TWO FAMILIES OF ALGORITHMS FOR 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@csd.uwo.ca

We consider multivariate polynomials with exponents that are themselves integer-valued multivariate polynomials, and we present algorithms to compute their GCD and factorization. The algorithms fall into two families: algebraic extension methods and interpolation methods. The first family of algorithms uses the algebraic independence of x, x^n, x^{n^2}, x^{nm}, etc, to solve related problems with more indeterminates. Some subtlety is needed to avoid problems with fixed divisors of the exponent polynomials. The second family of algorithms uses evaluation and interpolation of the exponent polynomials. While these methods can run into unlucky evaluation points, in many cases they can be more appealing. Additionally, we also treat the case of symbolic exponents on rational coefficients (e.g. $4^{n^2+n} - 81$) and show how to avoid integer factorization.

1. Introduction

We wish to work with polynomials where the exponents are not known in advance, such as $x^{2n} - 1$. There are various operations we may want to perform, such as squaring the value to get $x^{4n} - 2x^{2n} + 1$, or differentiating it to get $2nx^{2n-1}$. Expressions of this sort arise frequently in practice, for example in the analysis of algorithms, and it is very difficult to work with them effectively in current computer algebra systems.

We may think of these objects as sets of polynomials, one for each value of n, or we may think of them as single values belonging to some new ring. In the ring setting, we wish to perform as many of the usual polynomial operations on these objects as possible. Many computer algebra systems will allow one to work with polynomials with symbolic exponents. They do this, however, either by falling back on some form of weak manipulation of general expressions or by treating all symbolic powers as independent. There are therefore certain operations and simplifications they cannot perform as the relationship between exponents may be non-trivial. We would like, for example, to factorize symbolic polynomials such as

$$
\begin{aligned}
&x^{n^4-6n^3+11n^2-6(n+2m-3)} - 1000000^m = \\
&\quad x^{-12m} \times \left(x^{2p} + 10^m x^{p+2m} + 10^{2m} x^{4m}\right) \times \left(x^p + 10^m x^{2m}\right) \\
&\qquad\qquad \times \left(x^{2p} - 10^m x^{p+2m} + 10^{2m} x^{4m}\right) \times \left(x^p - 10^m x^{2m}\right) \\
&p = \ 1/6\ n^4 - n^3 + 11/6\ n^2 - n + 3
\end{aligned}
$$

and perform operations on symbolic integers

$$16^n - 81^m = (2^n - 3^m)(2^n + 3^m)(2^{2n} + 3^{2m}).$$

This paper examines the problem of working with such symbolic polynomials. The principal contributions are:

- to introduce a useful formulation of symbolic polynomials,
- to show this leads to a well-defined multiplicative structure, with unique factorization
- to present two families of algorithms to compute GCDs, factorizations, *etc.*,
- to extend the notion of symbolic polynomials to allow symbolic operations on the coefficients.

This extends ideas presented in an earlier paper.[7]

The remainder of the paper is organized as follows: Section 2 gives the definition that we shall use as our model for symbolic polynomials. Section 3 discusses the multiplicative properties of symbolic polynomials and shows they have a well-defined unique factorization structure. Section 4 presents a family of algorithms to compute values based on the multiplicative structure of symbolic polynomials. The two examples given are greatest common divisor and factorization. These algorithms are based on the algebraic independence of x, x^n, x^{n^2}, *etc* and work in extensions of polynomial rings. Section 5 presents a second family of algorithms for the same problems, but this time based on projection methods. These methods are based on evaluation and interpolation of the exponent variables. Section 6 addresses technical problems that can arise in term identification in projection methods. Section 7 discusses a number of generalizations of symbolic polynomials. One problem discussed there is treating elements of the coefficient ring with symbolic exponents without having to perform factorizations there. Finally, Section 8 concludes the paper.

2. Symbolic Polynomials

We can imagine a number of models for symbolic polynomials that have desirable properties. Most generally, we could say that any set S, which under an evaluation map gives a polynomial ring $R[x_1, ..., x_v]$, represents symbolic polynomials. This would allow such forms as

$$\gcd(x^n - 1, x^m - 1) + 1 \tag{1}$$

or

$$(x - 1) \sum_{i=0}^{n} x^i. \tag{2}$$

Working in terms of explicit ring operations will be useful to us, so we begin by generalizing to symbolic exponents only. This excludes expressions such as (1) and (2).

We recall the concept of a group ring: A *monoid ring* is a ring formed from a ring R and monoid M with elements being the finite formal sums

$$\sum_i r_i m_i, r_i \in R, m_i \in M.$$

A monoid ring has a natural module structure, with basis M, and addition defined in terms of coefficient addition in R. Multiplication is defined to satisfy distributivity, with $r_1 m_1 \times r_2 m_2 = (r_1 r_2)(m_1 m_2)$. When the monoid M is a group, then the algebraic structure is called a *group ring.* For example, the Laurent polynomials with complex coefficients may be constructed as the group ring $\mathbb{C}[\mathbb{Z}]$, viewing $\mathbb{Z}$ as an additive group.

We now define a useful class of symbolic polynomials.

Definition 2.1. 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 $e_{ij} \in \mathrm{Int}_{[n_1, n_2, ..., n_p]}(\mathbb{Z})$. 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 $R[n_1, ..., n_p; x_1, ..., x_v]$.

We make use of the integer-valued polynomials, $\mathrm{Int}_{[n_1, ... n_p]}(D)$. 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[3] and Pólya,[4] and we take the obvious multivariate generalization.

Our definition of symbolic polynomials is isomorphic to the group ring $R[\left(\mathrm{Int}_{[n_1,...,n_p]}(\mathbb{Z})\right)^v]$. We view $\mathrm{Int}_{[n_1,...n_p]}(\mathbb{Z})$ as an abelian group under addition and use the identification

$$x_1{}^{e_1} x_2{}^{e_2} \cdots x_v{}^{e_v} \cong (e_1, \ldots, e_v) \in \left(\mathrm{Int}_{[n_1,...,n_w]}(\mathbb{Z})\right)^v$$

We note that $R[;x_1,...,x_v] \cong R[x_1,...,x_v,-x_1,...,-x_v]$. Also, under any evaluation $\phi : \{n_1,...,n_p\} \to \mathbb{Z}$, we have

$$\phi : R[n_1,...,n_p;x_1,...,x_v] \to R[x_1,...,x_v,x_1^{-1},...,x_v^{-1}].$$

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. This, however, would require keeping track of cumbersome domain restrictions on the exponent variables.

By definition, these symbolic polynomials have a ring structure. What is more interesting is that they also have a useful unique factorization structure that can be computed effectively.

Symbolic polynomials, in the sense we have defined them, can be related to exponential polynomials[2,6] through the transformation $x_i{}^{n^j} \mapsto e^{n^j \log x_i}$. With exponential polynomials, however, it is awkward to capture the notion that the exponents of x_i must be integer valued.

There has also recently been some work on computing Gröbner bases with parametric exponents[5,8] and systems of algebraic equations with parametric exponents.[9] One of the questions asked in this setting is to classify all special cases under evaluation of the parameters. We ask an easier question. Instead, we seek to compute results that are correct under every specialization. This allows us to obtain algorithms for the multiplicative structure of the symbolic polynomials, something that had not been investigated earlier in the parametric setting.

3. Multiplicative Properties

We now show the multiplicative structure of our symbolic polynomials. For simplicity we treat the case when $R = \mathbb{Q}$.

Theorem 3.1. *$\mathbb{Q}[n_1, ..., n_p; x_1, ..., x_v]$ is a UFD, with monomials being units.*

Proof. We first consider the case when exponents are in $\mathbb{Z}[n_1, ..., n_p]$. The fact that $x, x^n, x^{n^2}, ...$ are algebraically independent can be used to remove exponent variables inductively. We observe that

$$x_k^{e_{ik}} = x_k^{\sum_j h_{ij} n_1^j} = \prod_j \left(x_k^{n_1{}^j} \right)^{h_{ij}} = \prod_j x_{kj}{}^{h_{ij}}, \qquad h_{ij} \in \mathbb{Z}[n_2, ..., n_p].$$

This gives the isomorphism

$$\mathbb{Q}[n_1, n_2, ..., n_p; x_1, ...x_v] \cong$$
$$\mathbb{Q}[n_2, ..., n_p; x_{10}, x_{11}, x_{12}, ...x_{1d_1}, ...x_{v0}, x_{v1}, x_{v2}, ...x_{vd_1}]$$

where d_1 is the maximum degree of n_1 in any exponent polynomial and x_{ij} corresponds to $x_i^{n_1{}^j}$. Repeating this process p times, we obtain

$$\mathbb{Q}[n_1, n_2, ..., n_p; x_1, ...x_v] \cong \mathbb{Q}[; x_{10...0}, ..., x_{vd_1...d_p}],$$

which is a ring of multivariate Laurent polynomials with the desired properties.

When the exponents come from the integer-valued polynomials $\mathrm{Int}_{[n_1,...,n_p]}(\mathbb{Z})$, as opposed to $\mathbb{Z}[n_1, ...n_p]$, care must be taken to find the fixed divisors of the exponent polynomials. These fixed divisors are given by the content when polynomials are written in a binomial basis. So to show explicitly unique factorization with exponents in $\mathrm{Int}_{[n_1,...,n_p]}(\mathbb{Z})$, we make the change of variables $x_k^{\binom{n_1}{i_1} \cdots \binom{n_p}{i_p}} \to X_{ki_1...i_p}$. Note that the $X_{ki_1...i_p}$ are in one to one correspondence with $x_{ki_1...i_p}$ and so are therefore also algebraically independent. □

Symbolic polynomials can be related to exponential polynomials, which also have a UFD structure.[2]

4. Extension Algorithms

The proof of Theorem 3.1 introduces new variables to replace $x_i^{n_1}$, $x_i^{n_2}$, $x_i^{\binom{n_1}{2}}$, $x_i^{n_1 n_2}$, $x_i^{\binom{n_2}{2}}$, etc. This idea may be used to obtain algorithms for GCD, factorization, square-free decomposition and similar quantities over $\mathbb{Q}[n_1, ...n_p;\ x_1, ..., x_v]$. We illustrate with algorithms for greatest common divisors and factorization.

Extension Algorithm for Symbolic Polynomial GCD

Input: Symbolic polynomials $f_1, f_2 \in \mathbb{Q}[n_1, ...n_p; x_1, ..., x_v]$.
Output: $g = \gcd(f_1, f_2) \in \mathbb{Q}[n_1, ...n_p; x_1, ..., x_v]$

(1) Put the exponent polynomials of f_1 and f_2 in the basis $\binom{n_i}{j}$.
(2) Construct polynomials $F_1, F_2 \in \mathbb{Q}[X_{10...0}, ..., X_{vd_1...d_p}]$, where d_i is the maximum degree of n_i in any exponent of f_1 or f_2, using the correspondence

$$\gamma : x_k^{\binom{n_1}{i_1}\cdots\binom{n_p}{i_p}} \mapsto X_{ki_1...i_p}.$$

(3) Compute $G = \gcd(F_1, F_2)$.
(4) Compute $g = \gamma^{-1}(G)$.

Under any evaluation map on the exponents, $\phi : \mathrm{Int}_{[n_1,...,n_p]}(\mathbb{Z}) \to \mathbb{Z}$, we have that $\phi(g) \mid \gcd(\phi(f_1), \phi(f_2))$. This g is the maximal uniform gcd in the sense that any other polynomial $g' \in \mathbb{Q}[n_1, ...n_p; x_1, ..., x_v]$ such that $\phi(g') \mid \phi(F_1)$ and $\phi(g') \mid \phi(F_2)$, for all ϕ, also satisfies $g' \mid g$.

Extension Algorithm for Symbolic Polynomial Factorization

Input: A symbolic polynomial $f \in \mathbb{Q}[n_1, ...n_p; x_1, ..., x_v]$.
Output: The factors $g_1, ..., g_n$ such that $\prod_i g_i = f$, unique up to units.

(1) Put the exponent polynomials of f in the basis $\binom{n_i}{j}$.
(2) Construct polynomial $F \in \mathbb{Q}[X_{10...0}, ..., X_{vd_1...d_p}]$, where d_i is the maximum degree of n_i in any exponent of f, using the correspondence

$$\gamma : x_k^{\binom{n_1}{i_1}\cdots\binom{n_p}{i_p}} \mapsto X_{ki_1...i_p}.$$

(3) Compute the factors G_i of F.
(4) Compute $g_i = \gamma^{-1}(G_i)$.

Under any evaluation map on the exponents, $\phi : \mathrm{Int}_{[n_1,...,n_p]}(\mathbb{Z}) \to \mathbb{Z}$, if $\phi(f)$ factors into $f_{\phi 1}, ..., f_{\phi r}$ these factors may be grouped to give the factors $\phi(g_i)$. That is, there is a partition of $\{1, ..., r\}$ into subsets I_i such that $\phi(g_i) = \prod_{j \in I_i} f_{\phi j}$. This factorization into g_i is the maximal uniform factorization in the sense that any other factorization g'_i has $\forall_i \exists_j g_i \mid g'_j$.

It may be that under every evaluation map there is a finer factorization. Erich Kaltofen gives the example $(x^n - 1) \times (y^{n+1} - 1)$. For each n, either the first or second factor is a difference of squares and therefore factors further. There is no further factorization, however, valid for all values of n.

Examples

We use the following pair of polynomials for our examples:

$$\begin{aligned} p = {} & 8x^{n^2+6n+4+m^2-m} - 2x^{2n^2+7n+2mn}y^{n^2+3n} \\ & - 3x^{n^2+3n+2mn}y^{n^2+3n} + 12x^{4+m^2-m+2n} \end{aligned} \tag{3}$$

$$\begin{aligned} q = {} & 4x^{n^2+4n+m^2+6m} - 28x^{n^2+8n+m^2+6m+2}y^{4n^2-4n} \\ & + 2x^{n^2+4n} - 14x^{n^2+8n+2}y^{4n^2-4n} + 6x^{m^2+6m} \\ & - 42x^{m^2+6m+4n+2}y^{4n^2-4n} - 21y^{4n^2-4n}x^{4n+2} + 3. \end{aligned} \tag{4}$$

We demonstrate the computation of the GCD of p and q and the factorization of p. To begin, we note that the exponents of x in p and q are polynomials in m and n of maximum degree 2. We therefore use

$$\left\{ \binom{n}{i}\binom{m}{j} \;\middle|\; 0 \le i+j \le 2 \right\} = \left\{ 1, n, m, \frac{n(n-1)}{2}, nm, \frac{m(m-1)}{2} \right\}.$$

as a basis for the exponents of x. Likewise we note that the exponents of y are polynomials in n alone and are of maximum degree 2. For them we use the basis

$$\left\{ \binom{n}{i} \;\middle|\; 0 \le i \le 2 \right\} = \left\{ 1, n, \frac{n(n-1)}{2} \right\}.$$

Now we make the change of variables

$$\begin{aligned} \gamma = \{ & x \mapsto A,\ x^n \mapsto B,\ x^{\binom{n}{2}} \mapsto C,\ x^m \mapsto D,\ x^{mn} \mapsto E,\ x^{\binom{m}{2}} \mapsto F, \\ & y \mapsto G,\ y^n \mapsto H,\ y^{\binom{n}{2}} \mapsto I \} \end{aligned}$$

to give:

$$p = 8A^4B^7C^2F^2 - 2B^9C^4E^2H^4I^2 - 3B^4C^2E^2H^4I^2 + 12A^4B^2F^2$$

$$\begin{aligned} q = {} & 4B^5C^2D^7F^2 - 28A^2B^9C^2D^7F^2I^8 + 2B^5C^2 - 14A^2B^9C^2I^8 \\ & + 6D^7F^2 - 42A^2B^4D^7F^2I^8 - 21A^2B^4I^8 + 3. \end{aligned}$$

We then obtain the GCD of p and q as

$$g = 2B^5C^2 + 3$$

and the factorization of p as

$$p = B^2 \times \left(2B^5C^2 + 3\right) \times \left(2A^2F - BCEIH^2\right) \times \left(2A^2F + BCEIH^2\right).$$

Applying γ^{-1}, we have the desired results:

$$\begin{aligned} g &= 2x^{n^2+4n} + 3 \\ p &= x^{2n} \times \left(2x^{n^2+4n} + 3\right) \\ &\quad \times \left(2x^{1/2\,m^2-1/2\,m+2} - x^{1/2\,n^2+mn+1/2\,n}y^{1/2\,n^2+3/2\,n}\right) \\ &\quad \times \left(2x^{1/2\,m^2-1/2\,m+2} + x^{1/2\,n^2+mn+1/2\,n}y^{1/2\,n^2+3/2\,n}\right). \end{aligned}$$

Remarks

We have described this transformation as though the exponent polynomials were dense, in which case transforming from a power basis to binomial basis introduces no new terms. This is often not the case, so blindly changing to a binomial basis is not always the best strategy.

In the worst case, the number of variables in the new polynomials will be $v(D+1)^p$, where v is the number of base variables, x_i, p is the number of exponent variables, n_i, and D is the degree bound on the n_i in the exponents. In practice, it is often the case that the number of variables occurring in exponents will be small and the exponent polynomials will be of low degree so the introduction of new variables may be acceptable. In other cases, such as when the exponent polynomials are sparse, other approaches may be preferable.

5. Projection Methods

If the number of exponent variables is large and the exponent polynomials are sparse, then it may be advantageous to use an evaluation/interpolation approach. Exponent polynomials may be mapped to integers at several points, the problem solved, and the images combined via interpolation. We illustrate with algorithms for greatest common divisors and factorization.

Projection Algorithm for Symbolic Polynomial GCD (Dense Version)

Input: Symbolic polynomials $f_1, f_2 \in \mathbb{Q}[n_1, ...n_p; x_1, ..., x_v]$.
Output: $g = \gcd(f_1, f_2) \in \mathbb{Q}[n_1, ...n_p; x_1, ..., x_v]$

(1) If $p = 0$ solve problem in $\mathbb{Q}[x_1, ..., x_v, x_1^{-1}, ..., x_v^{-1}]$. Return result.
(2) Let d be the degree bound of n_1 in any exponent of f_1 or f_2.
(3) Choose $d + 1$ distinct evaluation points $e_i \in \mathbb{Z}$.
Let ϕ_i be the evaluation map $n_1 \mapsto e_i$.
(4) Compute $d + 1$ GCD images $g_i = \gcd(\phi_i(f_1), \phi_i(f_2)) \in \mathbb{Q}[n_2, ..., n_p; x_1, ..., x_v]$ by recursive application of this algorithm.
(5) Identify corresponding terms in the g_i.
(6) Choose one set of corresponding terms and normalize the polynomials so these terms are equal (*e.g.* make those terms 1).
(7) For each set of corresponding terms, interpolate the exponent polynomial to form the corresponding term of g, the GCD.
(8) Return g.

This gives the same GCD as the Extension Algorithm for GCD.

If an evaluation gives a GCD image that is “larger” than the other images, then it is a special case evaluation and should be discarded and another point chosen. If an evaluation point gives a GCD image that is “smaller” than the other images, then the previous evaluations were all unlucky and new points must be chosen.

An important problem is that in step 5 it is not always straightforward to identify corresponding terms. We discuss this in Section 6.

Projection Algorithm for Symbolic Polynomial Factorization (Dense Version)

Input: A symbolic polynomial $f \in \mathbb{Q}[n_1, ...n_p; x_1, ..., x_v]$.
Output: The factors $g_1, ..., g_n$ such that $\prod_i g_i = f$, unique up to units.

(1) If $p = 0$ solve problem in $\mathbb{Q}[x_1, ..., x_v, x_1^{-1}, ..., x_v^{-1}]$. Return result.
(2) Let d be the degree bound of n_1 in any exponent of f.
(3) Choose $d + 1$ distinct evaluation points $e_i \in \mathbb{Z}$.
Let ϕ_i be the evaluation map $n_1 \mapsto e_i$.
(4) Compute $d + 1$ factorization images $g_{1i} \times \cdots \times g_{ni} = \text{factor}(\phi_i(f)) \in \mathbb{Q}[n_2, ..., n_p; x_1, ..., x_v]$ by recursive application of this algorithm.
(5) Identify corresponding factors in the images, and terms within the factors.

(6) For each set of corresponding polynomial images, choose one set of corresponding terms and normalize the polynomials so these terms are equal.
(7) For each term interpolate the exponent polynomial to form the corresponding term of g_k, the k^{th} factor.
(8) Return $g_1, \cdots, g_n$.

This gives the same factorization, up to units, as the Extension Algorithm for Factorization. As with the GCD computation, there is the problem is that in step 5 it may be difficult to identify corresponding terms. This is discussed later. As with other factorization algorithms, it may be the case that image factorizations have different numbers of factors and that combinations must be tried to form the g_{ki}.

Sparse Algorithms

With naive dense interpolation, a number of problems exponential in the number of variables must be solved in $\mathbb{Q}[x_1, ..., x_v]$. Using sparse interpolation techniques, this is not always necessary. The sparse versions of these algorithms use sparse interpolation of the individual exponent polynomials.

Examples

We use the same p and q as before, defined by equations (3) and (4), and compute the GCD of p and q and the factors of p. The maximum power of m or n in any exponent is 2. For simplicity, we use dense interpolation with $m \in \{1, 2, 3\}$ and $n \in \{1, 2, 3\}$. Letting p_{ij} denote p evaluated at $m = i, n = j$, we have:

$$\begin{aligned}
p_{11} &= -2x^{11}y^4 + 8x^{11} - 3x^6y^4 + 12x^6 \\
p_{12} &= -2x^{26}y^{10} + 8x^{20} - 3x^{14}y^{10} + 12x^8 \\
p_{13} &= -2x^{45}y^{18} + 8x^{31} - 3x^{24}y^{18} + 12x^{10} \\
p_{21} &= -2x^{13}y^4 + 8x^{13} - 3x^8y^4 + 12x^8 \\
p_{22} &= -2x^{30}y^{10} + 8x^{22} - 3x^{18}y^{10} + 12x^{10} \\
p_{23} &= -2x^{51}y^{18} + 8x^{33} - 3x^{30}y^{18} + 12x^{12} \\
p_{31} &= -2x^{15}y^4 + 8x^{17} - 3x^{10}y^4 + 12x^{12} \\
p_{32} &= -2x^{34}y^{10} + 8x^{26} - 3x^{22}y^{10} + 12x^{14} \\
p_{33} &= -2x^{57}y^{18} + 8x^{37} - 3x^{36}y^{18} + 12x^{16}
\end{aligned}$$

Similarly, letting q_{ij} denote q evaluated at $m = i, n = j$ gives:

$$\begin{aligned}
q_{11} &= 4x^{12} - 28x^{18} + 2x^5 - 14x^{11} + 6x^7 - 42x^{13} + 3 - 21x^6\\
q_{12} &= 4x^{19} - 28x^{29}y^8 + 2x^{12} - 14x^{22}y^8 + 6x^7 - 42x^{17}y^8 + 3 - 21y^8x^{10}\\
q_{13} &= 4x^{28} - 28x^{42}y^{24} + 2x^{21} - 14x^{35}y^{24} + 6x^7 - 42x^{21}y^{24} + 3 - 21y^{24}x^{14}\\
q_{21} &= 4x^{21} - 28x^{27} + 2x^5 - 14x^{11} + 6x^{16} - 42x^{22} + 3 - 21x^6\\
q_{22} &= 4x^{28} - 28x^{38}y^8 + 2x^{12} - 14x^{22}y^8 + 6x^{16} - 42x^{26}y^8 + 3 - 21y^8x^{10}\\
q_{23} &= 4x^{37} - 28x^{51}y^{24} + 2x^{21} - 14x^{35}y^{24} + 6x^{16} - 42x^{30}y^{24} + 3 - 21y^{24}x^{14}\\
q_{31} &= 4x^{32} - 28x^{38} + 2x^5 - 14x^{11} + 6x^{27} - 42x^{33} + 3 - 21x^6\\
q_{32} &= 4x^{39} - 28x^{49}y^8 + 2x^{12} - 14x^{22}y^8 + 6x^{27} - 42x^{37}y^8 + 3 - 21y^8x^{10}\\
q_{33} &= 4x^{48} - 28x^{62}y^{24} + 2x^{21} - 14x^{35}y^{24} + 6x^{27} - 42x^{41}y^{24} + 3 - 21y^{24}x^{14}
\end{aligned}$$

Then we calculate $g_{ij} = \gcd(p_{ij}, q_{ij})$:

$$\begin{array}{lll}
g_{11} = 2x^5 + 3 & g_{12} = 2x^{12} + 3 & g_{13} = 2x^{21} + 3\\
g_{21} = 2x^5 + 3 & g_{22} = 2x^{12} + 3 & g_{23} = 2x^{21} + 3\\
g_{31} = 2x^5 + 3 & g_{32} = 2x^{12} + 3 & g_{33} = 2x^{21} + 3
\end{array}$$

This gives one exponent polynomial to interpolate and we obtain

$$g = 2x^{n^2+4n} + 3.$$

We now turn our attention to factoring p. We factor the image polynomials in $\mathbb{Z}[x, y]$:

$$\begin{aligned}
p_{11} &= -x^6\left(y^2 - 2\right)\left(y^2 + 2\right)\left(3 + 2x^5\right)\\
p_{12} &= -x^8\left(3 + 2x^{12}\right)\left(x^3y^5 - 2\right)\left(x^3y^5 + 2\right)\\
p_{13} &= -x^{10}\left(3 + 2x^{21}\right)\left(x^7y^9 - 2\right)\left(x^7y^9 + 2\right)\\
p_{21} &= -x^8\left(y^2 - 2\right)\left(y^2 + 2\right)\left(3 + 2x^5\right)\\
p_{22} &= -x^{10}\left(3 + 2x^{12}\right)\left(x^4y^5 - 2\right)\left(x^4y^5 + 2\right)\\
p_{23} &= -x^{12}\left(3 + 2x^{21}\right)\left(x^9y^9 - 2\right)\left(x^9y^9 + 2\right)\\
p_{31} &= x^{10}\left(3 + 2x^5\right)\left(2x - y^2\right)\left(2x + y^2\right)\\
p_{32} &= -x^{14}\left(3 + 2x^{12}\right)\left(x^4y^5 - 2\right)\left(x^4y^5 + 2\right)\\
p_{33} &= -x^{16}\left(3 + 2x^{21}\right)\left(x^{10}y^9 - 2\right)\left(x^{10}y^9 + 2\right)
\end{aligned}$$

We determine which factors correspond by inspection. We let f_1 be the factor with coefficients $\{2, 3\}$, f_2 with $\{\pm 1, \mp 2\}$, f_3 with $\{1, 2\}$ and u the monomial.

Recall that, in the ring of symbolic polynomials, and in $\mathbb{Q}[x, y, x^{-1}, y^{-1}]$, monomials are invertible and factorization is unique up to units. We pick an arbitrary monomial in each of f_i to be the constant term and normalize. (In principle we could normalize the constant term to 1, but it is convenient here to divide through only by the power product $x^{k_1}y^{k_2}$.) The resulting factors are shown in the following table.

m	n	u	f_1	f_2	f_3
1	1	$-x^6$	$2x^5+3$	y^2-2	y^2+2
1	2	$-x^8$	$2x^{12}+3$	x^3y^5-2	x^3y^5+2
1	3	$-x^{10}$	$2x^{21}+3$	x^7y^9-2	x^7y^9+2
2	1	$-x^8$	$2x^5+3$	y^2-2	y^2+2
2	2	$-x^{10}$	$2x^{12}+3$	x^4y^5-2	x^4y^5+2
2	3	$-x^{12}$	$2x^{21}+3$	x^9y^9-2	x^9y^9+2
3	1	$-x^{12}$	$2x^5+3$	$x^{-1}y^2-2$	$x^{-1}y^2+2$
3	2	$-x^{14}$	$2x^{12}+3$	x^4y^5-2	x^4y^5+2
3	3	$-x^{16}$	$2x^{21}+3$	$x^{10}y^9-2$	$x^{10}y^9+2$

Interpolating the exponent polynomials, we obtain

$$\begin{aligned}
u &= -x^{4+m^2-m+2n} \\
f_1 &= 2x^{n^2+4n}+3 \\
f_2 &= x^{-1/2m^2+mn+1/2n^2+1/2m+1/2n-2}y^{1/2n^2+3/2n}-2 \\
f_3 &= x^{-1/2m^2+mn+1/2n^2+1/2m+1/2n-2}y^{1/2n^2+3/2n}+2.
\end{aligned}$$

This gives the factorization

$$p = u \times f_1 \times f_2 \times f_3,$$

which is the same, up to units, as what we obtained with the extension algorithm. To see this, let $e = m^2 - m + 4$ and multiply u by $-x^{-e}$, f_2 by $-x^{e/2}$ and f_3 by $x^{e/2}$.

6. Finding Corresponding Terms

In general, problems may arise in projection methods when identifying sets of terms for interpolation. In computing GCDs, for example, this amounts to determining which terms correspond in the GCD images. There are three problems that arise:

- The first problem is that, under certain evaluations of the exponent variables, exponent polynomials become equal and terms of the result combine. If there is only one exponent variable, then this can occur for at most $DT(T-1)/2$ evaluation points, where T is the number of terms in the GCD and D is the degree bound on the exponent variable. This is because there are up to $T(T-1)/2$ pairs of distinct exponent polynomials, each pair having at most D common values. For multivariate exponents, terms may combine at an unlimited number of points, but choosing random evaluation points effectively avoids the problem.

- The second problem is that, even if terms do not combine, it may still not be obvious which terms correspond. For example the GCD may have multiple terms with the the same coefficient and variables. If the coefficient ring is not large enough, then this can occur with high probability.
- The third problem is that one or more evaluation points may give special case results. This is the exceptional case, however. Depending on the problem, the special case results might give an interesting short-cut to a solution or they might be useless and simply be discarded.

In computing factorizations, we have the above problems as well as the usual problem of factor identification.

We illustrate the problem of difficulty identifying corresponding exponents under evaluation with another GCD example, using u and v given as:

$$u = x^{3n^2-4n+8} + 9x^{2n^2+4} + x^{n^3+n^2-4n+4} + 14x^{n^2+4n} + 2x^{n^3} \tag{5}$$

$$v = x^{3n^2+8} + 8x^{2n^2+4n+4} + x^{n^3+n^2+4} + 7x^{n^2+8n} + x^{n^3+4n}. \tag{6}$$

The exponent polynomials are of degree at most 3, so we evaluate at four points.

$$\begin{aligned}
n = 1 \Rightarrow &\qquad \gcd(u,v) = x^6 + 7x^5 + x\\
n = 2 \Rightarrow &\qquad \gcd(u,v) = 8x^{12} + x^8\\
n = 3 \Rightarrow &\qquad \gcd(u,v) = x^{27} + x^{22} + 7x^{21}\\
n = 4 \Rightarrow &\qquad \gcd(u,v) = x^{64} + x^{36} + 7x^{32}.
\end{aligned}$$

We see that the different evaluations give polynomials with different numbers of terms. It appears that there are three terms in the symbolic polynomial, and that the evaluation at $n = 2$ made two of the exponents equal, giving terms x^{12} and $7x^{12}$.

When the image has three terms, two of the coefficients are the same so it is not clear how to assign the images to symbolic terms for interpolation. Note that the evaluation does not necessarily preserve term order: for $n = 1$ the term with coefficient 7 is of middle degree, for $n = 2$ it is of highest degree and for $n = 3$ and $n = 4$ it is of lowest degree. We must therefore consider the possibility that the terms with coefficient 1 may appear in any order. Thus, even with only two terms having equal coefficients, we have a number of cases to consider exponential in the degree of n. These are shown in the table below. The entries are lists of values for the exponents e_i at $n = [1, 2, 3, 4]$ respectively.

Model	**Term 1**	**Term 2**	**Term 3**
	$1 \times x^{e_1}$	$1 \times x^{e_2}$	$7 \times x^{e_3}$
1	[6,12,27,64]	[1,8,22,36]	[5,12,21,32]
2	[6,12,27,36]	[1,8,22,64]	[5,12,21,32]
3	[6,12,22,64]	[1,8,27,36]	[5,12,21,32]
4	[6,12,22,36]	[1,8,27,64]	[5,12,21,32]
5	[6,8,27,64]	[1,12,22,36]	[5,12,21,32]
6	[6,8,27,36]	[1,12,22,64]	[5,12,21,32]
7	[6,8,22,64]	[1,12,27,36]	[5,12,21,32]
8	[6,8,22,36]	[1,12,27,64]	[5,12,21,32]

To discover which is the correct combination, we evaluate at one extra point.

$$n = 5 \Rightarrow \qquad \gcd(u, v) = x^{125} + x^{54} + 7x^{45}.$$

At $n = 5$ either (a) $e_1 = 125$, $e_2 = 54$ or (b) $e_1 = 54$, $e_2 = 125$. Interpolating each model with both choices, we see that model 4 with (b) gives $e_1 = 2n^2 + 4$ and $e_2 = n^3$ with degrees ≤ 3 as required. All other combinations give interpolants of degree 4. We therefore have

$$\gcd(u, v) = x^{2n^2+4} + x^{n^3} + 7x^{n^2+4n}$$

If there are T terms and N evaluation points, then there will be $(T!)^{N-1}$ possible assignments of evaluation points to terms. One of them will give interpolants satisfying the degree bound. Unless T and N are very small, this strategy will obviously be infeasible and another approach will be needed.

We also observe that if there is only one exponent variable, then there will be some value beyond which evaluations give images that have a consistent order. This is because a finite set of univariate polynomials will have a finite set of points that make two of the polynomials equal. If this bound can be determined, in principle it avoids the problem of determining which images correspond. In practice, however, it may be too large to be useful (at least in the case of factorization).

Interpolation of Symmetric Functions

There is a better alternative to address the problem of term identification. If there are terms that cannot be distinguished, then we may take advantage of the symmetry and interpolate symmetric functions of the exponent polynomials.

If $t_1, ..., t_T$ are the terms that cannot be distinguished, then we interpolate $S_j(t_1, ..., t_T)$ for different j, where S_j is the j-th elementary symmetric function. We then use *one* evaluation point to break the symmetry and solve for the exponents of the t_i.

We use this method to compute the GCD of u and v given by equations (5) and (6). We wish to determine the exponents of the two terms $x^{A(n)}$ and $x^{B(n)}$, where

$$\begin{aligned} A(n) &= a_3n^3 + a_2n^2 + a_1n + a_0 \\ B(n) &= b_3n^3 + b_2n^2 + b_1n + b_0 \end{aligned}$$

To do this we interpolate $S_1(A(n), B(n)) = A(n) + B(n)$ and $S_2(A(n), B(n)) = A(n) \times B(n)$. The polynomial for S_2 will be of degree ≤ 6, so we need three extra points. We compute:

$$\begin{aligned} n = 5 \Rightarrow &\qquad \gcd(u, v) = x^{125} + x^{54} + 7x^{45} \\ n = 6 \Rightarrow &\qquad \gcd(u, v) = x^{216} + x^{76} + 7x^{60} \\ n = 7 \Rightarrow &\qquad \gcd(u, v) = x^{343} + x^{102} + 7x^{77} \end{aligned}$$

We now have

n	$A(n) + B(n)$	$A(n) \times B(n)$
1	$1 + 6$	1×6
2	$8 + 12$	8×12
3	$22 + 27$	22×27
4	$36 + 64$	36×64
5		54×125
6		76×216
7		102×343
Interpolation	$n^3 + 2n^2 + 4$	$2n^5 + 4n^3$

To break the symmetry, we arbitrarily assign $A(1) = 1$ and $B(1) = 6$. Additionally, we equate coefficients in

$$\begin{aligned} A(n) + B(n) &= n^3 + 2n^2 + 4 \\ A(n) \times B(n) &= 2n^5 + 4n^3 \end{aligned}$$

to obtain 13 equations in the 8 unknowns $\{a_i, b_i\}$. Solving, we obtain:

$$\begin{array}{cccc} a_0 = 0 & a_1 = 0 & a_2 = 0 & a_3 = 1 \\ b_0 = 4 & b_1 = 0 & b_2 = 2 & b_3 = 0 \end{array}$$

This determines the two exponents.

7. Generalizations

As mentioned earlier, we may contemplate other algebraic structures to encompass a wider class of expressions. Without going to the most general model of polynomial-valued integer functions, we may consider

- Allowing exponent variables to also appear as regular variables. To do this we can work in $R[n_1, ..., n_p; n_1, ..., n_p, x_1, ..., x_v]$. This is useful if we require formal derivatives.
- Symbolic exponents on coefficients. We discuss these more below.[2,6]
- Non-uniform problems. That is, we may ask how to partition $\mathbb{Z}^p$ as $\bigcup_i D_i$ to obtain more specialized factorizations, gcd, *etc*, valid when restricted to substitutions on individual domains, $\phi : (n_1, ..., n_p) \to D_i$.
- Symbolic polynomials as exponents, or richer structures.
- Other polynomial forms, such as exponential polynomials
- Other problems, *e.g.* Gröbner bases of symbolic polynomials.[8,9]

Let us examine more closely the question of symbolic exponents on coefficients. Suppose we wish to factor a polynomial of the form $x^{4m} - 2^{4n}$. Assuming m and n may take on only integer values, the factorization over $\mathbb{Q}$ is $(x^{2m} + 2^{2n})(x^m + 2^n)(x^m - 2^n)$. This, however is equivalent to $x^{4m} - 16^n$, which is not manifestly the difference of fourth powers. So how can we approach symbolic integer coefficients?

If the coefficient ring is a principal ideal domain, then we may extend our definition to allow symbolic exponents on prime coefficient factors:

Definition 7.1. The ring of *symbolic polynomials in* $x_1, ..., x_v$ *with exponents in* $n_1, n_2, ..., n_p$ *and symbolic coefficients* over the coefficient ring R, a PID with quotient field K, is the ring consisting of finite sums of the form

$$\sum_i k_i \cdot \prod_j c_j^{d_{ij}} \cdot x_1^{e_{i1}} x_2^{e_{i2}} \cdots x_n^{e_{in}}$$

where each product has a finite number of nonzero d_{ij}, $k_i \in K$, c_j are primes $\in R$, $d_{ij} \in \mathrm{Int}_{[n_1,n_2,...,n_p]}(\mathbb{Z}) \backslash \mathbb{Z}$ and $e_{ij} \in \mathrm{Int}_{[n_1,n_2,...,n_p]}(\mathbb{Z})$. Multiplication is defined by

$$\begin{aligned} k_1 c_1^{d_{11}} \cdots c_m^{d_{1m}} x_1^{e_{11}} \cdots x_n^{e_{1n}} \quad \times \quad & k_2 c_1^{d_{21}} \cdots c_m^{d_{2m}} x_1^{e_{21}} \cdots x_n^{e_{2n}} = \\ & k_1 k_2 c_1^{d_{11}+d_{21}} \cdots c_m^{d_{1m}+d_{2m}} x_1^{e_{11}+e_{21}} \cdots x_n^{e_{1n}+e_{2n}} \end{aligned}$$

We consider the case of integer coefficients and initially restrict our attention to the situation where the c_j are prime so relationships among symbolic coefficients are apparent. We may use the algebraic independence of p_i^n, $p_i^{n^2}$, *etc* to treat $p_i^{\binom{n_1}{i_1}\cdots\binom{n_k}{i_k}}$ as new variables, as before, in algorithms for factoring, GCD, and related operations.

This straightforward approach requires factoring each integer that appears with a symbolic exponent. In practice we do not want to factor the constant coefficients. Instead, we can form, for any particular problem, a GCD-free basis.[1] For example, if 70^n and 105^n appear, then using the basis $\{X_1 = 2^n, X_2 3^n, X_3 = 35^n\}$ avoids factoring. Such a basis may be computed efficiently using only integer GCD and k-th roots.

8. Conclusions

We see a mathematically rich and practically important middle ground between the usual approaches of "symbolic computation" and "computer algebra." In this light, we have explored how to usefully work with symbolic polynomials — polynomial-like objects where the exponents can themselves be integer-valued polynomials.

We have modeled symbolic polynomials using the formal structure of a group ring. These are able to represent the kinds of symbolic polynomials we have seen in practice, for example in the analysis of algorithms. This algebraic structure allows us to perform arithmetic on symbolic polynomials, to simplify and transform them. We find, moreover, a UFD structure that admits algorithms for factorization, GCD, *etc.*

We have sketched two families of algorithms for symbolic polynomials. One puts the exponent polynomials in to a basis that makes their fixed divisors manifest, and then introduces new variables for the symbolic powers. The second family of algorithms is based on evaluation/interpolation, where multiple image problems are solved and the images combined. This approach sometimes has a technical problem in determining which images correspond to do the interpolation. Interpolating symmetric functions of the desired exponent polynomials can avoid some of these difficulties.

We have experimental implementations of both the extension and sparse projection methods, but it is too early to say which method will be most useful in practice.

References

1. E. Bach and J. Shallit, *Algorithmic Number Theory, Volume I: Efficient Algorithms*. MIT Press, 1996.
2. C.W. Henson, L. Rubel and M. Singer, Algebraic Properties of the Ring of General Exponential Polynomials. Complex Variables Theory and Applications, **13**, 1989, 1-20.
3. A. Ostrowski, Über ganzwertige Polynome in algebraischen Zahlköpern, J. Reine Angew. Math., 149 (1919), 117-124.
4. G. Pólya, Über ganzwertige Polynome in algebraischen Zahlköpern, J. Reine Angew. Math., 149 (1919), 97-116.
5. W. Pan and D. Wang. Uniform Gröbner bases for ideals generated by polynomials with parametric exponents. Proc ISSAC 2006, ACM, 269–276.
6. Baron Gaspard Riche 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, volume 1, cahier 22, 24-76 (1795).
7. S.M. Watt, Making Computer Algebra More Symbolic. pp 43-49, Proc. Transgressive Computing 2006: A conference in honor of Jean Della Dora, April 24-26, 2006, Granada, Spain.
8. V. Weispfenning, Gröbner bases for binomials with parametric exponents. Technical report, Universität Passau, Germany, 2004.
9. K. Yokoyama, On Systems of Algebraic Equations with Parametric Exponents. pp 312-319, ISSAC '04, July 4-7, 2004, Santander, Spain, ACM Press.