# Specialization of Symbolic Polynomials

Stephen M. Watt
David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Canada N2L 3G1
smwatt@uwaterloo.ca

**Abstract**

We consider "symbolic polynomials" that generalize the usual polynomials by allowing multivariate integer valued polynomials as exponents. We explore how a variety of algebraic properties specialize under the evaluation of the exponent variables.

## 1 Introduction

We have earlier introduced the notion of "symbolic polynomials", these being objects that are like polynomials, but allowing symbolic expressions as the exponents. For example, the expression $x^{6n}y^{m^2+m} - 4$ is a symbolic polynomial. This type of expression occurs frequently in applications of symbolic computation, but computer algebra systems have typically not dealt with them particularly well. Instead of making the full specturm of algebraic algorithms available, when symbols lie in the exponents, systems tend to fall back on naïve syntactic expression manipulation. For example, the previous expression would not be recognized as a difference of squares that can be factored as $x^{6n}y^{m^2+m} - 4 = (x^{3n}y^{\frac{m^2+m}{2}} + 2)(x^{3n}y^{\frac{m^2+m}{2}} - 2)$, with the exponents $\frac{m^2+m}{2}$ always giving values in $\mathbb{N}$ when $m \in \mathbb{N}$.

In this paper, we review the basic ideas of symbolic polynomials and explore properties of evaluation mappings on exponent variables. We discuss how evaluation behaves for differential ring operations and for GCD and factorization structure. We then present some preliminary thoughts relating to Gröbner bases.

## 2 Symbolic Polynomials

We define symbolic polynomials as follows.

**Definition 1.** *The ring of* symbolic polynomials in *base variables* $x_1, ..., x_v$ and *exponent variables* $n_1, ..., n_p$ 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*

$$c_1 x_1^{e_{11}} \cdots x_n^{e_{1n}} \quad \times \quad c_2 x_1^{e_{21}} \cdots x_n^{e_{2n}} = c_1 c_2 x_1^{e_{11}+e_{21}} \cdots x_n^{e_{1n}+e_{2n}}$$

*We denote this ring* $R[n_1, \ldots, n_p; x_1, \ldots, x_v]$.

We make use of integer-valued polynomials, $\mathrm{Int}_{[n_1,\ldots n_p]}(D)$. For an integral domain $D$ with quotient field $K$, univariate integer-valued polynomials, usually denoted $\mathrm{Int}(D)$, may be defined as

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

For example $\frac{1}{2}n^2 + \frac{1}{2}n \in \mathrm{Int}_{[n]}(\mathbb{Z})$. Integer-valued polynomials have been studied by Ostrowski [1] and Pólya [2], and we take the obvious multivariate generalization. Note that we could alternatively define symbolic polynomials as given by an algebra of terms with monomials and a finite number of ring operations.

These objects are both theoretically interesting and useful in applications of computer algebra. The usual operations of ring arithmentic and diffierential algebra ($+$, $-$, $\times$, $\partial/\partial x_i$) are straightforward. By restricting the exponents to be integer-valued polynomials, we find effective algebraic algorithms for greatest common divisor and factorization [3] and functional decomposition [4].

# 3 Evaluation

With 1, we have natural evaluation maps to Laurent polynomials,

$$\sigma : \mathbb{Z}^p \to R[n_1, \ldots, n_p; x_1, \ldots, x_v] \to R[x_1^{\pm} \ldots, x_v^{\pm}]$$

where $\sigma(a_1, \ldots, a_p)$ evaluates $n_i$ at $a_i$. For example, $\sigma(-2, 4) : \mathbb{Z}[n_1, n_2; x] \to \mathbb{Q}[x, x^{-1}]$ evaluates the symbolic polynomial $2x^{n_1^2+n_2} + x^{3n_1+n_2}$ to the Laurent polynomial $2x^8 + x^{-2}$. It is possible to work with evaluation homomorphisms that produce polynomial values in $R[x_1, \ldots, x_v]$, but this requires that the $\sigma(a_1, \ldots, a_p)$ be partial and keeping track of the domains of definition is typically more difficult that working with Laurent polynomials. Working with total evaluation maps does require, however, extending certain polynomial algorithms, see e.g. [5].

The evaluation maps are easily seen to be differential ring homomorphisms, *i.e.* when $\sigma = \sigma(b_1, \ldots, b_p)$ for any values $b_i$,

$$\begin{aligned}
\sigma 0 &= 0 \\
\sigma 1 &= 1 \quad \text{if } R \text{ has unity} \\
\sigma(u + v) &= \sigma u + \sigma v \\
\sigma(u \times v) &= \sigma u \times \sigma v \\
\sigma(\partial u/\partial x_i) &= \partial \sigma u/\partial x_i.
\end{aligned}$$

# 4 Specialization

We have seen [3] that $R[n_1, \ldots, n_p; x_1, \ldots, x_v]$ is a GCD domain if $R[x_1, \ldots, x_v]$ is a GCD domain and likewise $R[n_1, \ldots, n_p; x_1, \ldots, x_v]$ is a UFD (unique factorization domain) if $R[x_1, \ldots, x_v]$ is a UFD. Note that $R[n_1, \ldots, n_p; x_1, \ldots, x_v]$ and $R[x_1^{\pm} \ldots, x_v^{\pm}]$ have more units than $R[x_1, \ldots, x_v]$ since any monomial with unit coefficient in $R$ is a unit in the larger rings.

The GCDs and complete factorizations in $R[n_1, \ldots, n_p; x_1, \ldots, x_v]$ do not necessarily give GCDs and complete factorizations in $R[x_1^{\pm} \ldots, x_v^{\pm}]$ under $\sigma$, but they are closely related.

**Theorem 1** (Symbolic GCD Specialization)**.** *Suppose $R[x_1, \ldots, x_v]$ is a GCD domain and $u, v \in R[n_1, \ldots, n_p; x_1, \ldots, x_v]$. Then, for all evaluation maps $\sigma = \sigma(b_1, \ldots, b_p)$,*

$$\sigma \gcd(u, v) \mid \gcd(\sigma u, \sigma v) \in R[x_1^{\pm} \ldots, x_v^{\pm}].$$

Thus the evaluation of a symbolic polynomial GCD will give *a* common divisor of the corresponding symbolic polynomials, but not necessarily the greatest common divisor. The evaluation of the symbolic polynomial GCD will, however, be maximal in the sense that (up to units) it is the "greatest" symbolic polynomial whose image divides the GCD under *all* evaluations.

A similar property holds for factorization:

**Theorem 2** (Symbolic Factorization Specialization)**.** *Suppose $R[x_1, \ldots, x_v]$ is a UFD and $u \in R[n_1, \ldots, n_p; x_1, \ldots, x_v]$ with complete factorization*

$$u = f_1 \times \cdots \times f_k.$$

*Then, for all evaluation maps $\sigma = \sigma(b_1, \ldots, b_p)$,*

$$\sigma f_i \mid \sigma u \in R[x_1^{\pm} \ldots, x_v^{\pm}].$$

Similarly to the case of symbolic polynomial GCDs, the evaluation of a complete factorization of a symbolic polynomial is *a* factorization of the original polynomial evaluated, but it is not necessarily a complete factorization. That is, some of the $\sigma f_i$ may factor further in $R[x_1^{\pm} \ldots, x_v^{\pm}]$. The evaluation of the symbolic polynomial complete factorization will, however, be the "most complete" factorization for which every factor divides the original polynomial under all evaluations.

# 5 Toward Gröbner Bases

A natural next topic is about the ideals of $R[n_1, \ldots, n_p; x_1, \ldots, x_v]$ and how they relate to the ideals of $R[x_1, \ldots, x_v]$. We are therefore motivated to ask whehter Gröbner bases exist for symbolic polynomials, and, if so, to explore their behaviour under specialization.

We begin by noting that the existence and construction of Gröebner bases for Laurent polynomials has been addressed earlier [6]. This work introduces

a notion of generalized term orders based on conic decompositions. It finds application, for example, in computing elementary ideals of Alexander matrices [7]. Examples of generalized term orders given by [6] for monomials $x_1^{i_1} \cdot \cdots \cdot x_v^{i_v}$ use gradings such as $|i_1| + \cdots + |i_v|$, $-\min\{0, i_1, \ldots, i_v\}$, and $i_1 + \cdots + i_v - (v+1)\min\{0, i_1, \ldots, i_v\}$.

We are currently exploring the use of polynomial norms on the exponents of symbolic polynomials to give gradings on symbolic monomial ideals. Gröbner bases based on derived term orders should find useful application.

We note, though, that such term orders will not necessarily specialize under evaluation to term orders in the ring of Laurent polynomials. Consider two monomials, $x^{p_1}$ and $x^{p_2}$. For different evaluation maps, we may have $p_1 < p_2$, $p_1 = p_2$ or $p_1 > p_2$ in $\mathbb{Z}$, affecting the relative order of the two monomials in any term order. An potential approach to relating term orders for symbolic polynomials to term orders for Laurent polynomials would be to compute cylindrical algebraic decompositions on the sets of exponent polynomials for each base variable. This could be used to identify regions of exponent evaluation where monomials maintain their relative order. This is an ongoing topic of investigation.

# 6 Conclusion

We have seen that many algebraic properties of symbolic polynomials are preserved completely, or in a weaker form, under evaluation of the exponent variables. For Gröbner basis computation, it is an ongoing topic of investigation to relate term orders for symbolic polynomials to term orders under evaluation of the exponents.

# References


[1] A. Ostrowski, Über ganzwertige Polynome in algebraischen Zahlköpern, J. Reine Angew. Math., 149 (1919), 117-124.

[2] G. Pólya, Über ganzwertige Polynome in algebraischen Zahlköpern, J. Reine Angew. Math., 149 (1919), 97-116.

[3] Stephen M. Watt, *Two Families of Algorithms for Symbolic Polynomials*, in Computer Algebra 2006: Latest Advances in Symbolic Algorithms—Proceedings of the Waterloo Workshop, I. Kotsireas and E. Zima (editors), World Scientific.

[4] Stephen M. Watt, Functional Decomposition of Symbolic Polynomials, Proc. International Conference on Computational Science and Its Applications (ICCSA 2008), IEEE Computer Society, 193–210.

[5] Stephen M. Watt, Algorithms for the Functional Decomposition of Laurent Polynomials, Proc Conferences on Intelligent Computer Mathematics 2009, Springer Verlag LNAI 5625, 186–200.

[6] Franz Pauer and Andreas Unterkircher, Gröbner Bases for Ideas in Laurent Rings and their Application to Systems of Difference Equations, Applicable Algebra in Engineering, Communication and Computing, 9 (1999), 271–291.

[7] Jesús Gago-Vargas, Isabel Hartillo-Hermoso and José Maria Ucha-Enríquez, Algorithmic Invariants for Alexander Modules, Proc. Computer Algebra in Symbolic Computation, Springer-Verlag LNCS 4194, 149–154.