Raoul Blankertz, Joachim von zur Gathen & Konstantin Ziegler (2013). Compositions and collisions at degree p^2. *Journal of Symbolic Computation* **59**, 113–145. ISSN 0747–7171. URL http://dx.doi.org/10.1016/j.jsc.2013.06.001. Extended abstract in *Proceedings of the 2012 International Symposium on Symbolic and Algebraic Computation ISSAC 2012, Grenoble, France* (2012).

Compositions and collisions at degree p^2

Raoul Blankertz, Joachim von zur Gathen & Konstantin Ziegler
B-IT, Universität Bonn
D-53113 Bonn, Germany
blankertz@uni-bonn.de,{gathen,zieglerk}@bit.uni-bonn.de
http://cosec.bit.uni-bonn.de/

June 11, 2013

Abstract

A univariate polynomial f over a field is decomposable if $f = g \circ h = g(h)$ for nonlinear polynomials g and h. In order to count the decomposables, one wants to know, under a suitable normalization, the number of equal-degree collisions of the form $f = g \circ h = g^* \circ h^*$ with $(g, h) \neq (g^*, h^*)$ and $\deg g = \deg g^*$. Such collisions only occur in the wild case, where the field characteristic p divides $\deg f$. Reasonable bounds on the number of decomposables over a finite field are known, but they are less sharp in the wild case, in particular for degree p^2.

We provide a classification of all polynomials of degree p^2 with a collision. It yields the exact number of decomposable polynomials of degree p^2 over a finite field of characteristic p. We also present an efficient algorithm that determines whether a given polynomial of degree p^2 has a collision or not.

Keywords. computer algebra, finite fields, wild polynomial decomposition, equal-degree collisions, ramification theory of function fields, counting special polynomials

1 Introduction

The *composition* of two polynomials $g, h \in F[x]$ over a field F is denoted as $f = g \circ h = g(h)$, and then (g, h) is a *decomposition* of f, and f is *decomposable* if g and h have degree at least 2. In the 1920s, Ritt, Fatou, and Julia studied structural properties of these decompositions over $\mathbb{C}$, using analytic methods.

Particularly important are two theorems by Ritt on the uniqueness, in a suitable sense, of decompositions, the first one for (many) indecomposable components and the second one for two components, as above. Engstrom (1941) and Levi (1942) proved them over arbitrary fields of characteristic zero using algebraic methods.

The theory was extended to arbitrary characteristic by Fried & MacRae (1969), Dorey & Whaples (1974), Schinzel (1982, 2000), Zannier (1993), and others. Its use in a cryptographic context was suggested by Cade (1985). In computer algebra, the method of Barton & Zippel (1985) requires exponential time. A fundamental dichotomy is between the *tame case*, where the characteristic p does not divide $\deg g$, and the *wild case*, where p divides $\deg g$, see von zur Gathen (1990a,b). A breakthrough result of Kozen & Landau (1989) was their polynomial-time algorithm to compute tame decompositions. In the wild case, considerably less is known, both mathematically and computationally. Zippel (1991) suggests that the block decompositions of Landau & Miller (1985) for determining subfields of algebraic number fields can be applied to decomposing rational functions even in the wild case. A version of Zippel's algorithm in Blankertz (2013) computes in polynomial time all decompositions of a polynomial that are minimal in a certain sense. Avanzi & Zannier (2003) study ambiguities in the decomposition of rational functions over $\mathbb{C}$. A set of distinct decompositions of f is called a *collision*. The number of decomposable polynomials of degree n is thus the number of all pairs (g, h) with $\deg g \cdot \deg h = n$ reduced by the ambiguities introduced by collisions. In this paper, we study only *equal-degree* collisions of $f = g \circ h = g^* \circ h^*$, where $\deg g = \deg g^*$ and thus $\deg h = \deg h^*$.

The task of counting compositions over a finite field of characteristic p was first considered in Giesbrecht (1988). Von zur Gathen (2009) presents general approximations to the number of decomposable polynomials. These come with satisfactory (rapidly decreasing) relative error bounds except when p divides $n = \deg f$ exactly twice. The main result (Theorem 6.6) of the present work determines exactly the number of decomposable polynomials in one of these difficult cases, namely when $n = p^2$ and hence $\deg g = \deg h = p$.

This is shown in three steps. First, we exhibit some classes of collisions in Section 3. Their properties are easy to check. In the second step we show that these are all possibilities (Theorem 5.9). In Section 4 we use ramification theory of function fields to study the root multiplicities in collisions, and in Section 5 classify all collisions at degree p^2. In the third step we count the resulting possibilities (Section 6).

Our contribution is fourfold:

- We provide explicit constructions for collisions at degree r^2, where r is

a power of the characteristic $p > 0$ (Fact 3.1, Theorem 3.22).

- We provide a classification of all collisions at degree p^2, linking every collision to a unique explicit construction (Theorem 5.9).
- We use these two results to obtain an exact formula for the number of decomposable polynomials at degree p^2 (Theorem 6.6).
- The classification yields an efficient algorithm to test whether a given polynomial has a collision or not (Algorithm 5.14).

An Extended Abstract of this paper appeared as Blankertz, von zur Gathen & Ziegler (2012).

2 Definitions and examples

We consider a field F of positive characteristic $p > 0$. Composition of g and h with linear polynomials introduces inessential ambiguities in decompositions $f = g \circ h$. In order to avoid them, we normalize f, g, and h to be *monic original*, that is with leading coefficient 1 and constant coefficient 0 (so that the graph of f passes through the origin); see von zur Gathen (2009).

For a nonnegative integer k, an (equal-degree) *k-collision* at degree n is a set of k distinct pairs (g, h) of monic original polynomials in $F[x]$ of degree at least 2, all with the same composition $f = g \circ h$ of degree n and $\deg g$ the same for all (g, h). A k-collision is called *maximal* if it is not contained in a $(k+1)$-collision. We also say that f has a (maximal) k-collision. Furthermore, g is a *left component* and h a *right component* of f. For $n \geq 1$, we define

$$\begin{aligned} P_n(F) &= \{f \in F[x] \colon f \text{ is monic original of degree } n\}, \\ D_n(F) &= \{f \in P_n(F) \colon f \text{ is decomposable}\}, \\ C_{n,k}(F) &= \{f \in P_n(F) \colon f \text{ has a maximal } k\text{-collision}\}. \end{aligned} \tag{2.1}$$

Thus $\#P_n(\mathbb{F}_q) = q^{n-1}$. We sometimes leave out F from the notation when it is clear from the context.

Let $f \in P_n$ have a k-collision C, $f' \neq 0$, and m be a divisor of n. If all right components in C are of degree m and indecomposable, then $k \leq (n-1)/(m-1)$; see Blankertz (2011, Corollary 3.27). For $n = p^2$, both components are of degree p and thus indecomposable and we find $k \leq p+1$; see also von zur Gathen, Giesbrecht & Ziegler (2010, Proposition 6.5 (iv)). For counting all decomposable polynomials of degree p^2 over $\mathbb{F}_q$, it is sufficient

to count the sets $C_{p^2,k}$ of polynomials with maximal k-collision for $k \geq 2$, since

$$\#D_{p^2} = q^{2p-2} - \sum_{k\geq 2}(k-1)\cdot \#C_{p^2,k}. \tag{2.2}$$

Lemma 2.3. *In a decomposition (g,h), g is uniquely determined by $g\circ h$ and h.*

Proof. Let $f = g\circ h$. Consider the F-algebra homomorphism $\varphi\colon F[x] \to F[x]$ with $x \mapsto h$. Its kernel is trivial, since h is nonconstant, and thus φ is injective. Hence there is exactly one $u \in F[x]$ such that $\varphi(u) = f$, namely $u = g$. □

Furthermore, g is easy to compute from $g\circ h$ and h by the generalized Taylor expansion; see von zur Gathen (1990a, Section 2). The following is a simple example of a collision.

Example 2.4. Let $r = p^e$. For $h \in P_r(F)$, we have

$$x^r \circ h = \varphi_r(h) \circ x^r, \tag{2.5}$$

where φ_r is the eth power of the *Frobenius endomorphism* on F, extended to polynomials coefficientwise. If $h \neq x^r$, then $\{(x^r,h),(\varphi_r(h),x^r)\}$ is a 2-collision and we call it a *Frobenius collision.*

In the case $r = p$, we have the following description.

Lemma 2.6. *(i) Assume that $f \in P_{p^2}(F)$ has a 2-collision. Then it is a Frobenius collision if and only if $f' = 0$.*

(ii) A Frobenius collision of degree p^2 is a maximal 2-collision.

Proof. (i) If f is a Frobenius collision, then $f' = 0$ by definition. Conversely, let $f \in P_{p^2}(F)$ with $f' = 0$. Then $f \in F[x^p]$ and thus $f = g\circ x^p$ for some monic original polynomial g. Let $f = g^*\circ h^*$ be another decomposition of f. By Lemma 2.3, f and h^* determine g^* uniquely, hence $h^* \neq x^p$ and $h^{*\prime} \neq 0$. Thus from $f' = g^{*\prime}(h^*)\cdot h^{*\prime} = 0$ follows $g^{*\prime} = 0$ and hence $g^* = x^p$. Furthermore, $f = x^p\circ h^* = \varphi_p(h^*)\circ x^p$ by (2.5), $g = \varphi_p(h^*)$ by the uniqueness in Lemma 2.3, and f is a Frobenius collision.

(ii) Let $f = x^p\circ h = \varphi_p(h)\circ x^p$, with $h \neq x^p$, be a Frobenius collision, and (g^*,h^*) a decomposition of f. Then $0 = f' = g^{*\prime}(h^*)\cdot h^{*\prime}$ and thus $g^{*\prime} = 0$ or $h^{*\prime} = 0$. If $h^{*\prime} = 0$, then $h^* = x^p$ and thus $g^* = \varphi_p(h)$, by Lemma 2.3. If $g^{*\prime} = 0$, then $g^* = x^p$ and $f = \varphi_p(h^*)\circ x^p$ as in (i). Thus $\varphi_p(h^*) = \varphi_p(h)$ by the uniqueness in Lemma 2.3, which implies $h = h^*$. □

If F is perfect—in particular if F is finite or algebraically closed—then the Frobenius endomorphism φ_p is an automorphism on F. Thus for $f \in P_{p^2}(\mathbb{F}_q)$, $f' = 0$ implies that f is either a Frobenius collision or x^{p^2}.

For $f \in P_n(F)$ and $w \in F$, the *original shift* of f by w is

$$f^{(w)} = (x - f(w)) \circ f \circ (x + w) \in P_n(F).$$

We also simply speak of a *shift*. Original shifting defines a group action of the additive group of F on $P_n(F)$. Indeed, we have for $w, w' \in F$

$$\begin{aligned}(f^{(w)})^{(w')} &= (x - f^{(w)}(w')) \circ f^{(w)} \circ (x + w') \\ &= (x - (f(w' + w) - f(w))) \circ (x - f(w)) \circ f \circ (x + w) \circ (x + w') \\ &= (x - f(w' + w)) \circ f \circ (x + w' + w) = f^{(w'+w)}.\end{aligned}$$

Furthermore, for the derivative we have $(f^{(w)})' = f' \circ (x + w)$. Shifting respects decompositions in the sense that for each decomposition (g, h) of f we have a decomposition $(g^{(h(w))}, h^{(w)})$ of $f^{(w)}$, and vice versa. We denote $(g^{(h(w))}, h^{(w)})$ as $(g, h)^{(w)}$.

3 Explicit collisions at degree r^2

This section presents two classes of explicit collisions at degree r^2, where r is a power of the characteristic $p > 0$ of the field F. The collisions of Fact 3.1 consist of additive and subadditive polynomials. A polynomial A of degree r^κ is *r-additive* if it is of the form $A = \sum_{0 \le i \le \kappa} a_i x^{r^i}$ with all $a_i \in F$. We call a polynomial *additive* if it is p-additive. A polynomial is additive if and only if it acts additively on an algebraic closure $\overline{F}$ of F, that is $A(a + b) = A(a) + A(b)$ for all a, $b \in \overline{F}$; see Goss (1996, Corollary 1.1.6). The composition of additive polynomials is additive, see for instance Proposition 1.1.2 of the cited book. The decomposition structure of additive polynomials was first studied by Ore (1933). Dorey & Whaples (1974, Theorem 4) show that all components of an additive polynomial are additive. Giesbrecht (1988) gives lower bounds on the number of decompositions and algorithms to determine them.

For a divisor m of $r - 1$, the *(r, m)-subadditive* polynomial associated with the r-additive polynomial A is $S = x(\sum_{0 \le i \le \kappa} a_i x^{(r^i-1)/m})^m$ of degree r^κ. Then A and S are related as $x^m \circ A = S \circ x^m$. Dickson (1897) notes a special case of subadditive polynomials, and Cohen (1985) is concerned with the reducibility of some related polynomials. Cohen (1990a,b) investigates their connection to exceptional polynomials and coins the term "sub-linearized"; see also Cohen & Matthews (1994). Coulter, Havas & Henderson (2004)

derive the number of indecomposable subadditive polynomials and present an algorithm to decompose subadditive polynomials.

Ore (1933, Theorem 3) describes exactly the right components of degree p of an additive polynomial. Henderson & Matthews (1999) relate such additive decompositions to subadditive polynomials, and in their Theorems 3.4 and 3.8 describe the collisions of Fact 3.1 below. The polynomials of Theorem 3.22 popped up in the course of trying to prove that these examples might be the only ones; see the proof of Theorem 5.9. In Section 5, we show that together with the Frobenius collisions of Example 2.4, these examples and their shifts comprise all 2-collisions at degree p^2.

Fact 3.1. *Let r be a power of p, $u, s \in F^\times$, $\varepsilon \in \{0,1\}$, m a positive divisor of $r-1$, $\ell = (r-1)/m$, and*

$$\begin{aligned} f &= S(u,s,\varepsilon,m) = x(x^{\ell(r+1)} - \varepsilon u s^r x^\ell + u s^{r+1})^m \in P_{r^2}(F), \\ T &= \{t \in F \colon t^{r+1} - \varepsilon u t + u = 0\}. \end{aligned} \tag{3.2}$$

For each $t \in T$ and

$$\begin{aligned} g &= x(x^\ell - u s^r t^{-1})^m, \\ h &= x(x^\ell - st)^m, \end{aligned} \tag{3.3}$$

both in $P_r(F)$, we have $f = g \circ h$. Moreover, f has a $\#T$-collision.

The polynomials f in (3.2) are "simply original" in the sense that they have a simple root at 0. This motivates the designation S.

Proof. For $t \in T$, we have

$$\begin{aligned} g \circ h &= x(x^\ell - st)^m (x^\ell (x^\ell - st)^{r-1} - u s^r t^{-1})^m \\ &= x(x^\ell (x^\ell - st)^r - (x^\ell - st) u s^r t^{-1})^m \\ &= x(x^{\ell r + \ell} - s^r t^r x^\ell - u s^r t^{-1} x^\ell + u s^{r+1})^m \\ &= x(x^{\ell(r+1)} - s^r (t^r + u t^{-1}) x^\ell + u s^{r+1})^m \\ &= x(x^{\ell(r+1)} - \varepsilon u s^r x^\ell + u s^{r+1})^m = f. \end{aligned}$$

This proves that (g,h) is a decomposition of f. While f does not depend on t, the $\#T$ different choices for t yield $\#T$ pairwise different values for the coefficients of $x^{r-\ell}$ in h, namely

$$h_{r-\ell} = -mst \neq 0. \qquad \square$$

The polynomial $S(u, s, \varepsilon, m)$ is r-additive for $m = 1$ and (r, m)-subadditive for all m. Bluher (2004) shows that for $\varepsilon = 1$ and $F \cap \mathbb{F}_r$ of size Q, the cardinality of T is either 0, 1, 2, or $Q + 1$. This also holds for $\varepsilon = 0$. In either case, T is independent of m and ℓ. If T is empty, then $S(u, s, \varepsilon, m)$ has no decomposition of the form (3.3), but $r + 1$ such decompositions exist over the splitting field of the squarefree polynomial $y^{r+1} - \varepsilon uy + u \in F[y]$.

For a polynomial $f \in P_n(F)$ and an integer i, we denote the coefficient of x^i in f by f_i, so that $f = x^n + \sum_{1 \le i < n} f_i x^i$ with $f_i \in F$. The *second degree* of f is

$$\deg_2 f = \deg(f - x^n). \tag{3.4}$$

If $p \mid n$ and $p \nmid \deg_2 f$, then $\deg_2 f = \deg(f') + 1$.

Fact 3.5 (von zur Gathen, Giesbrecht & Ziegler (2010), Proposition 6.2)**.** *Let r be a power of p, and u, s, ε, m and u^*, s^*, ε^*, m^* satisfy the conditions of Fact 3.1. For $f = S(u, s, \varepsilon, m)$ and $f^* = S(u^*, s^*, \varepsilon^*, m^*)$, the following hold.*

(i) For $\varepsilon = 1$, we have $f = f^*$ if and only if $(u, s, \varepsilon, m) = (u^*, s^*, \varepsilon^*, m^*)$.

(ii) For $\varepsilon = 0$, we have $f = f^*$ if and only if $(us^{r+1}, \varepsilon, m) = (u^*(s^*)^{r+1}, \varepsilon^*, m^*)$.

(iii) The stabilizer of f under original shifting is F if $m = 1$, and $\{0\}$ otherwise. For $F = \mathbb{F}_q$, the orbit of f under original shifting has size 1 if $m = 1$, and size q otherwise.

(iv) The only polynomial of the form (3.2) in the orbit of f under original shifting is f itself.

Proof. The appearance of $O(x^i)$ for some integer i in an equation means the existence of some polynomial of degree at most i that makes the equation valid.

Let $\ell = (r - 1)/m$. Then $\gcd(r, \ell) = \gcd(r, m) = 1$ and $\ell m \equiv -1 \bmod p$. We have

$$\begin{aligned} f &= x(x^{\ell(r+1)} - \varepsilon u s^r x^\ell + u s^{r+1})^m \\ &= x(x^{r^2-1} - m\varepsilon u s^r x^{r^2-\ell r-1} + m u s^{r+1} x^{r^2-\ell r-\ell-1} + O(x^{r^2-2\ell r-1})) \\ &= x^{r^2} - m\varepsilon u s^r x^{r^2-\ell r} + m u s^{r+1} x^{r^2-\ell r-\ell} + O(x^{r^2-2\ell r}), \end{aligned} \tag{3.6}$$

$$f_{r^2-\ell r} = -m\varepsilon u s^r, \tag{3.7}$$

$$f_{r^2-\ell r-\ell} = m u s^{r+1} \neq 0, \tag{3.8}$$

$$\deg_2 f = \begin{cases} r^2 - \ell r & \text{if } \varepsilon = 1, \\ r^2 - \ell r - \ell & \text{if } \varepsilon = 0. \end{cases} \tag{3.9}$$

From the last equation, we find $\varepsilon = 1$ if $r \mid \deg_2 f$, and $\varepsilon = 0$ otherwise. For either value of ε, $\deg_2 f$ determines ℓ and $m = (r-1)/\ell$ uniquely. Similarly, $\deg_2 f^*$ determines ε^*, ℓ^*, and m^* uniquely. Therefore, if $\deg_2 f = \deg_2 f^*$, then

$$(\varepsilon, \ell, m) = (\varepsilon^*, \ell^*, m^*). \tag{3.10}$$

Furthermore, m and the coefficient $f_{r^2-\ell r-\ell}$ determine $us^{r+1} = f_{r^2-\ell r-\ell}/m$ uniquely by (3.8). Similarly, m^* and $f^*_{r^2-\ell^* r-\ell^*}$ determine $u^*(s^*)^{r+1}$ uniquely. Thus, if $m = m^*$ and $f_{r^2-\ell r-\ell} = f^*_{r^2-\ell^* r-\ell^*}$, then

$$us^{r+1} = u^*(s^*)^{r+1}. \tag{3.11}$$

(i) If $(u, s, \varepsilon, m) = (u^*, s^*, \varepsilon^*, m^*)$, then $f = f^*$. On the other hand, we have $f_{r^2-\ell r} = -mus^r \neq 0$ in (3.7) and with (3.8) this determines uniquely

$$\begin{aligned} s &= -f_{r^2-\ell r-\ell}/f_{r^2-\ell r}, \\ u &= -f_{r^2-\ell r}/ms^r = \ell f_{r^2-\ell r}/s^r. \end{aligned} \tag{3.12}$$

This implies the claim (i).

(ii) The condition $(us^{r+1}, \varepsilon, m) = (u^*(s^*)^{r+1}, \varepsilon^*, m^*)$ is sufficient for $f = f^*$ by direct computation from (3.2). It is also necessary by (3.10) and (3.11).

(iii) For $m = 1$, f is r-additive as noted after the proof of Fact 3.1 and $f^{(w)} = f$ for all $w \in F$. For $m > 1$ and $w \in F$, we find

$$\begin{aligned} f^{(w)} = x^{r^2} &- m\varepsilon us^r x^{r^2-\ell r} + mus^{r+1}x^{r^2-\ell r-\ell} \\ &+ wus^{r+1}x^{r^2-\ell r-\ell-1} + O(x^{r^2-\ell r-\ell-2}), \end{aligned} \tag{3.13}$$

$$f^{(w)}_{r^2-\ell r} = f_{r^2-\ell r} = -m\varepsilon us^r, \tag{3.14}$$

$$f^{(w)}_{r^2-\ell r-\ell} = f_{r^2-\ell r-\ell} = mus^{r+1} \neq 0, \tag{3.15}$$

$$f^{(w)}_{r^2-\ell r-\ell-1} = wus^{r+1}. \tag{3.16}$$

We have $f = f^{(0)}$ by definition and $f \neq f^{(w)}$ for $w \neq 0$ by (3.16) and $us^{r+1} \neq 0$.

(iv) For $m = 1$, the claim follows from (iii). For $m > 1$ and $w \in F$, assume $f_0 = S(u_0, s_0, \varepsilon_0, m_0) = f^{(w)}$ for parameters $u_0, s_0, \varepsilon_0, m_0$ satisfying the conditions of Fact 3.1. Then $\deg_2 f_0 = \deg_2 f^{(w)}$ by assumption and

$$\deg_2 f^{(w)} = \deg_2 f = \begin{cases} r^2 - \ell r & \text{if } \varepsilon = 1, \\ r^2 - \ell r - \ell & \text{if } \varepsilon = 0, \end{cases} \tag{3.17}$$

from (3.13) and (3.9). Thus, we have $\ell = \ell_0$ by (3.10). The coefficient of $x^{r^2-\ell r-\ell-1}$ is 0 in f_0 and wus^{r+1} in $f^{(w)}$ by (3.6) and (3.16), respectively. With $us^{r+1} \neq 0$, we have $w = 0$ and $f_0 = f^{(0)} = f$. □

Algorithm 3.18 identifies the examples of Fact 3.1 and their shifts. The algorithm involves divisions which we execute conditionally "if defined". Namely, for integers the quotient is returned, if it is an integer, and for field elements, if the denominator is nonzero. Otherwise, "failure" is returned. Besides the field operations $+$, $-$, $\cdot$, we assume a routine for computing the number of roots in F of a polynomial. Furthermore, we denote by $\mathsf{M}(n)$ a number of field operations which is sufficient to compute the product of two polynomials of degree at most n.

Algorithm 3.18: Identify simply original polynomials

Input: a polynomial $f = \sum_i f_i x^i \in P_{r^2}(F)$ with all $f_i \in F$ and r a power of $\operatorname{char} F$

Output: integer k, parameters u, s, ε, m as in Fact 3.1, and $w \in F$ such that $f = S(u, s, \varepsilon, m)^{(w)}$ has a k-collision with $k = \#T$ as in (3.2), if such values exist, and "failure" otherwise

if $\deg_2 f = -\infty$ **then return** *"failure"*
if $r \mid \deg_2 f$ **then**
  $\varepsilon \leftarrow 1$
  $\ell \leftarrow (r^2 - \deg_2 f)/r$ and $m \leftarrow (r-1)/\ell$ if defined
  $s \leftarrow -f_{r^2-\ell r-\ell}/f_{r^2-\ell r}$ if defined
else
  $\varepsilon \leftarrow 0$
  $\ell \leftarrow (r^2 - \deg_2 f)/(r+1)$ and $m \leftarrow (r-1)/\ell$ if defined
  $s \leftarrow 1$
end
$u \leftarrow -\ell f_{r^2-\ell r-\ell}/s^{r+1}$ if defined
if $us = 0$ **then return** *"failure"*
$w \leftarrow m f_{r^2-\ell r-\ell-1}/f_{r^2-\ell r-\ell}$ if defined
if $f = S(u, s, \varepsilon, m)^{(w)}$ **then**
  $k \leftarrow \#\{y \in F \colon y^{r+1} - \varepsilon u y + u = 0\}$
  return $k, u, s, \varepsilon, m, w$
end
return *"failure"*

Theorem 3.19. *Algorithm 3.18 works correctly as specified. If $F = \mathbb{F}_q$, it takes $O(\mathsf{M}(n)\log(nq))$ field operations on input a polynomial of degree $n = r^2$.*

Proof. For the first claim, we show that for $u_0, s_0, \varepsilon_0, m_0$ as in Fact 3.1 and $w_0 \in F$ the algorithm does not fail on input $f = S(u_0, s_0, \varepsilon_0, m_0)^{(w_0)}$.

We have $\deg_2 f > 0$ by (3.17). Thus, step 1 does not return "failure". By the same equation, we have $r \mid \deg_2 f$ if and only if $\varepsilon_0 = 1$. Therefore, $\varepsilon = \varepsilon_0$ after step 3 or 7, respectively, and since (3.17) determines $\ell_0 = (r-1)/m_0$ uniquely, we find $\ell = \ell_0$ and $m = (r-1)/\ell_0 = m_0$ after step 4 or 8, respectively. If $\varepsilon = 1$, then step 5 computes $s = s_0$ from (3.12), (3.14), and (3.15). Furthermore, step 11 computes $u = u_0$ from (3.8) and (3.15). If $\varepsilon = 0$, then

$$S(u_0, s_0, 0, m)^{(w_0)} = (x(x^{\ell(r+1)} + u_0 s_0^{r+1})^m)^{(w_0)} = S(u_0 s_0^{r+1}, 1, 0, m)^{(w_0)}. \tag{3.20}$$

Therefore, we can choose $s = 1$ in step 9 and set $u = -\ell f_{r^2-\ell r-\ell} = u_0 s_0^{r+1}$ by (3.8) and (3.15) in step 11. For either value of ε, we have $us \neq 0$ from $u_0 s_0 \neq 0$ and step 12 does not return "failure".

For $m = 1$, we have

$$S(u, s, \varepsilon, 1)^{(w_0)} = S(u, s, \varepsilon, 1)^{(0)}$$

by Fact 3.5 (iii) and $w = f_0/f_1 = 0$ in step 13 is a valid choice. For $m > 1$, we find w_0 from (3.15) and (3.16) as

$$w = m f_{r^2-\ell r-\ell-1}/f_{r^2-\ell r-\ell} = w_0.$$

A polynomial f of the assumed form passes the final test in step 14, while an f not of this form will fail here at the latest. The size k of the set $T = \{t \in F \colon t^{r+1} - \varepsilon u t + u = 0\}$ is computed in step 15 and f is a k-collision according to Fact 3.1.

In the following cost estimate for $F = \mathbb{F}_q$, we ignore the (cheap) operations on integers. The calculation of the right-hand side in step 14 takes $O(\mathsf{M}(n) \log n)$ field operations, and the test another n operations. In step 15, we compute k as $\deg_y(\gcd(y^q - y, y^{r+1} - \varepsilon u y + u))$ with $O(\mathsf{M}(r)(\log q + \log r))$ field operations. The cost of all other steps is dominated by these bounds. □

Let $C_{n,k}^{(S)}(F)$ denote the set of polynomials in $P_n(F)$ that are shifts of some $S(u, s, \varepsilon, m)$ with T as in (3.2) of cardinality k. Over a finite field, $\#C_{r^2,k}^{(S)}(\mathbb{F}_q)$ can be computed exactly, as in von zur Gathen, Giesbrecht & Ziegler (2010, Corollary 6.3).

Proposition 3.21. *Let r be a power of p, q a power of r, and τ the number*

of positive divisors of $r-1$. *For* $k \geq 2$, *we have*

$$\#C^{(S)}_{r^2,k}(\mathbb{F}_q) = \begin{cases} \dfrac{(\tau q - q + 1)(q-1)^2(r-2)}{2(r-1)} & \text{if } k = 2, \\ \dfrac{(\tau q - q + 1)(q-1)(q-r)}{r(r^2-1)} & \text{if } k = r+1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We count the polynomials in $C^{(S)}_{r^2,k}(\mathbb{F}_q)$ by counting the admissible parameters u, s, ε, m, w modulo the ambiguities described in Fact 3.5.

For $\varepsilon = 1$, we count the possible $u \in \mathbb{F}_q^\times$ such that $y^{r+1} - uy + u \in \mathbb{F}_q[y]$ has exactly k roots in $\mathbb{F}_q$. Let $a, b \in \mathbb{F}_q^\times$ and $u = a^{r+1}b^{-r}$. The invertible transformation $x \mapsto y = -ab^{-1}x$ gives a bijection

$$\{x \in \mathbb{F}_q^\times \colon x^{r+1} + ax + b = 0\} \leftrightarrow \{y \in \mathbb{F}_q^\times \colon y^{r+1} - uy + u = 0\}.$$

Theorem 5.1 and Proposition 5.4 of von zur Gathen, Giesbrecht & Ziegler (2010) determine the number $c^{(2)}_{q,r,k}$ of pairs $(a,b) \in (\mathbb{F}_q^\times)^2$ such that $x^{r+1}+ax+b$ has exactly k roots, as described below. Every value of u corresponds to exactly $q-1$ pairs (a,b), namely an arbitrary $a \in \mathbb{F}_q^\times$ and b uniquely determined by $b^r = u^{-1}a^{r+1}$. Hence, there are exactly $c^{(2)}_{q,r,k}/(q-1)$ values for u where $\#T = k$. For $m = 1$, the orbit under original shifting has size 1 by Fact 3.5 (iii) and taking into account the $q-1$ possible choices for s we find that there are $c^{(2)}_{q,r,k}$ polynomials of the form $S(u,s,1,1)^{(w)}$. For $m > 1$, the orbit under original shifting contains exactly one polynomial of the form (3.2) by Fact 3.5 (iv) and has size q by (iii). Taking into account the $q-1$ choices for s and the $\tau - 1$ possible values for m, we find that there are $c^{(2)}_{q,r,k} \cdot (\tau-1) \cdot q$ polynomials of the form $S(u,s,1,m)^{(w)}$.

For $\varepsilon = 0$, we have $S(u,s,0,m)^{(w)} = S(us^{r+1},1,0,m)^{(w)}$ as in (3.20) and $T = \{t \in \mathbb{F}_q \colon t^{r+1} + us^{r+1} = 0\}$ as in (3.2). This set has exactly $\gamma = \gcd(r+1, q-1)$ elements, if $-u$ is an $(r+1)$st power, and is empty otherwise. Then $\#T = k \geq 2$ if and only if $k = \gamma$ and $-u$ is an $(r+1)$st power. There are exactly $(q-1)/\gamma$ distinct $(r+1)$st powers in $\mathbb{F}_q^\times$ and therefore exactly $(q-1)/\gamma$ distinct values for us^{r+1} such that $\#T = \gamma$. With δ being Kronecker's delta function, we find, as above, that there are $\delta_{\gamma,k} \cdot (q-1)/\gamma$ polynomials of the form $S(u,s,0,1)^{(w)}$ in $C^{(S)}_{r^2,k}(\mathbb{F}_q)$ and $\delta_{\gamma,k} \cdot (\tau-1)q(q-1)/\gamma$ of the form $S(u,s,0,m)^{(w)}$ with $m > 1$.

This yields

$$\#C^{(S)}_{r^2,k}(\mathbb{F}_q) = (\tau q - q + 1) \cdot \left(c^{(2)}_{q,r,k} + \delta_{\gamma,k} \frac{q-1}{\gamma} \right).$$

The work cited above provides the following explicit expressions for $k \geq 2$, with $q = r^d$:

$$c^{(2)}_{q,r,2} = \begin{cases} \dfrac{(q-1)(qr-2q-2r+3)}{2(r-1)} & \text{if } q \text{ and } d \text{ are odd,} \\ \dfrac{(q-1)^2(r-2)}{2(r-1)} & \text{otherwise,} \end{cases}$$

$$c^{(2)}_{q,r,r+1} = \begin{cases} \dfrac{(q-1)(q-r^2)}{r(r^2-1)} & \text{if } d \text{ is even,} \\ \dfrac{(q-1)(q-r)}{r(r^2-1)} & \text{if } d \text{ is odd,} \end{cases}$$

and $c^{(2)}_{q,r,k} = 0$ for $k \notin \{2, r+1\}$. Furthermore, we have from Lemma 3.29 in von zur Gathen (2009, Preprint)

$$\gamma = \gcd(r+1, r^d - 1) = \begin{cases} 1 & \text{if } d \text{ is odd and } r \text{ is even,} \\ 2 & \text{if } d \text{ is odd and } r \text{ is odd,} \\ r+1 & \text{if } d \text{ is even.} \end{cases}$$

The claimed formulas follow from

$$c^{(2)}_{q,r,k} + \delta_{\gamma,k}\frac{q-1}{\gamma} = \begin{cases} \dfrac{(q-1)^2(r-2)}{2(r-1)} & \text{if } k = 2, \\ \dfrac{(q-1)(q-r)}{r(r^2-1)} & \text{if } k = r+1, \\ 0 & \text{otherwise.} \end{cases} \qquad \square$$

For a prime p, we have $\tau(p-1) \geq 4$ if $p \geq 7$. Large values of $\tau(p-1)$ occur when $m \approx \exp(k \log k)$ is the product of the first k primes and $p \leq m^C$ the smallest prime congruent 1 mod m for Linnik's constant C. Then $k \approx \log m / \operatorname{loglog} m \gtrsim C^{-1} \log p / \operatorname{loglog} p$ and $\tau(p-1) \geq 2^k \gtrsim 2^{C^{-1} \log p / \operatorname{loglog} p}$. By Heath-Brown (1992) and Xylouris (2011) we can take C just under 5. Except for the constant factor, $\tau(p-1)$ is asymptotically not more than this value (Hardy & Wright, 1985, Theorem 317). Luca & Shparlinski (2008) give general results on the possible values of $\tau(p-1)$. It follows that $\#C^{(S)}_{r^2,2}(\mathbb{F}_q) \approx \tau q^3/2$ is in $q^3 O(p^{1/\operatorname{loglog} p})$.

The odd/even distinctions for q, r, and d cancel out in the formula of Proposition 3.21. This might indicate that those distinctions are alien to the problem.

The second and new construction of collisions goes as follows.

Theorem 3.22. *Let r be a power of p, $b \in F^\times$, $a \in F \setminus \{0, b^r\}$, $a^* = b^r - a$, m an integer with $1 < m < r-1$ and $p \nmid m$, $m^* = r - m$, and*

$$\begin{aligned} f = M(a,b,m) &= x^{mm^*}(x-b)^{mm^*}\left(x^m + a^*b^{-r}((x-b)^m - x^m)\right)^m \\ &\quad \cdot \left(x^{m^*} + ab^{-r}((x-b)^{m^*} - x^{m^*})\right)^{m^*}, \\ g &= x^m(x-a)^{m^*}, \\ h &= x^r + a^*b^{-r}(x^{m^*}(x-b)^m - x^r), \\ g^* &= x^{m^*}(x-a^*)^m, \\ h^* &= x^r + ab^{-r}(x^m(x-b)^{m^*} - x^r). \end{aligned} \tag{3.23}$$

Then $f = g \circ h = g^* \circ h^* \in P_{r^2}(F)$ has a 2-collision.

The polynomials f in (3.23) are "multiply original" in the sense that they have a multiple root at 0. This motivates the designation M. The notation is set up so that * acts as an involution on our data, leaving b, f, r, and x invariant.

Mike Zieve (2011) points out that the rational functions of case (4) in Proposition 5.6 of Avanzi & Zannier (2003) can be transformed into (3.23). Zieve also mentions that this example already occurs in unpublished work of his, joint with Bob Beals.

Proof. Let

$$\begin{aligned} H &= h/x^{m^*} = x^m + a^*b^{-r}((x-b)^m - x^m), \\ H^* &= h^*/x^m = x^{m^*} + ab^{-r}((x-b)^{m^*} - x^{m^*}). \end{aligned} \tag{3.24}$$

Then $h - a = (x-b)^m H^*$ and $h^* - a^* = (x-b)^{m^*} H$. It follows that

$$g \circ h = g^* \circ h^* = x^{mm^*}(x-b)^{mm^*} H^m (H^*)^{m^*} = f. \tag{3.25}$$

If $g = g^*$, then the coefficients of x^{r-1} in g and g^* yield $mb^r = 0$, hence $p \mid m$, a contradiction. Thus f is a 2-collision. □

For $r \le 4$, there is no value of m satisfying the assumptions. The construction works for arbitrary $a \in F$ and $1 \le m \le r-1$. But when $a \in \{0, b^r\}$, we get a Frobenius collision; see Example 2.4. When $p \mid m$, we write $m = p^e m_0$ with $p \nmid m_0$ and have $f = x^{p^e} \circ M(a, b^{p^e}, m_0) \circ x^{p^e}$ with r/p^e instead of r in (3.23). When m is 1 or $r-1$, an original shift of (3.23) yields a polynomial of the form $S(u,s,\varepsilon,m)$. Indeed, for $m = 1$, let $w = a^*b^{-r+1}$, $c = (ab^{1-r})^r - a^*$, and

$$(u,s,\varepsilon,m,t,t^*) = \begin{cases} (-aa^*b^{1-r}, 1, 0, r-1, -a^*b^{1-r}, ab^{1-r}) & \text{if } c = 0, \\ (c/s^r, -aa^*b^{1-r}/c, 1, r-1, -c/a, c/a^*) & \text{otherwise.} \end{cases}$$

Then $M(a,b,1)^{(w)} = S(u,s,\varepsilon,m)$, $(g,h)^{(w)}$ is of the form (3.3), and so is $(g^*,h^*)^{(w)}$ with t replaced by t^*. Furthermore, for $m = r-1$, we have $M(a,b,r-1) = M(a^*,b,1)$ and the claimed parameters can be found as described by interchanging a and a^*.

Next, we describe the (non)uniqueness of this construction. We take all polynomial gcds to be monic, except that $\gcd(0,0) = 0$.

Proposition 3.26. *Let r be a power of p, $b \in F^\times$, $a \in F \setminus \{0, b^r\}$, m an integer with $1 < m < r-1$ and $p \nmid m$, and $f = M(a,b,m)$ as in (3.23). Then the following hold.*

(i) In the notation of Theorem 3.22 and with H and H^* as in (3.24), we have $\gcd(m,m^*) = 1$ and the four polynomials x, $x-b$, H, and H^* are squarefree and pairwise coprime.

(ii) The stabilizer of f under original shifting is $\{0\}$. For $F = \mathbb{F}_q$, the orbit of f under original shifting has size q.

(iii) For a_0, b_0, m_0 satisfying the conditions of Theorem 3.22, we have $M(a,b,m) = M(a_0,b_0,m_0)$ if and only if $(a_0,b_0,m_0) \in \{(a,b,m),(a^*,b,m^*)\}$. If we impose the additional condition $m < r/2$, then (a,b,m) is uniquely determined by $M(a,b,m)$.

(iv) There are exactly two polynomials of the form (3.23) in the orbit of f under original shifting, namely f and $f^{(b)} = M(-a^*,-b,m)$.

Proof. (i) If $d > 1$ was a common divisor of m and m^*, then $d \mid m + m^* = r$ and thus d would be a power of p—in particular $p \mid m$, a contradiction. Thus $\gcd(m,m^*) = 1$. From $mH - xH' = m^*a^*b^{1-r}(x-b)^{m-1}$ and $H(0)\cdot H(b) \neq 0$, we find that H is squarefree and coprime to $x(x-b)$, and similarly for H^*. Since $H \mid h$, $H^* \mid (h-a)$, and $\gcd(h, h-a) = 1$, we have $\gcd(H,H^*) = 1$.

(ii) For the coefficient of x^{r^2-r-2} in the composition $f = g \circ h$, we find

$$f_{r^2-r-2} = g_{r-1}(h_{r-1}^2 - h_{r-2}),$$

since $r > 2$. For the shifted composition $f^{(w)} = g^{(h(w))} \circ h^{(w)}$, we have the coefficients

$$\begin{aligned} g_{r-1}^{(h(w))} &= g_{r-1} = -m^*a \neq 0, \\ h_{r-1}^{(w)} &= h_{r-1} = -ma^*(-b)^{1-r} \neq 0, \\ h_{r-2}^{(w)} &= h_{r-2} - wh_{r-1}, \\ f_{r^2-r-2}^{(w)} &= g_{r-1}(h_{r-1}^2 - h_{r-2} + wh_{r-1}). \end{aligned}$$

Thus, $f_{r^2-r-2} = f^{(w)}_{r^2-r-2}$ if and only if $w = 0$.

(iii) Sufficiency is a direct computation. Conversely, assume that $f = M(a, b, m) = M(a_0, b_0, m_0) = f_0$. From (i) and the multiplicity mm^* of 0 and b in f, we find $mm^* = m_0 m_0^*$ and $b_0 = b$; see (3.25). If necessary, replacing (a, b, m) by (a^*, b, m^*), we obtain $m_0 = m$. Dividing f and f_0 by $x^{mm^*}(x-b)^{mm^*}$ yields $H^m(H^*)^{m^*} = H_0^m(H_0^*)^{m^*}$ by (3.25). Hence by (i), we find $H_0 = H$ and thus $a_0 = a$.

(iv) We find $f^{(b)} = M(-a^*, -b, m)$ by a direct computation. Conversely, we take a_0, b_0, m_0 as in Theorem 3.22 and assume that $f^{(w)} = M(a_0, b_0, m_0) = f_0$. By (iii), we may assume that $m, m_0 < r/2$. We have

$$\begin{aligned} g' &= m^* a x^{m-1}(x-a)^{m^*-1}, \\ h' &= m a^* b^{1-r} x^{m^*-1}(x-b)^{m-1}, \\ f' &= (g' \circ h) \cdot h' \\ &= mm^* a a^* b^{1-r}(x(x-b))^{mm^*-1} H^{m-1}(H^*)^{m^*-1}. \end{aligned} \tag{3.27}$$

Now (i) and $p \nmid mm^*$ show that f' has roots of multiplicity $mm^* - 1$ exactly at 0 and b and otherwise only roots of multiplicity at most $m^* - 1 < mm^* - 1$. Furthermore, $(f^{(w)})' = f'(x + w)$ has roots of multiplicity $mm^* - 1$ exactly at $-w$ and $b - w$. Similarly, f_0 has roots of multiplicity $m_0 m_0^* - 1$ at 0 and b_0, and all other roots have smaller multiplicity. It follows that $mm^* = m_0 m_0^*$ and $m = m_0$. Furthermore, one of $-w$ and $b - w$ equals 0, so that $w \in \{0, b\}$. Hence $(a_0, b_0, m_0, w) \in \{(a, b, m, 0), (a^*, b, m^*, 0), (-a^*, -b, m, b), (-a, -b, m^*, b)\}$. □

We now provide the exact number of these collisions over $\mathbb{F}_q$, matching Proposition 3.21. When $r \leq 4$, there are no polynomials of the form (3.23).

Corollary 3.28. *For $r \geq 3$ and $F = \mathbb{F}_q$, the number of polynomials that are of the form* (3.23) *or shifts thereof is*

$$\frac{q(q-1)(q-2)(r - \frac{r}{p} - 2)}{4}.$$

Proof. There are $q - 1$, $q - 2$, and $r - r/p - 2$ choices for the parameters b, a, and m, respectively. By Proposition 3.26 (iii), exactly two distinct triples of parameters generate the same polynomial (3.23). By (ii), the shift orbits are of size q and by (iv), they contain two such polynomials each. □

Over a field F of characteristic $p > 0$, Algorithm 3.29 finds the parameters for polynomials that are original shifts of (3.23), just as Algorithm 3.18 does for original shifts of (3.2). It involves conditional divisions and routines for

extracting pth and square roots. Given a field element, the latter produce a root, if one exists, and "failure" otherwise. If F is finite, then every element has a pth root. The algorithm for a square root yields a subroutine to determine the set of roots of a quadratic polynomial.

Theorem 3.30. *Algorithm 3.29 works correctly as specified. If $F = \mathbb{F}_q$, it takes $O(\mathsf{M}(n)\log n + n\log q)$ field operations on input a polynomial of degree $n = r^2$.*

Proof. For the correctness, it is sufficient—due to the check in step 24—to show that for a_0, b_0, m_0 as in Theorem 3.22 and $w_0 \in F$, the algorithm does not return "failure" on input $f = M(a_0, b_0, m_0)^{(w_0)}$. As remarked after Theorem 3.22, we have $r \geq 5$ and by Proposition 3.26 (iii), we may assume $m_0 < r/2$. Furthermore, (3.27) determines $\operatorname{lc}(f') \neq 0$ explicitly and step 1 is defined. The square root in step 3 is defined, since for $p = 2$, m_0 and $r - m_0$ are odd and all exponents in the monic version of (3.27) are even.

By (3.27) and Proposition 3.26 (i), we have after steps 1 and 3

$$f_0 = \begin{cases} \varphi^{m_0(r-m_0)-1} H_0^{m_0-1} H_0^{*r-m_0-1} & \text{if } p > 2, \\ \varphi^{(m_0(r-m_0)-1)/2} H_0^{(m_0-1)/2} H_0^{*(r-m_0-1)/2} & \text{if } p = 2, \end{cases} \tag{3.31}$$

with $\varphi = (x + w_0)(x - b_0 + w_0)$, $H_0 = H \circ (x + w_0)$, $H_0^* = H^* \circ (x + w_0)$, and H and H^* as in (3.24) with $a_0, a_0^*, b_0, m_0, m_0^*$ instead of a, a^*, b, m, m^*, respectively. By Proposition 3.26 (i), these three polynomials are squarefree and pairwise coprime. Let δ, ε, ε^* be 0 if p divides the exponent of φ, H_0, H_0^*, respectively, in (3.31), and be 1 otherwise. Then

$$\gcd(f_0, f_0') = \begin{cases} \varphi^{m_0(r-m_0)-1-\delta} H_0^{m_0-1-\varepsilon} H_0^{*r-m_0-1-\varepsilon^*} & \text{if } p > 2, \\ \varphi^{(m_0(r-m_0)-1)/2-\delta} H_0^{(m_0-1)/2-\varepsilon} H_0^{*(r-m_0-1)/2-\varepsilon^*} & \text{if } p = 2. \end{cases}$$

This gcd is nonzero, and step 4 computes

$$f_1 = f_0 / \gcd(f_0, f_0') = \varphi^\delta H_0^\varepsilon H_0^{*\varepsilon^*}.$$

We have

$$\delta = \begin{cases} 1 & \text{if } p = 2 \text{ or } p \nmid m_0^2 + 1, \\ 0 & \text{otherwise.} \end{cases} \tag{3.32}$$

For odd p, this follows from $m_0(r - m_0) - 1 \equiv -m_0^2 - 1 \bmod p$, and for $p = 2$ from $4 \nmid m_0^2 + 1$. The sum of the exponents of H_0 and H_0^* in (3.31) is $r - 2$ for odd p and $r/2 - 1$ for $p = 2$. In either case, it is coprime to p and at least one of ε and ε^* equals 1. If $p > 2$ and $\varepsilon = 0$, then $m_0 \equiv 1 \bmod p$, and thus

Algorithm 3.29: Identify multiply original polynomials

Input: a polynomial $f \in P_{r^2}(F)$ with r a power of $p = \operatorname{char} F$
Output: parameters a, b, m, as in Theorem 3.22, and $w \in F$ such that $f = M(a, b, m)^{(w)}$, if such values exist, and "failure" otherwise

$f_0 \leftarrow f'/\operatorname{lc}(f')$ if defined
if $p = 2$ **then** $f_0 \leftarrow f_0^{1/2}$
if defined
$f_1 \leftarrow f_0/\gcd(f_0, f_0')$ if defined
if $\deg f_1 < 4$ **or** $\deg f_1 > r + 2$ **then return** *"failure"*
determine the maximal k such that $f_1^k \mid f_0$ via the generalized Taylor expansion of f_0 in base f_1
if $p = 2$ **then** $k \leftarrow 2k$
$m \leftarrow \min\{k + 1, r - k - 1\}$
if $m < 2$ **then return** *"failure"*
if $p = 2$ *or* $p \nmid m^2 + 1$ **then**
    $f_2 \leftarrow \gcd(f_1^{r-m}, f_0)/\gcd(f_1^{r-m-1}, f_0)$
else
    $f_3 \leftarrow f_0/\gcd(f_1^{r-m-1}, f_0)$ if defined
    determine the maximal ℓ such that p^ℓ divides every exponent of x with nonzero coefficient in f_3
    $f_3 \leftarrow f_3^{1/p^\ell}$ if defined
    $f_2 \leftarrow f_3/\gcd(f_3, f_3')$
end
if $\deg f_2 \neq 2$ **then return** *"failure"*
compute the set X of roots of f_2 in F
if $\#X < 2$ **then return** *"failure"*
write X as $\{x_1, x_2\}$ and set $b \leftarrow x_2 - x_1$ and $w \leftarrow -x_1$
compute the set A of roots of $y^2 - b^r y - m^{-2} b^{r-1} \operatorname{lc}(f') \in F[y]$ in F
for $a \in A$ **do**
    if $f = M(a, b, m)^{(w)}$ **then**
        return a, b, m, w
    end
end
return *"failure"*

$m_0^2 \equiv 1 \bmod p$. Hence $p \nmid m_0^2 + 1$ and $\delta = 1$. Similarly, $\varepsilon^* = 0$ implies $\delta = 1$, and we find that at least two of δ, ε, and ε^* take the value 1. This also holds for $p = 2$.

Since $\deg \varphi = 2$, $\deg H_0, \deg H_0^* \geq 2$, and $\deg H_0 + \deg H_0^* = r$, this implies $4 \leq \deg f_1 \leq r+2$ and step 5 does not return "failure". The exponents in (3.31) satisfy $m_0 - 1 < r - m_0 - 1 < m_0(r - m_0) - 1$. If $p > 2$, then k as determined in step 6 equals $m_0 - 1$ if $\varepsilon = 1$, and $r - m_0 - 1$ otherwise. In characteristic 2, step 7 modifies $k \in \{(m_0 - 1)/2, (r - m_0 - 1)/2\}$, so that in any characteristic, step 8 recovers $m = m_0 \geq 2$ and step 9 does not return "failure".

The condition in step 10 reflects the case distinction in (3.32).

- If the condition holds, we have $\delta = 1$ and

$$\begin{aligned} \gcd(f_1^{r-m}, f_0) &= \varphi^{r-m} H_0^{\varepsilon(m-1)} H_0^{*\varepsilon^*(r-m-1)}, \\ \gcd(f_1^{r-m-1}, f_0) &= \varphi^{r-m-1} H_0^{\varepsilon(m-1)} H_0^{*\varepsilon^*(r-m-1)}, \end{aligned}$$

  and therefore $f_2 = \varphi$ in step 11.

- Otherwise, we have $\delta = 0$, $p > 2$, $\varepsilon = \varepsilon^* = 1$,

$$\begin{aligned} f_0 &= \varphi^{m(r-m)-1} H_0^{m-1} H_0^{*r-m-1}, \\ \gcd(f_1^{r-m-1}, f_0) &= H_0^{m-1} H_0^{*r-m-1}, \end{aligned}$$

  and $f_3 = \varphi^{m(r-m)-1}$ in step 13. After step 15, we have $f_3 = \varphi^e$ for some e with $p \nmid e$ and $f_2 = \varphi^e / \varphi^{e-1} = \varphi$ in step 16.

In any case, we have $f_2 = (x + w_0)(x - b_0 + w_0)$ with distinct roots $-w_0$ and $b_0 - w_0$ in F, and steps 18, 19, and 20 do not return "failure". We determine a, b, and w in steps 21–24. In step 21, we have $(b, w) \in \{(b_0, w_0), (-b_0, w_0 - b_0)\}$, depending on the choice of the order of x_1 and x_2. Since $f = M(a_0, b_0, m)^{(w_0)} = M(b_0^r - a_0, -b_0, m)^{(w_0 - b_0)}$ according to Proposition 3.26 (iv), we have $f = M(\bar{a}, b, m)^{(w)}$ for some $\bar{a} \in \{a_0, b_0^r - a_0\}$. The leading coefficient of f' is $-m^2 \bar{a} b^{1-r}(b^r - \bar{a})$ by (3.27) yielding a quadratic polynomial in $F[y]$ with roots $\bar{a}$ and $b^r - \bar{a}$ for step 22. There, we find $A = \{\bar{a}, b^r - \bar{a}\}$ and step 24 identifies $\bar{a}$.

For the cost over $F = \mathbb{F}_q$, the conditions in steps 5 and 9 ensure that all powers of f_1 in the gcd computations of steps 11 and 13 have degree at most $(r + 2)(r - 2) < n$ and we have $O(\mathsf{M}(n) \log n)$ field operations for the quotients, gcds, and products in steps 1, 4, 11, 13, 16, and 24. The f_1-adic expansion of f_0 is a sequence $a_0, \ldots, a_{\nu-1} \in \mathbb{F}_q[x]$ such that $f_0 = \sum_{0 \leq i < \nu} a_i f_1^i$ and $\deg a_i < \deg f_1$ for all $i < \nu$. We may bound ν by the smallest power of 2

greater than $\deg f_0/\deg f_1$. Then $\nu < 2\deg f_0/\deg f_1$ and for k in step 6 we have $k+1 = \min\{0 \le i < \nu \colon a_i \ne 0\}$. We can compute the expansion with $O(\mathsf{M}(\nu \deg f_1)\log \nu)$ field operations; see von zur Gathen & Gerhard (2013, Theorem 9.15). Thus the cost of step 6 is $O(\mathsf{M}(n)\log n)$ field operations. The calculation of the right-hand side in step 24 takes $O(\mathsf{M}(n)\log n)$ field operations, by first substituting $x+w$ for x in $M(a,b,m)$ as in (3.23), then computing its coefficients and leaving away the constant term. We ignore the (cheap) operations on integers in the various tests, in step 14, and the computation of derivatives in steps 1, 4, and 16. The polynomial square root in step 3 and the p^ℓth root in step 15 take $O(n\log q)$ field operations each using $u^{q^c/p^\ell} = u^{1/p^\ell}$ for $u \in \mathbb{F}_q$ and the smallest $c \ge 1$ with $q^c \ge p^\ell$. Taking the square roots in steps 19 and 22 can be done deterministically by first reducing the computations to the prime field $\mathbb{F}_p$, see von zur Gathen & Gerhard (2013, Exercise 14.40), and then finding square roots in $\mathbb{F}_p$ by exhaustive search. These take $O(\log q)$ and $O(\sqrt{n})$ field operations, respectively, since $n = r^2$ is a power of p. □

4 Root multiplicities in collisions

In this section we describe the structure of root multiplicities in collisions over an algebraic closure of F under certain conditions. In Section 5 these results will be used for the classification of 2-collisions at degree p^2. For the classification, its proof, and the lemmas in this section, we follow ideas of Dorey & Whaples (1974) and Zannier (1993); an earlier version can be found in Blankertz (2011).

After some general facts about root multiplicities, we state an assumption on 2-collisions (Assumption 4.7) under which we determine the root multiplicities of their components (Proposition 5.4). In Example 4.12 we see that this assumption holds for the 2-collisions in Fact 3.1 and in Theorem 3.22. Then we recall the well-known relation between decompositions of polynomials and towers of rational function fields. We reformulate a result by Dorey & Whaples (1974) about the ramification in such fields in the language of root multiplicities of polynomials (Proposition 4.22) and derive further properties about the multiplicities in collisions for which Assumption 4.7 holds.

We use the following notation. Let F be a field of characteristic $p > 0$ and $K = \overline{F}$ an algebraic closure of F. For a nonzero polynomial $f \in F[x]$ and $b \in K$, let $\mathrm{mult}_b(f)$ denote the *root multiplicity* of b in f, so that $f = (x-b)^{\mathrm{mult}_b(f)}u$ with $u \in K[x]$ and $u(b) \ne 0$. For $c \in K$, we denote as $f^{-1}(c)$ the set of all $b \in K$ such that $f(b) = c$.

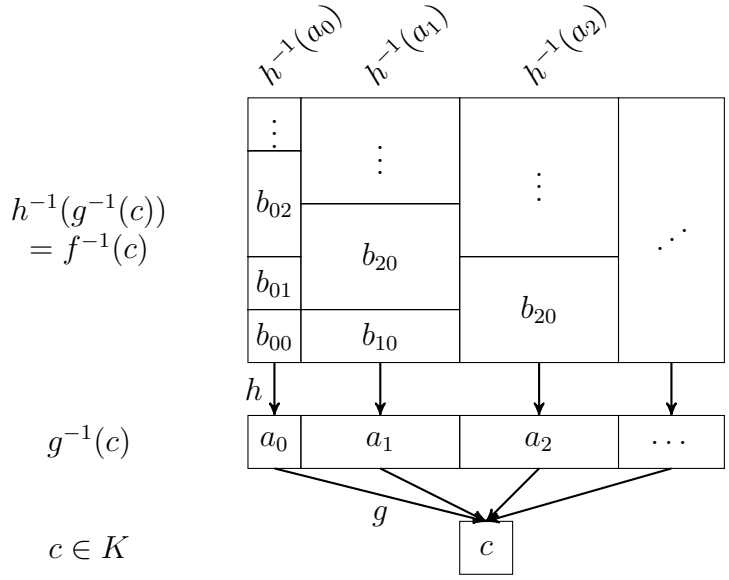

Figure 1: Partition of $f^{-1}(c)$

Lemma 4.1. *Let $f = g \circ h \in P_n(F)$ and $c \in K$. Then*

$$f^{-1}(c) = \dot{\bigcup_{a \in g^{-1}(c)}} h^{-1}(a)$$

is a partition of $f^{-1}(c)$, and for all $b \in f^{-1}(c)$, we have

$$\mathrm{mult}_b(f - c) = \mathrm{mult}_{h(b)}(g - c) \cdot \mathrm{mult}_b(h - h(b)). \tag{4.2}$$

The partition of $f^{-1}(c)$ from Lemma 4.1 is illustrated in Figure 1, where we write $g^{-1}(c) = \{a_0, \ldots, a_\ell\}$.

Proof. Let $b \in \bigcup_{a \in g^{-1}(c)} h^{-1}(a)$ and $a \in g^{-1}(c)$ such that $b \in h^{-1}(a)$. Hence $f(b) = g(h(b)) = g(a) = c$ and thus $b \in f^{-1}(c)$. On the other hand, let $b \in f^{-1}(c)$ and set $a = h(b)$. Then $b \in h^{-1}(a)$ and $a \in g^{-1}(c)$, since $g(a) = g(h(b)) = c$. Hence $b \in \bigcup_{a \in g^{-1}(c)} h^{-1}(a)$. Moreover if $b \in h^{-1}(a) \cap h^{-1}(a_0)$ for some a, $a_0 \in K$, then $a = h(b) = a_0$.

For (4.2), let $b \in f^{-1}(c)$, $a = h(b)$, $e = \mathrm{mult}_a(g - c)$, and $e_0 = \mathrm{mult}_b(h - a)$. Then $g - c = (x - a)^e G$ and $h - a = (x - b)^{e_0} H$ for some G, $H \in K[x]$ with $G(a) \cdot H(b) \neq 0$. Thus $f - c = g(h) - c = (h - a)^e G(h) = ((x - b)^{e_0} H)^e G(h) = (x - b)^{ee_0} H^e G(h)$ with $(H^e G(h))(b) = H(b)^e G(a) \neq 0$. □

Lemma 4.3. *Let $f \in K[x]$ and $b \in K$. Then b is a root of f' if and only if there is some $c \in K$ with $\mathrm{mult}_b(f - c) > 1$. Moreover, for any $c \in K$ with $p \nmid \mathrm{mult}_b(f - c)$, we have $\mathrm{mult}_b(f') = \mathrm{mult}_b(f - c) - 1$.*

Proof. Let b be a root of f' and set $c = f(b)$. Then b is a root of $f - c$. We write $f - c = (x - b)u$ for some $u \in K[x]$. Then $f' = (f - c)' = u + (x - b)u'$, and thus $u(b) = f'(b) = 0$. Hence b is a multiple root of $f - c$.

Now, let $c \in K$ with $e = \mathrm{mult}_b(f - c)$. Then $f - c = (x - b)^e u$ for some $u \in K[x]$ with $u(b) \neq 0$ and $f' = (f - c)' = (x - b)^{e-1}(eu + (x - b)u')$. Thus, b is a root of f' if $e > 1$. This proves the converse. Moreover, if $p \nmid e$ then $(eu + (x - b)u')(b) = eu(b) \neq 0$ and hence $\mathrm{mult}_b(f') = e - 1$. □

We use the following proposition. The second part was stated as Proposition 6.5 (i) in von zur Gathen, Giesbrecht & Ziegler (2010) for $F = \mathbb{F}_q$.

Proposition 4.4. *Let r be a power of p and $f \in P_{r^2}(F)$ have a 2-collision C such that $\deg g = \deg h = r$ and $g'h' \neq 0$ for all $(g, h) \in C$. Then $f' \neq 0$ and the following hold.*

(i) There are integers d_1 and d_2 such that $\deg g' = d_1$ and $\deg h' = d_2$ for all $(g, h) \in C$.

(ii) Furthermore, if $r = p$, then $d_1 = d_2$.

Proof. (i) Let $(g, h) \in C$ and $f = g \circ h$. Then

$$\deg f' = \deg g' \cdot \deg h + \deg h'. \tag{4.5}$$

Since $g'h' \neq 0$, this is an equation of nonnegative integers. Moreover, $\deg h' < \deg h = r$ and thus $\deg g'$ and $\deg h'$ are uniquely determined by $\deg f'$ and r, which proves the claim.

(ii) For $r = p$, let $\ell = \deg_2 g$ and $m = \deg_2 h$ with the second degree $\deg_2$ as in (3.4). Since $g'h' \neq 0$, we find $d_1 = \deg g' = \ell - 1$ and $d_2 = \deg h' = m - 1$ for all $(g, h) \in C$ and it is sufficient to show $\ell = m$. We have

$$\begin{aligned} g &= x^p + g_\ell x^\ell + O(x^{\ell-1}), \\ h &= x^p + h_m x^m + O(x^{m-1}) \end{aligned}$$

with $g_\ell, h_m \in F^\times$. The highest terms in h^ℓ and $g \circ h$ are given by

$$\begin{aligned} h^\ell &= (x^p + h_m x^m + O(x^{m-1}))^\ell \\ &= x^{\ell p} + \ell h_m x^{(\ell-1)p+m} + O(x^{(\ell-1)p+m-1}), \\ g \circ h &= x^{p^2} + h_m^p x^{mp} + O(x^{(m-1)p}) + g_\ell x^{\ell p} + \ell g_\ell h_m x^{(\ell-1)p+m} \\ &\quad + O(x^{(\ell-1)p+m-1}) + O(x^{(\ell-1)p}). \end{aligned} \tag{4.6}$$

Algorithm 4.10 of von zur Gathen (2013) computes the components g and h from f, provided that $h_{p-1} \neq 0$. We do not assume this, but can apply

the same method. Once g_ℓ and h_m are determined, the remaining coefficients first of h, then of g, are computed by solving linear equations of the form $uh_i = v$, where u and v are known at that point, and $u \neq 0$. Quite generally, g is determined by f and h.

For $(g^*, h^*) \in C$, we find that $(g_\ell, h_m) = (g^*_\ell, h^*_m)$ implies $(g, h) = (g^*, h^*)$ by the uniqueness of the procedure just sketched. Inspection of the coefficient of $x^{(\ell-1)p+m}$ in (4.6) shows that $g_\ell = g^*_\ell$ if and only if $h_m = h^*_m$.

Now take some $(g^*, h^*) \in C$ and assume that $\ell \neq m$. Then $\deg_2(g \circ h)$ is one of the two distinct integers mp or ℓp. If $m > \ell$, then h^p_m (and hence h_m) is uniquely determined by f, and otherwise g_ℓ is. In either case, we conclude from the previous observation that $(g, h) = (g^*, h^*)$. This shows $\ell = m$ if $(g, h) \neq (g^*, h^*)$. □

A *common right component* (over K) of two polynomials $h, h^* \in K[x]$ is a nonlinear polynomial $v \in K[x]$ such that $h = u \circ v$ and $h^* = u^* \circ v$ for some u, $u^* \in K[x]$. We now state an assumption which we use in Proposition 4.22, the lemmas thereafter, and in Proposition 5.4.

Assumption 4.7. *Let $f \in P_n(F)$ have a 2-collision $\{(g, h), (g^*, h^*)\}$. We consider the following conditions.*

(A_1) The derivative f' is nonzero.

(A_2) The degrees of all components are equal, that is, $\deg g = \deg g^* = \deg h = \deg h^*$.

(A_3) The right components h and h^* have no common right component over K.

(A_4) For all $c \in K$, neither $g - c$ nor $g^* - c$ have roots in K with multiplicity divisible by p.

(A_5) The degrees of g' and $h^{*\prime}$ are equal.

Lemma 4.8. *Let $f \in P_n(F)$ have a 2-collision $\{(g, h), (g^*, h^*)\}$.*

(i) Assumption (A_1) holds if and only if all derivatives g', $g^{*\prime}$, h', and $h^{*\prime}$ are nonzero.

(ii) If h or h^* is indecomposable, then (A_3) holds. In particular, it holds if $\deg h = \deg h^*$ is prime.

(iii) If $\deg g = p$ and (A_1) holds, then (A_4) holds.

(iv) If $n = p^2$ and (A_1) holds, then (A_5) holds.

(v) If (A_1), (A_2), *and* (A_5) *hold, then* $\deg g' = \deg g^{*\prime} = \deg h' = \deg h^{*\prime}$.

Proof. (i) The claim follows from the fact that $f' = g'(h) \cdot h'$.

(ii) Assume that h is indecomposable. Then a common right component of h and h^* would imply $h = h^*$ and thus $(g, h) = (g^*, h^*)$, by Lemma 2.3, a contradiction. Hence (A_3) holds. Moreover, polynomials of prime degree are indecomposable.

(iii) If a multiplicity of $g - c$ was divisible by p for some $c \in K$, then $g - c = (x - a)^p$ for some $a \in K$. This would imply $g' = 0$, contradicting (A_1). Similarly, for all $c \in K$ the multiplicities of $g^* - c$ are not divisible by p. Thus (A_4) holds.

(iv)–(v) We can apply Proposition 4.4, since $\deg g = \deg g^* = \deg h = \deg h^*$ by $n = p^2$ or (A_2), respectively, and $g'h'g^{*\prime}h^{*\prime} \neq 0$ by (A_1) and (i). Then (ii) of the cited proposition shows $\deg g' = \deg g^{*\prime} = \deg h' = \deg h^{*\prime}$, proving (iv) and (v). □

In Example 4.12 we show that Assumption 4.7 holds for the collisions in Fact 3.1 and in Theorem 3.22. We need the next two propositions to check (A_3) for these collisions.

Proposition 4.9. *Let* r *be a power of* p, *let* $a, a^* \in F$ *and* m *be a positive divisor of* $r - 1$, $\ell = (r - 1)/m$, *and*

$$h = x(x^\ell - a)^m,$$
$$h^* = x(x^\ell - a^*)^m.$$

If h *and* h^* *have a common right component, then* $h = h^*$. *In particular, the right components in* 2*-collisions of the form as in Fact 3.1 have no common right component.*

Proof. By Henderson & Matthews (1999, Theorem 4.1) it suffices to prove the claim for additive polynomials, that is, for $m = 1$. Furthermore, we can assume without loss of generality that F is algebraically closed. Let $v \in P_{p^\nu}(F)$ be a common right component of h and h^* with $h = u \circ v$ and $h^* = u^* \circ v$ for some $u, u^* \in P_{p^k}(F)$, $\nu \geq 1$, and $r = p^{k+\nu}$. Then u, u^*, and v are additive polynomials; see Cohen (1990b, Lemma 2.4). By Ore (1933, Theorem 3 in Chapter 1) and since F is algebraically closed, we may assume $\nu = 1$ and $v = x^p - bx$, for some $b \in F$. For $u = \sum_{0 \leq i \leq k} u_i x^{p^i}$, we have

$$\begin{aligned} h = x^r - ax &= u \circ (x^p - bx) \\ &= u_k x^r + \sum_{1 \leq i \leq k} (u_{i-1} - u_i b^{p^i}) x^{p^i} - u_0 bx. \end{aligned}$$

Thus $u_k = 1$ and $u_{i-1} = u_i b^{p^i} = \prod_{i \leq j \leq k} b^{p^j}$, for $1 \leq i \leq k$. Moreover, $a = u_0 b = \prod_{0 \leq j \leq k} b^{p^j}$ is uniquely determined by b. Thus $a = a^*$ and $h = h^*$. □

Proposition 4.10. *Let r, b, a, a^*, m, m^*, g, and h be as in Theorem 3.22. Then g and h are indecomposable.*

Proof. Let $g = u \circ v$ with $u \in P_k(F)$, $v \in P_\ell(F)$, $k\ell = r$, and $\ell > 1$. Then $p \mid \ell$. By Lemma 4.1 we have

$$\dot{\bigcup_{a_0 \in u^{-1}(0)}} v^{-1}(a_0) = g^{-1}(0) = \{0, a\}. \tag{4.11}$$

Since v is original, we have $\{0\} \subseteq v^{-1}(0) \subseteq \{0, a\}$. If $v^{-1}(0) = \{0\}$, then $v = x^\ell$ and thus $p \mid \ell \mid m$, by (4.2), in contradiction to $p \nmid m$. Thus $v^{-1}(0) = \{0, a\}$. Since the union in (4.11) is disjoint, we find that $u^{-1}(0) = \{0\}$ and 0 is the only root of u. Hence $u = x^k$ and $k \mid \gcd(m, m^*) = 1$, by (4.2) and Proposition 3.26 (i). Therefore u is linear and thus g is indecomposable.

By (3.24) and Proposition 3.26 (i), we find $h = x^{m^*}H$ and $h - a = (x - b)^m H^*$ with squarefree polynomials H and H^*. Thus $h^{(b)} = x^m \tilde{H}$ for squarefree $\tilde{H} = H^* \circ (x + b)$. We find that h is decomposable if and only if $h^{(b)}$ is decomposable. By Proposition 3.26 (iii) either $m > r/2$ or $m^* > r/2$. If $m > r/2$, then we rename h as $h^{(b)}$, H as $\tilde{H}$ and m as m^*. We have in either case $m^* > r/2$.

Now let $h = u \circ v$ with $u \in P_k(F)$, $v \in P_\ell(F)$, $k\ell = r$, and $\ell > 1$. Then $p \mid \ell$. The only multiple root in h is 0, since H is squarefree, by Proposition 3.26 (i). Its multiplicity is $\mathrm{mult}_0(h) = m^* = \mathrm{mult}_0(u) \cdot \mathrm{mult}_0(v)$. Thus $\mathrm{mult}_0(v) \mid m^*$ and hence $p \nmid \mathrm{mult}_0(v)$. Since the multiplicities of v sum up to ℓ, which is divisible by p, there is another root $b_0 \neq 0$ of v. Then $1 = \mathrm{mult}_{b_0}(h) = \mathrm{mult}_0(u) \cdot \mathrm{mult}_{b_0}(v)$ and thus $\mathrm{mult}_0(u) = 1$. Hence $\mathrm{mult}_0(v) = m^*$. We have $\ell > m^* > r/2$, thus $\ell = r$ and u is linear. □

Example 4.12. Assumption 4.7 holds for the $\#T$-collisions in Fact 3.1 with $\#T \geq 2$ and the 2-collisions in Theorem 3.22. In both cases (A_2) holds by definition. Assumption (A_3) follows from Proposition 4.9 and from Proposition 4.10 and Lemma 4.8 (ii), respectively.

The derivatives of the components in Fact 3.1 are

$$\begin{aligned} g' &= -us^r t^{-1}(x^\ell - us^r t^{-1})^{m-1}, \\ h' &= -st(x^\ell - st)^{m-1}. \end{aligned} \tag{4.13}$$

Since u, s, $t \in F^\times$, we find $\deg g' = \deg h' = \ell(m-1) \geq 0$, independent of $t \in T$, and thus (A_5) holds. By (4.5), $\deg f' \geq 0$ and thus (A_1) holds. If there is $c \in K$ such that $g - c$ has a multiple root $b \in K$, then b is also a root of g' by Lemma 4.3. Since ${g'}^{-1}(0) \subseteq g^{-1}(0)$ by (4.13), we have only simple roots in $g - c$ for $c \neq 0$. The multiple roots of g have multiplicity m and (A_4) follows from $p \nmid m \mid r - 1$.

For the collisions in Theorem 3.22, (A_4) follows similarly from $p \nmid mm^*$. Finally, (A_1) and (A_5) are satisfied by (3.27) and a, a^*, $b \in F^\times$.

Lemma 4.14. *Let $f \in F[x]$ be monic and y be transcendental over $K(x)$. Then $f - y \in K(y)[x]$ is irreducible.*

Proof. Assume $f - y = uv$ for some $u, v \in K[x, y]$. The degree in y of $f - y$ is $\deg_y(f - y) = 1 = \deg_y u + \deg_y v$. Thus we may assume $\deg_y u = 1$ and $\deg_y v = 0$. Then $av = -1$, where $a \in K[x]$ is the leading coefficient of u in y. Thus $v \in K[x]^\times = K^\times$ and $f - y$ is irreducible in $K[x, y]$. A factorization of $f - y$ in $K(y)[x]$ yields a factorization in $K[x, y]$, by the Lemma of Gauß, see Lang (2002, Corollary 2.2 in Capter IV). Hence $f - y$ is also irreducible in $K(y)[x]$. □

Let $f \in P_n(F)$ with $f' \neq 0$ and y be transcendental over $K(x)$. Then $f - y \in K(y)[x]$ is irreducible and separable over $K(y)$, by Lemma 4.14 and since the derivative of $f - y$ with respect to x is $(f - y)' = f' \neq 0$. In particular, $f - y \in F(y)[x]$ is irreducible and separable. Let $\alpha \in \overline{K(y)}$ be a root of $f - y$. Then $K(y)[\alpha] = K(\alpha)$ is a rational extension of $K(y)$ of degree n. Let $\mathcal{M}$ be the set of intermediate fields between $K(\alpha)$ and $K(y)$ and $\mathcal{R} = \{h \in P_m(K) \colon m \mid n \text{ and there is } g \in P_{n/m}(K) \text{ such that } f = g \circ h\}$ be the set of right components of f.

Fact 4.15 (Fried & MacRae (1969), Proposition 3.4)**.** *Let $f \in P_n(K)$ with $f' \neq 0$ and let $\alpha \in \overline{K(y)}$ be a root of $f - y \in K(y)[x]$. Then the map*

$$\begin{aligned} &\mathcal{R} \to \mathcal{M}, \\ &h \mapsto K(h(\alpha)) \end{aligned} \tag{4.16}$$

is bijective.

The fact follows from Fried & MacRae (1969, Proposition 3.4). Indeed, for each $u \in K[x]$ of degree m there is exactly one $v \in P_m(K)$ such that $u = \ell \circ v$ for some linear polynomial $\ell \in K[x]$; see von zur Gathen (2013, Section 2).

The sets $\mathcal{R}$ and $\mathcal{M}$ can be equipped with natural lattice structures for which (4.16) is an isomorphism.

We now use the theory of places and ramification indices in function fields; see Stichtenoth (2009) for the background. A *place* in a function field L over K is the maximal ideal of some valuation ring of L over K. For an finite extension M of L a place $\mathfrak{p}$ in M is said to lie over a place P in L if $P \subseteq \mathfrak{p}$. Then we write $\mathfrak{p} \mid P$ and define the ramification index of $\mathfrak{p} \mid P$ as the integer $e(\mathfrak{p} \mid P)$ such that $v_\mathfrak{p}(a) = e(\mathfrak{p} \mid P) \cdot v_P(a)$ for all $a \in L$, where $v_\mathfrak{p}$ and v_P are

the corresponding valuations of $\mathfrak{p}$ and P, respectively; see Stichtenoth (2009, Proposition 3.1.4 and Definition 3.1.5).

Later, we translate this into the language of root multiplicities of polynomials. First, we need the following result, which is proven in Dorey & Whaples (1974, Lemma 1) for rational function fields under the assumption that the characteristic of K is zero. Our proof avoids this assumption.

Theorem 4.17. *Let L, M, M^*, N be function fields over K such that $L \subseteq M, M^* \subseteq N$ are finite separable field extensions and $M \otimes_L M^* \cong MM^* = N$. Let P be a place in L, and $\mathfrak{p}$, $\mathfrak{p}^*$ be places over P in M and M^*, respectively. Assume that at least one of the ramification indices $m = e(\mathfrak{p} \mid P)$ and $m^* = e(\mathfrak{p}^* \mid P)$ is not divisible by the characteristic of K. Then there are $\gcd(m, m^*)$ places $\mathfrak{q}$ in N which lie over $\mathfrak{p}$ and over $\mathfrak{p}^*$. Moreover, for such a place we have $e(\mathfrak{q} \mid P) = \operatorname{lcm}(m, m^*)$.*

Proof. Abhyankar's Lemma says that for a place $\mathfrak{q}$ in N over $\mathfrak{p}$ and over $\mathfrak{p}^*$,

$$e(\mathfrak{q} \mid P) = \operatorname{lcm}(m, m^*), \tag{4.18}$$

see Stichtenoth (2009, Theorem 3.9.1). Now we proceed as in Dorey & Whaples (1974). For places $\mathfrak{p}$, $\mathfrak{p}^*$, and $\mathfrak{q}$ over P in M, M^*, and N, respectively, we denote by $\Lambda = \widehat{L}$, $\widehat{M}^{\mathfrak{p}}$, $\widehat{M}^{*\mathfrak{p}^*}$, and $\widehat{N}^{\mathfrak{q}}$ the completions of L, M, M^*, and N with respect to P, $\mathfrak{p}$, $\mathfrak{p}^*$, and $\mathfrak{q}$, respectively. The tensor product $N \otimes_M \widehat{M}^{\mathfrak{p}}$ is the direct sum of the completions of N with respect to the places in N over $\mathfrak{p}$, and $M^* \otimes_L \Lambda$ is the direct sum of the completions of M^* with respect to the places in M^* over P; see Neukirch (1999, Proposition 8.3 in Chapter II). Since $M \otimes_L M^* \cong N$, we have

$$\begin{aligned}\bigoplus_{\mathfrak{q}\mid\mathfrak{p}} \widehat{N}^{\mathfrak{q}} &\cong N \otimes_M \widehat{M}^{\mathfrak{p}} \cong M^* \otimes_L M \otimes_M \widehat{M}^{\mathfrak{p}} \cong M^* \otimes_L \widehat{M}^{\mathfrak{p}} \\ &\cong M^* \otimes_L (\Lambda \otimes_\Lambda \widehat{M}^{\mathfrak{p}}) \cong (M^* \otimes_L \Lambda) \otimes_\Lambda \widehat{M}^{\mathfrak{p}} \\ &\cong \bigoplus_{\mathfrak{p}_0^* \mid P} \widehat{M}^{*\mathfrak{p}_0^*} \otimes_\Lambda \widehat{M}^{\mathfrak{p}},\end{aligned}$$

where the last direct sum is taken over all places $\mathfrak{p}_0^*$ in M^* over P. We show that $\widehat{M}^{*\mathfrak{p}^*} \otimes_\Lambda \widehat{M}^{\mathfrak{p}}$ is the direct sum of the completions of N with respect to the places that lie over $\mathfrak{p}$ and $\mathfrak{p}^*$. For this purpose, consider the (external) composite fields of $\widehat{M}^{*\mathfrak{p}^*}$ and $\widehat{M}^{\mathfrak{p}}$ in an algebraic closure Ω of $\widehat{N}^{\mathfrak{q}}$; those are the field extensions $\Gamma \subseteq \Omega$ of Λ such that there are two field homomorphisms which map $\widehat{M}^{*\mathfrak{p}^*}$ and $\widehat{M}^{\mathfrak{p}}$, respectively, into Γ and whose images generate Γ. Then $\widehat{M}^{*\mathfrak{p}^*} \otimes_\Lambda \widehat{M}^{\mathfrak{p}}$ is the direct sum of the composite fields of $\widehat{M}^{*\mathfrak{p}^*}$ and $\widehat{M}^{\mathfrak{p}}$; see Jacobson (1964, Theorem 21 in Chapter I). Each such composite

field Γ is isomorphic to a summand in $\bigoplus_{\mathfrak{q}|\mathfrak{p}} \widehat{N}^{\mathfrak{q}}$, by the Krull-Remak-Schmidt Theorem; see Lang (2002, Theorem 7.5). Thus there exists $\mathfrak{q} \mid \mathfrak{p}$ such that $\Gamma = \widehat{N}^{\mathfrak{q}}$. Since Γ is an extension of $\widehat{M^*}^{\mathfrak{p}^*}$, we find $\mathfrak{q} \mid \mathfrak{p}^*$ as claimed. On the other hand, for a place $\mathfrak{q}$ in N over $\mathfrak{p}$ and $\mathfrak{p}^*$, $\widehat{N}^{\mathfrak{q}}$ is a composite field of $\widehat{M^*}^{\mathfrak{p}^*}$ and $\widehat{M}^{\mathfrak{p}}$ and thus is a summand in $\widehat{M^*}^{\mathfrak{p}^*} \otimes_\Lambda \widehat{M}^{\mathfrak{p}}$.

The summands of $\widehat{M^*}^{\mathfrak{p}^*} \otimes_\Lambda \widehat{M}^{\mathfrak{p}}$ are of degree $\operatorname{lcm}(m, m^*)$, by (4.18), and the Λ-dimension of $\widehat{M^*}^{\mathfrak{p}^*} \otimes_\Lambda \widehat{M}^{\mathfrak{p}}$ is mm^*. Thus there are $mm^*/\operatorname{lcm}(m, m^*) = \gcd(m, m^*)$ places over $\mathfrak{p}$ and $\mathfrak{p}^*$. □

In the following we link the notion of places and ramification indices to the notion of roots and root multiplicities. Let $K(t)$ be a rational function field. Then the local ring $\mathcal{O}_\infty = \{g/h \in K(t) \colon g, h \in K[t], \deg g \leq \deg h\}$ is the $1/t$-adic valuation ring of $K(t)$ and $P_\infty = (1/t)\mathcal{O}_\infty$ is its maximal ideal. For $c \in K$, the local ring $\mathcal{O}_{t-c} = \{g/h \in K(t) \colon g, h \in K[t], h(c) \neq 0\}$ is the $(t-c)$-adic valuation ring of $K(t)$ and $P_c = (t-c)\mathcal{O}_{t-c}$ is its maximal ideal. We denote the $(t-c)$-adic valuation by v_{P_c}. Then we have for $f \in K[x]$

$$v_{P_c}(f(t)) = \operatorname{mult}_c(f). \tag{4.19}$$

Since the irreducible polynomials in $K[t]$ are linear, the places P_∞ and P_c for all $c \in K$ are pairwise distinct and comprise all places in $K(t)$; see Stichtenoth (2009, Theorem 1.2.2). We call the places P_c *finite* places. The map

$$\begin{aligned} K &\to \{P \colon P \text{ is a finite place in } K(t)\}, \\ c &\mapsto P_c \end{aligned} \tag{4.20}$$

is bijective.

Lemma 4.21. *Let $f \in P_n(K)$ with $f' \neq 0$, let $\alpha \in \overline{K(y)}$ be a root of $f - y \in K(y)[x]$, let $b, c \in K$, and let P_c and $\mathfrak{q}_b$ be the corresponding finite places in $K(y)$ and $K(\alpha)$, respectively. Then $\mathfrak{q}_b \mid P_c$ if and only if $f(b) = c$. Furthermore*

$$e(\mathfrak{q}_b \mid P_c) = \operatorname{mult}_b(f - c).$$

Proof. Let $\mathfrak{q}_b \mid P_c$. Then $y - c \in \mathfrak{q}_b$ and thus $f(\alpha) - c = y - c = (\alpha - b)g/h$ for $g, h \in K[\alpha]$ with $h(b) \neq 0$. Hence, $f(b) - c = (b - b)g(b)/h(b) = 0$.

Conversely, let $f(b) = c$. Then $\alpha - b \mid f(\alpha) - c$ in $K[\alpha]$. Let $(y-c)g/h \in P_c$ for some $g, h \in K[y]$ with $h(c) \neq 0$. Then $h(f(b)) = h(c) \neq 0$ and thus $(y - c)g/h = (f(\alpha) - c)g(f(\alpha))/h(f(\alpha)) \in \mathfrak{q}_b$.

By (4.19) and since $v_{P_c}(y - c) = 1$, we have $e(\mathfrak{q}_b \mid P_c) = v_{\mathfrak{q}_b}(y - c) = v_{\mathfrak{q}_b}(f(\alpha) - c) = \operatorname{mult}_b(f - c)$. □

Proposition 4.22. *Let $c \in K$ and $f \in P_n(F)$ have a 2-collision $\{(g,h),(g^*,h^*)\}$ satisfying (A_1)–(A_4) in Assumption 4.7. For $a \in g^{-1}(c)$ and $a^* \in g^{*-1}(c)$, there are exactly $\gcd(\mathrm{mult}_a(g-c), \mathrm{mult}_{a^*}(g^*-c))$ roots $b \in f^{-1}(c)$ such that $h(b) = a$ and $h^*(b) = a^*$. Furthermore, for each such root b we have*

$$\mathrm{mult}_b(f-c) = \mathrm{lcm}\left(\mathrm{mult}_a(g-c), \mathrm{mult}_{a^*}(g^*-c)\right). \tag{4.23}$$

Proof. By (A_1) we have $f' \neq 0$ and thus $f - y \in F(y)[x]$ is irreducible and separable; see Lemma 4.14 and the paragraph thereafter. Let $\alpha \in \overline{K(y)}$ be a root of $f - y$, $M = K(h(\alpha))$ and $M^* = K(h^*(\alpha))$, as in (4.16). Then α is a root of $h - h(\alpha)$ and by Lemma 4.14, $h - h(\alpha)$ is irreducible in $M[x]$. Thus the minimal polynomial of α over M is $h - h(\alpha)$, and similarly the minimal polynomial of $h(\alpha)$ over $K(y)$ is $g - y$. Hence $[K(\alpha)\colon M] = \deg h$ and $[M\colon K(y)] = \deg g$. Figure 2 illustrates the relation between these field extensions and their respective minimal polynomials.

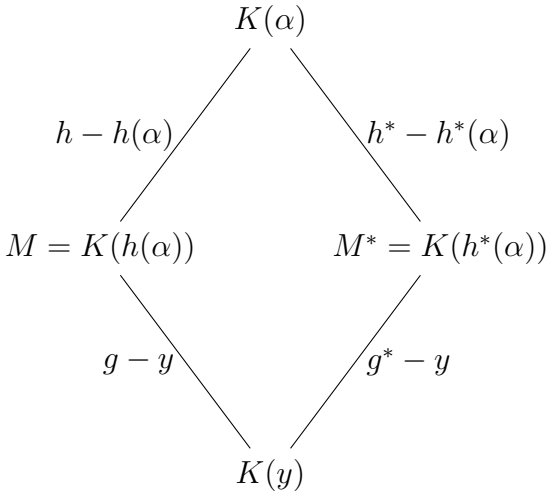

Figure 2: Lattice of subfields

By Fact 4.15 and since $MM^* \subseteq K(\alpha)$, there is a monic original $v \in K[x]$ such that $MM^* = K(v(\alpha))$. Since $M \subseteq MM^*$, there is $u \in K[x]$ such that $h = u \circ v$, by applying Fact 4.15 to $K(\alpha) \mid M$. Similarly, there is $u^* \in K[x]$ such that $h^* = u^* \circ v$. Hence $v = x$, by (A_3), and $MM^* = K(\alpha)$. Moreover, MM^* is contained in $M \otimes_{K(y)} M^*$ as a direct summand; see Jacobson (1964, Theorem 21 in Chapter I). Their $K(y)$-dimensions both equal $\deg f = \deg g \cdot \deg h = (\deg g)^2$, by (A_2). Thus $M \otimes_{K(y)} M^* \cong MM^* = K(\alpha)$. Let P_c be as in (4.20). Since, by Lemma 4.21, the root multiplicities of $g - c$ are the ramification indices of the places over P_c in M, (A_4) rules out finite

wildly ramified places in $M \mid K(y)$. Thus we can apply Theorem 4.17, as follows.

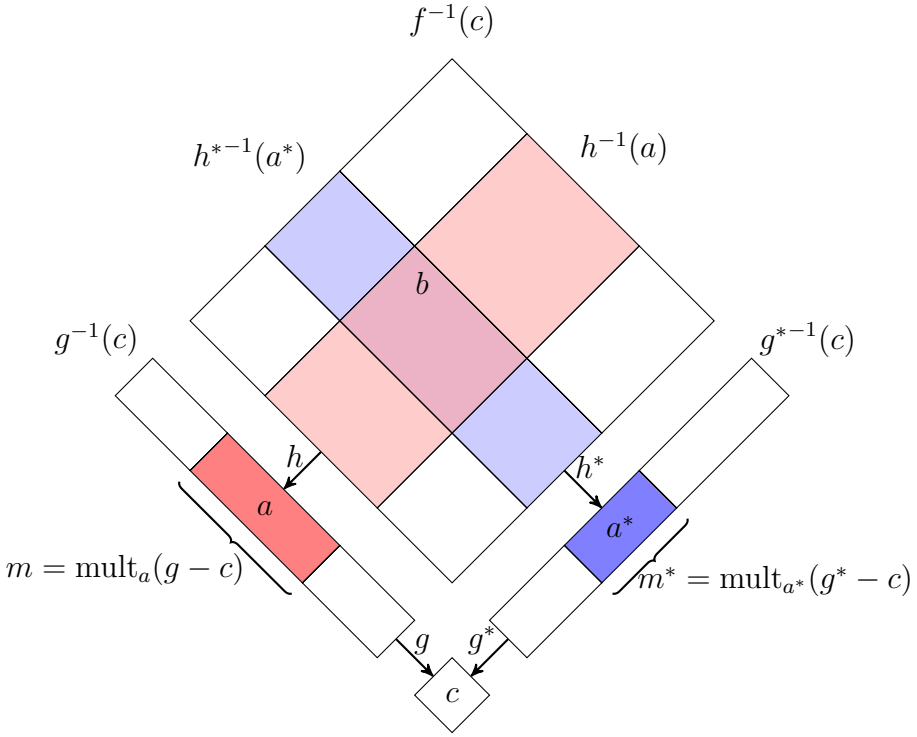

Figure 3: Roots and multiplicities

Let $m = \mathrm{mult}_a(g-c)$ and $m^* = \mathrm{mult}_{a^*}(g^*-c)$, see Figure 3. By Lemma 4.21, there are finite places $\mathfrak{p}_a$ and $\mathfrak{p}_{a^*}^*$ over P_c in M and M^*, respectively, with $m = e(\mathfrak{p}_a \mid P_c)$ and $m^* = e(\mathfrak{p}_{a^*}^* \mid P_c)$. Then, by Theorem 4.17, there are $\gcd(m, m^*)$ places $\mathfrak{q}$ over $\mathfrak{p}_a$ and $\mathfrak{p}_{a^*}^*$ in $K(\alpha)$. By the bijection (4.20), for each such place $\mathfrak{q}$ there is $b \in K$ such that $\mathfrak{q} = \mathfrak{q}_b$, and by applying Lemma 4.21 to $K(\alpha) \mid M$ and to $K(\alpha) \mid M^*$, we find $b \in h^{-1}(a) \cap h^{*-1}(a^*) \subseteq f^{-1}(c)$. On the other hand, for $b \in h^{-1}(a) \cap h^{*-1}(a^*)$, the place $\mathfrak{q}_b$ lies over $\mathfrak{p}_a$ and $\mathfrak{p}_{a^*}^*$. Thus $\#h^{-1}(a) \cap h^{*-1}(a^*) = \gcd(m, m^*)$ and $\mathrm{mult}_b(f-c) = e(\mathfrak{q}_b \mid P_c) = \mathrm{lcm}(m, m^*)$, by Theorem 4.17. □

Combining (4.23) and (4.2), for $b \in K$, $a = h(b)$, $a^* = h^*(b)$, and $c = f(b)$, we find $\mathrm{mult}_a(g-c) \cdot \mathrm{mult}_b(h-a) = \mathrm{mult}_b(f-c) = \mathrm{lcm}\left(\mathrm{mult}_a(g-c), \mathrm{mult}_{a^*}(g^*-c)\right)$ and thus

$$\mathrm{mult}_b(h-a) = \mathrm{lcm}\left(\mathrm{mult}_a(g-c), \mathrm{mult}_{a^*}(g^*-c)\right) / \mathrm{mult}_a(g-c). \qquad (4.24)$$

Hence, the root multiplicities of $h-a$ are determined by those of $g-c$ and g^*-c.

From Proposition 4.22 we derive further results about the root multiplicities of f, g, and g^*.

Lemma 4.25. *Let $c \in K$, r be a power of p, $f \in P_{r^2}(F)$ have a 2-collision $\{(g,h),(g^*,h^*)\}$ satisfying Assumption 4.7, and let $a \in g^{-1}(c)$ and $e = \mathrm{mult}_a(g-c)$. Then the following hold.*

(i) We have

$$\gcd\{\mathrm{mult}_{a^*}(g^*-c)\colon a^* \in g^{*-1}(c)\} = 1. \tag{4.26}$$

In particular, if e divides $\mathrm{mult}_{a^*}(g^*-c)$ for all roots $a^* \in g^{*-1}(c)$, then $e=1$.

(ii) The multiplicity e either equals 1 or divides $\mathrm{mult}_{a^*}(g^*-c)$ for all roots $a^* \in g^{*-1}(c)$ but exactly one.

Proof. (i) Let d be the gcd of all root multiplicities of g^*-c. Then d divides $\sum_{a^*\in g^{*-1}(c)} \mathrm{mult}_{a^*}(g^*-c) = \deg(g^*-c) = r$. Thus d is a power of p and hence all multiplicities of g^*-c are divisible by p if $d>1$, which contradicts (A_4), and (i) follows.

Before we start with the proof of (ii), we introduce some notation and results for arbitrary $c \in K$, $a \in g^{-1}(c)$, and $a^* \in g^{*-1}(c)$. We define

$$\begin{aligned} i(c,g) &= \sum_{a\in g^{-1}(c)} \mathrm{mult}_a(g'),\\ i(c,h^*) &= \sum_{b\in f^{-1}(c)} \mathrm{mult}_b(h^{*\prime}),\\ j(a,a^*) &= \sum_{b\in h^{-1}(a)\cap h^{*-1}(a^*)} \mathrm{mult}_b(h^{*\prime}), \end{aligned} \tag{4.27}$$

and have

$$\begin{aligned} \sum_{c\in K} i(c,g) &= \deg g',\\ \sum_{c\in K} i(c,h^*) &= \deg h^{*\prime},\\ \sum_{\substack{a\in g^{-1}(c)\\ a^*\in g^{*-1}(c)}} j(a,a^*) &= i(c,h^*), \end{aligned} \tag{4.28}$$

since $\dot{\bigcup}_{c\in K} g^{-1}(c) = K$, $\dot{\bigcup}_{c\in K} f^{-1}(c) = K$, and

$$f^{-1}(c) = \dot{\bigcup_{\substack{a\in g^{-1}(c)\\ a^*\in g^{*-1}(c)}}} h^{-1}(a) \cap h^{*-1}(a^*)$$

by Lemma 4.1.

By (A_4), $p \nmid \mathrm{mult}_a(g-c)$ and thus $\mathrm{mult}_a(g') = \mathrm{mult}_a(g-c) - 1$, by Lemma 4.3. Hence for $c \in K$ we have

$$i(c,g) = \sum_{a \in g^{-1}(c)} (\mathrm{mult}_a(g-c) - 1) = \deg g - \#g^{-1}(c). \tag{4.29}$$

Let $e = \mathrm{mult}_a(g-c)$ and $e^* = \mathrm{mult}_{a^*}(g^*-c)$. By Proposition 4.22, the set $h^{-1}(a) \cap h^{*-1}(a^*)$ has size $\gcd(e,e^*)$ and for a root $b \in h^{-1}(a) \cap h^{*-1}(a^*)$, we have $\mathrm{mult}_b(h^*-a^*) = \mathrm{mult}_b(f-c)/e^* = \mathrm{lcm}(e,e^*)/e^*$, by (4.24). Thus $\mathrm{mult}_b(h^{*\prime}) = \mathrm{lcm}(e,e^*)/e^* - 1$ by (A_4) and Lemma 4.3 and we have

$$j(a,a^*) = \gcd(e,e^*) \cdot (\mathrm{lcm}(e,e^*)/e^* - 1) = e - \gcd(e,e^*). \tag{4.30}$$

We now show

$$\sum_{a^* \in g^{*-1}(c)} j(a,a^*) \geq e - 1. \tag{4.31}$$

Let $a_0^*, \ldots, a_\ell^*$ be the roots of $g^* - c$ in K and $e_i^* = \mathrm{mult}_{a_i^*}(g^*-c)$ be their multiplicities. If e divides all e_i^*, then $e = 1$ by (i) and (4.31) follows trivially. If e divides all e_i^* except exactly one, say $e \nmid e_0^*$ and $e \mid e_i^*$ for $1 \leq i \leq \ell$, then the gcd of e and e_0^* divides all e_i^* and hence divides $\gcd\{e_i^* \colon 0 \leq i \leq \ell\} = 1$; see (4.26). Thus $\gcd(e,e_0^*) = 1$, $j(a,a_0^*) = e-1$ by (4.30), and (4.31) follows.

Now assume that e does not divide at least two e_i^*, say $e \nmid e_0^*$ and $e \nmid e_1^*$. Then $\gcd(e,e_i^*) \neq e$, $\gcd(e,e_i^*) \leq e/2$, and $j(a,a_i^*) \geq e/2$ by (4.30) for $i = 0, 1$. Hence, (4.31) holds with strict inequality. Summing both sides of the strict inequality (4.31) over all roots of $g - c$ yields

$$i(c,h^*) = \sum_{\substack{a \in g^{-1}(c) \\ a^* \in g^{*-1}(c)}} j(a,a^*) > \sum_{a \in g^{-1}(c)} (\mathrm{mult}_a(g-c) - 1) = i(c,g)$$

by (4.27) and (4.29). With (4.28), this leads to

$$\deg h^{*\prime} > \deg g',$$

a contradiction to (A_5). □

Lemma 4.32. *Let $c \in K$, r be a power of p, and let $f \in P_{r^2}(F)$ have a 2-collision $\{(g,h),(g^*,h^*)\}$ satisfying Assumption 4.7. Then the following statements are equivalent.*

(i) $g - c$ is squareful.

(ii) $g^* - c$ is squareful.

(iii) $f - c$ *is squareful.*

Furthermore, if $g - c$ *is squareful, then* $g - c$ *has at most one simple root.*

Proof. Assume that $g - c$ is squareful. Then there is a root of $g - c$ with multiplicity greater than 1. This multiplicity divides all multiplicities of $g^* - c$ but exactly one, by Lemma 4.25 (ii). Hence all multiplicities of $g^* - c$ but at most one are greater than 1. Thus $g^* - c$ is squareful and has at most one simple root. We interchange the rôles of g and g^* in Lemma 4.25 and obtain the equivalence of (i) and (ii) and the last claim.

Now let $a \in K$ be a multiple root of $g - c$, and $b \in h^{-1}(a)$. Then $\mathrm{mult}_b(f - c) = \mathrm{mult}_a(g - c) \cdot \mathrm{mult}_b(h - h(b)) > 1$, by Lemma 4.1, and thus $f - c$ is squareful.

It is left to prove that if $f - c$ is squareful, then $g - c$ or $g^* - c$ is squareful. Let $b \in K$ be a multiple root of $f - c$. Then $1 < \mathrm{mult}_b(f - c) = \mathrm{lcm}(\mathrm{mult}_{h(b)}(g - c), \mathrm{mult}_{h^*(b)}(g^* - c))$, by Proposition 4.22. Thus $\mathrm{mult}_{h(b)}(g - c) > 1$ or $\mathrm{mult}_{h^*(b)}(g^* - c) > 1$. □

Lemma 4.33. *Let* r *be a power of* p*, and let* $f \in P_{r^2}(F)$ *have a* 2*-collision* $\{(g, h), (g^*, h^*)\}$ *satisfying Assumption 4.7. Then the following hold.*

(i) There is at most one $c \in K$ *such that* $f - c$ *is squareful.*

(ii) For all $c \in K$, $\#g^{-1}(c) = \#g^{*-1}(c)$.

Proof. (i) Assume $g - c$ is squareful, for some $c \in K$. Then $g - c$ has at most one simple root, by Lemma 4.32. Thus $r = \deg g = \sum_{a \in g^{-1}(c)} \mathrm{mult}_a(g - c) \geq 1 + 2(\#g^{-1}(c) - 1)$. Hence $\#g^{-1}(c) \leq (r+1)/2$ and thus $i(c, g) = r - \#g^{-1}(c) \geq (r - 1)/2$, by (4.29). Now, if there is another value $c_0 \in K \setminus \{c\}$ such that $g - c_0$ is also squareful, then $r - 2 \geq \deg g' = \sum_{c \in K} i(c, g) \geq r - 1$, by (4.28). By this contradiction, there is at most one c in K such that $g - c$ is squareful. Hence there is at most one c in K such that $f - c$ is squareful, by Lemma 4.32.

(ii) If $g - c$ is squarefree, then so is $g^* - c$, by Lemma 4.32, and both have exactly $\deg g = \deg g^* = r$ roots. If $g - c$ is squareful, then by item (i), c is unique with this property and thus the roots of g' are the multiple roots of $g - c$ by Lemma 4.3. Hence

$$\deg g' = \mathrm{mult}_{a \in g^{-1}(c)} \mathrm{mult}_a(g') = i(c, g) = \deg g - \#g^{-1}(c) \tag{4.34}$$

by (4.29). Interchanging the rôles of g and g^* shows $\deg g^{*\prime} = \deg g^* - \#g^{*-1}(c)$ and Lemma 4.8 (v) yields $\deg g' = \deg g^{*\prime}$, thus $\#g^{-1}(c) = \#g^{*-1}(c)$. □

The previous lemmas deal with the root multiplicities over K. The next lemma shows that certain parameters are in F, when F is assumed to be perfect.

Lemma 4.35. *Let F be perfect, $c \in K$, r be a power of p, and $f \in P_{r^2}(F)$ have a 2-collision $\{(g,h),(g^*,h^*)\}$ satisfying Assumption 4.7. Then the following hold.*

(i) If $f-c$ is squareful, then $c \in F$.

(ii) If $g - c = g_1^{m_1} g_2^{m_2}$ for some monic squarefree coprime polynomials $g_1, g_2 \in K[x]$ and integers $m_1 \neq m_2$, then $c \in F$ and $g_1, g_2 \in F[x]$.

(iii) If $a \in F$ and $h - a = h_1^{m_1} h_2^{m_2}$ for some monic squarefree coprime polynomials $h_1, h_2 \in K[x]$ and positive integers $m_1 \neq m_2$, then $h_1, h_2 \in F[x]$.

Proof. Since F is perfect, K is Galois over F. An element $c \in K$ is fixed by all automorphisms in the Galois group $\mathrm{Gal}(K \mid F)$ if and only if $c \in F$.

(i) Let $f-c$ be squareful and $\sigma \in \mathrm{Gal}(K \mid F)$. Then $\sigma(f-c) = f - \sigma(c)$ is squareful as well. Indeed, if $f - c = (x-a)^2 u$ for some $a \in K$ and $u \in K[x]$, then $\sigma(f-c) = (x - \sigma a)^2 \sigma(u)$. But by Lemma 4.33 (i), c is unique and thus $c = \sigma(c)$. This holds for all $\sigma \in \mathrm{Gal}(K \mid F)$ and hence $c \in F$.

(ii) Since $m_1 \neq m_2$, $g - c$ is squareful and thus $f - c$ is squareful, by Lemma 4.32. By (i), we find $c \in F$. Let $\sigma \in \mathrm{Gal}(K \mid F)$. Then $g_1^{m_1} g_2^{m_2} = g - c = \sigma(g-c) = \sigma(g_1)^{m_1} \sigma(g_2)^{m_2}$. Since $m_1 \neq m_2$, unique factorization implies that $g_i = \sigma(g_i)$ and thus $g_i \in F[x]$ for $i = 1, 2$.

The proof of (iii) is analogous to that of (ii). □

5 Classification

We use the results of the previous section to describe in Proposition 5.4 the factorization of the components of 2-collisions at degree r^2 satisfying Assumption 4.7 over a perfect field F. All non-Frobenius collisions at degree p^2 satisfy this assumption and in Theorem 5.9 we provide a complete classification of 2-collisions at that degree over a perfect field. That is, the 2-collisions at degree p^2 are up to original shifting those of Example 2.4, Fact 3.1, and Theorem 3.22. This yields the maximality of these collisions (Corollary 5.11) and an efficient algorithm to determine whether a given polynomial $f \in P_{p^2}(F)$ has a 2-collision (Algorithm 5.14). In the next section we use this classification to count exactly the decomposable polynomials over a finite F.

Let F be a perfect field and denote by $K = \overline{F}$ an algebraic closure of F.

Definition 5.1. *Let r be a power of p and $f \in P_{r^2}(F)$ have a 2-collision $\{(g,h),(g^*,h^*)\}$ satisfying Assumption 4.7. We call f* multiply original *if there is some $c \in K$ such that $f - c$ has no simple roots in K. Otherwise, we call f* simply original.

By Lemma 4.33 (i), there is at most one $c \in K$ such that $f - c$ is squareful. Since F is perfect, such a c lies in F if it exists, by Lemma 4.35 (i). Furthermore, if f is multiply original, then there is some $c \in F$ such that $f - c$ is squareful. If f is simply original, then either $f - c$ is squarefree for all $c \in K$ or there is a unique $c \in F$ such that $f - c$ is squareful and has a simple root.

Example 5.2. Assumption 4.7 holds for the 2-collisions $M(a, b, m)$ of Theorem 3.22 and the $\#T$-collisions $S(u, s, \varepsilon, m)$ of Fact 3.1 with $\#T \geq 2$; see Example 4.12. Moreover, a polynomial $M(a, b, m)$ has no simple roots and is therefore multiply original. When $\#T \geq 2$, then $f = S(u, s, \varepsilon, m)$ is squareful with a simple root if $m > 1$, and $f - c$ is squarefree for all $c \in K$ if $m = 1$.

The following Proposition 5.4 and Theorem 5.9 answer the converse question, namely whether every simply original or multiply original polynomial can be obtained as $S(u, s, \varepsilon, m)^{(w)}$ or $M(a, b, m)^{(w)}$, respectively. We need the following graph-theoretic lemma.

Lemma 5.3. *Let $G = (V, E)$ be a directed bipartite graph with bipartition $V = A \cup A^*$, where the outdegree of each vertex equals $\ell > 1$ and $\#A = \#A^* = \ell + 1$. Then some vertex in A is connected to all other vertices in A by a path of length 2.*

Proof. Let $A = \{0, \ldots, \ell\}$, $A^* = \{\ell{+}1, \ldots, 2\ell{+}1\}$, and M the $(2\ell{+}2) \times (2\ell{+}2)$ adjacency matrix of G having for each edge from $i \in A \cup A^*$ to $j \in A \cup A^*$ the entry 1 at position (i, j) and entries 0 everywhere else. Since G is bipartite, we have

$$M = \begin{pmatrix} 0 & N \\ N^* & 0 \end{pmatrix},$$

where N and N^* are $(\ell{+}1) \times (\ell{+}1)$-matrices satisfying the following properties by the assumptions of the lemma.

(i) Each row in N has exactly one entry 0 and all other entries 1.

(ii) Exactly $\ell + 1$ entries of N^* are 0 and all other entries are 1.

The number of paths of length 2 that connect a vertex $i \in A$ to a vertex $j \in A$ is given by the entry (i, j) of

$$M^2 = \begin{pmatrix} N \cdot N^* & 0 \\ 0 & N^* \cdot N \end{pmatrix}.$$

If every column of N^* contains at least two 1's, then $N \cdot N^*$ has only positive entries, because of (i), and every vertex in A is connected to all other vertices

in A by a path of length 2. Otherwise, N^* has a column j that contains at most one 1. Because of (ii), every different column of N^* contains at most one 0. Because of $\ell > 1$ and (i), all entries at (j, j') with $j' \neq j$ in $N \cdot N^*$ are positive. Starting from j we can reach all other vertices by a path of length 2. □

Thanks go to Rolf Klein and an anonymous referee for this proof, much simpler than our original one.

Proposition 5.4. *Let r be a power of the characteristic $p > 0$ of the perfect field F and let $f \in P_{r^2}(F)$ have a 2-collision $\{(g, h), (g^*, h^*)\}$ satisfying Assumption 4.7. Then exactly one of the following holds.*

(s) *The polynomial f is simply original. Let $m = (r-1)/(r-1-\deg g')$. Then there are $w \in F$ and unique monic squarefree polynomials $\hat{f}$, $\hat{g}$, $\hat{h}$, $\hat{g}^*$, and $\hat{h}^*$ in $F[x]$, none of them divisible by x, with $\hat{f}$ of degree $(r^2-1)/m$ and the other four polynomials of degree $r-1-\deg g' = (r-1)/m$ such that*

$$\begin{aligned} f^{(w)} &= x\hat{f}^m, \\ g^{(h(w))} &= x\hat{g}^m, \\ h^{(w)} &= x\hat{h}^m, \\ (g^*)^{(h^*(w))} &= x(\hat{g}^*)^m, \\ (h^*)^{(w)} &= x(\hat{h}^*)^m. \end{aligned} \tag{5.5}$$

If $\deg f' > 0$, then w is unique. Otherwise, factorizations (5.5) with the claimed properties exist for all $w \in F$.

(m) *The polynomial f is multiply original and there are a, b, and m as in Theorem 3.22 and $w \in F$ such that*

$$f^{(w)} = M(a, b, m)$$

and the collision $\{(g, h)^{(w)}, (g^*, h^*)^{(w)}\}$ is as in Theorem 3.22.

Proof. Every polynomial satisfying the assumption of the proposition is either simply original or multiply original by Definition 5.1. So, at most one of the two statements holds and it remains to exhibit the claimed parameters in each case. We begin with two general observations.

(i) If $\deg f' = 0$, then $f - c$ is squarefree for all $c \in K$, by Lemma 4.3. Thus f is simply original. Moreover, $f^{(w)}$ has derivative $(f^{(w)})' = f' \circ (x + w) = f' \in F^\times$ for all $w \in F$ and is therefore squarefree.

(ii) If $\deg f' > 0$, then there is some $c \in K$ such that $f - c$ has a multiple root by Lemma 4.3. Moreover, c is unique by Lemma 4.33 (i), and in F by Lemma 4.35 (i). Let $\#g^{-1}(c) = \ell + 1$ be the number of distinct roots of $g - c$ in K. By Lemma 4.33 (ii), $g^* - c$ also has $\ell + 1$ roots in K and

$$\ell = r - 1 - \deg g' \geq 1, \tag{5.6}$$

by (4.34). Let $a_0, \ldots, a_\ell$ and $a_0^*, \ldots, a_\ell^*$ be the distinct roots of $g - c$ and $g^* - c$, respectively, and let $e_i = \mathrm{mult}_{a_i}(g - c)$ and $e_i^* = \mathrm{mult}_{a_i^*}(g^* - c)$ be their multiplicities, that is,

$$g - c = \prod_{0 \leq i \leq \ell} (x - a_i)^{e_i}, \quad g^* - c = \prod_{0 \leq i \leq \ell} (x - a_i^*)^{e_i^*}. \tag{5.7}$$

By Proposition 4.22, for each i and j the set $B_{i,j} = h^{-1}(a_i) \cap h^{*-1}(a_j^*) \subseteq K$ has cardinality $\gcd(e_i, e_j^*)$.

We now deal with the two cases of the theorem separately.

Case (s): Let f be simply original. First, if $\deg f' = 0$, then $\deg g' = 0$, by (4.5). Hence $m = (r-1)/(r-1-\deg g') = 1$ and $f^{(w)} = g^{(h(w))} \circ h^{(w)} = (g^*)^{(h^*(w))} \circ (h^*)^{(w)}$ is squarefree for all $w \in F$, by (i). Thus the monic polynomials $\hat{f} = f^{(w)}/x$, $\hat{g} = g^{(h(w))}/x$, $\hat{h} = h^{(w)}/x$, $\hat{g}^* = (g^*)^{(h^*(w))}/x$, and $\hat{h}^* = (h^*)^{(w)}/x$ are also squarefree and not divisible by x, and (5.5) holds for all $w \in F$.

Second, we assume $\deg f' > 0$ for the rest of case (s). By (ii), there is a unique $c \in F$ such that $f - c$ has multiple roots and we assume the notation of (5.7) for $g - c$ and $g^* - c$. By the definition of simple originality, $f - c$ has a simple root, say $b_0 \in f^{-1}(c)$. Furthermore, $g - c$ and $g^* - c$ also have simple roots, since

$$1 = \mathrm{mult}_{b_0}(f - c) = \mathrm{lcm}(\mathrm{mult}_{h(b_0)}(g - c), \mathrm{mult}_{h^*(b_0)}(g^* - c))$$

by Proposition 4.22. But $g - c$ and $g^* - c$ have at most one simple root by Lemma 4.32. We may number the roots so that these unique simple roots are $a_0 = h(b_0)$ and $a_0^* = h^*(b_0)$, both with multiplicity $e_0 = e_0^* = 1$, and $e_i, e_i^* > 1$ for all $i \geq 1$.

By Lemma 4.25 (ii) and using $e_0^* = 1$, each e_i with $i \geq 1$ divides all e_j^* with $j \geq 1$. Similarly, each e_j^* with $j \geq 1$ divides all e_i with $i \geq 1$. Thus all these multiplicities are equal to some integer $m \geq 2$, and with $r = \deg g = 1 + \ell m$ from (5.7), we have $m = (r-1)/\ell = (r-1)/(r-1-\deg g')$ by (5.6). Therefore

$$g - c = (x - a_0)\tilde{g}^m, \quad g^* - c = (x - a_0^*)(\tilde{g}^*)^m$$

with monic squarefree polynomials $\tilde{g} = \prod_{1\le i\le \ell}(x - a_i)$ and $\tilde{g}^* = \prod_{1\le i\le \ell}(x - a_i^*) \in K[x]$. We find $a_0, a_0^* \in F$ and $\tilde{g}$, $\tilde{g}^* \in F[x]$ by Lemma 4.35 (ii).

Next, we show that $h - a_0$ and $h^* - a_0^*$ have the same root multiplicities as $g^* - c$ and $g - c$, respectively. For $0 \le i \le \ell$, we find from (4.24) with the unique $b_i \in B_{0,i}$ and the unique $b_i^* \in B_{i,0}$ as implicitly defined in (ii) that

$$\begin{aligned}\operatorname{mult}_{b_i}(h - a_0) &= \operatorname{lcm}(\operatorname{mult}_{a_0}(g - c), \operatorname{mult}_{a_i^*}(g^* - c)) = \operatorname{mult}_{a_i^*}(g^* - c),\\ \operatorname{mult}_{b_i^*}(h^* - a_0^*) &= \operatorname{mult}_{a_i}(g - c).\end{aligned}$$

Since $\#B_{0,0} = 1$ by Proposition 4.22, we have $b_0 = b_0^*$ and arrive at

$$h - a_0 = (x - b_0)\tilde{h}^m, \quad h^* - a_0^* = (x - b_0)(\tilde{h}^*)^m$$

with monic squarefree polynomials $\tilde{h} = \prod_{1\le i\le \ell}(x - b_i)$ and $\tilde{h}^* = \prod_{1\le i\le \ell}(x - b_i^*) \in K[x]$. Again, we find $b_0 \in F$ and $\tilde{h}$, $\tilde{h}^* \in F[x]$, by Lemma 4.35 (iii).

Finally, we let $w = b_0$, $\hat{g} = \tilde{g} \circ (x + a_0)$, $\hat{h} = \tilde{h} \circ (x + b_0)$, $\hat{g}^* = \tilde{g}^* \circ (x + a_0^*)$, $\hat{h}^* = \tilde{h}^* \circ (x + b_0)$, and $\hat{f} = \hat{h} \cdot \hat{g}(x\hat{h}^m)$. Then $h(b_0) = a_0$, $f(b_0) = g(h(b_0)) = g(a_0) = c$, and

$$\begin{aligned}g^{(h(w))} &= (x - c) \circ g \circ (x + a_0) = x\hat{g}^m,\\ h^{(w)} &= (x - a_0) \circ h \circ (x + b_0) = x\hat{h}^m,\\ (g^*)^{(h^*(w))} &= (x - c) \circ g^* \circ (x + a_0^*) = x(\hat{g}^*)^m,\\ (h^*)^{(w)} &= (x - a_0^*) \circ h^* \circ (x + b_0) = x(\hat{h}^*)^m\end{aligned}$$

with squarefree monic $\hat{g}$, $\hat{g}^*$, $\hat{h}$, and $\hat{h}^*$ of degree $\ell = r-1-\deg g'$. Furthermore, $\hat{g}(0) = \tilde{g}(a_0) = \prod_{1\le i\le \ell}(a_0 - a_i) \ne 0$. This shows that $\hat{g}$ is coprime to x and similar arguments work for $\hat{g}^*$, and for $\hat{h}$ and $\hat{h}^*$ with $b_0 \ne b_i$ for $i \ge 1$, since $h(b_0) = a_0 \ne a_i = h(b_i)$ for $i \ge 1$. Moreover, $\hat{f} = \hat{h} \cdot \prod_{1\le i\le \ell}(x\hat{h}^m - a_i + a_0)$ is monic and not divisible by x, and $f^{(w)} = g^{(h(w))} \circ h^{(w)} = (x\hat{g}^m) \circ (x\hat{h}^m) = x\hat{f}^m$. Since $B_{0,0} = \{b_0\}$ and $\operatorname{lcm}(e_0, e_0^*) = 1$, we find that $f - c$ has a simple root b_0, by Proposition 4.22. Furthermore, $f-c$ has $\sum_{i+j\ge 1} \#B_{i,j} = 2\ell+\ell^2 m = \ell(r+1)$ roots with multiplicity m. Thus $\hat{f}$ is squarefree and of degree $\ell(r + 1) = (r^2 - 1)/m$, and the values as claimed in (s) indeed exist.

For the uniqueness in the case $\deg f' > 0$, we consider another factorization $f^{(w_0)} = x\hat{f}_0^m$ satisfying the conditions of case (s). Then $f(x) - f(w) = f^{(w)} \circ (x - w) = (x - w)(\hat{f}(x - w))^m$ and $f(x) - f(w_0) = f^{(w_0)} \circ (x - w_0) = (x-w_0)(\hat{f}_0(x-w_0))^m$. The value for c such that $f-c$ is squareful with a simple root is unique for a simply original polynomial with $\deg f' > 0$, as remarked in (i). Thus $c = f(w) = f(w_0)$ and $(x-w)(\hat{f}(x-w))^m = (x-w_0)(\hat{f}_0(x-w_0))^m$. Since $\deg f' > 0$, we have $\deg g' > 0$ and $m > 1$. Unique factorization yields $w = w_0$ and $\hat{f} = \hat{f}_0$. An analogous argument works for $\hat{g}$, $\hat{g}^*$, $\hat{h}$, and $\hat{h}^*$.

This concludes case (s), and we continue with the case (m).

Case (m): Let f be multiply original. Then $\deg f' > 0$ by (i) from the beginning of the proof. By (ii), there is a unique $c \in F$ such that $f - c$ is squareful, and then $f - c$ has no simple root by Definition 5.1 of multiple originality. By Lemma 4.32, $g - c$ and $g^* - c$ are also squareful.

Assume that $g - c$ has a simple root. Then $\ell > 0$ and we may number the roots of $g - c$ such that $e_0 = 1$ in the notation (5.7). By Lemma 4.32, $g - c$ has at most one simple root and thus $e_1 > 1$. By Lemma 4.25 (ii), e_1 divides all e_j^* but one and we may number the roots of $g^* - c$ such that $e_1 \mid e_j^*$ for $1 \leq j \leq \ell$. Interchanging the rôles of g and g^* in Lemma 4.25 (ii), we have $e_0^* \mid e_1$ since $e_0 = 1$. Combining these divisibility conditions shows $e_0^* \mid \gcd\{e_j^* \colon 0 \leq j \leq \ell\}$ and we find $e_0^* = 1$ from (4.26). Hence there exists some $b \in K$ such that $\mathrm{mult}_b(f - c) = \mathrm{lcm}(e_0, e_0^*) = 1$, by Proposition 4.22, contradicting Definition 5.1 of multiply original by the uniqueness of c. Therefore $g - c$ has no simple root and $e_i > 1$ for all $i \geq 0$. An analogous argument for g^* shows $e_i^* > 1$ for all $i \geq 0$.

We now proceed in three steps. First, we determine the factorizations of $g - c$ and $g^* - c$. Second, we derive the factorizations of $h - a_i$ and $h^* - a_i^*$ for the roots $a_i \in g^{-1}(c)$ and $a_i^* \in g^{*-1}(c)$, respectively. Third, we apply an appropriate original shift and prove the claimed form.

To compute ℓ, we translate Proposition 4.22 into the language of graphs. We consider the directed bipartite graph on the set $V = A \cup A^*$ of vertices, with disjoint $A = \{i \colon 0 \leq i \leq \ell\}$ and $A^* = \{i^* \colon 0 \leq i \leq \ell\}$. The set E of edges consists of all (i, j^*) with $e_i \mid e_j^*$ plus all (i^*, j) with $e_i^* \mid e_j$. Each vertex has outdegree ℓ, by Lemma 4.25 (ii), since no root is simple. If $\ell > 1$, then by Lemma 5.3 some vertex i in A is connected to all other vertices in A. Then $e_i > 1$ divides all other multiplicities of $g - c$, which contradicts (4.26) with g instead of g^*. Hence $\ell = 1$ and therefore

$$\begin{aligned} g - c &= (x - a_0)^{e_0}(x - a_1)^{e_1}, \\ g^* - c &= (x - a_0^*)^{e_0^*}(x - a_1^*)^{e_1^*} \end{aligned}$$

with $1 < e_i, e_i^* < r - 1$, for $i = 0, 1$. We know by Lemma 4.25 (i) applied to g and g^*, respectively, that $\gcd(e_0, e_1) = \gcd(e_0^*, e_1^*) = 1$ and since $e_i, e_i^* > 1$ for $i = 0, 1$, each e_i divides exactly one e_j^*, by (ii) of the cited lemma, and similarly each e_j^* divides exactly one e_i. By renumbering if required, we assume $e_0 \mid e_1^*$. If $e_1^* \mid e_1$, then $\gcd(e_0, e_1) = e_0 > 1$, a contradiction to Lemma 4.25 (i). Therefore $e_1^* \mid e_0$ and we have $e_0 = e_1^*$. Similar arguments show $e_0^* \mid e_1$ and $e_1 \mid e_0^*$, and hence $e_1 = e_0^*$. We write $m = e_0 = e_1^*$ and $m^* = e_1 = e_0^*$. Then m and m^* are coprime, $m^* = r - m$, since $r = e_0 + e_1$, and $p \nmid m$, by (A_4). Lemma 4.35 (ii) yields distinct $a_0, a_1 \in F$ and distinct

$a_0^*, a_1^* \in F$ with

$$g - c = (x - a_0)^m (x - a_1)^{m^*},$$
$$g^* - c = (x - a_0^*)^{m^*} (x - a_1^*)^m.$$

For the sets $B_{i,j}$ defined in (ii), we find $\#B_{0,0} = \#B_{1,1} = 1$, $\#B_{0,1} = m$, and $\#B_{1,0} = m^*$. The multiplicity of each $b_{i,j} \in B_{i,j}$ satisfies

$$\mathrm{mult}_{b_{i,j}}(h - a_i) = \frac{\mathrm{lcm}(e_i, e_j^*)}{e_i} = \begin{cases} m^* & \text{if } i = j = 0, \\ m & \text{if } i = j = 1, \\ 1 & \text{otherwise,} \end{cases}$$

by (4.24), and similarly

$$\mathrm{mult}_{b_{i,j}}(h^* - a_j^*) = \begin{cases} m & \text{if } i = j = 0, \\ m^* & \text{if } i = j = 1, \\ 1 & \text{otherwise.} \end{cases}$$

Writing $B_{0,0} = \{b_{0,0}\}$ and $B_{1,1} = \{b_{1,1}\}$, this shows

$$h - a_0 = (x - b_{0,0})^{m^*} H_0, \qquad h - a_1 = (x - b_{1,1})^m H_0^*,$$
$$h^* - a_0^* = (x - b_{0,0})^m H_0^*, \qquad h - a_1^* = (x - b_{1,1})^{m^*} H_0$$

with squarefree monic $H_0 = \prod_{b \in B_{0,1}} (x - b)$ and $H_0^* = \prod_{b \in B_{1,0}} (x - b)$ that do not vanish at $b_{0,0}$ or $b_{1,1}$. Lemma 4.35 (iii) implies that $b_{0,0}, b_{1,1} \in F$ and $H_0, H_0^* \in F[x]$.

We use this information to apply the appropriate original shift to our decompositions. Let $w = b_{0,0}$, $a = a_1 - a_0$, $a^* = a_1^* - a_0^*$, and $b = b_{1,1} - b_{0,0}$, with all differences being different from 0, and squarefree monic $H = H_0 \circ (x + w)$ and $H^* = H_0^* \circ (x + w)$. Then $h(w) = a_0$, $h^*(w) = a_0^*$, $g(a_0) = g^*(a_0^*) = c$, and

$$\begin{aligned} g^{(h(w))} &= x^m (x - a)^{m^*}, \\ h^{(w)} &= x^{m^*} H, \quad h^{(w)} - a = (x - b)^m H^*, \\ g^{*(h^*(w))} &= x^{m^*} (x - a^*)^m, \\ h^{*(w)} &= x^m H^*, \quad h^{*(w)} - a^* = (x - b)^{m^*} H. \end{aligned} \tag{5.8}$$

Equations (5.8) yield a system of linear equations

$$x^{m^*} H - (x - b)^m H^* = a,$$
$$-(x - b)^{m^*} H + x^m H^* = a^*$$

over $F(x)$ in H and H^*. We apply Cramer's rule and find

$$H = (ax^m + a^*(x-b)^m)/b^r,$$
$$H^* = (a^*x^{m^*} + a(x-b)^{m^*})/b^r,$$

and $a+a^* = b^r$, since H is monic. Therefore, the polynomials H and H^* are as in (3.24) and $f^{(w)} = g^{(h(w))} \circ h^{(w)} = x^{mm^*}(x-b)^{mm^*}H^m(H^*)^{m^*} = M(a,b,m)$, as in Theorem 3.22. □

For 2-collisions at degree p^2, we can refine the classification of Proposition 5.4.

Theorem 5.9. *Let F be a perfect field of characteristic p and $f \in P_{p^2}(F)$. Then f has a 2-collision $\{(g,h),(g^*,h^*)\}$ if and only if exactly one of the following holds.*

(F) *The polynomial f is a Frobenius collision as in Example 2.4.*

(S) *The polynomial f is simply original and there are u, s, ε, and m as in Fact 3.1 and $w \in F$ such that*

$$f^{(w)} = S(u,s,\varepsilon,m)$$

and the collision $\{(g,h)^{(w)},(g^*,h^*)^{(w)}\}$ is contained in the $\#T$-collision described in Fact 3.1, with $\#T \geq 2$.

(M) *The polynomial f is multiply original and there are a, b, and m as in Theorem 3.22 and $w \in F$ such that*

$$f^{(w)} = M(a,b,m)$$

and the collision $\{(g,h)^{(w)},(g^*,h^*)^{(w)}\}$ is as in Theorem 3.22.

Proof. By Lemma 2.6 (i), f is a Frobenius collision if and only if $f' = 0$.

The rest of the proof deals with the case $f' \neq 0$. Assumption 4.7 holds by Lemma 4.8, the assumptions in Definition 5.1 are satisfied, and f is either simply original or multiply original.

For a multiply original f, Proposition 5.4 yields the claimed parameters directly, and we now show their existence in the simply original case.

We take $w, m, \hat{g}, \hat{h}$ as in Proposition 5.4 (s) and have

$$g^{(h(w))} = x\hat{g}^m,$$
$$h^{(w)} = x\hat{h}^m.$$

We determine the form of $\hat{g}$ and $\hat{h}$. Let $\ell = \deg \hat{g} = (p-1)/m$. The derivative of $g^{(h(w))}$ is $\hat{g}^{m-1}(\hat{g} + mx\hat{g}')$, and its degree equals $\deg g' = p - 1 - \ell$, by (5.6). Thus $\deg g' = (m-1)\ell + \deg(\hat{g} + mx\hat{g}') = \deg g' + \deg(\hat{g} + mx\hat{g}')$ and $\deg(\hat{g} + mx\hat{g}') = 0$. We write $\hat{g} = \sum_{0 \le i \le \ell} \hat{g}_i x^i$ with $\hat{g}_i \in F$ for all $i \ge 0$. Then $\hat{g} + mx\hat{g}' = \sum_{0 \le i \le \ell}(1 + mi)\hat{g}_i x^i$ and we have $\hat{g}_0 \ne 0$ and $(1 + mi)\hat{g}_i = 0$ for all $i \ge 1$. Since $1 + mi \ne 0$ in F for $1 \le i < \ell$, it follows that $\hat{g}_i = 0$ for these values of i. Thus we get $\hat{g} = x^\ell - \hat{g}_0$ and $\hat{g}_0 \ne 0$. An analogous argument yields $\hat{h} = x^\ell - \hat{h}_0$ with $\hat{h}_0 \ne 0$. Therefore, we find

$$f^{(w)} = x(x^{\ell(p+1)} - (\hat{h}_0^p + \hat{g}_0)x^\ell + \hat{g}_0\hat{h}_0)^m. \tag{5.10}$$

Let

$$(u, s, \varepsilon, t) = \begin{cases} (\hat{g}_0\hat{h}_0, 1, 0, \hat{h}_0) & \text{if } \hat{h}_0^p + \hat{g}_0 = 0, \\ ((\hat{h}_0^p + \hat{g}_0)^{p+1}/(\hat{g}_0\hat{h}_0)^p, \hat{g}_0\hat{h}_0/(\hat{h}_0^p + \hat{g}_0), 1, \hat{h}_0/s) & \text{otherwise.} \end{cases}$$

In both cases, u, s, and t are in $F^\times$ and the equations $t^{p+1} - \varepsilon ut + u = 0$, $\hat{h}_0 = st$, $\hat{g}_0 = us^p t^{-1}$, and $f^{(w)} = g^{(h(w))} \circ h^{(w)} = S(u, s, \varepsilon, m)$ hold. Similarly, we find $g^{*(h^*(w))} = x(x^\ell - \hat{g}_0^*)^m$ and $h^{*(w)} = x(x^\ell - \hat{h}_0^*)^m$ for some $\hat{g}_0^*$, $\hat{h}_0^* \in F^\times$, and derive the parameters u^*, s^*, ε^*, and t^* analogously. Since $f^{(w)} = g^{*(h^*(w))} \circ h^{*(w)}$, it follows from (5.10) that $\hat{h}_0^p + \hat{g}_0 = (\hat{h}_0^*)^p + \hat{g}_0^*$ and $\hat{g}_0\hat{h}_0 = \hat{g}_0^*\hat{h}_0^*$. Hence $\varepsilon = \varepsilon^*$, $u = u^*$, and $s = s^*$. Since the decompositions are distinct, we have $t \ne t^*$ and thus $(g, h)^{(w)}$ and $(g^*, h^*)^{(w)}$ are both of the form (3.3) with different values for t. □

Corollary 5.11. *(i) A polynomial in case* (S) *of Theorem 5.9 has a maximal #T-collision with T as in* (3.2)*.*

(ii) A polynomial in case (M) *of Theorem 5.9 has a maximal* 2*-collision.*

Proof. For a polynomial f with collision C and $w \in F$, we write $C^{(w)} = \{(g, h)^{(w)} \colon (g, h) \in C\}$ for the corresponding collision of $f^{(w)}$.

If f is a Frobenius collision as in case (F) of Theorem 5.9, then f is maximal by Lemma 2.6 (ii). Now let f be a polynomial with a 2-collision $C = \{(g, h), (g^*, h^*)\}$ that does not fall into case (F) of Theorem 5.9.

(i) If f falls into case (S) of Theorem 5.9, we have by that theorem u, s, ε, and m as in Fact 3.1 and $w \in F$ such that $f = S(u, s, \varepsilon, m)^{(-w)}$ and $C \subseteq D(u, s, \varepsilon, m)^{(-w)}$, where $D(u, s, \varepsilon, m)^{(-w)}$ denotes the $\#T$-collision described in Fact 3.1 shifted by $-w$.

Take another decomposition $(g_0, h_0) \ne (g, h)$ of f. We apply Theorem 5.9 to f with 2-collision $C_0 = \{(g, h), (g_0, h_0)\}$. Due to the mutual exclusivity of the three cases this falls again in case (S), and we obtain u_0, s_0, ε_0, and

m_0 as in Fact 3.1, and $w_0 \in F$ such that $f = S(u_0, s_0, \varepsilon_0, m_0)^{(-w_0)}$ and $C_0 \subseteq D(u_0, s_0, \varepsilon_0, m_0)^{(-w_0)}$. Thus,

$$f^{(w_0)} = S(u, s, \varepsilon, m)^{(w_0 - w)} = S(u_0, s_0, \varepsilon_0, m_0).$$

By Fact 3.5 (iv), the only polynomial of the form (3.2) in the orbit of $S(u, s, \varepsilon, m)$ under original shifting is the polynomial itself. Therefore,

$$S(u, s, \varepsilon, m) = S(u_0, s_0, \varepsilon_0, m_0). \tag{5.12}$$

If $m > 1$, then the stabilizer of $S(u, s, \varepsilon, m)$ under original shifting is $\{0\}$ by Fact 3.5 (iii) and we have $w = w_0$. Otherwise, $m = 1$ and $S(u, s, \varepsilon, m)$, $D(u, s, \epsilon, m)$, and $D(u_0, s_0, \epsilon_0, m_0)$ consist only of additive polynomials which are invariant under original shifting. In that case, we can assume $w = w_0$ without loss of generality.

If $\varepsilon = 1$, then Fact 3.5 (i) yields $(u, s, \varepsilon, m) = (u_0, s_0, \varepsilon_0, m_0)$ from (5.12) and therefore $D(u, s, \varepsilon, m)^{(-w)} = D(u_0, s_0, \varepsilon_0, m_0)^{(-w_0)} \ni (g_0, h_0)$. Otherwise, $\varepsilon = 0$ and Fact 3.5 (ii) yields $(us^{p+1}, \varepsilon, m) = (u_0 s_0^{p+1}, \varepsilon_0, m_0)$ from (5.12). By the definition of $D(u_0, s_0, \varepsilon_0, m_0)^{(-w_0)}$ via Fact 3.1, there is some $t_0 \in F$ satisfying $t_0^{p+1} = -u_0$ such that

$$\begin{aligned} g_0^{(h_0(-w_0))} &= x(x^{p-m_0} - u_0 s_0^p t_0^{-1})^{m_0} = x(x^{p-m} - us^p t^{-1})^m, \\ h_0^{(-w_0)} &= x(x^{p-m_0} - s_0 t_0)^{m_0} = x(x^{p-m} - st)^m \end{aligned}$$

for $t = t_0 s_0 / s \in F$. Since t satisfies $t^{p+1} = -u$, this shows $(g_0, h_0) \in D(u, s, \varepsilon, m)^{(-w)}$.

(ii) Let f fall into case (M) of Theorem 5.9 and take another decomposition $(g_0, h_0) \neq (g, h)$ of f. We apply that theorem to f with 2-collisions C and $C_0 = \{(g, h), (g_0, h_0)\}$ and obtain a, b, m and a_0, b_0, m_0 as in Theorem 3.22 and $w, w_0 \in F$, respectively, such that

$$\begin{gathered} f = M(a, b, m)^{(-w)} = M(a_0, b_0, m_0)^{(-w_0)}, \\ C = E(a, b, m)^{(-w)}, \quad \text{and} \quad C_0 = E(a_0, b_0, m_0)^{(-w_0)}, \end{gathered}$$

where $E(a, b, m)^{(-w)}$ denotes the 2-collision defined in (3.23) shifted by $-w$, and $E(a_0, b_0, m_0)^{(-w_0)}$ is analogous. We have

$$M(a, b, m)^{(w_0 - w)} = M(a_0, b_0, m_0). \tag{5.13}$$

The only polynomials in the orbit of $M(a, b, m)$ that are of the form (3.23) are $M(a, b, m)$ itself and $M(a, b, m)^{(b)}$ according to Proposition 3.26 (iv); and by (ii), the stabilizer of $M(a, b, m)$ under original shifting is $\{0\}$. Hence, $w_0 - w = 0$ or $w_0 - w = b$.

If $w_0 = w$, then $M(a_0, b_0, m_0) = M(a, b, m)$ from (5.13) and with (iii) of the cited proposition

$$(a_0, b_0, m_0) \in \{(a, b, m), (a^*, b, m^*)\}.$$

If $w_0 = w + b$, then $M(a_0, b_0, m_0) = M(a, b, m)^{(b)} = M(-a^*, -b, m)$ and again with (iii)

$$(a_0, b_0, m_0) \in \{(-a^*, -b, m), (-a, -b, m^*)\}.$$

In either case, we check directly that $E(a_0, b_0, m_0)^{(-w_0)} = E(a, b, m)^{(-w)}$ and therefore $(g_0, h_0) \in C$. □

In particular, the polynomials of case (M) have no 3-collision. We combine Theorem 5.9 with the algorithms of Section 3 for a general test of 2-collisions in Algorithm 5.14.

Algorithm 5.14: Collision determination

Input: a polynomial $f \in P_{p^2}(F)$, where $p = \operatorname{char} F$
Output: "(F)", "(S)", or "(M)" as in Theorem 5.9, if f has a 2-collision, and "no 2-collision" otherwise

if $f \in F[x^p] \setminus \{x^{p^2}\}$ **then return** *"(F)"*
if *Algorithm 3.18 does not return "failure" on input f, but $k, u, s, \varepsilon, m, w$* **then**
  if $k \geq 2$ **then return** *"(S)"*
end
if *Algorithm 3.29 does not return "failure" on input f* **then**
  return *"(M)"*
end
return *"no 2-collision"*

Theorem 5.15. *Algorithm 5.14 works correctly as specified. If $F = \mathbb{F}_q$ and $n = p^2 = \deg f$, it takes $O(\mathsf{M}(n) \log(pq))$ field operations.*

The correctness follows from Theorem 5.9. Its cost is dominated by that of Algorithm 3.18, where the $\log n$ factor is subsumed in $\log(pq)$ since $n = p^2$ and $pq \geq p^2$. If f is found to have a collision, then that can be returned as well, using Example 2.4 for (F).

6 Counting at degree p^2

The classification of the composition collisions at degree p^2 yields the exact number of decomposable polynomials over a finite field $\mathbb{F}_q$.

Theorem 6.1. *Let p be a prime and q a power of p. For $k \geq 1$, we write c_k for $\#C_{p^2,k}(\mathbb{F}_q)$ as in (2.1), δ for Kronecker's delta function, and τ for the number of positive divisors of $p-1$. Then the following hold.*

$$\begin{aligned} c_1 &= q^{2p-2} - 2q^{p-1} + 2 - \frac{(\tau q - q + 1)(q-1)(qp-q-p)}{p} \\ &\quad - (1-\delta_{p,2})\frac{q(q-1)(q-2)(p-3)}{2}, \qquad (6.2) \\ c_2 &= q^{p-1} - 1 + \frac{(\tau q - q + 1)(q-1)^2(p-2)}{2(p-1)} \\ &\quad + (1-\delta_{p,2})\frac{q(q-1)(q-2)(p-3)}{4}, \qquad (6.3) \\ c_{p+1} &= \frac{(\tau q - q + 1)(q-1)(q-p)}{p(p^2-1)}, \qquad (6.4) \\ c_k &= 0, \quad \text{if } k \notin \{1, 2, p+1\}. \qquad (6.5) \end{aligned}$$

Proof. For $k \geq 2$, we consider $C_k = C_{p^2,k}(\mathbb{F}_q)$. Theorem 5.9 provides the partition

$$C_k = C_k^{(F)} \dot\cup C_k^{(S)} \dot\cup C_k^{(M)},$$

where the sets on the right-hand side correspond to the cases (F), (S), and (M), respectively. Lemma 2.6 (ii), Proposition 3.21, and Corollary 3.28 imply that

$$\#C_k^{(F)} = \begin{cases} q^{p-1} - 1 & \text{if } k = 2, \\ 0 & \text{if } k \geq 3, \end{cases}$$

$$\#C_k^{(S)} = \begin{cases} \dfrac{(\tau q - q + 1)(q-1)^2(p-2)}{2(p-1)} & \text{if } k = 2, \\ \dfrac{(\tau q - q + 1)(q-1)(q-p)}{p(p^2-1)} & \text{if } k = p+1, \\ 0 & \text{otherwise,} \end{cases}$$

$$\#C_k^{(M)} = \begin{cases} (1-\delta_{p,2})\dfrac{q(q-1)(q-2)(p-3)}{4} & \text{if } k = 2, \\ 0 & \text{if } k \geq 3. \end{cases}$$

Summing up yields the exact formulas (6.3), (6.4), and (6.5). Finally, there is a total of q^{2p-2} pairs $(g,h) \in P_p(\mathbb{F}_q) \times P_p(\mathbb{F}_q)$ and therefore (6.2) follows from

$$c_1 = q^{2p-2} - \sum_{k \geq 2} k \cdot c_k. \qquad \square$$

Equation (2.2) now yields the counting result of this paper, namely the following exact formula for the number of decomposable polynomials of degree p^2 over $\mathbb{F}_q$.

Theorem 6.6. *Let $\mathbb{F}_q$ be a finite field of characteristic p, δ Kronecker's delta function, and τ the number of positive divisors of $p-1$. Then*

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

Proof. By (2.2) and Theorem 6.1 we find

$$\#D_{p^2}(\mathbb{F}_q) = q^{2p-2} - c_2 - pc_{p+1},$$

from which the claim follows. $\square$

For $p = 2$, this yields

$$\#D_4(\mathbb{F}_q) = q^2 \cdot \frac{2 + q^{-2}}{3},$$

consistent with the result in von zur Gathen (2013). Furthermore, we have

$$\begin{aligned}\#D_9(\mathbb{F}_q) &= q^4\left(1 - \frac{3}{8}(q^{-1} + q^{-2} - q^{-3} - q^{-4})\right) \quad \text{for } p = 3, \\ \#D_{p^2}(\mathbb{F}_q) &= q^{2p-2}\left(1 - q^{-p+1} + O(q^{-(2p-5)+1/d})\right) \quad \text{for } q = p^d \text{ and } p \geq 5.\end{aligned}$$

We have two independent parameters p and d, and $q = p^d$. For two eventually positive functions $f, g\colon \mathbb{N}^2 \to \mathbb{R}$, here $g \in O(f)$ means that there are constants b and c so that $g(p,d) \leq c \cdot f(p,d)$ for all p and d with $p + d \geq b$. With the bounds on τ mentioned after the proof of Proposition 3.21, we have the following asymptotics.

Corollary 6.7. *Let $p \geq 5$, $d \geq 1$, and $q = p^d$. Then*

$$\begin{aligned}c_1 &= q^{2p-2}(1 - 2q^{-p+1} + O(q^{-2p+5+1/d})), \\ c_2 &= q^{p-1}(1 + O(q^{-p+4+1/d})), \\ c_{p+1} &= (\tau - 1)q^{3-3/d}\left(1 + O(q^{-\max\{2/d, 1-1/d\}})\right) \\ &= O\left(q^{3-3/d+1/(d\log\log p)}\right).\end{aligned}$$

Von zur Gathen (2009) considers the asymptotics of

$$\nu_{q,n} = \begin{cases} \#D_n/q^{2\ell-2} & \text{if } n = \ell^2, \\ \#D_n/2q^{\ell+n/\ell-2} & \text{otherwise,} \end{cases}$$

where ℓ is the smallest prime divisor of n. It turns out that for any composite n, $\limsup_{q\to\infty} \nu_{q,n} = 1$, and that $\liminf_{q\to\infty} \nu_{q,n} = 1$ for many n. But when ℓ divides n exactly twice, denoted as $\ell^2 \parallel n$, determining the limes inferior was left as an open question. If $n = \ell^2$, we obtain from Theorem 6.6

$$\lim_{q\to\infty} \nu_{q,\ell^2} = 1$$

for any prime $\ell > 2$. For $n = 4$, the sequence has no limit, but oscillates between close to $\liminf_{q\to\infty} \nu_{q,4} = 2/3$ and $\limsup_{q\to\infty} \nu_{q,4} = 1$, and these are the only two accumulation points of the sequence $\nu_{q,4}$. If $\ell^2 \parallel n$ and $n \neq \ell^2$, the question of good asymptotics is still open, as it is for $\nu_{q,n}$ when q is fixed and $n \to \infty$.

7 Conclusion

In the wild case of univariate polynomial decomposition, we present some (equal-degree) collisions in the special case where the degree is r^2 for a power r of the characteristic p, and determine their number. We give a classification of all 2-collisions at degree p^2 and an algorithm which determines whether a given polynomial has a 2-collision, and if so, into which class it falls. We compute the exact number of decomposable polynomials of degree p^2 over finite fields. This yields tight asymptotics on $\nu_{q,n} = (\text{number of decomposables})/q^{2\ell-2}$ for $q \to \infty$, when $n = \ell^2$ is the square of a prime ℓ.

Ritt's Second Theorem covers distinct-degree collisions, even in the wild case, see Zannier (1993), and they can be counted exactly in most situations; see von zur Gathen (2010). It would be interesting to see a similar classification for general equal-degree collisions.

This paper only deals with decomposition of univariate polynomials. The study of rational functions with our method remains open.

8 Acknowledgments

Many thanks go to Mike Zieve for useful comments and pointers to the literature and to Rolf Klein and an anonymous referee for simplifying our proof of Lemma 5.3.

This work was funded by the B-IT Foundation and the Land Nordrhein-Westfalen.

References

Roberto M. Avanzi & Umberto M. Zannier (2003). The equation $f(X) = f(Y)$ in rational functions $X = X(t)$, $Y = Y(t)$. *Compositio Math.* **139**(3), 263–295.

David R. Barton & Richard Zippel (1985). Polynomial Decomposition Algorithms. *Journal of Symbolic Computation* **1**, 159–168.

Raoul Blankertz (2011). *Decomposition of Polynomials*. Diplomarbeit, Universität Bonn. Modified version available at `http://arxiv.org/abs/1107.0687`.

Raoul Blankertz (2013). A polynomial time algorithm for computing all minimal decompositions of a polynomial. *To appear in ACM Communications in Computer Algebra*.

Raoul Blankertz, Joachim von zur Gathen & Konstantin Ziegler (2012). Compositions and collisions at degree p^2. In *Proceedings of the 2012 International Symposium on Symbolic and Algebraic Computation ISSAC2012,* Grenoble, France, 91–98. ACM Press, New York, USA. URL `http://dx.doi.org/10.1145/2442829.2442846`. Full version available at `http://arxiv.org/abs/1202.5810`.

Antonia W. Bluher (2004). On $x^{q+1} + ax + b$. *Finite Fields and Their Applications* **10**(3), 285–305. URL `http://dx.doi.org/10.1016/j.ffa.2003.08.004`.

John J. Cade (1985). A New Public-key Cipher Which Allows Signatures. In *Proceedings of the 2nd SIAM Conference on Applied Linear Algebra*, Raleigh NC A11. SIAM.

Stephen D. Cohen (1985). Reducibility of sub-linear polynomials over a finite field. *Bulletin of the Korean Mathematical Society* **22**, 53–56.

Stephen D. Cohen (1990a). Exceptional polynomials and the reducibility of substitution polynomials. *Enseign. Math. (2)* **36**(1-2), 53–65. ISSN 0013-8584.

Stephen D. Cohen (1990b). The Factorable Core of Polynomials Over Finite Fields. *Journal of the Australian Mathematical Society (Series A)* **49**(02), 309–318.

Stephen D. Cohen & Rex W. Matthews (1994). A class of exceptional polynomials. *Transactions of the American Mathematical Society* **345**(2), 897–909. ISSN 0002-9947. URL http://www.jstor.org/stable/2155005.

Robert S. Coulter, George Havas & Marie Henderson (2004). On decomposition of sub-linearised polynomials. *Journal of the Australian Mathematical Society* **76**(3), 317–328. URL http://dx.doi.org/10.1017/S1446788700009885.

L. E. Dickson (1897). The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *Annals of Mathematics* **11**, 65–120, 161–183.

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.

H. T. Engstrom (1941). Polynomial Substitutions. *American Journal of Mathematics* **63**, 249–255. URL http://www.jstor.org/stable/pdfplus/2371520.pdf.

Michael D. Fried & R. E. MacRae (1969). On the invariance of chains of Fields. *Illinois Journal of Mathematics* **13**, 165–171.

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 (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). Shift-invariant polynomials and Ritt's Second Theorem. *Contemporary Mathematics* **518**, 161–184.

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 & Jürgen Gerhard (2013). *Modern Computer Algebra*. Cambridge University Press, Cambridge, UK, Third edition. URL http://cosec.bit.uni-bonn.de/science/mca/. Other editions: 1999, 2003, Chinese edition, Japanese translation.

Joachim von zur Gathen, Mark Giesbrecht & Konstantin Ziegler (2010). Composition collisions and projective polynomials. Statement of results. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation ISSAC2010,* Munich, Germany, Stephen Watt, editor, 123–130. ACM Press. URL http://dx.doi.org/10.1145/1837934.1837962. Preprint available at http://arxiv.org/abs/1005.1087.

Mark William Giesbrecht (1988). *Some Results on the Functional Decomposition of Polynomials*. Master's thesis, University of Toronto, Department of Computer Science. Available as http://arxiv.org/abs/1004.5433.

David Goss (1996). *Basic Structures of Function Field Arithmetic*. Springer-Verlag. ISBN 3-540-61087-1.

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

D. R. Heath-Brown (1992). Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression. *Proceedings of the London Mathematical Society* **64**, 265–338.

Marie Henderson & Rex Matthews (1999). Composition behaviour of sub-linearised polynomials over a finite field. In *Finite fields: theory, applications, and algorithms (Waterloo, ON, 1997)*, volume 225 of *Contemp. Math.*, 67–75. Amer. Math. Soc., Providence, RI.

Nathan Jacobson (1964). *Lectures in abstract algebra: Volume III – Theory of fields and Galois theory*. Van Nostrand. ISBN 9780387901688.

Dexter Kozen & Susan Landau (1989). Polynomial Decomposition Algorithms. *Journal of Symbolic Computation* **7**, 445–456. An earlier version was published as Technical Report 209/88, University of Toronto, Department of Computer Science, Toronto, Ontario, Canada, 1988.

S. Landau & G. L. Miller (1985). Solvability by Radicals is in Polynomial Time. *Journal of Computer and System Sciences* **30**, 179–208.

Serge Lang (2002). *Algebra*. Springer-Verlag. ISBN 9780387953854.

H. Levi (1942). Composite Polynomials with coefficients in an arbitrary Field of characteristic zero. *American Journal of Mathematics* **64**, 389–400.

Florian Luca & Igor E. Shparlinski (2008). On the values of the divisor function. *Monatshefte für Mathematik* **154**, 59–69. URL `http://dx.doi.org/10.1007/s00605-007-0511-3`.

Jürgen Neukirch (1999). *Algebraic Number Theory*. Springer-Verlag. ISBN 3-540-65399-6.

O. Ore (1933). On a Special Class of Polynomials. *Transactions of the American Mathematical Society* **35**, 559–584.

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.

Henning Stichtenoth (2009). *Algebraic Function Fields and Codes*. Springer-Verlag. ISBN 978-3-540-76877-7.

Triantafyllos Xylouris (2011). Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression. Dissertation. Rheinische Friedrich-Wilhelms-Universität Bonn.

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

Michael Zieve (2011). Personal communication.

Richard Zippel (1991). Rational Function Decomposition. In *Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation ISSAC '91,* Bonn, Germany, Stephen M. Watt, editor, 1–6. ACM Press, Bonn, Germany. ISBN 0-89791-437-6.