A New Modular Interpolation Algorithm for Factoring Multivariate Polynomials

Ronitt Rubinfeld and Richard Zippel
Deptment of Computer Science
Cornell University
Ithaca, NY 14853

January 28, 1993

Abstract

In this paper we present a technique that uses a new interpolation scheme to reconstruct a multivariate polynomial factorization from a number of univariate factorizations. Whereas other interpolation algorithms for polynomial factorization depend on various extensions of the Hilbert irreducibility theorem, our approach is the first to depend only upon the classical formulation. The key to our technique is the interpolation scheme for multivalued black boxes originally developed by Ar et. al. [1]. We feel that this combination of the classical Hilbert irreducibility theorem and multivalued black boxes provides a particularly simple and intuitive approach to polynomial factorization.

Various versions of the problem of factoring polynomials, that is, writing a polynomial as the product of polynomials of smaller degree, have been studied for hundreds of years. In its earliest form it involved obtaining the zeroes of low degree univariate polynomials and was the subject of public competitions in the 15^{th} and 16^{th} centuries. In this case, the goal was to find linear factors with coefficients in a radical extension of the rational numbers, $\mathbb{Q}$.

The modern problem was first solved by Kronecker [25] and can be stated as follows. Let L be a field and $P(X, Y_1, \ldots, Y_n)$ a polynomial with coefficients in L. P is said to be *irreducible* if there do not exist two polynomials $Q_1, Q_2 \in L[X, Y_1, \ldots, Y_n]$, neither of which are elements of L, such that $P = Q_1 \cdot Q_2$. A *complete factorization* of P is a set of distinct, irreducible polynomials $P_1, \ldots, P_k$ such that

$$P(X, Y_1, \ldots, Y_n) = P_1^{e_1} \cdot P_2^{e_2} \cdots P_k^{e_k}. \tag{1}$$

The e_i are greater than or equal to 1 and not all of the P_i need have positive degree in X and the Y_i.

When P is a univariate polynomial, *i.e.*, $n = 0$, the following is known: If the coefficient field L is either a finite field, $\mathbb{F}_p$ or $\mathbb{F}_{p^r}$, or the rational integers $\mathbb{Q}$ then P can be factored in polynomial time. In the finite field case any of a number of algorithms can be used [3–5, 18, 19, 29]. When L is equal to $\mathbb{Q}$ various lattice reduction techniques can be used to factor P in polynomial time [26, 27, 31].

There are two main approaches to the multivariate factorization problem, the Hensel (or Newton) approach and the modular interpolation approach. Both approaches reduce the multivariate problem to a univariate or bivariate problem.

Intuitively the Hensel approach proceeds as follows: First, choose a random n-tuple $(y_1, \ldots, y_n) \in R^n$ and factor the univariate polynomial $P(X, y_1, \ldots, y_n)$. This is viewed as factorization of $P(X, Y_1, \ldots, Y_n)$ modulo the ideal $\mathfrak{m} = (Y_1 - y_1, \ldots, Y_n - y_n)$. Using a constructive version of Hensel's lemma (or equivalently Newton's method) this factorization is lifted to one modulo $\mathfrak{m}^2$, $\mathfrak{m}^3$ and so on, until we have a factorization modulo $\mathfrak{m}^D$, where D is larger than the degree of any variable in $P(X, Y_1, \ldots, Y_n)$. This must then be a true factorization of $P(X, Y_1, \ldots, Y_n)$ [21, 35, 36, 38].

The modular interpolation approach again chooses random values for the variables $Y_1, \ldots, Y_n$, but instead of using a single factorization of P, it uses interpolation techniques to combine many univariate factorizations to produce a multivariate factorization [22].

As described, both approaches reduce multivariate factorization to univariate factorization. The Hilbert irreducibility theorem guarantees that for most random choices the univariate factorizations have the same number of factors as the multivariate factorizations and thus the same structure. For technical reasons, the authors of [20, 22] use a different version of the Hilbert irreducibility theorem that is only valid for reductions to bivariate factorizations. Their algorithms thus require an additional technique to reduce the required bivariate factorizations to univariate factorizations.

Our technique overcomes these earlier technical problems, allows us to directly reduce multivariate factorization to univariate factorization and uses the classical version of the Hilbert irreducibility theorem. Briefly, we present a new, simple modular scheme for factoring a polynomial $P(X, Y_1, \ldots, Y_n)$ with integer coefficients:

$$P(X, Y_1, \ldots, Y_n) = P_1^{e_1}(X, Y_1, \ldots, Y_n) P_2^{e_2}(X, Y_1, \ldots, Y_n) \cdots P_k^{e_k}(X, Y_1, \ldots, Y_n).$$

The classical form of the Hilbert irreducibility theorem states that for almost all choices of integers $y_1, \ldots, y_n$, the factorization of $P(X, y_1, \ldots, y_n)$ has the same structure as the factorization of $P(X, Y_1, \ldots, Y_n)$. Our first step is to produce a black box $\mathscr{B}_{P_1, \ldots, P_k}$ that on input of $y_1, \ldots, y_n$ returns the set of factors of $P(X, y_1, \ldots, y_n)$. However, for different inputs, the factor corresponding to P_i may be returned in different positions. Nonetheless, using the techniques of Ar et. al. [1] we demonstrate how to construct k black boxes, each representing an individual factor P_i of P. These black boxes can then be interpolated using sparse polynomial interpolations schemes [2, 6, 37, 39].

The Hilbert irreducibility theorem is described in Section 1. In Section 2 we present the basic factoring algorithm. It relies on black box interpolation techniques discussed in Section 3 which in turn rely on well known Hensel techniques for solving equations that are described in Appendix B.

1 Hilbert Irreducibility Theorem

We make strong use of the Hilbert irreducibility theorem, which says that for almost all $\vec{y} = (y_1, \ldots, y_n)$, where $y_i \in \mathbb{Q}$, the univariate polynomial $P(X, y_1, \ldots, y_n)$ has the same number of irreducible factors as the multivariate polynomial $P(X, Y_1, \ldots, Y_n)$, and thus the degree distributions are the same.

We call an n-tuple $y_1, \ldots, y_n$ *Hilbertian for* P if the factorization of $P(X, y_1, \ldots, y_n)$ has no more factors than that of $P(X, Y_1, \ldots, Y_n)$. We need to quantify how often the factorization of $P(X, y_1, \ldots, y_n)$ corresponds to that of $P(X, Y_1, \ldots, Y_n)$. Let the number of non-Hilbertian n-tuples, $(y_1, \ldots, y_n)$ with $0 \leq y_i < N$, for an irreducible polynomial of degree d be denoted by $\bar{R}(d, n, N)$. More generally, the number of non-Hilbertian n-tuples $(y_1, \ldots, y_n)$ for a polynomial P, $R(d, n, N)$ is no greater than $k\bar{R}(d, n, N)$, where k is the number of irreducible factors of P.

The classical Hilbert irreducibility theorem asserts that $R(N)/N^n \to 0$, as N goes to infinity [9–14, 17, 23, 24, 30, 33, 34]. The sharpest result is due to Cohen [7]:

$$\bar{R}(d, n, N) < c(d) \cdot N^{n-\frac{1}{2}} \log N, \tag{2}$$

where c depends only on the degree of the irreducible polynomial. The distribution of non-Hilbertian points is invariant under translations of the Y_i, so we have the following proposition.

Proposition 1 *Let $P(X, Y_1, \ldots, Y_n)$ be a polynomial over $\mathbb{Q}$ and assume that the degree of X in P is less than D. Let $a_1, \ldots, a_n$ be any elements of $\mathbb{Z}$. For sufficiently large N, the number of n-tuples $(y_1, \ldots, y_n) \in \mathbb{Z}^n$, $a_i \leq y_i < N + a_i$, for which $P(X, y_1, \ldots, y_n)$ factors differently from $P(X, Y_1, \ldots, Y_n)$ is less than*

$$R(d, n, N) < c(d) \cdot D \cdot N^{n-\frac{1}{2}} \log N.$$

As a consequence of this use of the Hilbert irreducibility theorem, the values used in the interpolation must be chosen randomly from a large enough domain.

Extensive experience has shown that n-tuples at which an irreducible polynomial is reducible are exceedingly rare. We thus believe the following conjecture to be true. This is reinforced by the extensive use of the classical version of Hilbert irreducibility theorem to factor multivariate polynomials over $\mathbb{Q}$ in computer algebra systems, *e.g.*, Macsyma, Reduce and Axiom.

Conjecture 1 *In the previous proposition, there exists an absolute constants c_1, c_2 such that $c(d) < c_1 d^{c_2}$,* i.e.

$$R(d, n, N) < c_1 d^{c_2} \cdot D \cdot N^{n-\frac{1}{2}} \log N.$$

Using this original form of the Hilbert irreducibility theorem and the new techniques presented in this paper we derive a simple multivariate polynomial factorization algorithm. Assuming Conjecture 1, our algorithm runs in random polynomial time.

2 Factoring Multivariate Polynomials

Assume that we want to factor a polynomial $P(X, Y_1, \ldots, Y_n)$ with coefficients in $\mathbb{Q}$. For clarity, assume also that the polynomial is square free and monic as a polynomial in X.

Neither of these assumptions affect the complexity or correctness of the algorithm. The extension to non-square free polynomials is immediate. The extension to non-monic polynomials is less obvious and the details are outlined in Appendix C.

Assume the factorization of $P(X, Y_1, \ldots, Y_n)$ is

$$P(X, Y_1, \ldots, Y_n) = P_1(X, Y_1, \ldots, Y_n) \cdot P_2(X, Y_1, \ldots, Y_n) \cdots P_k(X, Y_1, \ldots, Y_n).$$

For any Hilbertian point $\vec{y} = (y_1, \ldots, y_n)$ the factorization of $P(X, y_1, \ldots, y_n)$ will be

$$P(X, y_1, \ldots, y_n) = P_{1\vec{y}}(X) \cdot P_{2\vec{y}}(X) \cdots P_{k\vec{y}}(X),$$

where $P_{i\vec{y}}(X) = P_i(X, y_1, \ldots, y_n)$ is a univariate polynomial in X.

We construct a black box $\mathscr{B}_{P_1,\ldots,P_k}$ that represents the *set* of multivariate polynomials $\{P_1, \ldots, P_k\}$. When given a Hilbertian point $(y_1, \ldots, y_n)$ as input, the black box factors the univariate polynomial $P(X, y_1, \ldots, y_n)$ and returns the *unordered set* of factors

$$\mathscr{B}(y_1, \ldots, y_n) = \{P_{1\vec{y}}(X), P_{2\vec{y}}(X), \ldots, P_{k\vec{y}}(X)\}.$$

Such a black box is called a *polynomial multivalued black box*, since it returns several unordered values on each call and each of these values is a univariate polynomial. By repeatedly querying this black box, we will recover the factors of P: $P_1, \ldots, P_k$. This process is called *interpolating* the black box. Thus, we have reduced the multivariate factorization problem to factoring univariate polynomials and interpolating "polynomial multivalued black boxes."

The black boxes we produce differ slightly from those studied by Ar et. al. [1], but in Section 3 we demonstrate how their techniques can be adapted to recover $P_1, \ldots, P_k$ in random polynomial time. Interpolating the black boxes requires factoring special bivariate polynomials, $Q(Z, \Theta)$, where we know the complete factorization of $Q(Z, \theta)$, for some integer θ. The bivariate polynomials $Q(Z, \Theta)$ have the special property that they have only linear factors of the form $Z - q_i(\Theta)$ where the q_i's are polynomials in Θ. With this additional information, factoring is not needed—instead, much faster, well known Hensel techniques suffice (Appendix B).

The complete time complexity and probability of success of the factoring algorithm is given at the end of Section 3.3.

3 Interpolation Schemes

The simplest form of black box is one that represents a single polynomial $P(Y_1, \ldots, Y_n)$ with coefficients in $\mathbb{Q}$. We use the notation $\mathscr{B}_P$ to indicate such a black box. On input of $y_1, \ldots, y_n \in \mathbb{Q}$, such a black box returns an element of $\mathbb{Q}$, $P(y_1, \ldots, y_n)$. Given such a black box it is not difficult to determine P in time polynomial in the number of non-zero monomials in P [2, 6, 37, 39]. Extensions to black boxes representing rational functions are given in [22]. We note that the original randomized interpolation algorithm of [37] can use uniformly distributed evaluation points.

In [1], the concept of a black box is extended to a *multivalued black box* $\mathscr{B}_{P_1,\ldots,P_k}$. On input $\vec{y}$, a multivariate black box returns an *unordered set* of values $\{P_1(\vec{y}), \ldots, P_k(\vec{y})\}$, where the $P_i(Y)$ are distinct polynomials. Given a collection of t different k-tuples returned by such a black box,

$$\{P_1(\vec{y}_1), \ldots, P_k(\vec{y}_1)\}, \{P_1(\vec{y}_2), \ldots, P_k(\vec{y}_2)\}, \ldots, \{P_1(\vec{y}_t), \ldots, P_k(\vec{y}_t)\},$$

we want to determine the polynomials $P_1(\vec{Y}), \ldots, P_k(\vec{Y})$. We call this process *interpolating the black box*. Since the values are unordered, we don't know which values in each list correspond with which P_i. To find the correspondence by brute force requires time exponential in t, thus the standard interpolation techniques for black boxes are inadequate.

Denote the coefficient of X^j in the polynomial $P_i(X, Y_1, \ldots, Y_n)$ by a_{ij}, which is a polynomial in $Y_1, \ldots, Y_n$. Our approach is to reduce interpolation of the black box $\mathscr{B}_{P_1,\ldots,P_k}$ to independent interpolations of the black boxes $\mathscr{M}^{(j)}_{a_{1j},\ldots,a_{kj}}$, $0 \leq j \leq d$, where d bounds the degree of X in the P_i. On input of integers $\vec{y} = (y_1, \ldots, y_n)$, $\mathscr{M}^{(j)}_{a_{1j},\ldots,a_{kj}}$ returns the unordered set of values $a_{1j}(\vec{y}), \ldots, a_{kj}(\vec{y})$, which are elements of $\mathbb{Q}$. Each of the black boxes $\mathscr{M}^{(j)}_{a_{1j},\ldots,a_{kj}}$ are then converted into several single valued black boxes $\mathscr{M}_{a_{ij}}$—in other words, the order of the values returned by $\mathscr{M}^{(j)}_{a_{1j},\ldots,a_{kj}}$ is determined. This is accomplished using intermediate univariate multivalued black boxes of the form $\mathscr{U}_{q_1,\ldots,q_k}$ where the q_i are univariate polynomials in a new variable Θ.

In Section 3.1, we use the techniques of [1] to reduce the univariate case to the problem of refining linear factors of a bivariate polynomial. The case of $\mathbb{Q}$-valued black boxes representing multivariate polynomials is discussed in Section 3.2 and is reduced to the univariate problem. In Section 3.3, we deal with multivalued black boxes whose values are polynomials. This is again reduced to the univariate case discussed in Section 3.1. Furthermore, in all of the following sections calls will be made on randomly distributed points.

3.1 Black Boxes of Univariate Polynomials

Let $q_1(\Theta), \ldots, q_k(\Theta)$ be distinct univariate polynomials of degree no more than D. Given a multivalued black box of univariate polynomials $\mathscr{U}_{q_1,\ldots,q_k}$, we provide a technique for explicitly determining the q_i's.

The symmetric functions in the $q_1(\theta), \ldots, q_k(\theta)$ are defined to be

$$\begin{aligned}
\sigma_1(\theta) &= q_1(\theta) + q_2(\theta) + \cdots + q_k(\theta), \\
\sigma_2(\theta) &= q_1(\theta)q_2(\theta) + q_1(\theta)q_3(\theta) + \cdots + q_{k-1}(\theta)q_k(\theta), \\
&\vdots \\
\sigma_k(\theta) &= q_1(\theta)q_2(\theta)\cdots q_k(\theta).
\end{aligned}$$

Notice that the symmetric functions can be computed given the values $\{q_1(\theta), \ldots, q_k(\theta)\}$ without knowing which values correspond with which q_i. Therefore, we can construct k different single valued black boxes $\mathscr{B}_{\sigma_i}$, one for each symmetric function. On input of θ, $\mathscr{B}_{\sigma_i}$ returns the value $\sigma_i(\theta)$. For each black box $\mathscr{B}_{\sigma_i}$, the univariate polynomial $\sigma_i(\Theta)$ is of degree no more than iD and can be determined by Lagrangian interpolation in $O((iD)^2)$ time and iD queries. This approach places no constraints on the points used in the interpolation process.

Using these univariate values as coefficients we can explicitly construct the polynomial

$$Q(Z,\Theta) = Z^k - \sigma_1(\Theta)Z^{k-1} + \sigma_2(\Theta)Z^{k-2} + \cdots + (-1)^k\sigma_k(\Theta),$$

which by construction has only linear factors:

$$Q(Z,\Theta) = (Z - q_1(\Theta))(Z - q_2(\Theta) \cdots (Z - q_k(\Theta)).$$

The zeroes of $Q(Z,\theta)$ are $q_1(\theta),\ldots,q_k(\theta)$, which are the values of $\mathscr{B}_{q_1,\ldots,q_k}(\theta)$. This additional information allows us to use the Hensel techniques of Section B to quickly find the factorization of $Q(Z,\Theta)$ and thus determine the $q_i(\Theta)$.

Proposition 2 *Let $q_1,\ldots,q_k$ be polynomials in $\mathbb{Q}[\Theta]$ and the degree of q_i is bounded by D. Then all of the q_i's can be interpolated from a multivalued black box $\mathscr{U}_{q_1,\ldots,q_k}$ using $kD+1$ evaluations and time $O(k^3D^2)$. Furthermore, the evaluations can be made at arbitrary points.*

Note that Lagrangian interpolation does not depend upon the values chosen for θ. Thus we can use the same θ's when we need to interpolate several different black boxes at the same time.

3.2 Black Boxes of Multivariate Polynomials

Given a multivalued black box of multivariate polynomials $\mathscr{M}_{p_1,\ldots,p_k}$, we provide a technique for explicitly determining the p_i's. The approach we use converts the multivalued black box $\mathscr{M}$ into an *ordered* multivalued black box $\mathscr{M}'$ where the values are always returned in the same order. Standard interpolation techniques can then be used to recover the p_i's.

This method is a modification of the one given in Section 3 of [1]. The problem in [1] uses black boxes that with each call only return the value of an arbitrary P_i. The factorization problem yields black boxes that return the values of all of the P_i at each call. This additional information allows our technique to work over arbitrary fields, while that of [1] is only valid over finite fields.

The concept of a *reference point* is used to impose an ordering on the values returned by the $\mathscr{M}_{p_1,\ldots,p_k}$. We say that $\vec{y} = (y_1,\ldots,y_m)$ is a reference point if, for all i and j, $p_i(\vec{y}) \neq p_j(\vec{y})$. Given the range from which the y_i's are chosen (the interval $[0, N_P]$, where N_P is defined in Proposition 4), it can be shown that significantly more than half of the $\vec{y}$'s are reference points. Thus a reference point can be found by choosing a random point and verifying that it is a reference point. For each black box $\mathscr{M}$, we need only choose one reference point. Given the reference point $\vec{y}$, we compute the ordered sequence of reference values

$$\mathscr{M}(\vec{y}) = \langle p_1(\vec{y}),\ldots,p_k(\vec{y})\rangle. \tag{3}$$

Define the multivalued black box $\mathscr{D}_{\vec{x},\vec{y}}(\theta)$, which on input θ calls the black box $\mathscr{M}(\vec{y}+\theta\cdot(\vec{x}-\vec{y}))$ and returns $\mathscr{M}$'s results. Fixing $\vec{x}, \vec{y}$, $\mathscr{D}_{\vec{x},\vec{y}}$ is a black box of univariate polynomials in θ of degree nD. Applying the techniques described in Section 3.1 to $\mathscr{D}_{\vec{x},\vec{y}}$, we explicitly get the unordered set of univariate polynomials

$$S_{\vec{x}} = \{p_1(\vec{y}+\Theta\cdot(\vec{x}-\vec{y})),\ldots,p_k(\vec{y}+\Theta\cdot(\vec{x}-\vec{y}))\}$$

By substituting $\Theta = 0$ into each of the polynomials in $S_{\vec{x}}$, and comparing with the reference values (3), we can determine the correspondence between polynomials in $S_{\vec{x}}$ and $p_1, \ldots, p_k$. By substituting $\Theta = 1$ into the polynomials in $S_{\vec{x}}$, we can now determine $p_1(\vec{x}), \ldots, p_k(\vec{x})$.

This technique allows us to create a set of single valued black boxes (for multivariate polynomials) from a multivalued black box. It is a simple matter to use the randomized multivariate polynomial interpolation techniques of [37] to explicitly determine the p_i's.

Proposition 3 *Let θ be a fixed integer and $\vec{y}$ be a fixed n-tuple. For $\vec{x}$ such that x_i is uniformly distributed in the interval $0 \leq x_i < N$, there exists an n-dimensional box I of volume $(\theta N)^n$ such that $\vec{y} + \theta \cdot (\vec{x} - \vec{y})$ is uniformly distributed on a subset of I of volume N^n.*

Proposition 4 *Let $p_1, \ldots, p_k$ be polynomials in $\mathbb{Q}[Y_1, \ldots, Y_n]$ and let the degree of every Y_j in every P_i is bounded by D. Furthermore, assume that no p_i has more than T non-zero terms. Then with likelihood of success $> 1/2$ the p_i can be interpolated from a multivalued black box $\mathscr{M}_{p_1,\ldots,p_k}$ using $O((knD)^2T)$ evaluations, inputs have magnitude less than $N_p = \tilde{O}((knD)^nT)$[1] bits and time $O(kn^2DT^3 + k^5(nD)^4T)$.*

Proof: To reconstruct the multivariate polynomials $p_1, \ldots, p_k$, we need the values of $p_1, \ldots, p_k$ at nDT evaluation points, where T is the maximum number of non-zero terms in any p_i. Each ordered set of values of $p_1, \ldots, p_k$ at $\vec{x}$ is determined by interpolating the black box $\mathscr{D}_{\vec{x},\vec{y}}$, described above. The black box $\mathscr{D}_{\vec{x},\vec{y}}$ represents univariate polynomials of degree at most nD. So by Proposition 2, we can produce the k univariate polynomials of each $\mathscr{D}_{\vec{x},\vec{y}}$ with $knD + 1$ evaluations of $\mathscr{M}$ and $O(k^3(nD)^2)$ operations.

The multivariate interpolation algorithm requires the values of $p_1(\vec{x}), \ldots, p_k(\vec{x})$ at $knDT$ randomly chosen $\vec{x}$, at most. So the total number of values of $\mathscr{M}$ is $k(nDT)(knD + 1) \approx (knD)^2T$. If $\vec{y} + \theta \cdot (\vec{x} - \vec{y})$ is a Hilbertian point, then each of these values can be computed by a univariate factorization. For success, each of these $(knD)^2T$ points must be Hilbertian. Since knD values of θ are needed we can assume that all of the θ are less than knD. The points $\vec{y} + \theta \cdot (\vec{x} - \vec{y})$ lie in a box I of volume $(knDN_P)^n$. There are at most $R(d, n, knDN_P)$ non-Hilbertian points in this box. By Proposition 3 the points $\vec{y} + \theta(\vec{x} - \vec{y})$ are uniformly distributed in a region of I of volume N_P^n. Therefore the likelihood that a single one of these points is Hilbertian is at least

$$1 - \frac{c(d)(knDN_P)^{n-\frac{1}{2}} \log knDN_P}{N_P^n} = 1 - \frac{c(d)(knd)^{n-\frac{1}{2}} \log kndN_P}{\sqrt{N_P}}.$$

The likelihood that $(knD)^2T$ points are all Hilbertian is at least

$$1 - c(d)(knD)^{n+\frac{3}{2}}T\frac{\log knDN_P}{\sqrt{N_P}},$$

for sufficiently large N_P. For some constant c_3, this expression is greater than $1 - \epsilon$ when $\log N_P > c_3(n \log knD + \log T)/\epsilon$. $\square$

[1] $\tilde{O}$ is used to indicate that we have ignored additional log factors.

3.3 Polynomial Multivalued Black Boxes

This section extends the results of the previous subsections to black boxes whose values are polynomials. That is, let $P_1, \ldots, P_k$ be polynomials in $\mathbb{Q}[Y_1, \ldots, Y_n][X]$:

$$P_1(X, Y_1, \ldots, Y_n) = a_{1d_1}(Y_1, \ldots, Y_n)X^{d_1} + \cdots + a_{10}(Y_1, \ldots, Y_n),$$

$$\vdots$$

$$P_k(X, Y_1, \ldots, Y_n) = a_{kd_k}(Y_1, \ldots, Y_n)X^{d_k} + \cdots + a_{k0}(Y_1, \ldots, Y_n),$$

where the a_{ij} are polynomials of degree no more than D in $Y_1, \ldots, Y_n$. Let d denote the maximum of the d_i. A *polynomial multivalued black box* for $P_1, \ldots, P_k$ is a multivalued black box whose values are polynomials:

$$\mathscr{B}_{P_1,\ldots,P_k}(y_1, \ldots, y_n) = \{P_1(X, y_1, \ldots, y_n), \ldots, P_k(X, y_1, \ldots, y_n)\}.$$

Given $\mathscr{B}_{P_1,\ldots,P_k}$, we could use the techniques of Sections 3.1 and 3.2 to reconstruct the P_i since $\mathbb{Q}[X]$ is a ring. However, this is not particularly efficient. Consider the univariate case, where $n = 1$. As in Section 3.1, we would construct black boxes for the symmetric functions in P_i. Since $\mathscr{B}_{P_1,\ldots,P_k}$ has polynomial values, the $\mathscr{B}_{\sigma_i}$ will also. In particular, the degree of X in each value of $\mathscr{B}_{\sigma_k}$ will be dk. Furthermore, the Q polynomial will be trivariate.

While Hensel techniques can still be used to factor Q in polynomial time, the approach is somewhat complex. Here we propose an alternative, simpler approach. First, we determine d, the actual maximum degree of X that appears in any P_i. We then replace the polynomial valued black box $\mathscr{B}_{P_1,\ldots,P_k}$ by $d + 1$, $\mathbb{Q}$-multivalued black boxes. The polynomials (in $Y_1, \ldots, Y_n$) that these black boxes represent can be reconstructed using the techniques of Sections 3.1 and 3.2. In more detail:

For two purposes, choose a random value $0 \le y_{i0} < N$ for each of the Y_i and compute:

$$\mathscr{B}_{P_1,\ldots,P_k}(y_{10}, \ldots, y_{n0}) = \{Q_1(X), \ldots, Q_k(X)\},$$

where we number the Q_i so that Q_i corresponds with P_i. We claim that with high probability,

(1) the maximum degree of the Q_i will be d_i, and

(2) for every i, j and ℓ, if $a_{i\ell}(Y_1, \ldots, Y_n) \not\equiv a_{j\ell}(Y_1, \ldots, Y_n)$, then $a_{i\ell}(y_{10}, \ldots, y_{n0}) \not\equiv a_{j\ell}(y_{10}, \ldots, y_{n0})$.

Now construct $d + 1$ black boxes, $\mathscr{M}^{(i)}_{P_1,\ldots,P_k}$, for $0 \le i \le d$, that represent polynomials in $Y_1, \ldots, Y_n$, as follows: the values returned by $\mathscr{M}^{(i)}_{P_1,\ldots,P_k}(y_1, \ldots, y_n)$ are the coefficients of X^i in the polynomials returned by $\mathscr{B}_{P_1,\ldots,P_k}(y_1, \ldots, y_n)$. Thus $\mathscr{M}^{(i)}_{P_1,\ldots,P_k}$ represents the polynomials

$$S_i = \{a_{1i}(Y_1, \ldots, Y_n), \ldots, a_{ki}(Y_1, \ldots, Y_n)\}.$$

The $\mathscr{M}^{(i)}_{P_1,\ldots,P_k}$ are $\mathbb{Q}$-multivalued black boxes, for which we can use the techniques of Sections 3.1 and 3.2 in order to determine the polynomials a_{ij}.

We reconstruct the $P_i(X, Y_1, \ldots, Y_n)$'s using the information in the $Q_i(X)$. Let the coefficient of X^j in P_i be a_{ij}. Further, assume $Q_i(X)$ has the form

$$Q_i(X) = q_{id_i} X^{d_i} + \cdots + q_{i0}.$$

Now, for each $0 \le j \le d_i$, a_{ij} is the entry in S_j whose value at $y_{10}, \ldots, y_{n0}$ is q_{ij}. By property (2), if there is more than 1 such element then they are equal.

Proposition 5 *Let $P(X, Y_1, \ldots, Y_n)$ be a polynomial over $\mathbb{Q}$, where the degree of X is not greater than d and the degrees of the Y_i are not greater than D. Using the interpolation schemes of Section 3.2 with evaluation points chosen with coordinates between 0 and $\tilde{O}(n \log nD)$, and with t in Proposition 4 chosen between 0 and $O(knD)$, the number of operations used to determine the factors of P is $O(n^2 d^2 D T^3 + d^6 (nD)^4 T)$ and the number of univariate factorizations is $O((ndD)^2 T)$, with high likelihood of success.*

Proof: The time complexity of interpolating polynomial multivalued black boxes is the same as that for $\mathbb{Q}$-multivalued black boxes in Proposition 4 except that we may have as many as d $\mathbb{Q}$ valued black boxes to interpolate. The number of values of each black box, k in Proposition 4 is also bounded by d.

The degree of $P_i(X, Y_1, \ldots, Y_n)$ in X will differ from that of $P_i(X, y_1, \ldots, y_n)$ if and only if $a_{id_i}(y_1, \ldots, y_n) = 0$. By the "DeMillo-Lipton-Schwartz-Zippel lemma" (Proposition 7) the fraction of the n-tuples in y_i that have this property is less than nD/N. Thus, with high probability, d is the maximum degree of the polynomials returned by $\mathscr{B}_{P_1,\ldots,P_k}(y_{10}, \ldots, y_{n0})$.

To ensure property (2) the y_{i0} must be chosen such that $W(y_{10}, \ldots, y_{n0}) \neq 0$, where

$$W(Y_1, \ldots, Y_n) = \prod_{0 \le \ell \le d} \prod_{\substack{1 \le i < j \le k \\ a_{i\ell} \not\equiv a_{j\ell}}} (a_{\ell i}(Y_1, \ldots, Y_n) - a_{\ell j}(Y_1, \ldots, Y_n)).$$

The maximum degree of any Y_i in W is $D(D+1)\binom{k}{2}$, so again by using Proposition 7, the fraction of n-tuples that are accidental zeroes of W is bounded by $nD(D+1)k(k-1)/2N$. The probability that a randomly chosen n-tuple, $(y_1, \ldots, y_n)$, will meet all of these conditions is thus

$$1 - \left(\frac{nD}{N} + \frac{nD(d+1)k(k-1)}{2N} \right) \ge 1 - \frac{ndDk^2}{N} \ge 1 - \frac{nd^3 D}{N},$$

or $N > nd^3 D$. Proposition 4 requires that N be at least this large. $\square$

Combining this result with the univariate factoring algorithm of V. Miller [27] gives the following proposition.

Proposition 6 *Let $P(X_1, \ldots, X_n)$ be a multivariate polynomial over $\mathbb{Q}$, where the degree of each X_i in P is bounded by d, and the sum of the absolute value of the coefficients in P is bounded by H. Then P can be factored into irreducible components in $O(n^3 d^{10+\epsilon} HT + nd^3 T^3)$ arithmetic operations (for any $\epsilon > 0$). With classical integer multiplication $O(n^3 d^{11+\epsilon} HT + nd^3 T^3)$ arithmetic operations are required.*

4 Acknowledgements

This work was supported in part by the Advanced Research Projects Agency of the Department of Defense under ONR Contract N00014–92–J–1989, by ONR Contract N00014–92–J–1839, NSF Contract IRI–9006137 and in part by the U.S. Army Research Office through the Mathematical Science Institute of Cornell University.

References

[1] Sigal Ar, Richard J. Lipton, Ronitt Rubinfeld, and Madhu Sudan. Reconstructing algebraic functions from mixed data. In *33th Symposium on Foundations of Computer Science*, pages 503–512. ACM, 1992.

[2] Michael Ben Or and Prasoon Tiwari. A deterministic algorithms for sparse multivariate polynomial interpolation. In *20th Symposium on Theory of Computing*, pages 301–309. ACM, 1988.

[3] Elwyn Ralph Berlekamp. Factoring polynomials over finite fields. *Bell System technical Journal*, 46:1853, 1967.

[4] Elwyn Ralph Berlekamp. Factoring polynomials over large finite fields. *Mathematics of Computation*, 24(111):713–735, July 1970.

[5] David G. Cantor and Hans Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Mathematics of Computation*, 36(154):587–592, April 1981.

[6] Michael Clausen, A. Dress, Johannes Grabmeier, and Marek Karpinski. On zero-testing and interpolation of k-sparse multivariate polynomials over finite fields. Research Report 8522–CS, Universität Bonn, May 1988.

[7] S. D. Cohen. The distribution of Galois groups and Hilbert's irreducibility theorem. *Proceedings of the London Mathematical Society (3)*, 43:227–250, 1981.

[8] Richard A. Demillo and Richard J. Lipton. A probabilistic remark on algebraic program testing. *Information Processing Letters*, 7(4):193–195, June 1978.

[9] K. Dörge. Über die Seltenheit der reduziblen Polynome und der Normalgleichungen. *Mathematische Annalen*, 95:247–256, 1926.

[10] K. Dörge. Zum Hilbertschen Irreduzibilitätssatz. *Mathematische Annalen*, 95:84–97, 1926.

[11] K. Dörge. Einfacher Beweis des Hilbertschen Irreduzibilitätssatzes. *Mathematische Annalen*, 96:176–182, 1927.

[12] Torsten Ekedahl. An effective version of the Hilbert irreducibility theorem. In Catherine Goldstein, editor, *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progress in Mathematics*, pages 241–249, Boston, 1990.

[13] W. Franz. Untersuchugen zum Hilbertschen Irreduzibilitätssatz. *Mathematische Zeitschrift*, 33:275–293, 1931.

[14] Michael D. Fried. On Hilbert's irreducibility theorem. *Journal of Number Theory*, 6:211–231, 1974.

[15] Dima Yu. Grigor'ev and Marek Karpinski. The matching problem for bipartite graphs with polynomial bounded perminants is NC. In *28th Symposium on Foundations of Computer Science*, pages 166–172. ACM, 1987.

[16] Dima Yu. Grigor'ev, Marek Karpinski, and Michael F. Singer. Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields. *SIAM Journal of Computing*, 19(6):1059–1063, 1990.

[17] David Hilbert. über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koefizienten. *Journal für reine und angewante Mathematik*, 110:104–129, 1892.

[18] Ming-Deh A. Huang. Factorization of polynomials over finite fields and decomposition of primes in algebraic number fields. *Journal of Algorithms*, 12(3):482–489, 1991.

[19] Ming-Deh A. Huang. Generalized Riemann hypothesis and factoring polynomials over finite fields. *Journal of Algorithms*, 12(3):464–481, 1991.

[20] Erich Kaltofen. Computing with polynomials given by straight-line programs II: Sparse factorization. In *26th Symposium on Foundations of Computer Science*, pages 451–457. ACM, 1985.

[21] Erich Kaltofen. A polynomial-time reduction from bivariate to univariate integral polynomial factorization. *SIAM Journal of Computing*, 14(2):469–489, May 1985.

[22] Erich Kaltofen and Barry Marshall Trager. Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators. *Journal of Symbolic Computation*, 9(3):301–320, March 1990.

[23] Hans-Wilhelm Knobloch. Zum Hilbertschen Irreduzibilitätssatz. *Abhandlung Mathematische Seminar Univ. Hamburg*, 19:176–190, 1955.

[24] Hans-Wilhelm Knobloch. Die seltenheit der reduziblen polynome. *Jarhesbericht der Deutsche Mathematische Vergeinung*, 59(1):12–19, 1956.

[25] Leopold Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Größen. *Journal für reine und angewante Mathematik*, 92:1–122, 1882.

[26] Arjen K. Lenstra, Hendrik W. Lenstra, Jr., and Laslo Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[27] Victor S. Miller. Factoring polynomials via relation-finding. In Danny Dolev, Zvi Galil, and Michael Rodeh, editors, *Theory of Computing and Systems*, volume 601 of *Lecture Notes in Computer Science*, pages 115–121, New York, 1992. Springer-Verlag.

[28] E. Ng, editor. *EUROSAM '79*, volume 72 of *Lecture Notes in Computer Science*, Berlin-Heidelberg-New York, 1979. Springer-Verlag.

[29] Lajos Rónyai. Galois groups and factoring polynomials over finite fields. In *30th Symposium on Foundations of Computer Science*, pages 99–104. ACM, 1989.

[30] Andrej Schinzel. On Hilbert's irreducibility theorem. *Annales Polinici Mathematici*, 16:333–340, 1965.

[31] Arnold Schönhage. Factorization of univariate integer polynomials by diophantine approximation and an improved basis reduction algorithm. In Jan Paredaens, editor, *Automata, Languages and Programming*, volume 172 of *Lecture Notes in Computer Science*, pages 436–447, Berlin-Heidelberg-New York, 1984. Springer-Verlag.

[32] Jacob T. Schwartz. Probabilistic algorithms for verification of polynomial identities. *Journal of the Association for Computing Machinery*, 27:701–717, 1980.

[33] V. G. Sprindžuk. Reducibility of polynomials and rational points on algebraic curves. *Soviet Mathematics*, 21:331–334, 1980.

[34] V. G. Sprindžuk. Arithmetic specializations in polynomials. *Journal für reine und angewante Mathematik*, 340:26–52, 1983.

[35] Joachim von zur Gathen. Hensel and Newton methods in valuation rings. *Mathematics of Computation*, 42(166):637–661, April 1984.

[36] Joachim von zur Gathen and Erich Kaltofen. Factoring sparse multivariate polynomials. *Journal of Computer and System Sciences*, 31:265–287, 1985.

[37] Richard Eliot Zippel. Probabilistic algorithms for sparse polynomials. In Ng [28], pages 216–226.

[38] Richard Eliot Zippel. Newton's iteration and the sparse Hensel algorithm. In Paul Wang, editor, *SYMSAC '81: Proceedings of the 1981 ACM Symposium on Symbolic and Algebraic Computation*, pages 68–72. Association for Computing Machinery, 1981. Number 505810.

[39] Richard Eliot Zippel. Interpolating polynomials from their values. *Journal of Symbolic Computation*, 9:375–403, March 1990.

A Example

A simple problem that illustrates the ideas of this paper is factoring

$$P(X,Y) = X^4 + 2X^3 - X^2Y^2 + X^2 + 2XY^2 - Y^2,$$

which is an element of $\mathbb{Z}[Y][X]$. Clearly, the maximum degree of Y in any factor of P is 2. The first step is to construct a black box that accepts a value $Y = y_i$ and returns the univariate factors of $P(X,y)$. For almost all $y_i \in \mathbb{Z}$, $P(X,y_i)$ factors into two irreducible quadratic polynomials:

$$\mathscr{B}(y_i) = \{X^2 + a_{11}(y_i)X + a_{10}(y_i), X^2 + a_{21}(y_i)X + a_{20}(y_i)\}.$$

For this small example we will bound our sample points such that $0 \le y < 100$, *i.e.*, $B = 100$. Thus the probability that a randomly chosen y will have properties (1) and (2) is greater than

$$1 - \frac{nD^2k^2}{B} = 1 - \frac{1 \cdot 2^2 \cdot 2^2}{100} \approx 84\%.$$

Choosing $t = 81$ we have

$$\mathscr{B}(81) = \{X^2 + 82X - 81, X^2 - 80X + 81\},$$

and $Q_1(X) = X^2+82X-81$ and $Q_2(X) = X^2-80X+81$. So, unless we have been unlucky, the maximum degree in X of any factor is 2. We now construct two $\mathbb{Z}$ multivalued black boxes,

$$\mathscr{M}^{(1)}(y) = \text{the set of coefficients of the linear terms of } \mathscr{B}(y)$$

$$\mathscr{M}^{(0)}(y) = \text{the set of coefficients of the constant terms of } \mathscr{B}(y)$$

The values of these black boxes are:

y	$\mathscr{M}^{(1)}$	$\mathscr{M}^{(0)}$
1	$\{2,0\}$	$\{1,-1\}$
2	$\{3,-1\}$	$\{2,-2\}$
3	$\{4,-2\}$	$\{3,-3\}$

Using the technique in Section 3.1 these values can be interpolated to produce (using the techniques of Section B)

$$\mathscr{M}^{(1)} \equiv \{1+Y, 1-Y\} \quad \text{and} \quad \mathscr{M}^{(0)} \equiv \{Y, -Y\}.$$

Let $P_i(X,Y)$ be the factor corresponding to $Q_i(X)$. Evaluating the two sets of polynomials above at $Y = 81$ and comparing the values of $Q_i(X)$, we see that

$$P_1(X,Y) = X^2 + (1+Y)X - Y,$$
$$P_2(X,Y) = X^2 + (1-Y)X + Y.$$

So

$$P(X,Y) = (X^2 + (1+Y)X - Y)(X^2 + (1-Y)X + Y).$$

Notice that, except for $Y = 0$, all elements of $\mathbb{Z}$ are Hilbertian for this problem.

B Finding Linear Factors of Bivariate Polynomials

In this section we demonstrate that, given the linear factors of $Q(Z,\theta)$, the linear factors of $Q(Z,\Theta)$ can be found in a very simple fashion.

A subcase of the work in [37,38], is the use of Newton's method to determine the linear factors of a bivariate square free polynomial $Q(Z,\Theta)$ from the linear factors of $Q(Z,\theta)$. Here we give a complete description of this subcase. For clarity we assume that the leading coefficient of Z in $Q(Z,\Theta)$ is 1. In Appendix C we describe how this technique can be adapted to non-monic polynomials.

Let $Q(Z,\Theta)$ be a square free monic polynomial over a ring $\mathbb{Q}[\Theta]$, where $\mathbb{Q}$ is a field. The linear factors of $Q(Z,\Theta)$ are of the form $Z - \alpha(\Theta)$ where α is a polynomial in Θ and $Q(\alpha(\Theta),\Theta) = 0$. Let $\alpha(\Theta)$ have the form

$$\alpha(\Theta) = a_0 + a_1(\Theta - \theta) + \cdots + a_\ell(\Theta - \theta)^\ell.$$

In the following paragraphs we develop an iteration formula based on Newton's method modulo powers of $(\Theta - \theta)$ that allows us to compute $\alpha(\Theta)$ efficiently from Q, θ and a_0, where $Q(a_0,\theta) = 0$. This technique is well known in the computer algebra literature [35,38]. The description is provided here for completeness.

For simplicity, we translate θ to the origin. Let $\bar{Q}(Z,\Theta) = Q(Z,\Theta+\theta)$. Then $Z - a_0$ will be a zero of $\bar{Q}(Z,0)$ and $Z - \bar{\alpha}(\Theta)$ will be a zero of $\bar{Q}(Z,\Theta)$ where

$$\bar{\alpha} = a_0 + a_1\Theta + a_2\Theta^2 + \cdots + a_\ell\Theta^\ell.$$

The image of $\bar{\alpha}$ modulo Θ^{k+1} is denoted by $\alpha^{(k)}$. Thus $\alpha^{(0)} = a_0$, $\alpha^{(1)} = a_0 + a_1\Theta$ and

$$\alpha^{(k)} = a_0 + a_1\Theta + \cdots + a_k\Theta^k.$$

Using the Taylor series expansion, we can write $\bar{Q}(Z,\Theta)$ as a polynomial in $Z - \alpha^{(k-1)}$ giving

$$\bar{Q}(Z,\Theta) = \bar{Q}(\alpha^{(k-1)},\Theta) + \bar{Q}'(\alpha^{(k-1)},\Theta)(Z - \alpha^{(k-1)}) + \frac{\bar{Q}''(\alpha^{(k-1)},\Theta)}{2}(Z - \alpha^{(k)})^2 + \cdots \quad (4)$$

```
LinearNewton (Q(Z,Θ), θ, a_0, ℓ) := {
    w ← -[∂Q(Z,Θ)/∂Z |_{Z=a_0, Θ=θ}]^{-1} ;
    α^(0) ← a_0 ;
    Q̄(Z,Θ) ← Q(Z,Θ+θ);
    for k = 1,...,ℓ do {
        set a_k to w times the coefficient of Θ^k in Q̄(α^(k-1), Θ)
        α^(k) ← α^(k-1) + a_k Θ^k ;
        }
    α ← α^(ℓ)(Θ - θ);
    return(α);
    }
```

Figure 1: Procedure to obtain linear factors

In this and all following expressions, primes ($'$) refer to the partial derivative with respect to the first argument.

Since $Z = \bar{\alpha}$ is a zero of $\bar{Q}(Z, \Theta)$, substituting $Z = \bar{\alpha}$ into (4) gives

$$0 = \bar{Q}(\bar{\alpha}, \Theta) = \bar{Q}(\alpha^{(k-1)}, \Theta) + \bar{Q}'(\alpha^{(k-1)}, \Theta)(\bar{\alpha} - \alpha^{(k-1)}) + \frac{\bar{Q}''(\alpha^{(k-1)}, \Theta)}{2}(\bar{\alpha} - \alpha^{(k)})^2 + \cdots.$$

Notice that $\bar{\alpha} - \alpha^{(k-1)} = a_k \Theta^k + a_{k+1}\Theta^{k+1} + \cdots$. Reducing the above equality modulo Θ^{k+1} gives

$$0 = \bar{Q}(\alpha^{(k-1)}, \Theta) + \bar{Q}'(\alpha^{(k-1)}, \Theta) \cdot a_k \cdot \Theta^k \pmod{\Theta^{k+1}} \tag{5}$$

Since $\alpha^{(k-1)}$ is the image of $\bar{\alpha}$ modulo Θ^k, $\bar{Q}(\alpha^{(k-1)}, \Theta) = 0 \bmod \Theta^k$. Thus we can write $\bar{Q}(\alpha^{((k-1)}, \Theta) = Q_k \Theta^k \bmod \Theta^{k+1}$ where Q_k is an element of the field F. Q_k is a function of Q and $a_0, \ldots, a_{k-1}$. Dividing by Θ^k in (5) gives

$$0 = Q_k + \bar{Q}'(\alpha^{(k-1)}, \Theta) a_k \pmod{\Theta}$$

Reducing the expression on the right hand side modulo Θ is equivalent to substituting $\Theta = 0$ into the right hand side, so solving for a_k gives

$$a_k = -\frac{Q_k}{\bar{Q}'(\alpha^{(k-1)}(0), 0)} = -\frac{Q_k}{\bar{Q}'(a_0, 0)} = -\frac{Q_k}{Q'(a_0, \theta)}. \tag{6}$$

If the characteristic of F is zero and $Q(Z, \theta)$ is square free then $Q'(a_0, \theta)$ does not vanish, since $Z = a_0$ is a simple zero of $Q(Z, \theta)$. If $Q(Z, \Theta)$ has factors over a ring R, then each of the divisions in (6) will be exact.

We have just provided a formula for computing a_k given $a_0, \ldots, a_{k-1}$. This allows us to compute $\alpha^{(k)}$ for any value of k efficiently. Since $\alpha(\Theta)$ does not contain any powers of Θ greater than ℓ, $\alpha(\Theta) = \alpha^{(\ell)}(\Theta - \theta)$.

The procedure in Figure 1 takes $Q(Z, \Theta)$, starting point (θ, a_0) and a degree bound ℓ as inputs and returns $\alpha(\Theta)$, a root of $Q(Z, \Theta)$ corresponding to $(Z, \Theta) = (\theta, a_0)$. `LinearNewton` is a linearly convergent iteration uses $O(\ell^3)$ operations and only requires one division. Quadratically convergent iterations can also be developed and are discussed in [35, 38].

C Non-Monic Polynomials

If we want to factor a non-monic square free polynomial $P(X, Y_1, \ldots, Y_n)$ over a field we proceed as follows. First assume that P is primitive, *i.e.*, no non-constant polynomial in $Y_1, \ldots, Y_n$ divides its coefficients. Assume the true factorization of $P(X, Y_1, \ldots, Y_n)$ is

$$P(X, Y_1, \ldots, Y_n) = P_1(X, Y_1, \ldots, Y_n) \cdots P_k(X, Y_1, \ldots, Y_n),$$

where the leading coefficient of P is $L(Y_1, \ldots, Y_n)$ and the leading coefficient of P_i is $\ell_i(Y_1, \ldots, Y_n)$. Construct a multivalued black box, $\mathscr{B}_P$ that proceeds as follows. Given $\vec{y} = (y_1, \ldots, y_n)$ it obtains the monic factorization:

$$\frac{P(X, y_1, \ldots, y_n)}{L(y_1, \ldots, y_n)} = \bar{P}_1(X) \cdots \bar{P}_k(X).$$

Note that the coefficients of the $\bar{P}(X)$ are the images of rational functions, not polynomials. $\mathscr{B}_P$ then returns the polynomials:

$$L(y_1, \ldots, y_n) \cdot \bar{P}_1(X), \ldots, L(y_1, \ldots, y_n) \cdot \bar{P}_k(X).$$

The coefficients of these polynomials are also polynomials, so we can use the techniques of this paper to compute the polynomials:

$$\tilde{P}_1(X, Y_1, \ldots, Y_n), \ldots, \tilde{P}_k(X, Y_1, \ldots, Y_n),$$

where

$$\tilde{P}_i(X, Y_1, \ldots, Y_n) = \frac{L(Y_1, \ldots, Y_n)}{\ell(Y_1, \ldots, Y_n)} P_i(X, Y_1, \ldots, Y_n).$$

Since the $P_i(X, Y_1, \ldots, Y_n)$ are primitive (by Gauss' lemma), P_i is the primitive part of $\tilde{P}$, *i.e.*, the quotient of $\tilde{P}$ and the GCD of the coefficients of $\tilde{P}$ (with respect to X).

Since L has no more terms than $P(X, Y_1, \ldots, Y_n)$, none of the $\tilde{P}$ will have more than T^2 terms, where T is the maximum number of terms of any of the P_i. Thus we have shown that primitive sparse multivariate polynomials can be factored in polynomial time.

If the polynomial is not primitive then we can still follow this general approach but it must be done one variable at a time. Immediately removing the content of P may not be satisfactory because it has not known how much larger the primitive part of a polynomial can be than its factorization.

D Probabilistic Zero Testing

Given a black box $\mathscr{B}_P$ for a polynomial $P(X_1, \ldots, X_n)$ over a field F, one can probabilistically determine if $P \equiv 0$, by examining $\mathscr{B}_P(x_1, \ldots, x_n)$ for randomly chosen x_i. If the value is ever different from zero then P cannot be the zero polynomial. An estimate of the number of times a non-zero polynomial can take on the value zero is given by the following proposition.

Proposition 7 *Let F be a field, $f \in F[X_1, \ldots, X_n]$ and the degree of f in each of X_i be bounded by d_i. Let $Z_n(B)$ be the number of zeroes of f, $\vec{x}$ such that x_i is chosen from a set with B elements, $B \gg d$. Then*

$$\begin{aligned} Z_n(B) &\leq B^n - (B - d_1)(B - d_2) \cdots (B - d_n) \\ &\approx O\left((d_1 + d_2 + \cdots + d_n)B^{n-1}\right). \end{aligned}$$

A proof of Proposition 7 is given in [39].

The idea of probabilistic zero testing was independently discovered by at least three different groups of researchers at almost the same time. DeMillo and Lipton presented essentially this result in the context of testing the correctness of algebraic programs [8] in 1978. Schwartz [32], used this result in the context of testing for polynomial identities. Zippel [37] used Proposition 7 not just to determine if a polynomial was identically zero, but as part of a complete randomized interpolation algorithm for sparse polynomials.

If a bound is known for the number of non-zero terms in P, then a deterministic algorithm for zero-testing and for sparse interpolation can be given. Results along these lines are given in [2, 6, 15, 16, 39].