Finite Fields and Their Applications 27 (2014) 41–71

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Normal form for Ritt's Second Theorem

Joachim von zur Gathen

B-IT, Universität Bonn, D-53113 Bonn, Germany

ARTICLE INFO

Article history:
Received 30 October 2012
Received in revised form 6 September 2013
Accepted 7 December 2013
Available online 23 January 2014
Communicated by D. Panario

MSC:
68W30
11T06
12E05

Keywords:
Computer algebra
Univariate polynomial decomposition
Bidecomposition
Ritt's Second Theorem
Finite fields
Combinatorics on polynomials

ABSTRACT

Ritt's Second Theorem deals with *composition collisions* $g \circ h = g^* \circ h^*$ of univariate polynomials over a field, where $\deg g = \deg h^*$. Joseph Fels Ritt (1922) presented two types of such decompositions. His main result here is that these comprise all possibilities, up to some linear transformations. We present a normal form for Ritt's Second Theorem, which is unique in many cases, and clarify the relation between the two types of examples. This yields an exact count of the number of such collisions in the "tame case", where the characteristic of the (finite) ground field does not divide the degree of the composed polynomial.

1. Introduction

In the 1920s, Ritt, Fatou, and Julia investigated the composition

$$f = g \circ h = g(h) \tag{1.1}$$

E-mail address: gathen@bit.uni-bonn.de.
URL: http://cosec.bit.uni-bonn.de/.

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2013.12.004

of univariate polynomials over a field F for $F = \mathbb{C}$. It emerged as an important question to determine the (distinct-degree) *collisions* (or nonuniqueness) of such decompositions, that is, different components $(g, h) \neq (g^*, h^*)$ with equal composition $g \circ h = g^* \circ h^*$ and equal sets of degrees: $\deg g = \deg h^* \neq \deg h = \deg g^*$.

Composition with linear polynomials (polynomials of degree 1) introduces inessential ambiguities. Ritt presented two types of essential collisions:

$$\begin{aligned} x^l \circ x^k w\big(x^l\big) &= x^{kl} w^l\big(x^l\big) = x^k w^l \circ x^l, \\ T_m\big(x, z^l\big) \circ T_l(x, z) &= T_{lm}(x, z) = T_l\big(x, z^m\big) \circ T_m(x, z), \end{aligned} \tag{1.2}$$

where $w \in F[x]$, $z \in F^\times = F \setminus \{0\}$, and T_m is the mth Dickson polynomial of the first kind. Ritt proved in his Second Theorem that these are essentially all possibilities. Details are given below.

Ritt worked with $F = \mathbb{C}$ and used analytic methods. Subsequently, his approach was replaced by algebraic methods, in the work of Levi [15] and Dorey and Whaples [5], and Schinzel [18] presented an elementary but long and involved argument. Thus Ritt's Second Theorem was also shown to hold in positive characteristic p. The original versions of this required $p > n = \deg f = \deg(g \circ h)$. Zannier [23] reduced this to the milder and more natural requirement $g'(g^*)' \neq 0$. His proof works over an algebraically closed field, and Schinzel's [19] monograph adapts it to finite fields. These results assume that $\gcd(\deg g, \deg g^*) = 1$; Tortrat [20] removed this condition provided that $p \nmid n$.

Ritt's Second Theorem, stated as Fact 3.3 below, involves four unspecified linear functions, and a uniqueness property is not obvious. Theorem 3.9 presents a normal form for the decompositions in Ritt's Theorem. It makes Zannier's assumption $g'(g^*)' \neq 0$ and the standard assumption $\gcd(l, m) = 1$, where $m = k + l \deg w$ in (1.2). This normal form is unique unless $p \mid m$. We also elucidate the relation between the first and the second type of example.

A fundamental dichotomy in this business is whether p divides n or not. The designation *tame* and *wild* was introduced in von zur Gathen [6,7] for the cases $p \nmid n$ and $p \mid n$, respectively, in analogy with ramification indices. An important consequence—and the original motivation—of the normal form presented in this paper is that we can count exactly the number of "collisions" as described by Ritt's Second Theorem (Fact 3.3), over a finite field and in the tame case. In turn, this is an essential ingredient for counting, approximately or exactly, the decomposable polynomials over a finite field; see von zur Gathen [11]. Equal-degree collisions, where the degree conditions are replaced by $\deg g = \deg g^*$, occur only in the wild case and are not considered in this paper.

Table 1.1 gives a précis of these counting results. The notation consists of a finite field $\mathbb{F}_q$ of characteristic p, integers l and m with $m > l \geqslant 2$, $n = lm$, the set $D_{n,l}$ of monic compositions of degree n with constant coefficient 0 and a left component of degree l (see (2.5)), $s = \lfloor m/l \rfloor$, $c = \lceil (m - l + 1)/l \rceil$, $t = \#(D_{n,l} \cap D_{n,m} \setminus \mathbb{F}_q[x^p])$, and Kronecker's δ.

The basic normal form result is augmented in several directions. Firstly, we can relinquish the condition $g'(g^*)' \neq 0$, keeping the assumption $\gcd(l, m) = 1$ (Theorem 5.2).