A Note on the 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

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 $3X^{(n^2+n)/2} - Y^{2m} + 2$, where n and m are integer-valued parameters. We consider the case where the exponents are multivariate integer-valued polynomials with coefficients in $\mathbb{Q}$ and call these "symbolic polynomials." Earlier work has presented algorithms to factor symbolic polynomials and compute GCDs [9, 10]. Here, we extend 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 $h(X) = X^{n^2/2+n/2} - X^{n^2/2-n/2}$.

Definition 1 (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 $\mathrm{Int}_{[X_1,\ldots,X_n]}(D) = \{f \mid f \in K[X_1, \ldots, X_n] \text{ and } f(a) \in D, \text{ for all } a \in D^n\}$.

Integer-valued polynomials have been studied for many years [5, 6]. Definition 1 is the obvious multivariate generalization.

Definition 2 (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 $\sum_i c_i X_1^{e_{i1}} X_2^{e_{i2}} \cdots X_v^{e_{iv}}$, where $c_i \in R$ and $e_{ij} \in \mathrm{Int}_{[n_1,n_2,\ldots,n_p]}(\mathbb{Z})$. Multiplication is defined by $bX_1^{e_1} \cdots X_v^{e_v} \times cX_1^{f_1} \cdots X_v^{f_v} = bc\, X_1^{e_1+f_1} \cdots X_v^{e_v+f_v}$ and distributivity. We denote this ring $R[n_1, ..., n_p; X_1, ..., X_v]$.

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, 4, 7, 8]. Algorithms for polynomial decomposition have been proposed and refined for use in computer algebra systems. Generalizations of this problem include decomposition of rational functions and algebraic functions. The relationship between polynomial composition and polynomial systems has also been studied [2, 3].

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 3 (Composition of univariate symbolic polynomials)**.** Let $g, h \in \mathcal{P} = R[n_1, ..., n_p; X]$. The composition $g \circ h$ of g and h, if it exists, is the finite sum $f = \sum_i c_i X^{e_i} \in \mathcal{P}$ such that $\phi f = \phi g \circ \phi h$ under all evaluation maps $\phi : \{n_1, ..., n_p\} \to \mathbb{Z}$.

We may now state the problem we wish to solve:

Problem 1. *Let $f \in R[n_1, ..., n_p; X]$. Determine whether there exist symbolic polynomials $g_1, ..., g_\ell \in R[n_1, ..., n_p; X]$ not of the form $c_1X + c_0 \in R[X]$, such that $f = g_1 \circ \cdots \circ g_\ell$ and, if so, find them.*

We restrict our attention to the case where the coefficient ring is $\mathbb{C}$. This allows roots of unity when required and avoids technicalities arising when the characteristic of the coefficient field divides the degree an outer composition factor. This so-called "wild" case is less important with symbolic polynomials because degrees are not always fixed values. We then have the following result.

Theorem 1. *Let* $g(X) = \sum_{i=1}^{R} g_i X^{p_i}$ *and* $h(X) = \sum_{i=1}^{S} h_i X^{q_i}$ *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* $g \circ h$ *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. $g \in \mathbb{C}[X]$.

Based on this theorem, we may compute a decomposition of a symbolic polynomial as follows.

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 $(\textbf{true}, g, h)$

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 composition 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, return **false**.

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

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

It may be possible to further decompose g and h. If $g \in \mathbb{C}[X]$, the standard polyomial decomposition algorithms may be applied. If $h = X^{a \times b}$, then h may be decomposed as $X^a \circ X^b$.

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.

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

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

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

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

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

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

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

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

[10] S. 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.