Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation

ISSAC'91

July 15-17, 1991
Bonn, Germany

Stephen M. Watt, Editor

acm PRESS

TP301-53
S986
1991

9461603

Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation

ISSAC'91

July 15-17, 1991
Bonn, Germany

Stephen M. Watt, Editor

acm PRESS

The Association for Computing Machinery
11 West 42nd Street
New York, New York 10036

Copyright © 1991 by the Association for Computing Machinery, Inc. Copying without fee is permitted provided that the copies are not made or distributed for direct commercial advantage, and credit to the source is given. Abstracting with credit is permitted. For other copying of articles that carry a code at the bottom of the first page, copying is permitted provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 27 Congress Street, Salem, MA 01970. For permission to republish write to: Director of Publications, Association for Computing Machinery. To copy otherwise, or republish, requires a fee and/or specific permission.

ISBN 0-89791-437-6

Additional copies may be ordered prepaid from:

ACM Order Department
P.O. Box 64145
Baltimore, MD 21264

ACM Order Number: 505910

Preface

The International Symposium on Symbolic and Algebraic Computation is a forum for the exchange of ideas and techniques in symbolic mathematical computation. ISSAC '91 will be held in Bonn, Germany from July 15th to 17th, 1991. Topics of the conference include, but are not limited to:

- Algorithms for symbolic mathematical computation
- Languages, systems and packages
- Computational geometry, group theory and number theory
- Automatic theorem proving and programming
- Interface of symbolics, numerics and graphics
- Applications in mathematics, science and engineering
- Symbolic and algebraic computation in education

This meeting marks the twenty fifth anniversary of the first symposium on the subject. That first conference was organized by Jean Sammet and sponsored by the ACM. There, 28 papers were presented and about 450 attended. Now the conference is held annually and ISSAC '91 is sixteenth in the series. Over the years, these meetings have used various abbreviated names — SYMSAM, SYMSAC, EUROSAM, EUROCAM and EUROCAL — before settling on the present name, ISSAC. A complete list and a bibliography of the proceedings is included at the end of this volume.

The program for ISSAC '91 includes invited talks, research contributions, system demonstrations and tutorials. It is a pleasure to be able to present such an excellent caliber of invitees. Papers for the invited talks cannot be included here but a list of speakers and titles appears before the table of contents.

This volume contains all the contributed papers to be presented at the meeting. Two forms of contribution were sought: full papers and application reports. The full papers present original research in the field and form the main body of the conference. The intent of the application reports was to bring interesting uses of symbolic mathematical computation to the attention of the community. Hopefully this range of concrete examples will be of use to those designing software and developing algorithms. In the table of contents the full papers are marked with a filled circle, •, and the application reports are marked with an open circle, ∘.

I would like to express my sincere gratitude to the members of the program committee and the external reviewers. These individuals have provided timely and careful reviews for an unexpectedly large number of submissions. Without their efforts, it would have been impossible to maintain the standards of the ISSAC meeting.

A total of 233 papers were submitted for consideration: 208 as full papers and 25 as application reports. Two papers were withdrawn and one is being presented in the form of an invited talk. The remaining contributions were evaluated by the members of the program committee and external reviewers. For each paper, at least two but usually three or more reports were obtained. At the end of the review process, 55 full papers and 9 application reports were accepted. In addition, 14 full papers with a particularly strong application interest were accepted on the condition that they be revised to meet the requirements of an application report.

These papers were not formally refereed. Although the reviewers were conscientious and in a good many cases made specific suggestions to the authors for improvement, time did not permit the revised papers to be recirculated for verification. It is expected that many of the papers here will be published in an extended and more polished form in scientific journals.

While the ACM remains a sponsor of the ISSAC meetings, they are now conducted internationally and the sponsorship is usually shared with an organization in the host country. This year, ISSAC '91 is sponsored by the German Gesellschaft für Informatik (GI) in cooperation with ACM SIGSAM, SAME and the Gesellschaft für Mathematik und Datenverarbeitung (GMD).

Finally, I would like to thank all authors who supported the conference by submitting papers. Without this work there would be no meeting.

Yorktown Heights, New York
May 1991

Stephen M. Watt

此为试读，需要完整PDF请访问：www.ertongbook.com

Conference Organization

Conference Chair

Fritz Schwarz, Sankt Augustin

Conference Co-Chair

Wolfgang Laßner, Leipzig

Program Committee

David Bayer (USA)
John Cannon (Australia)
Guy Cherry (USA)
Dominique Duval (France)
John Fitch (UK)
Joachim von zur Gathen (Canada)
Vladimir Gerdt (USSR)
Marc Giusti (France)
Malcolm MacCallum (UK)
Roman Mäder (Switzerland)
Michael Möller (Germany)
Teo Mora (Italy)
Michael Pohst, Chair (Germany)
Stephen Watt, Chair (USA)

Invited Presentations

Algebraic computation: The next decade
Anthony Hearn

Automatic differentiation: Applying the chain rule to numbers
Andreas Griewank

Computing tensor diagrams
Roger Penrose

Computer algebra in mechanics: Application to spacecraft dynamics
Pascal Rideau

Fast reduction and composition of binary quadratic forms
Arnold Schönhage

Portable computer algebra: Past, present and future
David Stoutemyer

Contents

Polynomial Algebra

Number Theory

Groups and Algebras

Differential Algebra

Systems

Symbolic/Numeric Computation

此为试读,需要完整PDF请访问: www.ertongbook.com

Applications

Rational Function Decomposition

Richard Zippel*
Cornell University
Ithaca, NY 14853
rz@cs.cornell.edu

Abstract

This paper presents a polynomial time algorithm for determining whether a given univariate rational function over an arbitrary field is the composition of two rational functions over that field, and finds them if so.

1 Introduction

The problem of determining if a function can be written as the composition of two "smaller" functions $f(x) = g(h(x))$ has been of interest for a long time. Until now, work has focused on the univariate, polynomial version of this problem: When can the polynomial $f(x)$ be written as $g(h(x))$, where both $g(x)$ and $h(x)$ are polynomials? The original work in the symbolic computation community was presented in 1976 [2], but the algorithms, which in the worst case required exponential time, were not published until 1985 [3]. This was soon followed by the work of Kozen and Landau [11] who provided a polynomial time algorithm for decomposition of polynomials over fields of characteristic zero, which did not require factorization of polynomials. Some additional improvements and analysis of the positive characteristic case where then presented by von zur Gathen [23, 21, 22]. A number of other papers have since been published on different extensions and variations of this problem [1, 7, 5, 4].

All of these results deal with polynomial decomposition. The generalization to rational functions, which has significantly wider applicability, appears to be a far harder problem. Notice that in the polynomial case, the degree of g and h must divide the degree of f. This limits the number of different polynomials that must be considered and even allows one to solve the problem by looking for solutions of non-linear algebraic equations (admittedly in exponential time). When f, g and h are rational functions, there is no immediately obvious bound on the degrees of the numerators of g and h, since the numerator and denominator of $g(h(x))$ could have a common factor. In fact, no such common factor can arise, as we prove below.

Furthermore, we demonstrate that in the rational function case, g and h can be determined from f in polynomial time. This algorithm is valid even if the charactertistic of the field is positive, which for the polynomial case is not a completely resolved problem. One other difference between our approach and other approaches, is that in this paper we obtain a decomposition over the field of definition of $f(x)$. Thus we may fail to find rational function decompositions that exist over algebraic extensions. Such issues do not arise for the corresponding problem of polynomials over a field of characteristic zero, but do for polynomials over fields of finite characteristic.

Section 2 provides some general background material. In Section 3 we present the new algorithms for rational function decomposition. Finally, we comment on previous work in and give some conclusions in Section 4.

2 Preliminaries

Let $f(x)$ be a rational function in x with coefficients in a field k. We extend the notion of degree of a polynomial by defining the *degree* of $f(x)$, denoted by $\deg f$, to be the maximum of the polynomial degrees of the (relatively prime) numerator and denominator of f. The degree of the field $k(x)$ over $k(f(x))$ is the degree of f, if f is a polynomial. This remains true even if f is a rational function, as shown by the following proposition.

Proposition 1 *Let $k(x)$ be an extension of the field $k(f(x))$ where $f(x)$ is a rational function of degree n.*

*This research was supported in part by the Advanced Research Projects Agency of the Department of Defense under Office of Naval Research Contract N00014-88-K-0591, the National Science Foundation through grant IRI-9006137, the Office of Naval Research through contract N00014-89-J-1946 and in part by the U.S. Army Research Office through the Mathematical Science Institute of Cornell University.

Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the ACM copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Association for Computing Machinery. To copy otherwise, or to republish, requires a fee and/or specific permission.

© 1991 ACM 0-89791-437-6/91/0006/0001...$1.50

$$\begin{tikzcd}
k(x) \arrow[d, dash] & \\
k(h(x)) \arrow[d, dash] & k(y) \arrow[l, "\varphi_h"'] \arrow[d, dash] \\
k(f(x)) & k(g(y)) \arrow[l, "\varphi_h"']
\end{tikzcd}$$

Figure 1: Fields involved in decomposition

Then $[k(x):k(f(x))] = n$.

Proof: Denote the numerator of $f(x)$ by $p(x)$ and the denominator by $q(x)$. We can instead consider the isomorphic fields $k(y) \cong k(f(x))$ and

$$k(y)[x]/(p(x) - yq(x)) \cong k(x).$$

$P(x, y) = p(x) - yq(x)$ is primitive as a polynomial in y since $p(x)$ and $q(x)$ are relatively prime. Since it is linear in y it is irreducible. Therefore, the degree of x over the field $k(y)$ is

$$\deg_x P(x, y) = \max(\deg p, \deg q) = \deg f.$$

□

Let $f(x) = g(h(x))$ be a rational function decomposition over a field k. The following proposition provides bounds on the degrees of $g(x)$ and $h(x)$ in terms of the degree of $f(x)$. In principle, this result gives an algorithm for rational function decomposition, albeit an exponential time algorithm.

Proposition 2 *Assume $f(x)$, $g(x)$ and $h(x)$ are elements of $k(x)$ such that $f(x) = g(h(x))$. Then*

$$\deg f = (\deg g) \cdot (\deg h)$$

Proof:

Consider the fields shown in Figure 1. The degrees of the extensions are $[k(x) : k(h(x))] = \deg h$, $[k(x) : k(f(x))] = \deg f$ and $[k(y):k(g(y))] = \deg g$. $k(h(x))$ is an algebraic extension of $k(f(x))$ inside $k(x)$. Thus,

$$\begin{aligned}
\deg f &= [k(x):k(f(x))] \\
&= [k(x):k(h(x))] \cdot [k(h(x)):k(f(x))] \\
&= [k(x):k(h(x))] \cdot [k(y):k(g(y))] \\
&= (\deg h) \cdot (\deg g),
\end{aligned}$$

using Proposition 1. □

A function that is the ratio of to linear polynomials is called a *fractional linear function*, *viz.*

$$\lambda(x) = (ax + b)/(cx + d).$$

Fractional linear functions have degree 1. If two fields $k(f_1(x))$ and $k(f_2(x))$ are isomorphic then there exist rational functions such that

$$\begin{aligned}
f_1(x) &= R_1(f_2(x)) \\
f_2(x) &= R_2(f_1(x)) = R_2(R_1(f_2(x)))
\end{aligned}$$

By Proposition 2 $(\deg R_1) \cdot (\deg R_2) = 1$ and R_1 and R_2 must be fractional linear functions.

We say that two rational functions are linearly equivalent if there exists fractional linear functions λ_1 and λ_2 such that

$$f(x) = \lambda_1(g(\lambda_2(x))).$$

Two decompositions (polynomial or rational function)

$$\begin{aligned}
f &= g_1 \circ g_2 \circ \cdots \circ g_m \\
&= h_1 \circ h_2 \circ \cdots \circ h_n
\end{aligned}$$

are said to be *equivalent* if $m = n$ and g_i is linearly equivalent to h_i.

The link between field structure and function decomposition comes from *Lüroth's theorem*, which was proven by Lüroth [15] for $k = \mathbb{C}$ and by Steinitz in general [18].

Proposition 3 (Lüroth) *If $k \subsetneq K \subset k(x)$ then $K = k(g(x))$ where $g(x)$ is a rational function in x over k.*

An elementary proof of Lüroth's theorem may be found in van der Waerden [20]. An effective proof appears in Weber [24] §124, and in English in Schinzel [17].

The key insight in studying functional decomposition is the following corollary of Lüroth's theorem.

Proposition 4 *Let k be an arbitrary field and $f(x)$ a rational function over k. There is a one to one correspondence between the lattice of subfields between $k(x)$ and $k(f(x))$ and the rational function decompositions of $f(x)$ up to equivalence.*

Proof: If $f(x)$ has a nontrivial decomposition $f(x) = g(h(x))$, then $k(h(x))$ will be an intermediate field between $k(x)$ and $k(f(x))$. Conversely, if K is field intermediate between $k(x)$ and $k(f(x))$ then it must be of the form $k(h(x))$, where $h(x)$ is a rational function in x. $k(h(x))$ is canonically isomorphic to $k(y)$ as shown in Figure 1, where $\varphi_h(y) \mapsto h(x)$. $k(f(x))$ is intermediate between $k(y) = k(h(x))$ and k, so by Lüroth's theorem, there is a rational function $g(y)$ such that $k(f(x)) = k(g(y))$. Thus $f(x)$ is linearly equivalent to $g(h(x))$. □

The following two propositions follow from Proposition 2 and are quite useful.

Proposition 5 *Let k be an arbitrary field and g_1 and g_2 relatively prime elements of $k[x]$. Then for all polynomials $h(x) \in k[x]$, $g_1(h(x))$ and $g_2(h(x))$ are relatively prime.*

Proof: Without loss of generality assume that $\deg g_1 \geq \deg g$. Define $g(x)$ to be the ratio of $g_1(x)$ and $g_2(x)$. Since g_1 and g_2 are relatively prime and $\deg g_1 \geq \deg g_2$, $\deg g(x) = \deg g_1$. Let

$$f(x) = g(h(x)) = \frac{g_1(h(x))}{g_2(h(x))} = \frac{f_1(x)}{f_2(x)},$$

where f_1 and f_2 are relatively prime. Thus

$$\deg f_i(x) \leq \deg g_i(h(x)) = (\deg g_i) \cdot (\deg h),$$

where equality holds if and only if $g_1(h(x))$ and $g_2(h(x))$ are relatively prime. Furthermore, $\deg f_1 \geq \deg f_2$ so $\deg f = \deg f_1$. By Proposition 2

$$\deg f(x) = (\deg g) \cdot (\deg h) = (\deg g_1) \cdot (\deg h)$$

so $\deg f_1(x) = (\deg g_1) \cdot (\deg h)$ and $g_1(h(x))$ and $g_2(h(x))$ are relatively prime. $\square$

The argument of previous proposition applies equally when $h(x)$ is a rational function. In this case, it is best to view g_1 and g_2 as bivariate homogeneous functions of the same degree, which gives the following result.

Proposition 6 *Let g_1 and g_2 be relatively prime, homogeneous polynomials in two variables. If h_1 and h_2 are also relatively prime polynomials, then $g_1(h_1, h_2)$ and $g_2(h_1, h_2)$ are also relatively prime.*

Notice that the requirement that g_1 and g_2 be homogeneous is necessary as the following example shows:

$$\left.\begin{aligned} g_1(x, y) &= x + 1 \\ g_2(x, y) &= y - 2 \\ h_1(t) &= t \\ h_2(t) &= t^2 + 1 \end{aligned}\right\} \longrightarrow \left\{\begin{aligned} g_1(h_1, h_2) &= t + 1 \\ g_2(h_1, h_2) &= t^2 - 1 \end{aligned}\right.$$

As a consequence of Proposition 6, rational function decomposition can be viewed as a coupled polynomial decomposition problem, *viz.*

$$\begin{aligned} f_1(x, y) &= g_1(h_1(x, y), h_2(x, y)), \\ f_2(x, y) &= g_2(h_1(x, y), h_2(x, y)), \end{aligned}$$

where f_i, g_i and h_i are homogeneous polynomials and the pairs $\{f_1, f_2\}$, $\{g_1, g_2\}$ and $\{h_1, h_2\}$ have the same degree.

3 Rational Function Decomposition

The bounds of Proposition 2 provide significant insight into rational function decomposition. In particular, if the degree of $f(x)$ is prime, then it has no non-trivial decomposition. A simple, exponential time algorithm for determining a decomposition can be constructed by using undetermined coefficients. Assume that $\deg f = rs$ and we are looking for a decomposition $f(x) = g(h(x))$, where $\deg g = r$ and $\deg h = s$. We can write g and h in terms undetermined coefficients, *e.g.*

$$g(x) = \frac{g_n(x)}{g_d(x)} = \frac{g_0 x^r + g_1 x^{r-1} + \cdots + g_r}{g_{r+1} x^r + g_{r+2} x^{r-1} + \cdots + g_{2r+1}}.$$

There are $2r + 2$ undetermined coefficients in $g(x)$ and $2s+2$ in $h(x)$. By Proposition 6, we can treat the numerator and denominator of $f(x)$ independently. Equating the coefficients of x^i in the following equations gives a system of $2rs + 2$ algebraic equations in the g_i and h_i.

$$\begin{aligned} f_0 x^{rs} &+ \cdots + f_{rs} \\ &= g_0 h_n(x)^r + \cdots + g_r h_d(x)^r \\ f_{rs+1} x^{rs} &+ \cdots + f_{2rs+1} \\ &= g_{r+1} h_n(x)^r + \cdots + g_{2r+1} h_d(x)^r \end{aligned} \tag{1}$$

Any decomposition of $f(x)$ is a solution to this system of equations. Conversely, any solution to this system for which $\deg g = r$ and $\deg h = s$ gives a decomposition of $f(x)$. However, this approach is not very efficient. Nonetheless, it does demonstrate the existence of an algorithm.

The efficient techniques that have been developed all tend to be divided into two phases, computing $h(x)$ and then given $h(x)$ computing $g(x)$. (The hard part is finding $h(x)$.) We discuss the phases out of order for simplicity. Determining g from f and h is discussed in Section 3.1, while the determination of h is discussed in Section 3.2.

3.1 Determining g from f and h

The most direct way to obtain $g(x)$ such that $f(x) = g(h(x))$, when f and h are known is to explicitly solve the *linear* equations for the coefficients of $g(x)$ that arise from (1). This approach is discussed in detail by Dickerson [5, 4] as "computing the left composition factor." In this section we present a simple analytic technique that relies on reversion of power series and is valid when the coefficient field has characteristic 0.

Let λ_f be a fractional linear function such that $\hat{f} = \lambda_f \circ f$ has a zero at 0. Define $\hat{h}$ and λ_h similarly. If $\hat{f} = \hat{g} \circ \hat{h}$ then

$$f(x) = (\lambda_f^{-1} \circ \hat{g} \circ \lambda_h) \circ h(x),$$

$$\begin{tikzcd}
k(x) \arrow[r, dash] \arrow[d, dash] & E[\alpha]/(f(\alpha)-t) = F \arrow[d, dash] \\
k(h(x)) \arrow[r, dash] \arrow[d, dash] & E[\beta]/(h(\beta)-t) \arrow[d, dash] \\
k(f(x)) \arrow[r, dash] & k(t) = E
\end{tikzcd}$$

Figure 2: Field Structure

and $g(x) = (\lambda_f^{-1} \circ \hat{g} \circ \lambda_h)(x)$. So without loss of generality we can assume $f(0) = h(0) = 0$.

$h(x)$ has a power series expansion of the form

$$h(x) = h_\ell x^\ell + h_{\ell+1} x^{\ell+1} + \cdots$$

Using standard techniques [10] we can obtain a power series in t for x in $t = h(x)$

$$x = h^{-1}(t) = h'_1 t^{1/\ell} + h'_2 t^{2/\ell} + \cdots.$$

Replacing x by this power series in the power series for $f(x)$ we get a power series in t. If there are any fractional powers then there does not exist a "left composition factor." Compute the first $2r$ terms of the power series expansion of $f(h^{-1}(x))$ at 0. The (r, r) Padé approximate [16] to this power series is the only possible candidate for $g(x)$. This power series technique may be easier to program than Dickerson's technique, and using fast power series techniques [12] it might have better asymptotic complexity.

3.2 Determination of h

For rational function decomposition, we determine $h(x)$ by explicitly determining a subfield of $k(x)$ and then use a constructive version of Lüroth's theorem to compute a generator for the subfield. The tower of fields we will be working with is shown in Figure 2. Note that the fields on the same horizontal line in Figure 2 are isomorphic. By Proposition 3 every subfield of F is of the form $k(h(x))$ and there exists a rational function g such that $g(h(x)) = f(x)$, since $k(f(x))$ lies between $k(y) = k(h(x))$ and k. Thus every non-trivial subfield of F yields a non-trivial decomposition of $f(x)$.

To illustrate our procedure consider the following example:

$$\begin{aligned} f(x) &= \left(\frac{x^2+1}{x^2-2}\right) \circ \left(\frac{x^2+1}{x^2+2}\right) \\ &= -\frac{2x^4+6x^2+5}{x^4+6x^2+7} = \frac{f_n(x)}{f_d(x)}, \end{aligned}$$

where f_n and f_d are relatively prime. We want to find an intermediate field between $k(x)$ and $k(f(x))$. Our first step is to convert these fields to a more conventional form. If $E = k(t) = k(f(x))$ and $E[\alpha] = k(x)$ then α satisfies the minimal polynomial

$$\hat{f}(t, Z) = f_n(Z) - t f_d(Z) = (t+2)Z^4 + (6t+6)Z^2 + 7t + 5.$$

This polynomial's factorization over $E[\alpha]$ is

$$\hat{f}(t, Z) = (Z-\alpha)(Z+\alpha)((t+2)Z^2 + (t+2)\alpha^2 + 6(t+1)). \qquad (2)$$

Over a proper subfield of $E[\alpha]$, $\hat{f}(t, Z)$ will not factor so much. In particular, over a subfield it cannot have a linear factor. Given (2), the only possible factors of $\hat{f}(t, Z)$ over the subfield $E[\beta]$ are $Z - \alpha^2$ and $((t+2)Z^2 + (t+2)\alpha^2 + 6(t+1))$. Thus $E[\beta]$ must contain the coefficients of these two polynomials. If $E[\beta]$ is the smallest subfield of $E[\alpha]$ for which $\hat{f}(t, Z)$ has such a factorization, then it must be generated by the coefficients of these two polynomials. In this case we can assume that $\beta = \alpha^2$, whose minimal polynomial is

$$\hat{h}(t, Z) = (t+2)Z^2 + (6t+6)Z + 7t + 5. \qquad (3)$$

To convert $E[\beta]$ back to the form $k(f(x))$ we observe that the elements of $E[\beta]$ are rational functions in x over k by Lüroth's theorem. When t is replaced by $f(x)$, (3) must have linear factors, *viz.*

$$\hat{h}(f(x), Z) = (Z - x^2)\left(Z - \frac{3x^2+4}{2x^2+3}\right),$$

which leads to the intermediate fields $k(x^2)$ and $k((3x^2+4)/(2x^2+3))$. These two fields are isomorphic by the fractional linear map $x \mapsto (3x+4)/(2x+3)$. Using the $k(x^2)$ as the intermediate field, we have $h(x) = x^2$, and thus the irreducible decomposition:

$$-\frac{2x^4+6x^2+5}{x^4+6x^2+7} = -\frac{2x^2+6x+5}{x^2+6x+7} \circ x^2.$$

The original decomposition is equivalent to this one since

$$\begin{aligned} \frac{x^2+1}{x^2+2} &= \left(\frac{x+1}{x+2}\right) \circ x^2 \\ \frac{x^2+1}{x^2-2} &= \left(-\frac{2x^2+6x+5}{x^2+6x+7}\right) \circ \left(\frac{-2x+1}{x-1}\right) \end{aligned}$$

This basic approach is applicable to the general problem except for deciding which factors of $\hat{f}(t, Z)$ should be recombined to generate a factorization over a subfield of $E[\alpha]$. We could try all possible combinations of factors of $\hat{f}(t, Z)$ until we find one that yields a proper subfield of $E[\alpha]$. However, in the worst case this would require an exponential number of trials. Instead, we use a version of Landau and Miller's algorithm **BLOCKS** in [14] to find a non-trivial block, which will generate a proper subfield of $E[\alpha]$. As pointed out by Kozen and Landau [11], this algorithm only requires that the extension $E[\alpha]/E$ be separable. Kozen and Landau may need to examine as many as $O(n^{\log n})$ non-trivial blocks to find a decomposition. However, in our case, any non-trivial block will give a rational function decomposition. These techniques allow us to decide which factors of $\hat{f}(t, Z)$ should be recombined in polynomial time.

Furthermore, observe that Trager's polynomial time reduction of factorization over algebraic extensions [19], which was used by Landau to show that factoring over algebraic number fields is polynomial time [13] is applicable here also, so the factorization of $\hat{f}(t, Z)$ over the function field $E[\alpha]$ can be done in polynomial time.

The coefficients of such a factorization generate the intermediate field $E[\beta]$. Since we are seeking any intermediate field, a single coefficient that is not in E suffices. The minimal polynomial of for that coefficient can be determined using resultants and square free decompositions to give $E[\beta]/(p_\beta(t, \beta))$. $h(x)$ is then deduced from a linear factor of $p_\beta(f(x), Z)$, which need only be factored over k. (Factoring bivariate polynomials is polynomial time by Kaltofen [9].)

It is worth commenting on the practicality of this algorithm. Its dominant cost is the factorization of $\hat{f}(t, Z)$ over $k(t)[\alpha]$, which is about as costly as factoring a polynomial of degree $(\deg f)^2$. Given the practical difficulties of factoring polynomials of degree greater than about 100, it seems that it will be very difficult to determine the decomposition of $f(x)$ if the degree of $f(x)$ is greater than about 10.

3.3 Characteristic p case

Determining any decomposition, as opposed to determining a decomposition with a particular degree pattern over a field of characteristic p is only slightly more difficult than the characteristic 0 case, using the technique of Section 3.2. Assume that $\operatorname{char} k = p$ and $f(x)$ is a rational function over k. The decomposition of $f(x)$ may no longer be unique, but Proposition 4 shows that there is still a one to one correspondence between the inequivalent decompositions of $f(x)$ and the fields intermediate between $k(x)$ and $k(f(x))$.

Referring to Figure 2, let $\hat{f}(t, Z)$ be the (irreducible) minimal polynomial of α over E. If $\hat{f}(t, Z)$ is separable, then $E[\alpha]$ is separable over E and a subfield can be computed using the techniques of the previous section. If $\hat{f}(t, Z)$ is inseparable then it can be written as

$$\hat{f}(t, Z) = \bar{f}(t, Z^{p^\mu}),$$

for some positive value of μ. Furthermore, $\bar{f}$ is separable over E. Clearly, the field $E[\alpha^{p^\mu}]$ lies between $E[\alpha]$ and E and thus a linear factor of $\bar{f}(f(x), Z)$ will give a decomposition factor of $f(x)$. Since $E[\alpha^{p^\mu}]$ is separable over E, the techniques of the previous section can be used to find additional right decomposition factors. Left decompositions factors can be found from the fields $E[\alpha^{p^i}]$, which lie between $E[\alpha]$ and $E[\alpha^{p^\mu}]$ for $1 \leq i < \mu$.

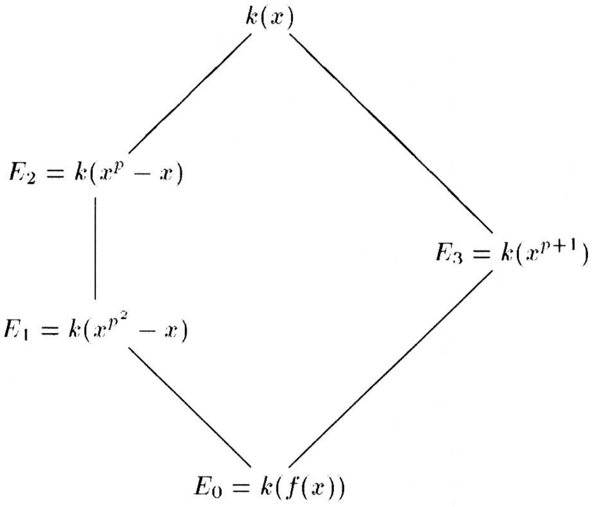

Figure 3: Field Structure for $f(x) = x^{p^3+p^2} - x^{p^3+1} - x^{p^2+p} + x^{p+1}$

It is worth noting that even the pathological example suggested by Dorey and Whaples [6]

$$\begin{aligned} f(x) &= x^{p+1} \circ (x^p + x) \circ (x^p - x), \\ &= (x^{p^2} - x^{p^2-p+1} - x^p + x) \circ x^{p+1}, \\ &= x^{p^3+p^2} - x^{p^3+1} - x^{p^2+p} + x^{p+1}, \end{aligned}$$

is can be handled straightforwardly, since the derived polynomial

$$\hat{f}(t, Z) = Z^{p^3+p^2} - Z^{p^2+p} - Z^{p^3+1} + Z^{p+1} - t$$

is separable. The fields associated with the two decompositions of $f(x)$ are shown in Figure 3.

In the case of polynomial decomposition, notice that $\hat{f}(t, Z)$ is inseparable if and only if $f(x)$ is a rational function of x^p. Thus the distinction made by von zur Gathen [21, 22] between "tame" and "wild" might more appropriately be made on whether or not $f(x)$ is a rational function in x^p.

Note that this approach only finds *some* decomposition of $f(x)$. It cannot find a prescribed one. In particular, if one is looking for a decomposition $f(x) = g(h(x))$ where $p \mid \deg g$ then the extension $k(x)/k(f(x))$ may be inseparable and we would thus have no algorithm for finding intermediate fields. This problem is raised in [22].

此为试读,需要完整PDF请访问: www.ertongbook.com