Decomposition of Algebraic Functions

Dexter Kozen*
Susan Landau**
Richard Zippel*

TR 94-1410
February 1994

Department of Computer Science
Cornell University
Ithaca, NY 14853-7501

* Computer Science Department, Cornell University, Ithaca, NY 14853.
** Computer Science Department, University of Massachusetts, Amherst, MA 01003.

Decomposition of Algebraic Functions

Dexter Kozen*
Cornell University
kozen@cs.cornell.edu

Susan Landau†
University of Massachusetts, Amherst
landau@cs.umass.edu

Richard Zippel*
Cornell University
rz@cs.cornell.edu

February 8, 1994

Abstract

Functional decomposition—whether a function $f(x)$ can be written as a composition of functions $g(h(x))$ in a nontrivial way—is an important primitive in symbolic computation systems. The problem of univariate polynomial decomposition was shown to have an efficient solution by Kozen and Landau [8]. Dickerson [5] and von zur Gathen [11] gave algorithms for certain multivariate cases. Zippel [13] showed how to decompose rational functions.

In this paper, we address the issue of decomposition of algebraic functions. We show that the problem is related to univariate resultants in algebraic function fields, and in fact can be reformulated as a problem of *resultant decomposition*. We give an algorithm for finding a nontrivial decomposition of a given algebraic function if it exists. The algorithm involves genus calculations and constructing transcendental generators of fields of genus zero.

1 Introduction

Functional decomposition is the problem of representing a given function $f(x)$ as a composition of "smaller" functions $g(h(x))$. Decomposition of polynomials is useful in simplifying the representation of field extensions of high degree, and is provided as a primitive by all major symbolic algebra systems.

The first analyzed algorithms for polynomial decomposition were provided in 1985 Barton and Zippel [2] and Alagar and Thanh [1], who gave algorithms for the problem of decomposing univariate polynomials over fields of characteristic zero. Both solutions involved polynomial factorization and took exponential time. Kozen and Landau [8] discovered a

*Computer Science Department, Cornell University, Ithaca, NY 14853
†Computer Science Department, University of Massachusetts, Amherst, MA 01003

simple and efficient polynomial time solution that does not require factorization and works in characteristic zero and whenever the degree of h does not divide the characteristic of the underlying field, and NC algorithms for irreducible polynomials over finite fields and all polynomials over characteristic zero. Dickerson [5] and von zur Gathen [11] gave algorithms for certain multivariate cases. In addition, von zur Gathen also found algorithms for the case in which the degree of h divides the characteristic of the field [12]. Zippel [13] showed how to decompose rational functions.

In this paper we address the decomposition problem for algebraic functions. We show that the problem bears an interesting and useful relationship to univariate resultants over algebraic function fields, and in fact can be reformulated as a certain resultant decomposition problem: whether some power of a given irreducible bivariate polynomial $f(x,z)$ can be expressed as the resultant with respect to y of two other bivariate polynomials $g(x,y)$, $h(y,z)$. We determine necessary and sufficient conditions for an algebraic function to have a nontrivial decomposition, and classify all such decompositions up to isomorphism. We give an exponential-time algorithm for finding a nontrivial decomposition of a given algebraic function if one exists. The algorithm involves calculating the genus of certain algebraic function fields and constructing transcendental generators of fields of genus zero.

The paper is organized as follows. In §2, we review the basic properties of univariate resultants, state the decomposition problem for algebraic functions, and describe the relationship between the two. In §3 we prove a general theorem that characterizes the set of all possible decompositions of an algebraic function. In §4 we give an exponential time algorithm for the decomposition problem. We conclude in §5 with an example.

2 Resultants and Algebraic Functions

2.1 The Univariate Resultant

Here we review some basic facts about the univariate resultant; see [7, 14] for a detailed introduction.

The *resultant* of two polynomials

$$\begin{aligned} g(y) &= a\prod_{i=1}^{m}(y-\alpha_i) \\ h(y) &= b\prod_{j=1}^{n}(y-\beta_j) \end{aligned}$$

with respect to y is the polynomial

$$\begin{aligned} \mathbf{res}_y(g,h) &= a^n b^m \prod_{i,j}(\beta_j-\alpha_i) \\ &= b^m \prod_{h(\beta)=0} g(\beta)\,. \end{aligned}$$

The resultant vanishes iff g and h have a common root. It can be calculated as the determinant of a certain $(m+n)\times(m+n)$ matrix containing the coefficients of g and h.

The following are some useful elementary properties.

$$\begin{aligned}
\mathbf{res}_y(g,h) &= (-1)^{mn}\mathbf{res}_y(h,g) \\
\mathbf{res}_y(g_1g_2,h) &= \mathbf{res}_y(g_1,h)\cdot\mathbf{res}_y(g_2,h) \\
\mathbf{res}_y(g,h_1h_2) &= \mathbf{res}_y(g,h_1)\cdot\mathbf{res}_y(g,h_2) \\
\mathbf{res}_y(c,h) &= c^n \\
\mathbf{res}_y(g,1) &= \mathbf{res}_y(1,h) = 1 \\
\mathbf{res}_y(g,y-\beta) &= g(\beta)
\end{aligned}$$

We extend the definition to pairs of rational functions $g_1(y)/g_2(y)$ and $h_1(y)/h_2(y)$ as follows:

$$\mathbf{res}_y(\frac{g_1}{g_2},\frac{h_1}{h_2}) = \frac{\mathbf{res}_y(g_1,h_1)\cdot\mathbf{res}_y(g_2,h_2)}{\mathbf{res}_y(g_1,h_2)\cdot\mathbf{res}_y(g_2,h_1)} .$$

This quantity is defined if neither g_1, h_2 nor g_2, h_1 have a common root. It is easily checked that this definition reduces to the previous one in the case of polynomials, and that all the properties listed above still hold, taking $m = \deg g_1 - \deg g_2$ and $n = \deg h_1 - \deg h_2$.

2.2 Resultants and Decomposition

Algebraic functions of z over K are usually defined as elements of some finite extension of $K(z)$, the field of rational functions of z. Over algebraically closed fields K, they can be represented more concretely as multivalued functions $K \rightarrow 2^K$ or binary relations on K defined by their minimum polynomials. Let K be algebraically closed, and let α be an algebraic function of γ with irreducible equation $f(\alpha,\gamma) = 0$, $f(x,z) \in K[x,z]$. Let

$$V(f) = \{(a,c) \mid f(a,c) = 0\} \subseteq K^2$$

be the irreducible affine curve generated by f. We say that α is *decomposable* if there exist polynomials $g(x,y)$ and $h(y,z)$ such that $V(f) = V(g) \circ V(h)$, the relation-theoretic composition of the curves $V(g)$ and $V(h)$. The relational composition operator $\circ$ can be expressed algebraically in terms of the univariate resultant:

$$\begin{aligned}
V(f) &= V(g) \circ V(h) \\
&= \{(a,c) \mid \exists b \in K\ (a,b) \in V(g),\ (b,c) \in V(h)\} \\
&= \{(a,c) \mid \exists b \in K\ g(a,b) = 0,\ h(b,c) = 0\} \\
&= \{(a,c) \mid \mathbf{res}_y(g(a,y),h(y,c)) = 0\} \\
&= V(\mathbf{res}_y(g(x,y),h(y,z))) .
\end{aligned}$$

By the Nullstellensatz, this occurs iff

$$f(x,z)^k = \mathbf{res}_y(g(x,y),h(y,z)) \qquad (1)$$

for some $k \geq 0$. Regarding $f(x,z)^k$ and $f(x,z)$ as representations of the same curve, the *decomposition problem* then becomes: given an irreducible polynomial $f(x,z)$, do there exist polynomials $g(x,y)$ and $h(y,z)$ and a positive integer k such that $f^k = \mathbf{res}_y(g,h)$?

Under this definition, every bivariate polynomial f is decomposable in infinitely many ways:

$$\begin{aligned} \mathbf{res}_y(f(x,y^k),y^k-z) &= \prod_{\beta^k=z} f(x,\beta^k) \\ &= \prod_{\beta^k=z} f(x,z) \\ &= f^k \ . \end{aligned} \tag{2}$$

However, these decompositions are trivial in a sense to be made precise in the next section. We will show that up to isomorphism there are only finitely many nontrivial minimal decompositions.

2.3 Irreducible Decompositions

A nontrivial decomposition $f = \mathbf{res}_y(g,h)$ is called *irreducible* if both g and h are irreducible as polynomials in $K[x,y]$ and $K[y,z]$, respectively. By the multiplicativity of the resultant, every decomposition factors into a product of irreducible decompositions.

2.4 Monic Decompositions

A decomposition $f = \mathbf{res}_y(g,h)$ is called *monic* if $g \in K(y)[x]$ and $h \in K(z)[y]$ are monic. The next result says that we can restrict our attention to monic decompositions without loss of generality.

Lemma 1 *Let $f \in K[x,z]$, $g \in K[x,y]$, $h \in K[y,z]$, g, h irreducible, f a power of an irreducible polynomial. Let $\widehat{f}$, $\widehat{g}$, and $\widehat{h}$ be the monic associates of f, g, h in $K(z)[x]$, $K(y)[x]$, and $K(z)[y]$ respectively. Then $f = \mathbf{res}_y(g,h)$ iff $\widehat{f} = \mathbf{res}_y(\widehat{g},\widehat{h})$.*

Proof. Let $f_n(z)$, $g_m(y)$, and $h_\ell(z)$ be the lead coefficients of f, g and h, respectively. Let

$$u(z) \ = \ \mathbf{res}_y(g_m,h)\cdot h_\ell^{\deg_y g - \deg_y g_m} \ .$$

Then

$$\begin{aligned} \mathbf{res}_y(g,h) &= \mathbf{res}_y(g_m,h)\cdot\mathbf{res}_y(\widehat{g},h_\ell)\cdot\mathbf{res}_y(\widehat{g},\widehat{h}) \\ &= u\cdot\mathbf{res}_y(\widehat{g},\widehat{h}) \ . \end{aligned}$$

But since $\widehat{g}$ and $\widehat{h}$ are monic, so is $\mathbf{res}_y(\widehat{g},\widehat{h})$, therefore if $f = \mathbf{res}_y(g,h) = u\cdot\mathbf{res}_y(\widehat{g},\widehat{h})$, then $u = f_n$ and $\widehat{f} = \mathbf{res}_y(\widehat{g},\widehat{h})$.

Conversely, if $\widehat{f} = \mathbf{res}_y(\widehat{g},\widehat{h})$, then $uf = f_n\mathbf{res}_y(g,h)$. Remove common factors to get $vf = w\cdot\mathbf{res}_y(g,h)$, where $v,w \in K[z]$ are relatively prime. Now f has no factor in $K[z]$, so w is a unit. Likewise, if v were of nonzero degree, then it would have a root $a \in K$, and $\mathbf{res}_y(g(x,y),h(y,a))$ would vanish identically. But this can happen only in degenerate cases in which one of g,h does not depend on one of its variables, contrary to assumption. Therefore v is also a unit. □

3 A Characterization of All Decompositions

In this section we give a characterization of all possible irreducible decompositions of an algebraic function that can arise. We assume that K is algebraically closed.

Let γ be transcendental over K. We work in a fixed algebraic closure Ω of $K(\gamma)$. Let α be a nonconstant algebraic function of γ with monic minimum polynomial $f(x,\gamma) \in K(\gamma)[x]$ of degree n. By results of the previous section, the functional decomposition problem reduces to the problem of finding all monic irreducible decompositions of the form

$$\begin{aligned} f(x,\gamma)^k &= \mathbf{res}_y(g(x,y), h(y,\gamma)) \\ &= \prod_{h(\beta,\gamma)=0} g(x,\beta)\ . \end{aligned}$$

Let A be the set of conjugates of α over $K(\gamma)$, $|A| = n$. Let **Sym** A denote the field symmetric functions of A. This is the smallest field containing all the coefficients of $f(x,\gamma)$. Note that **Sym** A properly contains K, for otherwise $f(x,\gamma)$ would factor into linear factors since K is algebraically closed, contradicting the assumption that α is nonconstant.

Now consider the following condition on algebraic functions β of γ:

Condition 2 *The minimum polynomial $g(x,\beta)$ of α over $K(\beta)$ divides $f(x,\gamma)$.*

If β is algebraic over $K(\gamma)$, then g exists, since α is algebraic over $K(\gamma)$ and γ is algebraic over $K(\beta)$. A subtle but important point to note is that Condition 2 does not imply that $f(x,\gamma)$ factors over $K(\beta)$. Indeed, $K(\beta)$ need not contain the coefficients of f or f/g. We give an example of this in Section 5. The following theorem states that any β satisfying Condition 2 uniquely determines a monic irreducible decomposition of α; moreover, all monic irreducible decompositions of α arise in this way.

Theorem 3 *Let α be an algebraic function of γ with monic minimal polynomial $f(x,\gamma) \in K(\gamma)[x]$ of degree n. Let β be algebraic over $K(\gamma)$ with monic minimal polynomial $h(y,\gamma) \in K(\gamma)[y]$ of degree ℓ. Let $g(x,\beta) \in K(\beta)[x]$ of degree m be the monic minimal polynomial of α over $K(\beta)$. If β satisfies Condition 2, i.e. if $g(x,\beta)$ divides $f(x,\gamma)$, then*

$$f(x,z)^{\frac{\ell m}{n}} = \mathbf{res}_y(g(x,y), h(y,z))$$

is a monic irreducible decomposition of α. Moreover, all monic irreducible decompositions of α arise in this way.

Proof. Let $B = B_\beta \subseteq A$ be the set of roots of $g(x,\beta)$. If η is a conjugate of β over $K(\gamma)$, let B_η be the set of roots of $g(x,\eta)$. The set B_η is the image of B under any Galois automorphism over $K(\gamma)$ mapping β to η. For any such conjugate η, $|B_\eta| = |B| = m$ and $B_\eta \subseteq A$, since the Galois group over $K(\gamma)$ preserves A setwise.

By the symmetry of the action of the Galois group on A, each $\delta \in A$ occurs in the same number of the B_η, say k. We determine k by counting in two ways the number of pairs (δ,η) such that $\delta \in B_\eta$. First, it is the number of conjugates η of β times the size of each B_η, or ℓm. Second, it is the number of $\delta \in A$ times the number of B_η containing δ, or nk. Equating

these two values gives $k = \ell m/n$, the exponent in the statement of the theorem. Moreover, it follows from the same argument that

$$\begin{aligned} f(x,\gamma)^k &= \prod_{\delta \in A} (x-\delta)^k \\ &= \prod_{h(\eta,\gamma)=0} \prod_{\delta \in B_\eta} (x-\delta) \\ &= \prod_{h(\eta,\gamma)=0} g(x,\eta) \\ &= \mathbf{res}_y(g(x,y), h(y,\gamma)) \ . \end{aligned}$$

Since γ is transcendental over K, we might as well replace it with the indeterminate z to get

$$f(x,z)^k = \mathbf{res}_y(g(x,y), h(y,z)) \ .$$

The decomposition is monic and irreducible by definition.

Now we show that every monic irreducible decomposition of α arises in this way. Suppose

$$f(x,z)^k = \mathbf{res}_y(g(x,y), h(y,z))$$

is such a decomposition. Let β be a common root of $g(\alpha, y)$ and $h(y,\gamma)$. Such a β exists, since $f(\alpha,\gamma)$ vanishes, hence so does the resultant $\mathbf{res}_y(g(\alpha,y), h(y,\gamma))$. Then β is algebraic over $K(\gamma)$ with minimum polynomial $h(y,\gamma)$, $g(x,\beta)$ is the minimum polynomial of α over $K(\beta)$, and

$$\begin{aligned} f(x,\gamma)^k &= \mathbf{res}_y(g(x,y), h(y,\gamma)) \\ &= \prod_{h(\eta,\gamma)=0} g(x,\eta) \ . \end{aligned}$$

Since $g(x,\beta)$ is one of the factors in the product, it divides $f(x,\gamma)$. □

At this juncture we make a few observations about minimal decompositions and uniqueness.

Minimal decompositions There may exist β of arbitrarily high degree over $K(\gamma)$ satisfying Condition 2. For example, for any k, $\beta = \sqrt[k]{\gamma}$ gives the decomposition

$$(x-z)^k = \mathbf{res}_y(x - y^k, y^k - z) \ .$$

This is also the situation with (2) above. However, we can bound the search as follows. Observe that if there exists a β satisfying Condition 2 with factor $g(x,\beta)$ of f, say with roots $B \subseteq A$, then α will have the same degree over any subfield of $K(\beta)$ containing the coefficients of g. Furthermore, any such subfield is again a purely transcendental extension of K by Lüroth's Theorem (see [10, 14]), so a transcendental generator of that subfield would give a decomposition with the same g and smaller degree h and smaller k. For a given g, the degree of h and exponent k are minimized by taking the smallest subfield containing the coefficients of g, namely $\mathbf{Sym}\ B$.

Nontrivial decompositions If the minimum polynomial $g(x,\beta)$ of α over $K(\beta)$ is f (as would occur in the case $\beta = \gamma$), then the minimal decomposition with this g occurs when β is a transcendental generator of **Sym** A. Since **Sym** $A \subseteq K(\gamma)$, β would be a rational function of γ and h would be linear of the form $y - u(\gamma)$, $u \in K(z)$, giving the decomposition

$$\begin{aligned} f(x,z) &= \mathbf{res}_y(g(x,y), y - u(z)) \\ &= g(x,u(z)) \ . \end{aligned}$$

In this case α is the composition of an algebraic function and a rational function.

In case $g(x,\beta)$ is linear, say $g = x - v(\beta)$, the smallest field containing the coefficients of g is $K(v(\beta))$, so by using $v(\beta)$ instead of β we would obtain the trivial decomposition

$$\begin{aligned} f(x,z) &= \mathbf{res}_y(x - y, h(y,z)) \\ &= h(x,z) \ . \end{aligned}$$

To find a nontrivial decomposition, we must find a β such that $K(\beta)$ does not contain α.

Uniqueness up to linear composition factors The decomposition determined by β essentially depends only on the field $K(\beta)$, not on the choice of transcendental generator β. Any other transcendental generator of $K(\beta)$ is related to β by a nonsingular fractional linear transformation

$$\beta \ \mapsto \ \frac{a\beta + b}{c\beta + d} \ , \quad ad - bc \neq 0 \ ,$$

which extends to an automorphism of $K(\beta)$. Any two decompositions defined with respect to two transcendental generators of the same field are equivalent up to invertible composition factors of the form $(cz + d)y - (az + b)$.

One can see from the above observations that up to fractional linear transformations, there are only finitely many minimal irreducible monic decompositions, at most one for each subset of A. We have thus reduced the decomposition problem to the problem of finding a subset $B \subseteq A$ such that the field **Sym** B is a purely transcendental extension of K, and then finding a transcendental generator β of **Sym** B. Such a β is automatically algebraic over $K(\gamma)$, since **Sym** $B \subseteq K(A)$, the splitting field of f over $K(\gamma)$.

The problem of determining whether a given field extension $K(\alpha_1, \ldots, \alpha_n)$ is a purely transcendental extension is essentially the problem of determining the genus of algebraic function fields. We discuss these issues in the next section.

4 An Algorithm

As determined in the previous section, the key question in decomposing an irreducible polynomial f is determining whether f has a factor g whose coefficients lie in a purely transcendental extension of K. Equivalently, we want to know when the field **Sym** B of symmetric functions in the roots B of g is isomorphic to a rational function field over K, *i.e.* is of genus zero. We outline our approach in the following procedure.

1. Let $K(\gamma, \eta)$ be a finite extension of $K(\gamma)$ over which f factors, and let g be one of the monic irreducible factors. The coefficients of g all lie in $K(\gamma, \eta)$, so g can be written

$$g(x, \eta, \gamma) = x^m + u_{m-1}(\eta, \gamma)x^{m-1} + \cdots + u_0(\eta, \gamma) .$$

   For each such g, perform steps 2 and 3.

2. Let u be one of the coefficients u_i of g not in K. Construct the field $K(u_0, \ldots, u_{m-1})$. This is the field **Sym** B, where B is the set of roots of g. We have two cases:

   (a) If $K(u_0, \ldots, u_{m-1}) = K(u)$, we are done: u is a transcendental generator of **Sym** B.

   (b) If $K(u_0, \ldots, u_{m-1}) \neq K(u)$, construct a primitive element θ of the extension such that $K(u_0, \ldots, u_{m-1}) = K(u, \theta)$. Compute the genus of $K(u, \theta)$ by the Hurwitz genus formula or in some other fashion. An efficient algorithm is given in [3]. If the genus is nonzero, then no decomposition arises from this factor of f. If the genus is zero, compute a rational generator β of $K(u, \theta)$. Coates [4], Trager [9], and Huang and Ierardi [6] give efficient algorithms for computing rational generators. The coefficients of g can then be written as rational functions of β.

3. Let $h(y, \gamma)$ be the minimal polynomial of β over $K(\gamma)$. Return $g(x, y)$ and $h(y, z)$ as the decomposition factors.

Under suitable assumptions about the complexity of operations in K, the complexity of the algorithm as given above is exponential in the worst case, since there are an exponentially many potential factors. For each such factor, the computation for that factor can be performed in polynomial time in the size of the representation of the algebraic numbers needed to express the result, or exponential time in the bit complexity model [6].

5 An Example

The following gives an example of a decomposition involving a β such that $g(x, \beta)$ divides $f(x, \gamma)$, but $f(x, \gamma)$ does not factor over $K(\beta)$. Consider the polynomial

$$f(x, z) = x^4 - zx^2(x + 1) + z^3(x + 1)^2 .$$

Let γ be transcendental over K, and let

$$\begin{aligned} \beta &= \frac{\gamma(1 + \sqrt{1 - 4\gamma})}{2} \\ \eta &= \frac{\gamma(1 - \sqrt{1 - 4\gamma})}{2} \\ g(x, y) &= x^2 - y(x + 1) \\ h(y, z) &= y^2 - zy + z^3 . \end{aligned}$$

Then β and η are conjugates over $K(\gamma)$ with minimum polynomial $h(y,\gamma)$, and

$$f(x,\gamma) \;=\; g(x,\beta)\cdot g(x,\eta)\;,$$

thus Theorem 3 says that g and h should give a decomposition of f. Indeed,

$$\mathbf{res}_y(g(x,y),h(y,z)) \;=\; \begin{vmatrix} -(x+1) & 0 & 1 \\ x^2 & -(x+1) & -z \\ 0 & x^2 & z^3 \end{vmatrix} \;=\; f(x,z)\;.$$

To show $f(x,\gamma)$ does not factor over $K(\beta)$, it suffices to show that its trace γ is not in $K(\beta)$. But γ is a root of the irreducible polynomial $h(\beta,z)$, therefore is algebraic of degree three over $K(\beta)$.

Acknowledgements

We thank John Little, Paul Pedersen, Moss Sweedler and Barry Trager for their help.

This work was supported by the U.S. Army Research Office through the ACSyAM branch of the Mathematical Sciences Institute of Cornell University under contract DAAL03-91-C-0027, the National Science Foundation under grants CCR-9204630 and CCR-8806096, and the Advanced Research Projects Agency of the Department of Defense under Office of Naval Research grant N00014-92-J-1989. This work was performed while the second author was visiting the Cornell University Computer Science Department.

References

[1] V. S. Alagar and M. Thanh, *Fast polynomial decomposition algorithms*, in Proc. EUROCAL85, Springer-Verlag Lect. Notes in Comput. Sci. 204, 1985, pp. 150–153.

[2] D. R. Barton and R. E. Zippel, *Polynomial decomposition algorithms*, J. Symb. Comp., 1 (1985), pp. 159–168.

[3] G. A. Bliss, *Algebraic Functions*, Amer. Math. Soc., 1933.

[4] J. Coates, *Construction of rational functions on a curve*, Proc. Camb. Phil. Soc., 68 (1970), pp. 105–123.

[5] M. Dickerson, *Polynomial decomposition algorithms for multivariate polynomials*, Tech. Rep. TR87-826, Comput. Sci., Cornell Univ., April 1987.

[6] M.-D. Huang and D. Ierardi, *Efficient algorithms for the effective Riemann-Roch problem and for addition in the Jacobian of a curve*, in Proc. 32nd Symp. Found. Comput. Sci., IEEE, November 1991.

[7] D. Ierardi and D. Kozen, *Parallel resultant computation*, in Synthesis of Parallel Algorithms, J. Reif, ed., Morgan Kaufmann, 1993, pp. 679–720.

[8] D. Kozen and S. Landau, *Polynomial decomposition algorithms*, J. Symb. Comput., 7 (1989), pp. 445–456.

[9] B. M. TRAGER, *Integration of Algebraic Functions*, PhD thesis, Massachusetts Institute of Technology, Cambridge, MA, September 1984.

[10] B. L. VAN DER WAERDEN, *Algebra*, vol. 1, Frederick Ungar, fifth ed., 1970.

[11] J. VON ZUR GATHEN, *Functional decomposition of polynomials: the tame case*, J. Symb. Comput., 9 (1990), pp. 281–299.

[12] ——, *Functional decomposition of polynomials: the wild case*, J. Symb. Comput., 10 (1990), pp. 437–452.

[13] R. E. ZIPPEL, *Rational function decomposition*, in International Symposium on Symbolic and Algebraic Computation, S. Watt, ed., New York, July 1991, ACM, pp. 1–6.

[14] ——, *Effective Polynomial Computation*, Kluwer Academic Press, Boston, 1993.