_n(\mathbb{F}_q)) \\ &\le \#A \cdot q^{-3k} \#B_n(\mathbb{F}_q) < q^{-k} \#B_n(\mathbb{F}_q). \end{aligned}$$ □

For a lower bound on $\#S_n(A:\mathbb{F}_q)$, it would be sufficient to bound appropriately the codimension of $s_{P,\mathbb{F}_q} \cap s_{Q,\mathbb{F}_q}$ in $B_n(\mathbb{F}_q)$ for "most" $P, Q \in A$. For large k, the previous results do not yield good bounds. However, Weil's Theorem gives an estimate for polynomials with singularities in any extension.

THEOREM 5.15. *For $n \geq 3$, the number $\tau_n(q)$ of absolutely singular and rationally nonsingular polynomials in $B_n(\mathbb{F}_q)$ satisfies*

$$\tau_n(q) < \#B_n(\mathbb{F}_q) \cdot 13n^{13}q^{-3/2}.$$

PROOF. We consider an algebraic closure F of $\mathbb{F}_q$ and the rational points over $\mathbb{F}_q$ on $S_n(F)$, that is

$$T = S_n(F:\mathbb{F}_q) = S_n(F) \cap B_n(\mathbb{F}_q).$$

We recall that $b_n = \dim B_n(F) = (n+1)(n+2)/2$ and that the Zariski closure of $S_n(F)$ is an absolutely irreducible hypersurface in $B_n(F)$ of degree at most $d = (n+1)n^2$, by Theorem 5.6 (i). The explicit form of Weil's Theorem in Cafure & Matera (2006), Theorem 5.2, implies that

$$\left|\#T - q^{b_n-1}\right| \leq (d-1)(d-2)q^{b_n-3/2} + 5d^{13/3}q^{b_n-2} < 13n^{13}q^{b_n-3/2} - q^{b_n-2}/2.$$

The last inequality holds for $q = 2$ and $n = 3$, and follows in general by monotonicity. Any polynomial with a rational singularity is in T, so that

$$S_n(\mathbb{F}_q) \subseteq T.$$

Its complement consists precisely of those absolutely singular $f \in B_n(\mathbb{F}_q)$ that are rationally nonsingular. We have by Theorem 5.6 (ii)

$$\begin{aligned}\tau_n(q) &= \#(T \setminus S_n(\mathbb{F}_q)) \\ &\leq q^{b_n-1} + 13n^{13}q^{b_n-3/2} - q^{b_n-2}/2 - (q^{-1} - q^{-2}/2)q^{b_n} \\ &= 13n^{13}q^{b_n-3/2}.\end{aligned}$$

□

Thus $\tau_n(q) < q^{-1}\#B_n(\mathbb{F}_q)$ when $q > 13^2n^{26}$.

Unlike our previous estimates, this upper bound is unlikely to be sharp, and a more precise estimate remains an open question.

CONJECTURE 5.16. *For $n \geq 3$, we have*

$$\left|\frac{\tau_n(q)}{\#B_n(\mathbb{F}_q)} - q^{-2}\right| = \mathrm{O}(q^{-3}).$$

We now make some remarks about the singular points on squareful and relatively irreducible polynomials.

REMARK 5.17. When $f \in F[x,y]$ is squareful, so that the square of some nonconstant $g \in F[x,y]$ divides f, then each point on $\{g=0\}$ is singular for f, and f is singular unless $\{g=0\}=\varnothing$. On the other hand, suppose that f is squarefree and $g \in E[x,y]$ is an irreducible common factor of $f=gh$, f_x, and f_y, where $F \subseteq E$ are perfect fields and f_x and f_y are the two partial derivatives of f. Then g divides $g_x h = f_x - g h_x$, hence it divides g_x and thus $g_x = 0$. Similarly, $g_y = 0$. It follows that $p = \operatorname{char} F > 0$, and if E contains a pth root of any of its elements, then g is the pth power of some polynomial, contradicting its irreducibility. Thus over a finite field, a polynomial is squareful if and only if its singular locus contains a curve given by a nonconstant polynomial or each of its multiple factors defines the empty set over $\mathbb{F}_q$. (Such factors will define many points over sufficiently large extension fields.)

REMARK 5.18. Does every relatively irreducible polynomial, as considered in Section 4, have a rational singular point? In the smallest case, where $g \in \mathbb{F}_{q^2}[x,y] \setminus \mathbb{F}_q[x,y]$ is linear, σ generates $\operatorname{Gal}(\mathbb{F}_{q^2}\colon \mathbb{F}_q)$, and $f = g \cdot g^\sigma \in \mathbb{F}_q[x,y]$, this is indeed true unless the coefficient of x or that of y in g vanishes.

To see this, we write $g = ax + by + c$, with $a,b,c \in \mathbb{F}_{q^2}$, and $\mathbb{F}_{q^2} = \mathbb{F}_q[\beta]$, where β is the square root of a nonsquare in $\mathbb{F}_q$. Then $\beta^\sigma = -\beta$. We may assume $a \neq 0$, divide g by a and thus assume $a = 1$. The only solution $(u,v) \in \mathbb{F}_q^2$ of $g(u,v) = g^\sigma(u,v) = 0$ is given by $v = (c - c^\sigma)/(b^\sigma - b) \in \mathbb{F}_q$, provided that $b^\sigma \neq b$, and $u = -bv - c$. One checks that $(c^\sigma - c)/(b^\sigma - b)$, v, and u are in $\mathbb{F}_q$. If $b^\sigma - b = 0$, so that $b \in \mathbb{F}_q$, then $c \notin \mathbb{F}_q$, the two lines given by g and g^σ are parallel with rational slope, and their common point is at infinity, that is, in $\mathbb{P}^2(\mathbb{F}_q) \setminus \mathbb{F}_q^2$. It is a rational singularity for f.

However, already for a quadratic polynomial like $g = x^2 + \beta y^2 - a\beta \in \mathbb{F}_{q^2}[x,y]$, where $a \in \mathbb{F}_q$ is a nonsquare, $f = g \cdot g^\sigma$ has no rational point in $\mathbb{P}^2(\mathbb{F}_q)$, and in particular no singular one. If we take $\mathbb{F}_{q^3} = \mathbb{F}_q(\beta)$, σ generating $\operatorname{Gal}(\mathbb{F}_q(\beta)\colon \mathbb{F}_q)$, $g = x + \beta y + \beta^2 \in \mathbb{F}_{q^3}[x,y]$, then $f = g \cdot g^\sigma \cdot g^{\sigma^2}$ also does not have any rational points in $\mathbb{P}^2(\mathbb{F}_q)$.

REMARK 5.19. How many singularities can a curve have? An irreducible smooth (planar) curve of degree n has genus $(n-1)(n-2)/2$, and if there are ℓ singularities, the genus is at most $(n-1)(n-2)/2 - \ell$. Since the genus is nonnegative, the curve has at most $(n-1)(n-2)/2$ singularities. If a curve of degree n has r distinct irreducible components of degrees $n_1, \dots, n_r$, with $\sum_{1 \le i \le r} n_i = n$, then there are at most

$$M(n_1, \dots, n_r) = \sum_{1 \le i \le r} \frac{(n_i - 1)(n_i - 2)}{2} + \sum_{1 \le i \le j \le r} n_i n_j$$

many singular points. The second sum corresponds to the intersections of different components. Now M takes its maximum value $n(n-1)/2$ at $(1, \dots, 1)$,

since M is symmetric and $M(n_1, \ldots, n_r) < M(n_1, \ldots, n_r - 1, 1)$ if $n_r \geq 2$. In other words, a union of n distinct lines has the maximal number of singularities among the squarefree polynomials of degree n.

REMARK 5.20. What is the largest k for which a polynomial of degree n has a singularity in $\mathbb{F}_{q^k}^2$? Suppose that $P \in \mathbb{F}_{q^k}^2$ is a singular point for f, and its coordinates do not lie in a proper subfield of $\mathbb{F}_{q^k}$. Then the k conjugates under $\mathrm{Gal}(\mathbb{F}_{q^k} : \mathbb{F}_q)$ of P are pairwise distinct and also singular for f. It follows that $k \leq n(n-1)/2$. Based on a suggestion by Cathy O'Neil, the following example gives an extension of degree n and the maximal number of singularities, for large enough q. We have some integer $n \geq 1$ and elements $a, b \in \mathbb{F}_{q^n}$ which together generate $\mathbb{F}_{q^n}$ as a field over $\mathbb{F}_q$, let $G = \mathrm{Gal}(\mathbb{F}_{q^n} : \mathbb{F}_q)$, and take the relatively irreducible polynomial

$$f = \prod_{\sigma \in G} (x + \sigma(a)y + \sigma(b)) \in \mathbb{F}_q[x, y]. \tag{5.21}$$

Thus $V(f)$ consists of n lines, and each intersection point of two of them is singular for f. There are exactly $n(n-1)/2$ such points if and only if no three lines share a common point. We now translate this into a condition on a and b. Namely, suppose that the point (u, v) lies on three distinct lines belonging to $\rho, \sigma, \tau \in G$, so that

$$u + \rho(a)v + \rho(b) = u + \sigma(a)v + \sigma(b) = u + \tau(a)v + \tau(b) = 0.$$

Elimination of n and v leads to the condition $R(a, b) = 0$, where

$$R(a, b) = (\rho(a) - \tau(a))(\rho(b) - \sigma(b)) - (\rho(a) - \sigma(a))(\rho(b) - \tau(b)).$$

Any $\sigma \in G$ can be represented by a polynomial, namely $\sigma(x) = x^{q^i}$ for some i with $0 \leq i < n$. Thus also R can be represented by a polynomial $r \in \mathbb{F}_q[x, y]$. Its degree is at most $q^{n-1} + q^{n-2} < 2q^{n-1}$, since ρ, σ, τ are pairwise different and the two terms $\pm\rho(a)\rho(b)$ cancel. On the other hand, the term $-\rho(a)\sigma(b) = -x^{q^i} y^{q^j}$ for some $i, j < n$ does not cancel with any other summand, so that $r \neq 0$.

Now we let s be the product of these $r \in \mathbb{F}_q[x, y]$ for all $\rho, \sigma, \tau \in G$. Then $s \neq 0$ and $\deg s < 2n^3 q^{n-1}$. Any $(a, b) \in \mathbb{F}_{q^n}^2$ with $s(a, b) \neq 0$ will provide the maximal number of singular points for f, and such a, b exist as soon as $q^n \geq 2n^3 q^{n-1}$ by the nonzero preservation lemma (sometimes called the Schwartz-Zippel Lemma; see Lemma 6.44 in von zur Gathen & Gerhard (2003)).

A related question is: what is the maximal degree of the field extension generated by the coordinates of all singularities?

6 Conclusion

We have presented several estimates for special types of multivariate polynomials, with exponentially decreasing relative error bounds. An open question is the exact determination for polynomials with nonrational singularities, for which Theorem 5.15 contains only a rough upper bound.

Most polynomials in $\mathbb{F}_q[x, y]$ are absolutely irreducible. One may wonder if interesting subclasses of these can be counted, for example those with a given Galois (over $\mathbb{F}_q(x)$) or monodromy group, or sparse polynomials, in particular *separated* polynomials of the form $f(x) - g(y)$, or even $(f(x) - f(y))/(x - y)$.

Acknowledgements

My conversations with Guillermo Matera and Antonio Cafure at the conference Latin 2006 motivated this work. Hendrik Lenstra found his precise bound for Ragot's probability during my lecture at the 2006 Meeting on Polynomials over Finite Fields and Applications in Banff. I thank him for permission to include this here, and BIRS for making the conference possible. I thank Cathy O'Neil for discussions about absolutely singular curves, Daniel Panario for pointing out several references, and Daniel Loebenberger and Michael Nüsken for producing the figures.

This work was funded by the B-IT Foundation and the State of Nordrhein-Westfalen. An Extended Abstract appeared as von zur Gathen (2007).

References

Arnaud Bodin (2008). Number of irreducible polynomials in several variables over finite fields. *American Mathematical Monthly, to appear.* URL `http://fr.arxiv.org/abs/0706.0157`.

A. Cafure & G. Matera (2002). Explicit estimates for the number of solutions of polynomial equation systems over finite fields. *Anales Jornadas Argentinas de Informática e Investigación Operativa* **31**, 26–41. Proceedings of the 2002 Argentine Workshop on Theoretical Computer Science, WAIT 2002, Santa Fe, Argentina, Septiembre 2002.

Antonio Cafure & Guillermo Matera (2006). Improved explicit estimates on the number of solutions of equations over a finite field. *Finite Fields and Their Applications* **12**, 155–185.

Leonard Carlitz (1936). On factorable polynomials in several indeterminates. *Duke Mathematical Journal* **2**, 660–670.

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.

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 D. Cohen (1970). The Distribution of Polynomials over Finite Fields. *Acta Arithmetica* **17**, 255–271.

M.L. Fredman (1972). The distribution of absolutely irreducible polynomials in several indeterminates. *Proceedings of the American Mathematical Society* **31**, 387–390.

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 (1985). Irreducibility of Multivariate Polynomials. *Journal of Computer and System Sciences* **31**(2), 225–264. URL `http://dx.doi.org/10.1016/0022-0000(85)90043-1`.

Joachim von zur Gathen (2007). Counting Reducible and Singular Bivariate Polynomials. In *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation ISSAC2007,* Waterloo, Ontario, Canada, Christopher W. Brown, editor, 369–376. URL `http://doi.acm.org/10.1145/1277548.1277598`.

Joachim von zur Gathen & Jürgen Gerhard (2003). *Modern Computer Algebra*. Cambridge University Press, Cambridge, UK, 2nd edition. ISBN 0-521-82646-2, 800. URL `http://cosec.bit.uni-bonn.de/science/mca.html`. First edition 1999.

Joachim von zur Gathen, Marek Karpinski & Igor E. Shparlinski (1996). Counting curves and their projections. *computational complexity* **6**, 64–99. URL `http://dx.doi.org/10.1007/BF01202042`. Extended abstract in *Proceedings of the Twenty-fifth Annual ACM Symposium on the Theory of Computing,* San Diego CA (1993), 805-812.

Joachim von zur Gathen, Igor Shparlinski & Alistair Sinclair (2003). Finding points on curves over finite fields. *SIAM Journal on Computing* **32**(6), 1436–1448. URL `http://dx.doi.org/10.1137/S0097539799351018`. Extended abstract in von zur Gathen & Shparlinski (1995).

Joachim von zur Gathen & Igor E. Shparlinski (1995). Finding points on curves over finite fields. In *Proceedings of the 36th Annual IEEE Symposium on Foundations of Computer Science,* Milwaukee WI, 284–292. IEEE Computer Society Press. Final version see von zur Gathen *et al.* (2003).

Joachim von zur Gathen & Igor E. Shparlinski (1998). Computing components and projections of curves over finite fields. *SIAM Journal on Computing* **28**(3), 822–840. URL `http://dx.doi.org/10.1137/S009753979427741X`.

Joachim von zur Gathen & Alfredo Viola (2008). Exact counting of reducible multivariate polynomials. *Preprint* .

Robert M. Guralnick & Peter Müller (1997). Exceptional Polynomials of Affine Type. *Journal of Algebra* **194**(2), 429–454. ISSN 0021-8693. URL http://dx.doi.org/10.1006/jabr.1997.7028.

G. H. Hardy & E. M. Wright (1985). *An introduction to the theory of numbers*. Clarendon Press, Oxford, 5th edition. First edition 1938.

Joe Harris (1992). *Algebraic Geometry. A First Course*. Graduate Texts in Mathematics. Springer-Verlag, New York.

W. V. D. Hodge & D. Pedoe (1952). *Methods of Algebraic Geometry*. Cambridge University Press.

M.-D. Huang & D. Ierardi (1993). Counting Rational Points on Curves over Finite Fields. In *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science,* Palo Alto CA, 616–625. IEEE Computer Society Press, Los Alamitos CA.

Rudolf Lidl & Harald Niederreiter (1983). *Finite Fields*. Number 20 in Encyclopedia of Mathematics and its Applications. Addison-Wesley, Reading MA.

Preda Mihăilescu (2006). On the representation of extensions of finite fields as simple extensions. Preprint.

Jean-François Ragot (1997). *Sur la factorisation absolue des polynômes*. Thèse, Université de Limoges. URL http://www.unilim.fr/laco/theses/1997/T1997_02.pdf. 133 pages.

Jean-François Ragot (1999). Counting polynomials with zeros of given multiplicities in finite fields. *Finite Fields and Their Applications* **5**, 219–231.

I. R. Shafarevich (1974). *Basic algebraic geometry*. Number 213 in Grundlehren. Springer-Verlag.

Daqing Wan (1992a). Hilbert sets and zeta functions over finite fields. *Journal für die reine und angewandte Mathematik* **427**, 193–207. URL http://arxiv.org/PS_cache/math/pdf/9811/9811191v1.pdf.

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

CORRECTION TO "COUNTING REDUCIBLE AND SINGULAR BIVARIATE POLYNOMIALS"

Joachim von zur Gathen

1. Correction

The penultimate paragraph on page 951 of von zur Gathen (2008) should be corrected to:

"For $n = 3$, the bound in (ii) needs to be strengthened, and in fact we have

$$\frac{\#R_3^=(\mathbb{F}_q)}{\#B_3^=(\mathbb{F}_q)} - \rho_3(q) = \rho_3(q) \cdot \frac{-(q^4 + 2q^3 + 4q^2 - 1)}{3q^2(q+1)(q^2+1)};$$

the last factor is absolutely not more than $(3q)^{-1}(1 + q^{-1} + 2q^{-2})$."

Thanks go to Konstantin Ziegler for noting the discrepancy between the erroneous statement on page 951 and the correct result in Table 2.1 on page 948.

References

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`.

Joachim von zur Gathen
b-it
Universität Bonn
D-53113 Bonn
`gathen@bit.uni-bonn.de`
`http://www.b-it-center.de/`