Functional Decomposition of Symbolic Polynomials

Stephen M. Watt
Ontario Research Centre for Computer Algebra
Department of Computer Science, University of Western Ontario
London Ontario, CANADA N6A 5B7
watt@uwo.ca

Abstract

Earlier work has presented algorithms to factor and compute GCDs of symbolic Laurent polynomials, that is multivariate polynomials whose exponents are themselves integer-valued polynomials. This article extends the notion of univariate polynomial decomposition to symbolic polynomials and presents an algorithm to compute these decompositions. For example, the symbolic polynomial $f(X) = 2X^{n^2+n} - 4X^{n^2} + 2X^{n^2-n} + 1$ *can be decomposed as* $f = g \circ h$ *where* $g(X) = 2X^2 + 1$ *and* $h(X) = X^{n^2/2+n/2} - X^{n^2/2-n/2}$.

1. Introduction

It often arises that the general form of a polynomial is known, but the particular values for the exponents are unknown. For example, we may know a polynomial is of the form $3X^{n^2+1} - X^{2n} + 2$, where n is an integer-valued parameter. We call this a “symbolic polynomial”—a notion we define more precisely later—and ask what computations we can perform on such values.

Computer algebra systems are very good at performing arithmetic in particular algebraic domains, such as polynomials with coefficients from a particular ring or matrices of a given size with elements from a known ring. They do not do very well in other settings, however, when certain quantities are not known in advance. For example, when the coefficient ring, the dimension of a matrix or the degree of a polynomial is not known. In this case, a person can perform arithmetic by hand where a computer algebra system will abandon knowledge of algebraic algorithms and fall back on general term-rewriting techniques. It is a significant gap in the field of symbolic mathematical computation that algorithms for polynomials or matrices with symbolic degrees or sizes remain largely unexplored.

In the current work, we show how the notion of polynomial decomposition may be extended to symbolic polynomials and how such decompositions may be computed.

In earlier work we have observed that there is an important gap between the current worlds of computer algebra and symbolic computation [23]. We have shown that under certain conditions symbolic polynomials form a unique factorization domain and have given algorithms to compute their factorizations and GCDs [23, 25]. We have explored the question of how t make these algorithms more efficient when the exponents of the symbolic polynomials are themselves sparse [12, 13, 24]. In related work, we have examined how to perform arithmetic on matrices with blocks of symbolic size [21]. We are interested in results that are valid for all values of the symbolic parameters, *e.g.* for all values of n. This notion of symbolic polynomial is related to exponential polynomials [3, 5, 6, 19, 20] and to parametric families of polynomials [16, 27, 28].

This paper is organized as follows: Section 2 gives the preliminaries necessary to phrase our problem precisely. Section 3 then states the decomposition problem. Sections 4 and 5 provide the necessary theory on which symbolic polynomial decomposition depends. Section 4 gives theorems about the existence and uniqueness of symbolic polynomial composition and Section 5 shows that complete decompositions exist, the form they must take and how different decompositions must be related. Section 6 presents our algorithm for finding symbolic polynomial decompositions and Section 7 concludes the paper.

2. Preliminaries

Our model of symbolic polynomials is one where exponents are expressed as integer-valued functions of parameters. We model the exponents using integer-valued polynomials. It would be possible to model exponents using a larger class of functions, but integer-valued polynomials have been sufficient for our purposes.

In this section, present the notion of integer-valued polynomials and define symbolic polynomials in terms of them. We also present some basic facts that are used later in the article.

Integer-Valued Polynomials

Definition 1 (Integer-valued polynomial)**.** For an integral domain D with quotient field K, the (univariate) integer-valued polynomials over D, denoted $\mathrm{Int}(D)$, are defined as

$$\mathrm{Int}(D) = \{f \mid f \in K[X] \text{ and } f(a) \in D, \text{ for all } a \in D\}.$$

For example, $\frac{1}{2}n^2 - \frac{1}{2}n \in \mathrm{Int}(\mathbb{Z})$ because if $n \in \mathbb{Z}$, either n or $n-1$ is even. Integer-valued polynomials have been studied for many years, with classic papers dating back 90 years [14, 17]. We make the obvious generalization to multivariate polynomials.

Definition 2 (Multivariate integer-valued polynomial)**.** For an integral domain D with quotient field K, the (multivariate) integer-valued polynomials over D in variables $X_1, \ldots, X_n$, denoted $\mathrm{Int}_{[X_1,\ldots,X_n]}(D)$, are defined as

$$\begin{aligned}&\mathrm{Int}_{[X_1,\ldots,X_n]}(D) = \\ &\{f \mid f \in K[X_1, \ldots, X_n] \text{ and } f(a) \in D, \text{ for all } a \in D^n\}.\end{aligned}$$

For consistency we will use the notation $\mathrm{Int}_{[X]}(D)$ for univariate integer-valued polynomials.

If a polynomial is integer-valued, then there may be a non-trivial common divisor of all its integer evaluations.

Definition 3 (Fixed divisor)**.** A fixed divisor of an integer-valued polynomial $f \in \mathrm{Int}(D)$ is a value $q \in D$ such that $q|f(a)$ for all $a \in D$. When D is totally ordered, the largest fixed divisor is called *the* fixed divisor.

When written in the binomial basis, integer-valued polynomials have the following useful property:

Property 1. *If $f \in \mathrm{Int}_{[n_1,\ldots,n_p]}(\mathbb{Z}) \subset \mathbb{Q}[n_1, \ldots n_p]$, then when f is written using basis elements $\binom{n_1}{i_1} \cdots \binom{n_p}{i_p}$ its coefficients are integers.*

The following result tells how to compute the largest fixed divisor of a multivariate integer-valued polynomial.

Property 2. *If $f \in \mathrm{Int}_{[n_1,\ldots,n_p]}(\mathbb{Z})$, then the fixed divisor of f may be computed as the* gcd *of the coefficients of f when written in the binomial basis.*

Symbolic Polynomials

Definition 4 (Symbolic polynomial)**.** The ring of symbolic polynomials in $X_1, ..., X_v$ with exponents in $n_1, ..., n_p$ over the coefficient ring R is the ring consisting of finite sums of the form

$$\sum_i c_i X_1^{e_{i1}} X_2^{e_{i2}} \cdots X_n^{e_{in}}$$

where $c_i \in R$ and $e_{ij} \in \mathrm{Int}_{[n_1,n_2,\ldots,n_p]}(\mathbb{Z})$. Multiplication is defined by

$$bX_1^{e_1} \cdots X_n^{e_n} \times cX_1^{f_1} \cdots X_n^{f_n} = bc\, X_1^{e_1+f_1} \cdots X_n^{e_n+f_n}.$$

We denote this ring $R[n_1, ..., n_p; X_1, ..., X_v]$.

Symbolic polynomials are isomorphic to the group ring $R[\left(\mathrm{Int}_{[n_1,\ldots,n_p]}(\mathbb{Z})\right)^v]$, taking $\mathrm{Int}_{[n_1,\ldots n_p]}(\mathbb{Z})$ as an abelian group under addition and making the identification

$$X_1{}^{e_1} X_2{}^{e_2} \cdots X_v{}^{e_v} \cong (e_1, \ldots, e_v) \in \left(\mathrm{Int}_{[n_1,\ldots,n_p]}(\mathbb{Z})\right)^v$$

We note that

$$R[; X_1, ..., X_v] \cong R[X_1, ..., X_v, X_1^{-1}, ..., X_v^{-1}].$$

Definition 5 (Base variables, Exponent variables)**.** In the ring of symbolic polynomials $R[n_1, ..., n_p; X_1, ..., X_v]$, we call $X_1, ..., X_v$ the base variables and $n_1, ..., n_p$ the exponent variables.

In a ring of symbolic polynomials, the sets of base and exponent variables need not be disjoint. Indeed, when considering differentiation of symbolic polynomials it is useful to have the exponent variables to be a subset of the base variables.

It is possible to define symbolic polynomials somewhat more generally, with integer-valued polynomials also as exponents on the coefficients in R, as discussed elsewhere [23, 25]. We call these *extended symbolic polynomials*, but do not consider them in this article.

Evaluation Homomorphisms

We may evaluate any of the n_i at integer values. Such a map evaluates $R[n_1, ..., n_p; X_1, ..., X_v] \to R[n_1, ..., n_{i-1}, n_{i+1}, ..., n_p; X_1, ..., X_v](\mathbb{Z})$ as a ring homomorphism. A set of evaluation maps for $\{n_{i_1}, ..., n_{i_k}\}$ with distinct $i_1, ..., i_k$ is associative and commutative. We may therefore apply a set of evaluations at once, without regard to the order in which the variables are evaluated.

All exponent variables may be evaluated to give

$$\phi : R[n_1, ..., n_p; X_1, ..., X_v] \to R[X_1, ..., X_v, X_1^{-1}, ..., X_v^{-1}].$$

That is, ϕ evaluates symbolic polynomials to Laurent polynomials. It would be possible to construct a model for symbolic polynomials that under evaluation had no negative variable exponents. That would, however, require keeping track of cumbersome domain restrictions on the exponent variables.

Algebraic Structure

By definition, symbolic polynomials have a ring structure and algorithms to add and multiply them can be obtained straightforwardly from the definition. Symbolic polynomials also have a useful multiplicative structure.

Theorem 1 (Symbolic polynomial unique factorization)**.** *The ring $R[n_1, ...n_p; X_1, ...X_v]$ is a UFD if and only if the ring $R[X_1, ..., X_k]$ is a UFD.*

In previous articles [23, 25] we have shown how to compute GCDs and factorizations of symbolic polynomials. These algorithms fall into two families: *extension methods*, based on the algebraic independence of variables to different monomial powers (*e.g.* x, x^n, x^{n^2},...), and *homomorphism methods*, based on the evaluation and interpolation of exponent polynomials.

Both these methods become costly if multivariate exponent polynomials are treated as dense [12, 13]. This was a problem in particular for extension methods because the first algorithms converted exponent polynomials to a binomial basis to handle fixed divisors, thus making exponent polynomials dense. A transformation for efficient sparse exponents eliminates this problem [24].

Theorem 2 (Integer exponent coefficients)**.** *If* $f \in R[n_1, ..., n_p; X_1, ..., X_v]$ *with exponents in* $\mathrm{Int}_{[n_1,...,n_p]}(\mathbb{Z})$, *then the substitution* $\sigma : X_i \mapsto X_i^{d!^p}$ *gives* $\sigma f \in R[n_1, ..., n_p; X_1, ..., X_v]$ *with exponents in* $\mathbb{Z}[n_1, ...n_p]$.

3. The Problem

Polynomial Decomposition

If a univariate polynomial is regarded as a function of its variable, then we may ask whether the polynomial is the composition of two polynomial functions of lower degree. This can be useful in simplifying expressions, solving polynomial equations exactly or determining the dimension of a system. Polynomial decomposition has been studied for quite some time, with early work by Ritt and others [1, 2, 10, 18]. Algorithms for polynomial decomposition have been proposed and refined for use in computer algebra systems.

The univariate polynomial decomposition problem may be stated as:

Problem 1. *Let* $f \in R[X]$. *Determine whether there exist two polynomials* $g, h \in R[X]$ *of degrees greater than 1 such that* $f(X) = g(h(X))$ *and, if so, find them.*

If g and h are further decomposed, then we may find $f = g_1 \circ \cdots \circ g_k$. Ritt showed that (over a field of characteristic zero) this full decomposition is unique up to the equivalences $X^m \circ X^n = X^n \circ X^m$ and $T_n \circ T_m = T_m \circ T_n$, where $T_n(X)$ is the Chebyshev polynomial $\cos(n \arccos X)$.

Generalizations of this problem include decomposition of multivariate polynomials [4, 22], rational functions [30], algebraic functions [11] and Laurent polynomials [15, 29]. The relationship between polynomial composition and polynomial systems has also been studied [7, 8, 9]. Here we generalize the problem to the decomposition of symbolic polynomials.

Symbolic Polynomial Decomposition

Unlike polynomial rings, symbolic polynomial rings are not closed under functional composition. For example, if $g(X) = X^n$ and $h(X) = X + 1$ then $g(h(X)) = \sum_{i=0}^{n} \binom{n}{i} X^i$ cannot be expressed in finite terms of group ring operations. We therefore make the following definition.

Definition 6 (Univariate composition of symbolic polynomials)**.** Let $g, h \in R[n_1, ..., n_p; X]$. A composition of g and h is a finite sum $f = \sum_i f_i X^{e_i} \in R[n_1, ..., n_p; X]$ such that under all evaluation maps, $\phi : \{n_1, ..., n_p\} \to \mathbb{Z}$, $\phi f = \phi g \circ \phi h$.

For brevity, we make the use the following definition.

Definition 7 (Trivial symbolic polynomial)**.** A symbolic polynomial $f \in R[n_1, ..., n_p; X]$ is trivial if $f = c_1 X + c_0 \in R[X]$ or $f = c_{-1} X^{-1} \in R[X, X^{-1}]$.

We may now state the problems we wish to solve. First we have the basic question.

Problem 2. *Let* $f \in \mathcal{P} = R[n_1, \ldots, n_p; X]$. *Determine whether there exist two non-trivial symbolic polynomials* $g, h \in \mathcal{P}$ *such that* $f(X) = g(h(X))$ *and, if so, find such a pair.*

More generally, we have:

Problem 3. *Let* $f \in \mathcal{P} = R[n_1, \ldots, n_p; X]$. *Determine whether there exist* T *non-trivial indecomposable symbolic polynomials* $g_1, \ldots, g_T \in \mathcal{P}$ *such that* $f = g_1 \circ \cdots \circ g_T$ *and, if so, find such a decomposition.*

Can there be more than one such decomposition? We ask:

Problem 4. *Determine what forms can decompositions* $f = g_1 \circ \cdots \circ g_T$ *can take.*

This article answers these questions.

4. Composition Theorems

We now present theorems on the uniqueness and existence of symbolic polynomial compositions. We first show uniqueness.

Theorem 3 (Composition uniqueness)**.** *If a composition of two symbolic polynomials exists, then it is unique.*

Proof. Let $g, h \in R[n_1, ..., n_p; X]$. Suppose there are two compositions p and q of g and h. Then, under any evaluation map ϕ for $n_1, ..., n_p$, we must have $\phi p = \phi q$. Since the exponents of p are all distinct polynomials in $\mathbb{Q}[n_1, ..., n_p]$, and likewise for the exponents of q, we may find an infinite number of evaluations which keep all exponents of p

distinct and all exponents of q distinct. As there are only a finite number of ways to put the terms of p into correspondence with the terms of q, this means there is at least one correspondence of terms for which the exponents agree on an unbounded number of distinct evaluations for each variable n_i. Since the exponents are polynomials of fixed degree this implies there is a correspondence equating the terms of p and terms of q, and hence $p = q$. □

We denote this unique composition, if it exists, as $g \circ h$ or $g(h(X))$.

We now restrict our attention to the case where the coefficient ring is the field of complex numbers. This allows the case where roots of unity are required and avoids technicalities arising when the characteristic of the coefficient field divides the degree of g. This so-called "wild" case is less important with symbolic polynomials because degrees are not always fixed values.

Theorem 4 (Composition existence)**.**
Let

$$g(X) = \sum_{i=1}^{R} g_i X^{p_i} \qquad h(X) = \sum_{i=1}^{S} h_i X^{q_i}$$

be symbolic polynomials in $\mathcal{P} = \mathbb{C}[n_1, ..., n_p; X]$*, with* $g_i \neq 0$*,* $h_i \neq 0$*, and with the* p_i *all distinct and the* q_i *all distinct. The functional composition* $g(h(X))$ *exists in* $\mathcal{P}$ *if and only if at least one of the following conditions hold:*

Condition 1. *h is a monomial and $g \in \mathbb{C}[X, X^{-1}]$,*

Condition 2. *h is a monomial with coefficient h_1 a d^{th} root of unity, where d is a fixed divisor of all p_i,*

Condition 3. $g \in \mathbb{C}[X]$.

Proof.

If any of the conditions hold, then $g(h(X)) \in \mathcal{P}$ $(\Rightarrow)$

If Condition 1 holds, then

$$g(h(X)) = \sum_{i=1}^{R} g_i (h_1 X^{q_1})^{p_i} = \sum_{i=1}^{R} g_i h_1^{p_i} X^{q_1 + p_i}$$

Since $p_i \in \mathbb{Z}$, we have $h_1^{p_i} \in \mathbb{C}$ and $g(h(X)) \in \mathbb{C}[n_1, ..., n_p; X]$.
If Condition 2 holds, then there is a $d \in \mathbb{Z}$ such that $h_1^d = 1$ and $p_i = dp_i'$ for some $p_i' \in \text{Int}_{[n_1,...,n_p]}(\mathbb{Z})$. We then have

$$g(h(X)) = \sum_{i=1}^{R} g_i \left(h_1 X^{q_1}\right)^{p_i} = \sum_{i=1}^{R} g_i \left(h_1^d\right)^{p_i'} X^{q_1 + p_i}$$
$$= \sum_{i=1}^{R} g_i X^{q_1 + p_i} \in \mathbb{C}[n_1, ..., n_p; X].$$

If Condition 3 holds, then

$$g(h(x)) = \sum_{i=1}^{R} g_i \left(\sum_{j=1}^{S} h_j X^{q_j} \right)^{p_i}$$
$$= \sum_{i=1}^{R} g_i \sum_{j_1 + \cdots + j_S = 0}^{p_i} \binom{p_i}{j_1, ..., j_S} (h_1 X^{q_1})^{j_1} \cdots (h_S X^{q_S})^{j_S}$$
$$= \sum_{i=1}^{R} \sum_{j_1 + \cdots + j_S = 0}^{p_i} \left(g_i \binom{p_i}{j_1, ..., j_S} \prod_{k=1}^{S} h_k^{j_k} \right) X^{\sum_{k=1}^{S} j_k q_k}.$$

Because each $p_i \in \mathbb{N}_0$, this is a finite sum with coefficients in $\mathbb{C}$ and powers of X in $\text{Int}_{[n_1,...,n_p]}(\mathbb{Z})$. Therefore $g(h(X)) \in \mathbb{C}[n_1, ..., n_p; X]$.

If $g(h(X)) \in \mathcal{P}$, then one of the conditions must hold $(\Leftarrow)$

We consider three disjoint and exhaustive cases:

- Case A, where h is a monomial,
- Case B, where h is not a monomial and asymptotically all $p_i \geq 0$,
- Case C, where h is not a monomial and asymptotically some $p_i < 0$.

Case A: h is a monomial

We have

$$g(h(x)) = g(h_1 X^{q_1}) = \sum_{i=1}^{R} g_i h_1^{p_i} X^{p_i + q_1}$$

If all $p_i \in \mathbb{Z}$, then $h_1^{p_i} \in \mathbb{C}$ and Condition 1 is satisfied. Otherwise there exists at least one i_0 for which $p_{i_0} \notin \mathbb{Z}$. Then p_{i_0} is a polynomial in $n_1, ..., n_p$ that takes on some number of distinct integer values, $m_1, m_2, ...$ We must have $h_1^{m_i} = h_1^{m_j}$ so so $h_1^{m_i - m_j} = 1$. Since $m_i \neq m_j$ if $i \neq j$, h_1 must be a root of unity. For each pair (i, j) there exist $q, r \in \mathbb{Z}, 0 \leq r < |m_j|$ such that $m_i = qm_j + r$ so $h_1^{m_i} = (h_1^{m_j})^q h_1^r = h_1^r = 1$. Repeating this gives $h_1^{\gcd(m_i, m_j)} = 1$ and we have shown h_1 must be a d^{th} root of unity for some fixed divisor d of p_{i_0}. Likewise h_1 must be a d_i^{th} root of unity for some fixed divisor d_i for each other p_i. Therefore Condition 2 is satisfied.

Case B: h not a monomial and asymptotically all $p_i \geq 0$

We assume that $g(h(X)) \in \mathcal{P}$ with some exponent $p_i \notin \mathbb{N}_0$ and show this leads to a contradiction and therefore that Condition 3 must hold.

We consider two sub-cases depending on whether q_1 is asymptotically positive or negative. In both cases, choose one of the variables n_i and call it n. Evaluate the other n_i at integer points that do not make p_i constant if it contains n. We show the contradiction with these univariate exponents.

Case B.1: $q_1 > 0$

We consider the case where all p_i and q_1 remain positive as n grows. In this case, there exists N_B such that for $n > N_B$ we have $p_i \geq 0, q_1 > 0$, all the p_i are distinct and retain their relative order and likewise for the q_i. Label the exponent polynomials such that $p_1 > p_2 > \cdots > p_R$ and $q_1 > q_2 > \cdots > q_R$.

We have

$$g(h(X)) = \sum_{i=1}^{R} g_i (\sum_{j=1}^{S} h_j X^{q_j})^{p_i}$$

Let

$$h(X) = h_1 X^{q_1} + h_2 X^{q_2} + \eta$$

where $\eta = h_3 X^{q_3} + \cdots + h_S X^{q_S}$.

Since $p_1 > p_2 \geq 0$, we may write binomial expansions of the terms $h(X)^{p_1}$ and $h(X)^{p_2}$.

$$\begin{aligned} g(h(X)) =& \sum_{i=1}^{R} g_i (h_1 X^{q_1} + h_2 X^{q_2} + \eta)^{p_i} \\ =& \;\; g_1 \bigg((h_1 X^{q_1})^{p_1} + p_1 (h_1 X^{q_1})^{p_1 - 1} (h_2 X^{q_2} + \eta) \\ & \qquad + \binom{p_1}{2} (h_1 X^{q_1})^{p_1 - 2} (h_2 X^{q_2} + \eta)^2 + L_1 \bigg) \\ & + g_2 \bigg((h_1 X^{q_1})^{p_2} + p_2 (h_1 X^{q_1})^{p_2 - 1} (h_2 X^{q_2} + \eta) \\ & \qquad + \binom{p_2}{2} (h_1 X^{q_1})^{p_2 - 2} (h_2 X^{q_2} + \eta)^2 + L_2 \bigg) \\ & + L_*, \end{aligned}$$

where one or more of η, L_1, L_2 and L_* may be zero. If $R = 1$ then the g_2 term and L_* are zero and the argument specializes.

Expanding the quadratic terms $(h_2 X^{q_2} + \eta)^2$, we have

$$\begin{aligned} & g(h(X)) = \\ & \quad g_1 h_1^{p_1} X^{A_1} \;+\; g_1 p_1 h_1^{p_1 - 1} h_2 X^{A_2} + g_1 p_1 h_1^{p_1 - 1} X^{A_3} \eta \\ & + g_1 \binom{p_1}{2} h_1^{p_1 - 2} h_2^2 X^{A_4} \\ & \qquad + 2 g_1 \binom{p_1}{2} h_1^{p_1 - 2} h_2 X^{A_5} \eta + g_1 \binom{p_1}{2} h_1^{p_1 - 2} X^{A_6} \eta^2 \\ & + g_1 L_1 \\ & + g_2 h_1^{p_2} X^{B_1} \;+\; g_2 p_2 h_1^{p_2 - 1} h_2 X^{B_2} + g_2 p_1 h_1^{p_2 - 1} X^{B_3} \eta \\ & + g_2 \binom{p_2}{2} h_1^{p_2 - 2} h_2^2 X^{B_4} \\ & \qquad + 2 g_2 \binom{p_2}{2} h_1^{p_2 - 2} h_2 X^{B_5} \eta + g_2 \binom{p_2}{2} h_1^{p_2 - 2} X^{B_6} \eta^2 \\ & + g_2 L_2 \\ & + L_* \end{aligned}$$

where

$$\begin{aligned} A_1 &= q_1 p_1 & B_1 &= q_1 p_2 \\ A_2 &= q_1 (p_1 - 1) + q_2 & B_2 &= q_1 (p_2 - 1) + q_2 \\ A_3 &= q_1 (p_1 - 1) & B_3 &= q_1 (p_2 - 1) \\ A_4 &= q_1 (p_1 - 2) + 2 q_2 & B_4 &= q_1 (p_2 - 2) + 2 q_2 \\ A_5 &= q_1 (p_1 - 2) + q_2 & B_5 &= q_1 (p_2 - 2) + q_2 \\ A_6 &= q_1 (p_1 - 2) & B_6 &= q_1 (p_2 - 2) \end{aligned}$$

We adopt the conventions $\mathbf{deg}\ 0 = -\infty$, $p_3 = -\infty$ if $R = 2$, and $q_3 = -\infty$ if $S = 2$. The argument can be made more precise by dividing into cases where various terms are zero, thereby avoiding degrees of $-\infty$. We then have

$$\begin{aligned} \mathbf{deg}\ L_1 &\leq q_1 (p_1 - 3) + 3 q_2 \\ \mathbf{deg}\ L_2 &\leq q_1 (p_2 - 3) + 3 q_2 \\ \mathbf{deg}\ L_* &\leq q_1 p_3 \\ \mathbf{deg}\ \eta &\leq q_3 \end{aligned}$$

with equality whenever the quantities are non-zero.

Examining the degrees of each term of our expansion, we observe that the terms with A_1 and A_2 are distinct from each other and from all the rest involving A_i, L_1 and L_*.

We have

$$\begin{aligned}
&A_1 > A_2 && \text{since } A_1 = q_1p_1 = q_1(p_1-1)+q_1\\
& && \qquad > q_1(p_1-1)+q_2 = A_2.\\
&A_2 > A_3 + \mathbf{deg}\,\eta && \text{since } A_2 = q_1(p_1-1)+q_2\\
& && \qquad > q_1(p_1-1)+q_3\\
& && \qquad = A_3 + \mathbf{deg}\,\eta.\\
&A_2 > A_4 && \text{since } A_2 = q_1(p_1-1)+q_2\\
& && \qquad = q_1(p_1-2)+q_1+q_2\\
& && \qquad > q_1(p_1-2)+2q_2 = A_4.\\
&A_4 > A_5 + \mathbf{deg}\,\eta && \text{since } A_4 = q_1(p_1-2)+2q_2\\
& && \qquad > q_1(p_1-2)+q_2+q_3\\
& && \qquad = A_5 + \mathbf{deg}\,\eta.\\
&A_5 + \mathbf{deg}\,\eta && \\
&\quad > A_6 + 2\mathbf{deg}\,\eta && \text{since } A_5 + \mathbf{deg}\,\eta\\
& && \qquad = q_1(p_1-2)+q_2+q_3\\
& && \qquad > q_1(p_1-2)+2q_3\\
& && \qquad = A_6 + 2\mathbf{deg}\,\eta\\
&A_2 > \mathbf{deg}\,L_1 && \text{since } A_2 = q_1(p_1-1)+q_2\\
& && \qquad = q_1(p_1-3)+2q_1+q_2\\
& && \qquad > q_1(p_1-3)+3q_2\\
& && \qquad \geq \mathbf{deg}\,L_1\\
&A_2 > \mathbf{deg}\,L_* && \text{since } A_2 = q_1(p_1-1)+q_2\\
& && \qquad > q_1(p_1-1)-q_1\\
& && \qquad = q_1(p_1-2)\\
& && \qquad \geq q_1p_3 \geq \mathbf{deg}\,L_*
\end{aligned}$$

In the last inequality we have used the fact that $p_i \geq p_{i+1}+1$ and $q_1 > 0$. Likewise, we observe that the terms with B_1 and B_2 are distinct from each other and from all the rest involving B_i, L_2 and L_*.

$$\begin{aligned}
B_1 >\,& B_2 > B_3 + \mathbf{deg}\,\eta\\
& B_2 > B_4 > B_5 + \mathbf{deg}\,\eta > B_6 + 2\mathbf{deg}\,\eta\\
& B_2 > \mathbf{deg}\,L_2\\
& B_2 > \mathbf{deg}\,L_*
\end{aligned}$$

The terms involving A_i and B_i are related by the inequalities

$$\begin{aligned}
&A_1 > B_1 && \text{since } A_1 = q_1p_1 > q_1p_2 = B_1,\\
&A_2 > B_2 && \text{since } A_2 = q_1(p_1-1)+q_2\\
& && \qquad > q_1(p_2-1)+q_2 = B_2.
\end{aligned}$$

The possible situations are:

$$\begin{aligned}
&A_1 > A_2 > B_1 \geq \text{all the rest involving } A_i, B_i, L_i, L_*,\\
&A_1 > B_1 = A_2 > \text{all the rest involving } A_i, B_i, L_i, L_*,\\
&A_1 > B_1 > A_2 > \text{all the rest involving } A_i, B_i, L_i, L_*.
\end{aligned}$$

If $A_2 \neq B_1$, we have

$$\begin{aligned}
g(h(X)) =& g_1h_1^{p_1}X^{p_1q_1} + g_1p_1h_1^{p_1-1}h_2X^{(p_1-1)q_1+q_2}\\
&+ \text{lower order terms.}
\end{aligned}$$

If $A_2 = B_1$, we have

$$\begin{aligned}
g(h(X)) =& g_1h_1^{p_1}X^{p_1q_1} + \big(g_1p_1h_1^{p_1-1}h_2 + g_2h_1^{p_2}\big)X^{q_1p_2}\\
&+ \text{lower order terms.}
\end{aligned}$$

In all situations p_1 appears in a coefficient so it must be constant. Since the p_i are integer-valued polynomials, and since $p_i \geq 0$, we now have that all p_i are non-negative integers, contradicting our hypothesis that at least one of them was non-constant. Therefore Condition 3 must be satisfied.

Case B.2: $q_1 \leq 0$

Let $q_i' = -q_i$ and $h'(X) = h(X^{-1})$. Then

$$h'(X) = h(X^{-1}) = \sum_{i=0}^{S} h_iX^{-q_i} = \sum_{i=0}^{S} h_iX^{q_i'}.$$

Note that $q_1 = 0 \geq q_2 + 1$ so $q_2 < 0$ and $q_2' > 0$. Relabeling the q_i' to reverse their order gives $g \circ h'$ satisfying the conditions of Case B.1. Therefore Condition 3 must be satisfied.

Case C: h not a monomial and asymptotically $\exists p_i < 0$

Again, label the p_i and q_i so that asymptotically $p_1 > p_2 > \cdots > p_R$ and $q_1 > q_2 > \cdots > q_S$. In this case not all of the p_i will be asymptotically non-negative. Let i_0 be the smallest i such that as $n \to \infty$ we have $p_i < 0$. There then exists a value N_C such that for all $n > N_C$ we have $p_i \geq 0$ for $i < i_0$ and $p_i < 0$ for $i \geq i_0$.

We may write

$$g(h(X)) = A + B, \text{ where}$$
$$A = \sum_{i=1}^{i_0-1} g_ih(X)^{p_i} \qquad B = \sum_{i=i_0}^{S} g_i\frac{1}{h(X)^{-p_i}}.$$

For $n > N_C$, the exponent polynomials p_i are non-negative in A and the $-p_i$ are non-negative in B. We may put the sum B over a common denominator.

$$g(h(X)) = \sum_{i=1}^{i_0-1} g_ih(X)^{p_i} \;+\; \frac{\sum_{i=i_0}^{S} g_i\prod_{\substack{j=i_0\\ j\neq i}}^{S} h(X)^{-p_j}}{\prod_{j=i_0}^{S} h(X)^{-p_j}}.$$

For each $n > N_C$, we have $A \in \mathbb{Z}[X]$ and $B \in \mathbb{Z}(X)$ with numerator degree strictly less than denominator degree. Since $h(X)$ is not a monomial and since the powers in the denominator of B are non-zero, the denominator of B will have poles other than at 0 and infinity. Therefore, for B to be a Laurent polynomial its numerator must be identically zero. To examine this case, let

$$\tilde{p}_i = \sum_{\substack{j=i_0 \\ j \neq i}}^{S} -p_j, \qquad \text{for } i \geq i_0.$$

Then the numerator of B is

$$\tilde{g}(h(X)) = \sum_{i=i_0}^{S} g_i h(X)^{\tilde{p}_i}$$

Note that all $\tilde{p}_i > 0$ for $n > N_C$. We have already shown that for $\tilde{g}(h(X))$ to exist in $\mathcal{P}$ under these conditions we must have $\tilde{g}(X) \in \mathbb{Z}[X]$. Therefore for to have $\tilde{g}(h(X)) = 0$ we must have $\tilde{g}(X) = 0$. That is, we must have $g_i = 0$ for $i \geq i_0$, contradicts the conditions regarding g.

Therefore there can be no compositions in $\mathcal{P}$ in Case C. □

5. Decomposition Theorems

A symbolic polynomial may be a composition in more than one way. We address the question of how such decompositions are related. We begin by introducing the notion of a complete decomposition.

Definition 8 (Decomposition, decomposition factor, complete and partial decomposition)**.** If $f = g_1 \circ \cdots \circ g_T$, $g_1, \ldots, g_t \in \mathcal{P} = R[n_1, ..., n_p; X]$, and no g_i is trivial unless $T = 1$, then the list $(g_1, \ldots, g_t)$ is a decomposition of f. Each of the g_i is a decomposition factor of f. If no $g_i = h_1 \circ h_2$ for non-trivial $h_1, h_2 \in \mathcal{P}$, then $(g_1, ..., g_T)$ is a complete decomposition and otherwise it is a partial decomposition.

We may write the list $(g_1, ..., g_T)$ as $g_1 \circ \cdots \circ g_T$ when no confusion will arise.

Theorem 5 (Decomposition shape)**.**
Let $f \in \mathcal{P} = \mathbb{C}[n_1, ..., n_p; X]$. Then any decomposition of f is of the form

$$f = p_1 \circ \cdots \circ p_N \circ S \circ U_1 \circ \cdots \circ U_M, \quad N \geq 0, M \geq 0,$$

where $p_i \in \mathbb{C}[X]$, $U_i = u_i X^{e_i} \in \mathcal{P}$ is a monomial whose coefficients must be certain roots of unity, either $S \in \mathcal{P}$ or $S = \ell \circ H$ where $\ell \in \mathbb{C}[X, X^{-1}]$ and $H = \alpha X^{\nu} \in \mathcal{P}$ is a monomial with no conditions on its coefficient.

Proof. By Theorem 4, f may be a composition in one of only three ways. The decomposition factors may themselves be decomposed only in the same ways, *etc*. Induction on the number of composition operators and associativity of functional composition gives the result. □

Theorem 6 (Complete decomposition existence)**.**
For every $f \in \mathcal{P} = \mathbb{C}[n_1, ..., n_p; X]$ there is a number N such that every decomposition of f has at most N decomposition factors.

Proof. If f is trivial or is not the composition of two non-trivial symbolic polynomials, then $f = g_1$ is a complete decomposition and $N = 1$. If f is non-trivial and $f = h_1 \circ h_2$ for non-trivial $h_1, h_2 \in \mathcal{P}$, it may be possible to decompose h_1 or h_2 further non-trivially and then to decompose the decomposition factors non-trivially, and so on. We show this process must terminate.

Choose an asymptotic ordering of terms, $\prec$, and let $\mathbf{deg}\, p$ and $\mathbf{ldeg}\, p$ be the exponents of the leading and trailing terms of p with respect to that order. Let $\mathbf{deg}\ f = ae_1 \times \cdots \times e_Q$ be the complete factorization of $\mathbf{deg}\ f$ in $\mathbb{Q}[n_1, ..., n_p]$ with $e_i = \tilde{e}_i / d_i$, where $\tilde{e}_i \in \mathbb{Z}[n_1, ..., n_p]$ is primitive and d_i is the fixed divisor of $\tilde{e}_i$. Then e_i is integer-valued with fixed divisor 1 and $a \in \mathbb{Z}$ because $\mathbf{deg}\ f$ is integer-valued. Let the factorization of a into integer primes be $a = u \times a_1 \times \cdots \times a_W$, with $u = \pm 1$. This means there can be at most $Q + W$ decomposition factors with $\mathbf{deg}$ other than ± 1. A similar bound exists for $\mathbf{ldeg}$.

It remains to show that there cannot be an unbounded number of composition factors with both $\mathbf{deg}$ and $\mathbf{ldeg}$ equal to ± 1. We have stipulated that none of the decomposition factors may be trivial, so if $\mathbf{deg}\ h_{ik} = 1$ then $\mathbf{ldeg}\, h_{ik} \leq -1$, and if $\mathbf{deg}\, h_{ik} = -1$ then $\mathbf{ldeg}\, h_{ik} \leq -2$. We can have a bounded number of decomposition factors not of the form $c_1 X + c_0 + c_{-1} X^{-1}$ with $c_1, c_{-1} \neq 0$ and by Theorem 5 we can have at most one of these. □

We now turn turn to the question of how distinct compositions can be related. From Theorem 5 we see that we will need to consider distinct decompositions of polynomials, of symbolic monomials and of a polynomial with a Laurent polynomial or indecomposable symbolic polynomial.

It has been well understood since the early work by Ritt how distinct polynomial decompositions are related: any complete decomposition of a polynomial in $\mathbb{C}[X]$ may be obtained from any other by use of the identities

$$\begin{aligned} (aX + b) \circ (1/aX - b/a) &= x \\ X^n \circ X^m\, p(X^n) &= X^m p(X)^n \circ X^n \\ T_n(X) \circ T_m(X) &= T_m(X) \circ T_n(X) \end{aligned}$$

where $p(X) \in \mathbb{C}[X]$ and T_n, T_m Chebyshev polynomials.

Decompositions involving a polynomial left decomposition factor and a Laurent polynomial left decomposition factor have been characterized by Zieve.

Theorem 7 (Zieve [29] 5.6)**.**
Let $g_1, g_2 \in \mathbb{C}[X]\backslash\mathbb{C}$ and $h_1, h_2 \in \mathbb{C}[X, X^{-1}]\backslash\mathbb{C}$ satisfy $g_1 \circ h_1 = g_2 \circ h_2$. Then, perhaps after switching (g_1, g_2) and (h_1, h_2), we have

$$\begin{aligned} g_1 &= G \circ G_1 \circ \mu_1 \\ g_2 &= G \circ G_2 \circ \mu_2 \\ h_1 &= \mu_1^{-1} \circ H_1 \circ H \\ h_2 &= \mu_2^{-1} \circ H_2 \circ H \end{aligned}$$

for some $G \in \mathbb{C}[X]$, some $H \in \mathbb{C}(X)$, and some linear $\mu_1, \mu_2 \in \mathbb{C}[X]$, where (G_1, G_2) satisfy one of

(1) $(X^n, X^r p(X)^n)$ *where* $0 \leq r < n$ *and* $\gcd(r, n) = 1$*;*

(2) $(X^2, (X^2 - 4)p(X)^2)$*;*

(3) $(D_m(X), D_n(X))$*;*

(4) $((X^2/3 - 1)^3, 3X^4 - 4X^3)$*;*

(5) $(D_{dm}(X), -D_{dn}(X))$*, where* $d > 1$

and (H_1, H_2) is the corresponding pair below:

(1) $(X^r p(X^n), X^n)$*;*

(2) $((X - 1/X)p(X + 1/X), X + 1/X)$*;*

(3) $(D_n(X), D_m(X))$*;*

(4) $(X^2 + 2X + \frac{1}{X} - \frac{1}{4X^2}, \frac{1}{3}((X + 1 - \frac{1}{2X})^3 + 4))$*;*

(5) $(X^n{+}1/X^n, (\zeta X)^m{+}1/(\zeta X)^m)$*, where* $\zeta^{dmn} = -1$.

Here $p(n) \in \mathbb{C}[X]$ and D_n is the Dickson polynomial defined by $D_n(x + 1/x) = x^n + 1/x^n$, related to the Chebychev polynomials via $D_n(x) = 2T_n(x/2)$. Cases 1 and 3 correspond to the polynomial setting and the others are new for Laurent polynomials.

We are now in a position to make a statement about the relationship between complete decompositions of symbolic polynomials.

Theorem 8 (Complete decomposition equivalence)**.**
Let $f \in \mathcal{P} = \mathbb{C}[n_1, ..., n_p; X]$ be a non-trivial symbolic polynomial. If f has two complete decompositions, they must be of the form

$$\begin{aligned} f &= p_1 \circ \cdots p_N \circ S \circ U_1 \circ \cdots \circ U_M \\ &= q_1 \circ \cdots q_N \circ R \circ V_1 \circ \cdots \circ V_M, \end{aligned}$$

with $N, M \geq 0$, $p_i, q_i \in \mathbb{C}[X]$ and $U_i, V_i \in \mathcal{P}$ monomials and one of the following conditions must hold:

Condition 1. *$S, R \in \mathbb{C}[X]$ and either decomposition may be obtained from the other by successive application of the identities*

$$\begin{aligned} (aX + b) \circ (1/aX - b/a) &= x \\ X^n \circ X^m\, p(X^n) &= X^m p(X)^n \circ X^n \\ D_n(X) \circ D_m(X) &= D_m(X) \circ D_n(X) \end{aligned} \tag{1}$$

between decomposition factors left of S or R and of the identity

$$(aX^s) \circ (bX^t) = ab^s X^{st} \tag{2}$$

between decomposition factors right of S or R;

Condition 2. *$S = S_1 \circ H$, $R = R_1 \circ H$, $S, S_1, R, R_1 \in \mathbb{C}[X, X^{-1}]\backslash\mathbb{C}[X]$, $H \in \mathbb{C}(X)$, and either decomposition may be obtained from the other by successive application of the identities (1) and*

$$\begin{aligned} & X^2 \circ (X - 1/X)p(X + 1/X) = \\ & \quad (X^2 - 4)p(X)^2 \circ (X + 1/X) \\ & (X^2/3 - 1)^3 \circ (X^2 + 2X + \frac{1}{X} - \frac{1}{4X^2}) \\ & \quad (3X^4 - 4X^3) \circ \frac{1}{3}((X + 1 - \frac{1}{2X})^3 + 4) \\ & (X^n + 1/X^n) \circ D_{dm}(X) = \\ & \quad (\zeta X)^m + 1/(\zeta X)^m) \circ -D_{dn}(X) \end{aligned} \tag{3}$$

between decomposition factors to the left of H or the identity (2) to the right of H;

Condition 3. *$S, R \in \mathcal{P}\backslash\mathbb{C}[X, X^{-1}]$ and either decomposition may be obtained from the other by successive application of the identities (1) to the left of S or R or the identity (2) to the right of S or R.*

Here $n, m \in \mathbb{N}$, $s, t \in \mathbb{Z}$, $a, b, \zeta \in \mathbb{C}$, $p(X) \in \mathbb{C}[X]$ and $\zeta^{dnm} = 1$.

Proof. That the complete decompositions must be of the form specified is guaranteed by Theorem 5.

For both decompositions we can extract the greatest degree monomial right composition factor with respect to a particular asymptotic term order. As this decomposition must exist for all particular evaluations of the exponent variables, this left composition factor will be unique for any particular asymptotic order. The decomposition of symbolic monomials is straightforwardly related to the factorization of the exponents. As in the proof of Theorem 6, we can split the exponent of the maximal right monomial composition factor into the product of a polynomial part with no fixed divisor and an integer. Both of these can be factored separately and each permutation of these factors gives a distinct decomposition. Conditions 1 and 2 are then provided by Theorem 7.

We now consider the situation where $g_1 \circ h_1 = g_2 \circ h_2$ and $g_1, g_2 \in \mathbb{C}[X]$, $h_1, h_2 \in \mathcal{P} = \mathbb{C}[n_1, ..., n_p; X] \backslash \mathbb{C}[X, X^{-1}]$ with no right monomial composition factor. The only non-trivial decompositions h_i can have all give a left decomposition factor in $\mathbb{C}[X]$. We may therefore associate this with g_i and restrict our attention to the case where $\tilde{h}_i \in \mathcal{P}$ are not monomials and have no further non-trivial decomposition.

Now, under any evaluation of the exponent variables in h_i, Theorem 7 must apply. In each of cases (1)–(5), however, the minimum and maximum degrees of G_1 and G_2 are determined by $g_1, g_2 \in \mathbb{C}[X]$ and these determine the degrees of termsH_1 and H_2 (in the notation of Theorem 7). Therefore, under each evaluation the decomposition factors H_1 and H_2 are the same so all the symbolic exponents must lie in H, which is the same for both decompositions. As we have excluded the case where H is a monomial, we must have $G \circ G_i \circ H_i \in \mathbb{C}[X]$ so H is a polynomial under any evaluation and is therefore a symbolic polynomial. □

6. Computing Decompositions

To find a decomposition $f = g \circ h$ we consider two cases: h being a monomial (Conditions 1 and 2) and g being an ordinary polynomial (Condition 3).

When h is a monomial

If $h = h_1 x^{q_1}$ is a symbolic monomial, then q_1 will be a common factor of the exponents of x in f. The co-factors of q_1 in the exponents of x in f will give the exponents p_i of g.

When g is an ordinary polynomial

If $g \in R[X]$ then we may substitute X^{n_1}, $X^{n_1^2}$, X^{n_2}, $X^{n_1 n_2}$, *etc* with new variables to obtain a multivariate Laurent polynomial. We may then perform a uni-multivariate Laurent polynomial decomposition, as described in [26].

In order to ensure that the coefficients of the exponent polynomials are integers, we first make the substitution $X \mapsto X^L$ where L is the smallest integer such that $Lp_1, ..., Lp_r \in \mathbb{Z}[n_1, ..., n_p]$. Then, with all integer coefficients in the exponents, we able to transform X^P to a product of new variables raised to integer powers. For example, if $p = 2$ we can introduce the new variables $X_{ij} = X^{n_1^i n_2^j}$ and the term $cX^{3n_1^2 - 4n_2}$ becomes $cX_{20}^3 X_{01}^{-4}$. This choice of L does not make explicit all fixed divisors of the exponent polynomials. If no decomposition is obtained with this L, then try again with $L = d!^p$, where d is the maximum degree of any n_i in any exponent in f. This will be sufficient to detect any fixed divisor of exponent polynomials [24].

Algorithm 1 (Symbolic polynomial decomposition)**.**

INPUT: $f = \sum_{i=1}^{T} f_i X^{e_i} \in \mathcal{P} = \mathbb{C}[n_1, ..., n_p; X]$

OUTPUT: If there exists a decomposition $f = g \circ h$, $g, h \in \mathcal{P}$ not of the form $c_1 X + c_0 \in \mathbb{C}[X]$, then output **true**, g and h. Otherwise output **false**.

Step 1. *Handle the case of monomial h.*
Let $q :=$ primitive part of $\gcd(e_1, ..., e_T)$, $k := \gcd(\text{max fixed divisor } e_1, \ldots, \text{max fixed divisor } e_T)$.
If $kq \neq 1$, let $g = \sum_{i=1}^{T} f_i X^{e_i/(kq)}$ and $h = X^{kq}$. Return $(\mathbf{true}, g, h)$

Step 2. *Remove fractional coefficients that occur in f.*
Let L be smallest integer such that $Le_1, ..., Le_T \in \mathbb{Z}[n_1, ..., n_p]$. Construct $f' = \rho f \in \mathcal{P}$, using the substitution $\rho : X \mapsto X^L$.

Step 3. *Convert to multivariate problem.* Construct $f'' = \gamma f' \in \mathbb{C}[X_{0\ldots0}, ..., X_{d\ldots d}]$, using the correspondence $\gamma : X^{{n_1}^{i_1} \cdots {n_p}^{i_p}} \mapsto X_{i_1 \ldots i_p}$.

Step 4. *Determine possible degrees.* Let D be the total degree of f''. The possible degrees of the decomposition factors are the integers that divide D.

Step 5. *Try uni-multivariate decompositions.* For each integer divisor r of D, from largest to smallest until a decomposition is found or there are no more divisors, try a uni-multivariate Laurent polynomial decomposition $f'' = g \circ h''$ where g has degree r. If no decomposition is found, try again with $L = d!^p$. If no decomposition if found, return **false**.

Step 6. *Compute h.* Invert the substitutions to obtain $h = \rho^{-1} \gamma^{-1} h''$.

Step 7. *Return* $(\mathbf{true}, g, h)$.

Figure 1.
Symbolic Polynomial Decomposition

Symbolic Polynomial Decomposition Algorithm

We can now give our algorithm for symbolic polynomial decomposition. This is shown in Figure 1. This algorithm may be applied repeatedly to obtain a complete decomposition. It may be possible to further decompose g and h. If $g \in \mathbb{C}[X]$, the standard polynomial decomposition algorithms may be applied. If $h = X^{a \times b}$, then h may be decomposed as $X^a \circ X^b$. Note the lower first value for L is for efficiency only.

7. Conclusions

We have extended the notion of functional decomposition of polynomials to the domain of symbolic polynomials and have shown that if such a decomposition exists either the inner decomposition factor must be a monomial or the outer decomposition factor must be an ordinary polynomial. We have also shown that maximal decompositions exist and how they are related. Finally, we have presented an algorithm to compute these decompositions based on uni-multivariate Laurent decomposition.

Some interesting problems remain open to future investigation: One is to decompose symbolic polynomials over fields of finite characteristic. Another is to compute the functional decomposition of extended symbolic polynomials, where elements of the coefficient ring may have symbolic exponents.

References

[1] D. R. Barton and R. E. Zippel. A polynomial decomposition algorithm. In *Proc. 1976 ACM Symposium on Symbolic and Algebraic Computation*, pages 356–358. ACM Press, 1976.

[2] T. Crampton and G. Whaples. Additive polynomials ii. *Trans. American Math. Society*, 78(1):239–252, 1955.

[3] B. G. R. de Prony. Essai éxperimental et analytique: sur les lois de la dilatabilité de fluides élastique et sur celles de la force expansive de la vapeur de l'alkool, à différentes températures. *Journal de l'École Polytechnique*, 1(22):24–76, 1795.

[4] M. T. Dickerson. *The Functional Decomposition of Polynomials*. PhD thesis, Cornell University, 1989.

[5] G. Everest and A. V. D. Poorten. Factorisation in the ring of exponential polynomials. *Proc. American Math. Society*, 125(5):1293–1298, 1997.

[6] C. Henson, L. Rubel, and M. Singer. Algebraic properties of the ring of general exponential polynomials. *Complex Variables Theory and Applications*, 13:1–20, 1989.

[7] H. Hong. Groebner basis under composition II. In *International Symposium on Symbolic and Algebraic Computation*, pages 79–85, 1996.

[8] H. Hong. Subresultants under composition. *J. Symbolic Computation*, 23:355–365, 1997.

[9] H. Hong. Groebner basis under composition I. *J. Symbolic Computation*, 25:643–663, 1998.

[10] D. Kozen and S. Landau. Polynomial decomposition algorithms. *J. Symbolic Computation*, 22:445–456, 1989.

[11] D. Kozen, S. Landau, and R. Zippel. Decomposition of algebraic functions. *J. Symbolic Computation*, 22(3):235–246, 1996.

[12] M. Malenfant. A comparison of two families of algorithms for symbolic polynomials. Master's thesis, Dept of Computer Science, University of Western Ontario, December 2007.

[13] M. Malenfant and S. M. Watt. Sparse exponents in symbolic polynomials. In *Proc. Symposium on Algebraic Geometry and Its Applications: in honor of the 60th birthday of Gilles Lachaud, (SAGA 2007)*, Papeete, Tahiti, 2007.

[14] A. Ostrowski. Über ganzwertige Polynome in algebraischen Zahlköpern. *J. Reine Angew. Math.*, 149:117–124, 1919.

[15] F. Pakovich. Prime and composite Laurent polynomials, 2008. Preprint: arXiv.org:0710.3860v3.

[16] W. Pan and D. Wang. Uniform gröbner bases for ideals generated by polynomials with parametric exponents. In *Proc. ISSAC 2006*, pages 269–276. ACM Press, 2006.

[17] G. Pólya. Über ganzwertige Polynome in algebraischen Zahlköpern. *J. Reine Angew. Math.*, 149:97–116, 1919.

[18] J. Ritt. Prime and composite polynomials. *Trans. American Math. Society*, 23(1):51–66, 1922.

[19] J. Ritt. A factorization theory for functions $\sum_{i=1}^{n} a_i e^{\alpha_i x}$. *Trans. American Math. Society*, 29(3):584–596, 1927.

[20] J. Ritt. Algebraic combinations of exponentials. *Trans. American Math. Society*, 31(4):654–679, 1929.

[21] A. P. Sexton, V. Sorge, and S. M. Watt. Abstract matrix arithmetic. Technical Report TR 713, University of Western Ontario, Dept of Computer Science, 2007.

[22] J. von zur Gathen, J. Gutierrez, and R. Rubio. Multivariate polynomial decomposition. *Applied Algebra in Engineering, Communication and Computing*, 14:11–31, 2003.

[23] S. M. Watt. Making computer algebra more symbolic. In *Proc. Transgressive Computing 2006: A conference in honor of Jean Della Dora*, pages 43–49, 2006.

[24] S. M. Watt. Symbolic polynomials with sparse exponents. In *Proc. Milestones in Computer Algebra 2008: A conference in honour of Keith Geddes' 60th birthday*, pages 91–97, Stonehaven Bay, Trinidad and Tobago, 2007. University of Western Ontario. ISBN 978-0-7714-2682-7.

[25] S. M. Watt. Two families of algorithms for symbolic polynomials. In I. Kotsireas and E. Zima, editors, *Computer Algebra 2006: Latest Advances in Symbolic Algorithms – Proceedings of the Waterloo Workshop*, pages 193–210. World Scientific, 2007.

[26] S. M. Watt. Functional decomposition of Laurent polynomials. Technical Report ORCCA TR 08-02, Ontario Research Centre for Computer Algebra, University of Western Ontario, London Ontario, 2008.

[27] V. Weispfenning. Gröbner bases for binomials with parametric exponents. Technical report, Universität Passau, Germany, 2004.

[28] K. Yokoyama. On systems of algebraic equations with parametric exponents. In *Proc. ISSAC 2004*, pages 312–319. ACM Press, 2004.

[29] M. E. Zieve. Decompositions of Laurent polynomials, 2007. Preprint: arXiv.org:0710.1902v1.

[30] R. E. Zippel. Rational function decomposition. In *Proc. ISSAC 2001*, pages 1–6. ACM Press, 1991.