On Functional Decomposition of Multivariate Polynomials with Differentiation and Homogenization[1]

Shangwei Zhao, Ruyong Feng and Xiao-Shan Gao
KLMM, Academy of Mathematics and Systems Science
Chinese Academy of Sciences, Beijing 100190, China

Abstract. In this paper, we give a theoretical analysis for the algorithms to compute functional decomposition for multivariate polynomials based on differentiation and homogenization which are proposed by Ye, Dai, Lam (1999) and Faugère, Perret (2006, 2008, 2009). We show that a degree proper functional decomposition for a set of randomly decomposable quartic homogenous polynomials can be computed using the algorithm with high probability. This solves a conjecture proposed by Ye, Dai, and Lam (1999). We also propose a conjecture such that the decomposition for a set of polynomials can be computed from that of its homogenization with high probability. Finally, we prove that the right decomposition factors for a set of polynomials can be computed from its right decomposition factor space. Combining these results together, we prove that the algorithm can compute a degree proper decomposition for a set of randomly decomposable quartic polynomials with probability one when the base field is of characteristic zero, and with probability close to one when the base field is a finite field with sufficiently large number under the assumption that the conjecture is correct.

Keywords. Functional decomposition, multivariate polynomial, homogeneous polynomials, right factor space, cryptosystem analysis.

1 Introduction

Public key cryptography often relies on a hard mathematical problem. One of the hard mathematical problems used in cryptosystems is the functional decomposition problem (FDP) for multivariate polynomials [16]. The general FDP for multivariate polynomials has been proved NP-hard by Dickerson (1989). Based on this fact, Patarin and Goubin (1997) proposed $2R$ scheme which is based on the difficulty of decomposing a set of quartic polynomials. In the original design, K denotes a finite field of q elements. The private key consists of:

1. Three linear bijections r, s, t: $K^n \to K^n$.

[1)] Partially supported by a National Key Basic Research Project of China and by a grant from NSFC.

2. Two quadratic polynomial mappings ψ, ϕ: $K^n \to K^n$.

The public key consists of:

1. The field K and n.

2. The composition of polynomial mapping $\pi = t \circ \psi \circ s \circ \phi \circ r$, which is a set of polynomials of degree four.

In the encryption system, the quadratic polynomials are chosen from the given S-boxes, which can be inverted easily. Given the composition of two quadratic polynomials, if we know the private key, then we can obtain the plaintext. Otherwise, it is difficult to invert the polynomials of degree four directly. So, attack on the 2R scheme is reduced to the functional decomposition of quartic polynomials.

Efficient algorithms for several special forms of FDP are known. Polynomial-time algorithms are proposed for univariate decomposition of multivariate polynomials and multivariate decomposition of univariate polynomials [5, 6, 7]. Efficient algorithms for a kind of monomial decompositions of rational functions are proposed in [1], which is further extended to a complete decomposition algorithm for rational parametrization of ruled-surfaces [13, 14].

Ye, Dai, and Lam (1999) proposed an efficient algorithm for decomposing a set of n polynomials of degree four into two sets of quadratic polynomials [19]. The key idea of computing the FDP is to differentiate f to obtain a set of cubic polynomials and try to recover the right decomposition factors from these cubic polynomials. The idea of differentiation introduced in [19] is a very powerful technique in tackling FDP of multivariate polynomials. In a series of papers [8, 9, 10], Faugère and Perret made significant contributions to this problem by integrating the idea of differentiation and fast Gröbner basis computation. In particular, they proposed polynomial-time algorithms for FDP of semi-regular multivariate polynomial sets. As a consequence, the current known schemes based on FDP of multivariate polynomials are considered broken.

As far as we know, the method based on differentiation and homogenization is the only efficient approach to tackle some of the general FDP. But, these algorithms make strong assumptions on the input polynomial sets and these assumptions are expected to be valid and can be removed. This paper focuses on the theoretical analysis of the decomposition algorithm based on differentiation and homogenization. The main contribution is that the algorithm can be used to compute a degree proper decomposition for a set of randomly decomposable quartic homogeneous polynomials with probability one when the base field is of characteristic zero, and with probability close to one when the base field is a finite field with sufficiently large number in polynomial time. And if the conjecture we proposed is correct, it holds for nonhomogeneous case.

We show that a degree proper functional decomposition for a set of randomly decomposable quartic homogenous polynomials can be computed using the algorithm with high probability. This solves a conjecture proposed by Ye, Dai, and Lam (1999). We also propose a conjecture such that the decomposition for a set of polynomials can be computed from that of its homogenization with high probability. Finally, we prove that the right decomposition factors for a set of polynomials can be computed from its right decomposition factor space. Combining these results together, we prove that if the conjecture is correct then the algorithm can compute a degree proper decomposition for a set of randomly decomposable

quartic polynomials with probability one when the base field is of characteristic zero, and with probability close to one when the base field is a finite field with sufficiently large number.

The rest of this paper is organized as follows. In section 2, we give the main result. In sections 3, 4 and 5, we prove our results for the three major steps of the algorithm. In section 6, the algorithm is given and its complexity is analyzed. In section 7, we conclude the paper by proposing two open problems.

2 Problem and main result

In this section, we will present the problem and give the main results of the paper.

Let K be a field and $\mathcal{R} = K[x_1, \ldots, x_n]$ the polynomial ring in indeterminates $x_1, \ldots, x_n$ over K. For natural numbers u and m, the functional composition of two sets of multivariate polynomials $g = (g_1, \ldots, g_u) \in K[x_1, \ldots, x_m]^u$ and $h = (h_1, \ldots, h_m) \in \mathcal{R}^m$ is a set of polynomials in $\mathcal{R}^u$:

$$(f_1, \ldots, f_u) = (g_1(h_1, \ldots, h_m), \ldots, g_u(h_1, \ldots, h_m)). \tag{1}$$

That is,

$$f = g \circ h$$

We call g and h the left and right **decomposition factors** of f respectively. The decomposition is called nontrivial if both g and h contain nonlinear polynomials.

The **functional decomposition problem** (FDP) of multivariate polynomials is the inverse of the above functional composition procedure. That is, given a set of u polynomials $f = (f_1, \ldots, f_u) \in \mathcal{R}^u$ and a positive number m, to find $g = (g_1, \ldots, g_u) \in K[x_1, \ldots, x_m]^u$ and $h = (h_1, \ldots, h_m) \in \mathcal{R}^m$ such that $f = g \circ h$.

It is shown that f always has a nontrivial decomposition when $m > n$, which is easy to construct [4]. Then we assume that $1 \leq m \leq n$. Moreover, note that in cryptosystems, the field K is usually finite and we usually consider the case that $m = n$. So in the following paper, assume that $m = n$.

A basic idea of the differentiation approach is to compute the linear space generated by the right factors of f from the linear space generated by certain differentiations of the polynomials in f. For a polynomial sequence $f = (f_1, \ldots, f_u) \in \mathcal{R}^u$ with a decomposition like (1), let

$$R_{(f:h)} = \mathrm{span}_K\{h_1, \ldots, h_n\}$$

be the linear space generated by h_i over K, called a **right factor space** of f.

Another idea of the approach is to use homogenization. More precisely, we first compute a decomposition for the homogenization of f and then try to recover a decomposition of f from this decomposition. Let $d_f = \max(d_{f_i})$, $d_g = \max(d_{g_i})$, $d_h = \max(d_{h_i})$. The **homogenizations** of f, g, h are respectively defined as follows [9, 19]:

$$f^* = (x_0^{d_f}, x_0^{d_f} f_1(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}), \ldots, x_0^{d_f} f_u(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}))$$

$$g^* = (x_0^{d_g}, x_0^{d_g} g_1(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}), \ldots, x_0^{d_g} g_u(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}))$$
$$h^* = (x_0^{d_h}, x_0^{d_h} h_1(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}), \ldots, x_0^{d_h} h_n(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})).$$

Then the approach proposed in [8, 9, 10, 19] can be divided into three major steps which will be explained later.

Algorithm FDPMP

- Compute a right factor space $R_{(f^*:h^*)}$ for the homogenization f^* of f.
- Compute a right factor space $R_{(f:h)}$ from $R_{(f^*:h^*)}$.
- Compute an FDP for f from $R_{(f:h)}$.

We will show that there exists a complete polynomial time algorithm for Step 3, while for Step 1, there exist probabilistic algorithms in certain cases. We will discuss Steps 1, 2, 3 in the next three sections.

A decomposition $f = g \circ h$ satisfying the following condition

$$d_f = d_g \cdot d_h \tag{2}$$

is called a **degree proper decomposition**, where d_f, d_g, and d_h are the degrees of f, g, and h respectively. All decompositions in this paper are assumed to be degree proper unless mentioned otherwise. In this paper, we will show that the scheme **FDPMP** can be developed into a polynomial time decomposition algorithm for certain degree proper decompositions with high probability for random homogeneous polynomials. Here, a set of polynomials f is called **random** or **randomly decomposable** if $f = g \circ h$ and g, h are random polynomials.

Theorem 2.1 *Let $f \in K[x_1, \ldots, x_n]^n$ be a set of quartic homogeneous polynomials, each polynomial is of the same degree, for $n \geq 5$, we have a polynomial time probabilistic algorithm to find a degree proper decomposition $f = g \circ h$ for $g, h \in K[x_1, \ldots, x_n]^n$. For a random decomposition f, the algorithm will give correct result with probability one when K is of characteristic zero, and with probability close to one when $K = F_q$ and q is a sufficiently large number.*

If the conjecture proposed in Step 2 is correct, then we have the following theorem.

Theorem 2.2 *Let $f \in K[x_1, \ldots, x_n]^n$ be a set of polynomials with degree less than or equal to four, and at least one polynomial has degree four. Assume that Conjecture 5.4 is correct, then, for $n \geq 5$, we have a polynomial time probabilistic algorithm to find a degree proper decomposition $f = g \circ h$ for $g, h \in K[x_1, \ldots, x_n]^n$. For a random decomposition f, the algorithm will give correct result with probability one when K is of characteristic zero, and with probability close to one when $K = F_q$ and q is a sufficiently large number.*

The main idea to prove the above result is to consider the generic FDP. A generic polynomial of degree d in $K[x_1, \ldots, x_n]$ is of the form $\sum u_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n}$ $(i_1 + \cdots + i_n \leq d)$ where $u_{i_1 \ldots i_n}$ are indeterminates. An FDP $f = g \circ h$ is call a **generic decomposition** if g and h are generic polynomials of degrees greater than one.

We will show that if $f = g \circ h$ is a generic FDP for two quadratic polynomials g and h, then we can compute g and h with a polynomial number of arithmetic operations in the coefficients fields of g and h. Furthermore, when the coefficients of g and h specialize to concrete values in the base field K, the algorithm still works with probability close to one.

Remark 2.3 *Let $N = n(n+1)(n+2)$. Then the coefficients of g and h can be considered as an element of K^N. For convenience, we can also say that (g, h) is an element of K^{2N}. From the above analysis, if K is of characteristic zero, then the coefficients of g and h for which the algorithm fails to compute the decomposition $g \circ h$ consists of an algebraic variety in K^N. In other words, these (g, h) is a subset of K^N with dimensions lower than $2N$. In this sense, we say that the algorithm will succeed with probability one. If K is a finite field, we will give an estimation of the size of the failure subset and show that it is very small compared with N.*

3 Compute an FDP from a right factor space

In this section, we will show how to compute a decomposition for f from its right factor space efficiently. We discuss this problem first, because the result in this section will be used in Section 5. Also, among the three steps of the Algorithm **FDPMP**, this is the only step that has a complete solution.

We first prove several basic properties for $R_{(f:h)}$.

Lemma 3.1 *Two equivalent decompositions of f have the same right factor space.*

Proof. Suppose that f has two equivalent decompositions $g \circ h = g' \circ h'$. By the definition of equivalent decompositions, there exists a nonsingular matrix $A \in GL_n(K)$ such that $h' = h \cdot A$. Therefore, $\mathrm{span}_K\{h_1, \ldots, h_n\} = \mathrm{span}_K\{h'_1, \ldots, h'_n\}$. ∎

The following result shows that the FDP of a set of polynomials can be reduced to the FDP of several single polynomials. Denote the set of all right factor spaces of F by SR_F.

Lemma 3.2 *If $f = (f_1, \ldots, f_u) \in \mathcal{R}^u$, then*

$$SR_f = \cap_{i=1}^{u} SR_{f_i}. \tag{3}$$

Proof. It is clear that $SR_f \subseteq \cap_{i=1}^{u} SR_{f_i}$. Assume that $W \in \cap_{i=1}^{u} SR_{f_i}$ and $h_1, \cdots, h_m$ be a basis of W. Then there are $g_i \in K[x_1, \cdots, x_m]$ such that $f_i = g_i(h_1, \cdots, h_m)$. Hence $W \in SR_f$. ∎

Since computing the intersection of two linear spaces is easy, we may reduce the FDP of f to the FDP of a single polynomial f_i.

The approaches in [8, 19] are based on the idea of right factor space. But, the power of this idea is not fully explained in previous work. For instance, it is assumed that the rank of R_f is n in [9]. It is clear that this condition is not necessarily correct since h can be a set of arbitrary polynomials. For instance, if $h = (\sum_{i=1}^{n} x_i^2, x_2^2, \ldots, x_2^2)$ then the rank of R_f is always two for any decomposition $f = g \circ h$.

The following result shows that we can recover a right decomposition factor for f from $R_{(f:h)}$ under any condition.

Theorem 3.3 *Let $B = \{b_1, \ldots, b_k\}$ be a basis of $R_{(f:h)} = \mathrm{span_K}\{h_1, \ldots, h_n\}$. If $\dim(R_{(f:h)}) = k = n$, then B is a right decomposition factor of f. If $\dim(R_{(f:h)}) = k < n$, then $(b_1, \ldots, b_k, b_1, \ldots, b_1)$ is a right decomposition factor of f.*

Proof. Firstly, assume that $\dim(R_{(f:h)}) = n$. Since $\{h_1, \ldots, h_n\} \in R_{(f:h)}$ and B is a basis of $R_{(f:h)}$, each h_i can be expressed as a linear combination of $\{b_1, \ldots, b_n\}$. That is, there exists an invertible matrix $P \in GL_n(K)$ such that $(h_1, \ldots, h_n) = (b_1, \ldots, b_n) \cdot P$. Then $f = g \circ h = g(X \cdot P) \circ (h \cdot P^{-1}) = g(X \cdot P) \circ (b_1, \ldots, b_n)$, where $X = (x_1, \ldots, x_n)$. Therefore, B is also a right decomposition factor of f.

Secondly, let $\dim(R_{(f:h)}) = k < n$. For the decomposition of $f = g \circ h$, since $\{h_1, \ldots, h_n\} \in R_{(f:h)}$ and B is a basis of $R_{(f:h)}$, $h_i = \sum_{j=1}^{k} a_{i,j} b_j$.

Therefore, we have

$$(h_1, \ldots, h_n) = (b_1, \ldots, b_k) \begin{pmatrix} a_{11} & \ldots & a_{n1} \\ \vdots & \ddots & \vdots \\ a_{1k} & \ldots & a_{nk} \end{pmatrix}.$$

and $(a_{ij})_{k \times n}$ contains a nonsingular $k \times k$ submatrix, or else $\dim(\mathrm{span}_K\{h_1, \ldots, h_n\}) < k$, a contradiction.

Suppose that

$$\det \begin{pmatrix} a_{11} & \ldots & a_{k1} \\ \vdots & \ddots & \vdots \\ a_{1k} & \ldots & a_{kk} \end{pmatrix} \neq 0.$$

Then $(h_1, \ldots, h_n) = (b_1, \ldots, b_k, h_{k+1}, \ldots, h_n)A$, where

$$A = \begin{pmatrix} a_{11} & \ldots & a_{k1} & \\ \vdots & \ddots & \vdots & \\ a_{1k} & \ldots & a_{kk} & \\ & & & I_{n-k} \end{pmatrix}$$

is an $n \times n$ invertible matrix. Moreover, let

$$B = \begin{pmatrix} & -a_{k+1,1}+1 & -a_{k+2,1}+1 & \dots & -a_{n,1}+1 \\ & -a_{k+1,2} & -a_{k+2,2} & \dots & -a_{n,2} \\ I_k & \vdots & \vdots & \ddots & \vdots \\ & -a_{k+1,k} & -a_{k+2,k} & \dots & -a_{n,k} \\ & & I_{n-k} & & \end{pmatrix}$$

be an $n \times n$ invertible matrix. It is easy to see that

$$(b_1, \dots, b_k, b_1, \dots, b_1) = (b_1, \dots, b_k, h_{k+1}, \dots, h_n)B.$$

Hence,

$$(h_1, \dots, h_n) = (b_1, \dots, b_k, b_1, \dots, b_1)B^{-1}A.$$

Since $B^{-1}A$ is nonsingular, there exists a g'' such that $f = g'' \circ (b_1, \dots, b_k, b_1, \dots, b_1)$ which is an equivalent form of $f = g \circ h$. So we can choose $(b_1, \dots, b_k, b_1, \dots, b_1)$ as a right decomposition factor of f. ∎

Note that the last $n - k$ elements b_1 in the right factor can be replaced with any b_i in Theorem 3.3.

Corollary 3.4 *Corresponding to a given right factor space $R_{(f:h)}$, f has a unique decomposition under the relation of equivalence.*

Restricted to decomposition of quartic polynomials considered in Theorem 2.2, we have the following result.

Theorem 3.5 *Use the same assumption as Theorem 2.2. If $R_{(f:h)}$ is known, we can compute g with $O(n^{3\omega})$ arithmetic operations in the field K, where $2 \le \omega < 3$.*

Proof. Suppose $R_{(f:h)} = \mathrm{span}_K(h_1, \dots, h_k)$ is known. Then a right decomposition factor of f is also known by Theorem 3.3. To find g, we may simply by solving a system of linear equations with the coefficients of g as indeterminates. Note that g has $nC_n^2 = O(n^3)$ coefficients. Then we need $O((n^3)^\omega) = O(n^{3\omega})$ arithmetic operations in K to find g, where ω is the matrix exponent [2] to measure the complexity of solving linear equations. ∎

4 Decomposition of a set of homogenous polynomials

In this section, we consider the decomposition of f when each polynomial of it is homogeneous of the same degree. More precisely, we will consider the following problem: "Let f be a set of quartic homogeneous polynomials. Find a decomposition $f = g \circ h$ where g, h are sets of quadratic homogeneous polynomials."

We may consider the problem in two steps. First, we compute the following linear space over K

$$\widetilde{V}_f = \mathrm{span}_K\{\frac{\partial f_i}{\partial x_j} : 1 \le i \le u, 1 \le j \le n\}. \tag{4}$$

Since $f = g \circ h$ and g consists of quadratic polynomials, it is clear that $\widetilde{V}_f$ is contained in the following linear space.

$$V_f = \mathrm{span}_K\{x_i h_j : 1 \le i, j \le n\}. \tag{5}$$

The following example shows that $\widetilde{V}_f$ could be a proper subset of V_f.

Example 4.1 *Let* $f = (xy^2z, x^2y^2 + xy^2z, xy^2z + y^2z^2)$, $g = (xz, x^2 + xz, xz + z^2), h = (xy, y^2, yz)$. *It is easy to check that* $f = g \circ h$. *We have* $\widetilde{V}_f = \mathrm{span}_K\{xyz, y^2z, yz^2, xy^2, x^2y\}$ *and* $V_f = \mathrm{span}_K\{xyz, y^2z, yz^2, xy^2, x^2y, y^3\}$. $\widetilde{V}_f$ *is a proper subset of* V_f. *Later in this section, we will see that* h *cannot be recovered from its corresponding* $\widetilde{V}_f$ *in this example.*

The idea of the algorithm is to compute $\widetilde{V}_f$ first, then try to recover V_f from $\widetilde{V}_f$, and finally compute $R_{(f:h)}$ from V_f. We will analyze the above procedure in the following two subsections. The problem is divided into two cases: $u = n$ or $u < n$.

4.1 The case when $u = n$

We divide the procedure into two steps: to compute V_f from $\widetilde{V}_f$ and to recover $R_{(f:h)}$ from V_f.

A. Compute V_f from $\widetilde{V}_f$

When $u = n$, $\widetilde{V}_f$ is generated by n^2 cubic polynomials, and $\dim(\widetilde{V}_f) \le \dim(V_f) \le n^2$. In the next theorem, we will show that the probability for $\widetilde{V}_f = V_f$ is close to one under some conditions. The idea of the proof is to find a nonsingular matrix A in some indeterminates such that if a set of specialization of these indeterminates does not vanish $|A|$ then $\widetilde{V}_f = V_f$.

Theorem 4.2 *For randomly chosen* g *and* h, *let* $f = g \circ h$. *Then*

1. $\widetilde{V}_f = V_f$ *with probability one when the field* K *is of characteristic zero.*
2. $\widetilde{V}_f = V_f$ *with probability close to one when* $K = GF(q)$ *and* q *is sufficiently large.*

Proof. Assume that

$$f_i = \sum_{1 \le k,l \le n} a_{k,l}^{(i)} h_k h_l, (1 \le i \le n)$$

where $a_{k,l}^{(i)} = a_{l,k}^{(i)}$ for $1 \le k, l \le n$, and

$$h_i = \sum_{1 \le k \le l \le n} b_{k,l}^{(i)} x_k x_l, (1 \le i \le n).$$

Then

$$\frac{\partial f_i}{\partial x_j} = \sum_{1\le k,l\le n} a_{k,l}^{(i)}(h_k\frac{\partial h_l}{\partial x_j} + h_l\frac{\partial h_k}{\partial x_j}).$$

Let

$$U_i = \left(\frac{\partial f_1}{\partial x_i}, \frac{\partial f_2}{\partial x_i}, \cdots, \frac{\partial f_n}{\partial x_i}\right), V_i = (x_ih_1, x_ih_2, \cdots, x_ih_n), \text{ for } i = 1, \cdots, n.$$

Let $U = (U_1, U_2, \cdots, U_n)^T$ and $V = (V_1, V_2, \cdots, V_n)^T$. Each $\frac{\partial f_i}{\partial x_j}$ can be represented by a linear combination of $\{x_kh_l, 1 \le k, l \le n\}$ over K and the coefficients are expressions in $a_{k,l}^{(i)}, b_{k,l}^{(i)}$. So, there exists an $n^2 \times n^2$ matrix A such that $U = A \cdot V$ where the elements of A are polynomials in $a_{k,l}^{(i)}, b_{k,l}^{(i)}$. We will prove the $\det(A) \neq 0$. We make the following substitutions in A: $a_{k,l}^{(i)} = (k+l)^i$ and $b_{k,l}^{(i)} = \delta_{k,l}$ and denote the new matrix by $\bar{A}$, where $\delta_{k,l}$ is the Kronecker's delta. After making these substitutions, one has $f_i = \sum_{k,l}(k+l)^i x_k^2 x_l^2$ and $h_i = x_i^2$ for $1 \le k, l, i \le n$. Now we have

$$\frac{\partial f_i}{\partial x_s} = 4\sum_{k=1}^{n}(s+k)^i x_s x_k^2, \text{ for } i, s = 1, \cdots, n,$$

which imply that for all $s = 1, \cdots, n$,

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_s} \\ \frac{\partial f_2}{\partial x_s} \\ \vdots \\ \frac{\partial f_n}{\partial x_s} \end{pmatrix} = \begin{pmatrix} 4(1+s) & 4(2+s) & \dots & 4(n+s) \\ 4(1+s)^2 & 4(2+s)^2 & \dots & 4(n+s)^2 \\ \vdots & \vdots & & \vdots \\ 4(1+s)^n & 4(2+s)^n & \dots & 4(n+s)^n \end{pmatrix} \cdot \begin{pmatrix} x_s x_1^2 \\ x_s x_2^2 \\ \vdots \\ x_s x_n^2 \end{pmatrix}.$$

Therefore $\det(\bar{A})$ is the products of a constant and n Vandermonde determinants, which is nonzero. Hence $\det(A) \neq 0$. One can easily see that the total degree of $\det(A)$ in $a_{k,l}^{(i)}, b_{k,l}^{(i)}$ equals $2n^2$.

When g and h specialize to concrete polynomials in $K[x_1, \ldots, x_n]^n$, if A is invertible then each element of V_f can be represented by a linear combination of the elements of $\widetilde{V}_f$. So, $V_f = \widetilde{V}_f$.

When K is of characteristic zero, $\det(A) \neq 0$ with probability one in the sense explained in Remark 2.3. When $K = GF(q)$, $\det(A) \neq 0$ with probability at least $\frac{q-d}{q} = \frac{q-2n^2}{q}$ which is close to one when q is sufficiently large [15]. These conclude the theorem. ∎

When $\widetilde{V}_f \neq V_f$, Ye et al proposed a heuristic method to enlarge $\widetilde{V}_f$, but there is no theoretical guarantee that the enlarged $\widetilde{V}_f$ is equal to V_f [19].

B. Recover $R_{(f:h)}$ from V_f

In this subsection, we assume that the space V_f is known and show how to recover $R_{(f:h)}$ from V_f. Given a vector space $V \subseteq K[x_1, \cdots, x_n]$ and a set $S \subseteq K[x_1, \cdots, x_n]$, we define $(V : S) = \{h | \forall s \in S,\ sh \in V\}$.

By the definition of V_f, $x_i h_j \in V_f$ for all i, j. Hence, $h_j \in (V_f : x_i)$, and then $R_{(f:h)} \subseteq (V_f : x_i)$, for all i. So we have

$$R_{(f:h)} \subseteq \cap_i (V_f : x_i) = (V_f : L),$$

where L is the linear space generated by the variables $x_1, \ldots, x_n$.

Note that $R_{(f:h)} \subseteq (\widetilde{V}_f : L)$ does not always hold. In Example 4.1, $(\widetilde{V}_f : L) = \{yz, xy\}$ while $R_{(f:h)} = \{yz, xy, y^2\}$. $(\widetilde{V}_f : L)$ is a proper subset of $R_{(f:h)}$. However, by Theorem 4.2, in the general case, $R_{(f:h)} \subseteq (V_f : L) = (\widetilde{V}_f : L)$ with probability one when K is of characteristic zero and close to one when $K = GF(q)$ and q is sufficiently large.

One may ask that whether $R_{(f:h)} = (V_f : L)$? It is not always true as shown by the following example.

Example 4.3 *Let* $f = (x^2y^2, x^4 + y^4)$, $g = (xy, x^2 + y^2)$ *and* $h = (x^2, y^2)$. $(V_f : L) = \text{span}_K\{xy, x^2, y^2\}$. $R_{(f:h)}$ *is a proper subset of* $(V_f : L)$.

Ye et al proposed a conjecture which suggests that for random $R_{(f:h)}$, the two spaces are equal with probability close to one no matter whether $\dim(R_{(f:h)}) = n$ or $\dim(R_{(f:h)}) < n$ [19]. The conjecture is as follows:

Conjecture Y[19, p319] Let W be a linear space of dimension $\leq n$ consisting of quadratic forms in n variables $x_1, \ldots, x_n$, and L be the linear space generated by $x_1, \ldots, x_n$, $V = \sum_{1 \leq i \leq n} x_i W$. For randomly chosen W, the probability ρ that $(V : L) = W$ is very close to one when $n > 2$.

It is one of the theoretical foundations of the differentiation approach. The authors [19] did not prove it and just gave a justification with some heuristic arguments. The work of Faugère and Perret is also based on this basic fact. When the number of $(V_f : L)$ equals n, they regarded $(V_f : L)$ as $R_{(f:h)}$ in their algorithm [8, 9].

We will give a proof of the conjecture when $n \geq 5$. Actually, we will extend the conjecture into a more general case that W and L are linear spaces consisting of homogeneous polynomials with higher degree and give a proof for this extension of the conjecture. The assumption $n \geq 5$ is not a strict limitation since in practical usages, n is much larger than five. The number q is always large in $2R$ or $2R^-$ scheme [8, 9]. Before proving the conjecture, we need a technical lemma. Let $P = (p_1, \cdots, p_n) \in \mathbb{N}^n$. In the following, we will always use X^P to denote the monomial $x_1^{p_1} \cdots x_n^{p_n}$ and $M(d', x_1, \cdots, x_n)$ to denote the set of all monomials in $x_1, \cdots, x_n$ with degree d'.

Lemma 4.4 *Assume that* $h_i = \sum_{|P|=d} a_P^{(i)} X^P \in K[a_P^{(i)}, x_1, \cdots, x_n]$ *are homogeneous polynomials in* $x_1, \cdots, x_n$ *with degree* d, *where* $i = 1, \cdots, n+1$ *and* $a_P^{(i)} \in K$. *Assume that* $d' < d$ *and* $n \geq 2d$. *Then if* $\{mh_i | m \in M(d', x_1, \cdots, x_n), i = 1, 2, \cdots, n+1\}$ *are linearly dependent over* K, *then* $\left(a_P^{(i)}\right)$ *will vanish a set of polynomials with total degree at most* $n\binom{n+d'-1}{d'}$.

Proof. Let us consider $a_P^{(i)}$ as indeterminates for a moment. Assume that $H = \sum c_{m,i} m h_i$ where $c_{m,i}$ are indeterminates. Regarding H as a polynomial in $x_1, \cdots, x_n$, one can see

that H is a polynomial with $\binom{n+d+d'-1}{d+d'}$ monomials whose coefficients are polynomials in $c_{m,i}, a_P^{(i)}$. Setting $H = 0$, one can get a system of the equations as follows: $A\vec{c} = 0$, where A is a $\binom{n+d+d'-1}{d+d'}$ by $n\binom{n+d'-1}{d'}$ matrix with entries linearly in the $a_P^{(i)}$, and $\vec{c} = (c_{m_1,1}, \cdots, c_{m_j,i}, \cdots)$. By the computation, one can show that $\binom{n+d+d'-1}{d+d'} > n\binom{n+d'-1}{d'}$. Hence A is of full rank if and only if $\{mh_i | m \in M(d', x_1, \cdots, x_n), i = 1, \ldots, n+1\}$, are linearly independent. To prove A is of full rank, one only need to prove this for a specialization of A. Since $n \geq 2d$, let $h_1 = x_1^d, h_2 = x_2^d, \ldots, h_n = x_n^d, h_{n+1} = x_1x_2\cdots x_d + x_{d+1}x_{d+2}\cdots x_{2d}$. It leads to a specialization of the matrix A. Denote this specialization by $\bar{A}$. We claim that $\bar{A}$ is of full rank, which is equivalent to claim that the polynomials $mx_j^d, m(x_1\cdots x_d + x_{d+1}\cdots x_{2d}), m \in M(d', x_1, \cdots, x_n), j = 1, \cdots, n$, are linearly independent. Assume that

$$\bar{H} = \sum_{m,i} \bar{c}_{m,i} m x_i^d + \sum_m \bar{b}_m m(x_1\cdots x_d + x_{d+1}\cdots x_{2d}) = 0$$

where $\bar{c}_{m,i}, \bar{b}_m \in K$. For convenience, denote $\partial x_1^{q_1}\cdots\partial x_n^{q_n}$ by ∂m where $m = x_1^{q_1}\cdots x_n^{q_n}$. One can see that

$$\frac{\partial^{d+d'}(\bar{H})}{\partial m x_i^d} = \begin{cases} *\bar{c}_{m,i} & \forall\ m' \in M, m'x_1\cdots x_d \neq mx_i^d \text{ and } m'x_{d+1}\cdots x_{2d} \neq mx_i^d; \\ *\bar{c}_{m,i} + *\bar{b}_{m'} & \exists\ m' \in M \text{ s.t. } m'x_1\cdots x_d = mx_i^d \text{ or } m'x_{d+1}\cdots x_{2d} = mx_i^d; \end{cases}$$

$$\frac{\partial^{d+d'}(\bar{H})}{\partial m h} = \begin{cases} *\bar{b}_m & h = x_1\cdots x_d \text{ and } \forall\ m' \in M\ \forall\ i,\ mx_1\cdots x_d \neq m'x_i^d; \\ *\bar{c}_{m',i} + *\bar{b}_m & h = x_{d+1}\cdots x_{2d} \text{ and } \exists\ m' \in M\ \exists\ i\ s.t.\ mx_1\cdots x_d = m'x_i^d; \end{cases}$$

where $*$ denote positive integers. Since $\frac{\partial^{d+d'}(\bar{H})}{\partial \tilde{m}} = 0$ for all monomials $\tilde{m}$, the claim is proved. Therefore A is of full rank. Now consider the $a_P^{(i)}$ as the elements in K. If $\{mh_i | m \in M(d', x_1, \cdots, x_n), i = 1, 2, \cdots, n+1\}$ are linearly dependent, which implies that $A\vec{c} = 0$ has a nontrivial solution, then $\left(a_P^{(i)}\right)$ must vanish the determinants of all $n\binom{n+d'-1}{d'}$ by $n\binom{n+d'-1}{d'}$ submatrices of A. This completes the proof. ∎

Let $h = (h_1, h_2, \cdots, h_n)$ where the h_i are homogeneous polynomials with the same degrees in $K[x_1, \cdots, x_n]$ and let d_h be the degree of h_i. Denote

$$U(h, d') = \text{span}_K\{mh_i | m \in M(d', x_1, \cdots, x_n), i = 1, 2, \cdots, n\}.$$

Let $W = \text{span}_K\{h_1, \cdots, h_n\}$. Then we have

Theorem 4.5 *For randomly chosen $h_1, h_2, \cdots, h_n$, if $d' < d_h$ and $n > 2d_h$, then the probability ρ that $(U(h, d') : x_1^{d'}) = W$ is one when the field K is of characteristic zero and close to one when $K = GF(q)$ with q sufficiently large.*

Proof. Assume that $h_i = \sum_{|P|=d_h} a_P^{(i)} X^P \in K[x_1, \cdots, x_n]$, where the $a_P^{(i)} \in K$. Denote $\overline{U} = \{H \in U(h, d') |\ x_1^{d'} | H\}$. For $\sum_i G_i h_i \in \overline{U}$, let

$$G_i = \widetilde{G}_{0,i}x_1^{d'} + \widetilde{G}_{1,i}x_1^{d'-1} + \ldots + \widetilde{G}_{d'-2,i}x_1^2 + \widetilde{G}_{d'-1,i}x_1 + \widetilde{G}_{d',i}$$

and

$$h_i = \widetilde{h}_{0,i}x_1^{d_h} + \widetilde{h}_{1,i}x_1^{d_h-1} + \ldots + \widetilde{h}_{d_h-2,i}x_1^2 + \widetilde{h}_{d_h-1,i}x_1 + \widetilde{h}_{d_h,i},$$

where $\widetilde{G}_{0,i}, \widetilde{G}_{1,i}, \ldots, \widetilde{G}_{d',i}$ are homogeneous polynomials in $x_2, \ldots, x_n$ with degree $0, 1, \ldots, d'$ respectively and $\widetilde{h}_{0,i}, \widetilde{h}_{1,i}, \ldots, \widetilde{h}_{d_h,i}$ are homogeneous polynomials in $x_2, \ldots, x_n$ with degree $0, 1, \ldots, d_h$ respectively. Since $\sum_i G_i h_i \equiv 0 \bmod x_1^{d'}$, we have

$$\begin{aligned}\sum_i G_i h_i \equiv \sum_i \Big(& x_1^{d'-1}\left(\widetilde{G}_{1,i}\widetilde{h}_{d_h,i} + \widetilde{G}_{2,i}\widetilde{h}_{d_h-1,i} + \ldots + \widetilde{G}_{d',i}\widetilde{h}_{d_h-d'+1,i}\right) \\ & + x_1^{d'-2}\left(\widetilde{G}_{2,i}\widetilde{h}_{d_h,i} + \widetilde{G}_{3,i}\widetilde{h}_{d_h-1,i} + \ldots + \widetilde{G}_{d',i}\widetilde{h}_{d_h-d'+2,i}\right) + \ldots \\ & + x_1^2\left(\widetilde{G}_{d'-2,i}\widetilde{h}_{d_h,i} + \widetilde{G}_{d'-1,i}\widetilde{h}_{d_h-1,i} + \widetilde{G}_{d',i}\widetilde{h}_{d_h-2,i}\right) \\ & + x_1\left(\widetilde{G}_{d'-1,i}\widetilde{h}_{d_h,i} + \widetilde{G_{d',i}}\widetilde{h}_{d_h-1,i}\right) + \widetilde{G}_{d',i}\widetilde{h}_{d_h,i}\Big) \\ \equiv 0 \bmod & \ x_1^{d'}.\end{aligned}$$

Therefore,

$$\sum_i \left(\widetilde{G}_{1,i}\widetilde{h}_{d_h,i} + \widetilde{G}_{2,i}\widetilde{h}_{d_h-1,i} + \ldots + \widetilde{G}_{d',i}\widetilde{h}_{d_h-d'+1,i}\right) = 0, \tag{6}$$

$$\sum_i \left(\widetilde{G}_{2,i}\widetilde{h}_{d_h,i} + \widetilde{G}_{3,i}\widetilde{h}_{d_h-1,i} + \ldots + \widetilde{G}_{d',i}\widetilde{h}_{d_h-d'+2,i}\right) = 0, \tag{7}$$

$$\vdots$$

$$\sum_i \left(\widetilde{G}_{d'-2,i}\widetilde{h}_{d_h,i} + \widetilde{G}_{d'-1,i}\widetilde{h}_{d_h-1,i} + \widetilde{G}_{d',i}\widetilde{h}_{d_h-2,i}\right) = 0, \tag{8}$$

$$\sum_i \left(\widetilde{G}_{d'-1,i}\widetilde{h}_{d_h,i} + \widetilde{G_{d',i}}\widetilde{h}_{d_h-1,i}\right) = 0, \tag{9}$$

$$\sum_i \widetilde{G}_{d',i}\widetilde{h}_{d_h,i} = 0. \tag{10}$$

Assume that for each $1 \le k \le d'$, $\{mx_i^d | m \in M(k, x_2, \cdots, x_n), i = 2, \cdots, n\}$ are linearly independent. Then by the equalities (6) - (10), one has $\widetilde{G}_{j,i} = 0$ for $j = 1, \cdots, d'$ and $i = 1, \cdots, n$. Therefore $\overline{U} = \{\sum_i \widetilde{G}_{0,i}h_i\} \subseteq W$. Note that $(U(h, d') : x_1^{d'}) = \overline{U}$. Hence $(U(h, d') : x_1^{d'}) = W$. By Lemma 4.4, the $a_P^{(i)}$ such that for some $k \le d'$, $\{mh_i | m \in M(k, x_2, \cdots, x_n), i = 1, \cdots, n\}$ are linearly dependent are the zeroes of some polynomials with degree at most $(n-1)\binom{n+d+k-2}{d+k}$ $\left(\le (n-1)\binom{n+d+d'-2}{d+d'} \triangleq N\right)$.

Hence when K is of characteristic zero, the probability that $(U(h, d') : x_1^{d'}) = W$ is one; when $K = GF(q)$, the probability that $(U(h, d') : x_1^{d'}) = W$ is at least $\frac{q-N}{q}$ which is close to one when q is sufficiently large [15]. ∎

Remark 4.6 *In general, when K is algebraically closed, Theorem 4.5 does not hold for sufficiently large integer d'. For randomly chosen $h_1, \cdots, h_n$, the set of zeroes of $\{h_1, \cdots, h_n\}$ in $\mathbb{P}(K)^{n-1}$ is empty, where $\mathbb{P}(K)^{n-1}$ is $n-1$ dimension projective space over K. Then by*

the Projective Weak Nullstellensatz Theorem (Theorem 8, p.374, [3]), there is some integer r *such that* $< x_1, \cdots, x_n >^r \subseteq < U(h, r - d_h) >$. *Let* $d' = r - d_h$. *Then* $M(r, x_1, \cdots, x_n) \subseteq U(h, d')$, *which implies that* $M(d_h, x_1, \cdots, x_n) \subseteq (U(h, d') : x_1^{d'})$. *However, in general,* $W \neq \text{span}_K(M(d_h, x_1, \cdots, x_n))$.

Corollary 4.7 Conjecture Y *is correct over* K *when* $n \geq 5$, *where* K *is of characteristic zero or is a finite field consisting of a sufficiently large number of elements.*

As a consequence of Theorem 4.2 and Corollary 4.7, we have the following result.

Theorem 4.8 *If* f *is a random decomposition and* $n \geq 5$, *then* $(\widetilde{V}_f : L) = R_{(f:h)}$ *with probability one when* K *is of characteristic zero and with probability close to one when* q *is sufficiently large where* $K = GF(q)$.

Therefore, we can recover $R_{(f:h)}$ from $\widetilde{V}_f$ directly with high probability if the FDP of f is randomly chosen.

Faugère and Perret assumed that $\widetilde{V}_f = V_f$ in their papers, since they assumed that the decomposition is random, the dimension of $R_{(f:h)}$ spanned by $h_1, \ldots, h_n$ is n, and $\dim(\widetilde{V}_f) \geq \dim(V_f)$ [8].

Theorem 4.9 *Under the same assumptions as Theorem 4.8. If* $\widetilde{V}_f$ *is known, we can compute* $R_{(f:h)}$ *with complexity* $O(n^{3\omega})$ *arithmetic operations in* K *with probability one when* K *is of characteristic zero and with probability close to one when* q *is sufficiently large when* $K = GF(q)$.

Proof. It suffices to randomly choose a linear polynomial l in $x_1, \ldots, x_n$ and compute $(\widetilde{V}_f : l)$ to obtain $R_{(f:h)}$. Without loss of generality, assume that $l = x_1 + c_2 x_2 + \cdots + c_n x_n$. Denote it by $X = M_l \cdot Y$.

For all $f \in K[x_1, \ldots, x_n]$, define $M_l(f) = f|_{X = M_l \cdot Y}$, $M_l^{-1}(g) = g|_{Y = M_l^{-1} \cdot X}$, where $g \in K[y_1, \ldots, y_n]$. Then $M_l^{-1} M_l(f) = f$, and $M_l(f_1 f_2) = M_l(f_1) M_l(f_2)$. So $M_l(l) = l|_{X = M_l \cdot Y} = y_1$. Let $M_l(\widetilde{V}_f) = \{p|_{X = M_l \cdot Y} : \text{for all } p \in \widetilde{V}_f\}$.

Then we have $r \in (\widetilde{V}_f : l) \Leftrightarrow rl \in \widetilde{V}_f \Leftrightarrow M_l(rl) \in M_l(\widetilde{V}_f) \Leftrightarrow M_l(r) M_l(l) \in M_l(\widetilde{V}_f) \Leftrightarrow M_l(r) \in (M_l(\widetilde{V}_f) : M_l(l)) \Leftrightarrow M_l(r) \in (M_l(\widetilde{V}_f) : y_1) \Leftrightarrow r \in M_l^{-1}(M_l(\widetilde{V}_f) : y_1)$. That is, $(\widetilde{V}_f : l) = M_l^{-1}(M_l(\widetilde{V}_f) : y_1)$.

So in order to compute $(\widetilde{V}_f : l)$, we can first transform the polynomials in $\widetilde{V}_f$ by a nonsingular coordinate substitution $X = M_l \cdot Y$ to obtain $M_l(\widetilde{V}_f)$, and then compute $(M_l(\widetilde{V}_f) : y_1)$. Finally, transform $(M_l(\widetilde{V}_f) : y_1)$ to $(\widetilde{V}_f : l)$ by the inverse transformation $Y = M_l^{-1} \cdot X$. The main arithmetic complexity relies on the computation of $(M_l(\widetilde{V}_f) : y_1)$.

We construct a matrix S to represent the polynomials of $M_l(\widetilde{V}_f)$ in a basis of monomials of degree three. Each row of S corresponds to the coefficients of each polynomial of $M_l(\widetilde{V}_f)$ with respect to the monomials of degree three. Suppose that the monomials are sorted so

that the last $n(n+1)/2$ columns of S correspond to monomials which can be divided by y_1. Then perform linear elimination to S, we can obtain polynomials which can be divided by y_1, denoted by $t_i, i = 1, \ldots, k$, if $n \geq 5$, then $k \leq n$ [10]. Then $(M_l(\widetilde{V}_f) : y_1) = \{t_i/y_1, i = 1, \ldots, k\}$. Note that S is an $n^2 \times C_{n+2}^3$ matrix. Then we need $O((n^3)^\omega) = O(n^{3\omega})$ arithmetic operations to compute $(M_l(\widetilde{V}_f) : y_1)$. The whole arithmetic complexity of computing $(\widetilde{V}_f : l)$ is also $O(n^{3\omega})$. ∎

4.2 The case when $u < n$

We now consider the case of $u < n$. In this case, Faugère and Perret extended $\widetilde{V}_f$ and V_f to new linear spaces $\widetilde{V_{fd}}$ and V_{fd}:

$$\widetilde{V_{fd}} = \mathrm{span}_K\{m\frac{\partial f_i}{\partial x_j} : m \in M(d), 1 \leq i \leq u, 1 \leq j \leq n\}, \tag{11}$$

$$V_{fd} = \mathrm{span}_K\{m'h_j : m' \in M(d+1), 1 \leq i, j \leq n\}, \tag{12}$$

where $M(d)$ represents the set of monomials of degree d. It is obvious that $\widetilde{V_{fd}} \subseteq V_{fd}$. The authors [8, 9] required $\dim(\widetilde{V_{fd}}) \geq \dim(V_{fd})$ by choosing a proper integer d, which means $\widetilde{V_{fd}} = V_{fd}$.

Assume V_{fd} is known, and try to recover $R_{(f:h)}$ from V_{fd}. By the definition of V_{fd}, $mh_j \in V_{fd}$ for all $m \in M(d+1)$ and j. Hence, $h_j \in (V_{fd} : x_i^{d+1})$, and then $R_{(f:h)} \subseteq (V_{fd} : x_i^{d+1})$, for all i. Hence, $R_{(f:h)} \subseteq \cap_i (V_{fd} : x_i^{d+1})$. The approach in [8, 9, 10] makes use of this property, and recovers $R_{(f:h)}$ by computing the quotient $(V_{fd} : x_i^{d+1})$ for some i. The authors [8, 9, 10] chose that $i = n$.

In the case that $d_g = d_h = 2$, Theorem 4.5 fails.

However, in the general case, if the degrees of g and h are more than 2, then from Theorem 4.5, we can compute $R_{(f:h)}$ by computing the quotient $(V_{fd} : x_i^{d+1})$ when $d + 1 < d_h$.

From the above discussion, we can see that the results listed above provide a theoretical guarantee for the previous work [8, 9, 10, 19] in certain sense.

5 Recover the decomposition of f from f^*

In this section, we study the relationship between the FDPs of a set of polynomials f and that of its homogenization f^*. We will show that with high probability, we can recover a decomposition for f from a decomposition of f^*.

For a general FDP $f = g \circ h$, the following result gives the connection between the FDP of f and the FDP of its homogenization f^*.

Lemma 5.1 *If $f = g \circ h$, then $x_0^{d_g d_h - d_f} f^* = g^* \circ h^*$, where d_g, d_h, d_f are the degrees of g, h, f respectively.*

Proof. If $f = g \circ h$, we have $d_g \cdot d_h \geq d_f$. Hence,

$$f_i(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}) = g_i(h_1(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}), \ldots, h_n(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})).$$

Then

$$\begin{aligned} g^* \circ h^* &= (x_0^{d_g d_h}, x_0^{d_g d_h} g_1(h_1(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}), \ldots, x_0^{d_g d_h} h_n(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})), \\ &\quad \ldots, x_0^{d_g d_h} g_u(h_1(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}), \ldots, h_n(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}))) \\ &= (x_0^{d_g d_h}, x_0^{d_g d_h} f_1(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}), \ldots, x_0^{d_g d_h} f_u(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})) \\ &= x_0^{d_g d_h - d_f}(x_0^{d_f}, x_0^{d_f} f_1(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}), \ldots, x_0^{d_f} f_u(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})) \\ &= x_0^{d_g d_h - d_f} f^*. \quad \blacksquare \end{aligned}$$

As a consequence, we have $(f \circ g)^* = f^* \circ g^*$ if $d_f \cdot d_g = d_h$ [9, 19].

By a *homogeneous decomposition* $f = g \circ h$, we mean that each component of f, g, and h are homogeneous of the same degree d_f, d_g, and d_h respectively. It is clear that a homogenous decomposition is always degree proper.

The following result gives a necessary and sufficient condition for f to have an FDP in terms of its homogenization f^*.

Theorem 5.2 *Let $f = (f_1, \ldots, f_u) \in \mathcal{R}^u$. Then, f has a decomposition if and only if there exist natural numbers s, t such that $x_0^s f^* = g' \circ h'$ is a homogeneous decomposition and $x_0^t \in \mathrm{span}_K\{h'_0, \ldots, h'_n\}$.*

Proof. If f has a decomposition $f = g \circ h$, let $s = x_0^{d_g d_h - d_f}, g' = g^*, h' = h^*, t = d_h$ in Lemma 5.1. Then the conclusion holds.

We now prove the other direction. If there are natural numbers s, t such that $x_0^s f^* = g' \circ h'$ is a homogeneous decomposition and $x_0^t \in \mathrm{span_K}\{h'_0, \ldots, h'_n\}$, then $\deg(h') = t$, $\deg(g') = \frac{s+d_f}{t}$, and we can choose g', h' such that $x_0^s f^*$ has the following homogeneous decomposition form by Theorem 3.3:

$$\begin{aligned} x_0^s f^* &= (x_0^{s+d_f}, x_0^{s+d_f} f_1(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}), \ldots, x_0^{s+d_f} f_u(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})) \\ &= (x_0^{\frac{s+d_f}{t}}, g'_1, \ldots, g'_n) \circ (x_0^t, h'_1, \ldots, h'_n)) \end{aligned}$$

and $\deg(g'_i) = \frac{s+d_f}{t}$, $\deg(h'_i) = t$. Let $x_0 = 1$. We have

$$\begin{aligned} f &= (f_1, \ldots, f_u) \\ &= (g'_1(1, x_1, \ldots, x_n), \ldots, g'_u(1, x_1, \ldots, x_n)) \circ (h'_1(1, x_1, \ldots, x_n), \ldots, h'_n(1, x_1, \ldots, x_n)), \end{aligned}$$

which is a decomposition of f. $\blacksquare$

As a consequence of Lemma 5.1 and Theorem 5.2, we have

Corollary 5.3 *Let $f = (f_1, \ldots, f_u) \in \mathcal{R}^u$. Then, f has a degree proper decomposition if and only if there is a natural number t such that f^* has a homogeneous decomposition $f^* = g' \circ h'$ and $x_0^t \in \mathrm{span}_K\{h'_0, \ldots, h'_n\}$.*

In order to use the idea of homogenization, we need to solve the following problem.

Conjecture 5.4 *For all homogeneous decompositions of $f^* = G \circ H$, we have $x_0^{d_H} \in \mathrm{span}_K\{H_0, \ldots, H_n\}$.*

If the conjecture is true, we may conclude that to compute a degree proper decomposition of f is equivalent to compute a homogeneous decomposition of f^*. Therefore, we can obtain a right factor space $R_{(f:h)}$ of f from $R_{(f^*:h^*)}$ in the same way with the method in the proofs of Theorem 5.2.

Theorem 5.5 *Conjecture 5.4 has a positive answer in the field of complex numbers if the degrees of f^*, G and H are 4,2,2 respectively and $n = 2$.*

Proof. In the field $K = \mathbb{C}$, if G is nondegenerate, we can assume that G has the following standard form $G = x_0^2 + x_1^2 + x_2^2$ by nonsingular linear substitution (If G is degenerate, then we can assume that $G = x_0^2 + x_1^2$ or $G = x_0^2$, it is easy to see that the Conjecture holds in either case).

Firstly, we claim that we can assume $H_0 = x_0^2 + c_0$, $H_1 = b_1x_0 + c_1$, and $H_2 = b_2x_0 + c_2$ where c_i are quadratic homogeneous polynomials and b_i are linear homogeneous polynomials in variables x_1 and x_2. Since we consider the decomposition over the field of complex numbers, we may assume that $H_k = a_kx_0^2 + G_k (k = 0, 1, 2)$, where G_k does not contain x_0^2. Since $x_0^4 = H_0^2 + H_1^2 + H_2^2$, $a_0^2 + a_1^2 + a_2^2 = 1$. Without loss of generality, we may assume $a_0^2 + a_1^2 \neq 0$. Let $H'_0 = \frac{a_1H_1}{\sqrt{a_0^2+a_1^2}} + \frac{a_0H_0}{\sqrt{a_0^2+a_1^2}}$ and $H'_1 = \frac{a_0H_1}{\sqrt{a_0^2+a_1^2}} - \frac{a_1H_0}{\sqrt{a_0^2+a_1^2}}$. We have

$$H_0^2 + H_1^2 = (H'_0)^2 + (H'_1)^2$$

and H'_1 does not contain the term x_0^2. Repeat the above procedure one more time, we obtain three new polynomials H''_0, H''_1, H''_2 such that H''_1 and H''_2 do not contain x_0^2. Since $x_0^4 = H_0^2 + H_1^2 + H_2^2$, we have $H''_0 = x_0^2 + b_0x_0 + c_0$. Comparing the coefficients of x_0^3, we have $b_0 = 0$. Thus, the claim is proved.

Since $x_0^4 = H_0^2 + H_1^2 + H_2^2$, we have $-c_0(c_0 + 2x_0^2) = H_1^2 + H_2^2 = (H_1 + iH_2)(H_1 - iH_2)$. We will discuss it in the following two cases.

(1) When $c_0+2x_0^2$ is irreducible, then there exist constants $\alpha, \beta \in K$ such that $H_1+iH_2 = \alpha(c_0 + 2x_0^2), H_1 - iH_2 = \beta c_0$, or $H_1 - iH_2 = \alpha(c_0 + 2x_0^2), H_1 + iH_2 = \beta c_0$. In either case, we have $x_0^2 \in \mathrm{span}_K\{H_1, H_2\}$.

(2) When $c_0 + 2x_0^2$ is reducible, then there exists a linear polynomial p in variables x_1, x_2 such that $c_0 + 2x_0^2 = (\sqrt{2}x_0 + p)(\sqrt{2}x_0 - p)$ where $c_0 = -p^2$.

If H_1+iH_2 has a factor $\sqrt{2}x_0+p$ or $\sqrt{2}x_0-p$, without loss of generality, assume $\sqrt{2}x_0+p$ is a factor of H_1+iH_2, then there exists constants $\alpha, \beta \in K$ such that $H_1+iH_2 = \alpha p(\sqrt{2}x_0+p)$

and $H_1 - iH_2 = \beta p(\sqrt{2}x_0 - p)$. Then $p^2 \in \mathrm{span}_K\{H_1, H_2\}$. Since $H_0 = x_0^2 + c_0 = x_0^2 - p^2$, then $p^2 \in \mathrm{span}_K\{H_0, H_1, H_2\}$.

If $c_0 + 2x_0^2$ is a factor of $H_1 + iH_2$, then the same as the case (1), $x_0^2 \in \mathrm{span}_K\{H_1, H_2\}$.

The above discussion shows that $x_0^2 \in \mathrm{span}_K\{H_0,\ H_1, H_2\}$. ∎

The proof of Conjecture 5.4 is still open.

6 Algorithm and complexity

Let $f \in K[x_1, \ldots, x_n]^n$ be a set of polynomials with degrees less than or equal to four, and at least one polynomial has degree four. We now give the algorithm to find a degree proper decomposition of f. We prove that it is a polynomial time algorithm with high successful probability if Conjecture 5.4 is correct. Note that the algorithm is essentially the same as that given in [19]. Our main contribution is the analysis of the algorithm.

Algorithm FDPMP4.

Input: $f \in K[x_1, \ldots, x_n]^n$ be a set of polynomials with degrees less than or equal to four, and at least one polynomial has degree four.

Output: $g, h \in K[x_1, \ldots, x_n]^n$ such that $f = g \circ h$ is a degree proper decomposition of f. The algorithm may fail even if such a decomposition exists.

Step 1. Let $f_0^*(x_0, x_1, \ldots, x_n) := x_0^4$, $f_i^*(x_0, x_1, \ldots, x_n) := x_0^4 f_i(\frac{x_1}{x_0}, \ldots, \frac{x_1}{x_0}), 1 \le i \le n$, and $\widetilde{V_f} := \mathrm{span}_K\{\frac{\partial f_i^*}{\partial x_j} : i, j = 0, 1, \ldots, n\}$.

Step 2. Compute $R^*_{(f:h)} := (\widetilde{V_f} : l)$ as stated in the proof of Theorem 4.9.

Step 3. Set $x_0 = 1$ in $R^*_{(f:h)}$ to obtain $R_{(f:h)}$: $R_{(f:h)} := R^*_{(f:h)}|_{x_0=1}$.

Step 4. Perform linear elimination to the generators of $R_{(f:h)}$ to obtain a basis $(h_1, \ldots, h_k)$ of $R_{(f:h)}$. If $k = n$, then $h = (h_1, \ldots, h_n)$; otherwise $h = (h_1, \ldots, h_k, h_1, \ldots, h_1)$.

Step 5. Compute the coefficients of g by solving a system of linear equations as shown in Theorem 3.5.

Theorem 6.1 Algorithm FDPMP4 *needs $O(n^{3\omega})$ arithmetic operations in the field K, where $2 \le \omega < 3$. For a random decomposition f, the algorithm computes the decomposition with probability one when K is of characteristic zero, and with probability close to one when $K = GF(q)$ q is a sufficiently large odd number under the assumption that Conjecture 5.4 is correct.*

Proof. Assume that Conjecture 5.4 is correct, the complexity of the whole algorithm depends on Step 2 and Step 5, both of them cost $O(n^{3\omega})$ arithmetic operations by Theorem 3.5 and Theorem 4.9. Then we have a polynomial time algorithm to find a degree proper decomposition $f = g \circ h$ for $g, h \in K[x_1, \ldots, x_n]^n$ with probability one when K is of characteristic zero, and with probability close to one when $K = GF(q)$ q is a sufficiently large number. ∎

This proves Theorem 2.2.

7 Conclusion and problems

In this paper, we give a theoretical analysis for the approaches of computing functional decomposition for multivariate polynomials based on differentiation and homogenization proposed in [8, 9, 10, 19]. We show that a degree proper functional decomposition for a set of quartic homogenous polynomials can be computed using the algorithm with high probability from randomly decomposable polynomials. We proposed a conjecture such that the decomposition for a set of polynomials can be computed from its homogenization with high probability. Finally, we prove that the right decomposition factors for a set of polynomials can be computed from its right decomposition factor space. Combining these results together, we show that the algorithm can compute a degree proper decomposition for a set of quartic randomly decomposable polynomials with high probability if the conjecture we proposed is correct. Conjecture 5.4 seems to be correct while it is unsolved.

Despite of the significant progresses, the general FDP for multivariate polynomials is widely open. Some of the basic problems related to FDP of multivariate polynomials are not resolved. We will give two basic open problems below.

The first problem is about the existence of an algorithm for FDP.

Problem 7.1 *Given $f \in \mathcal{R}^n$, to find an FDP for f is decidable or not.*

Note that in a decomposition $f = g \circ h$, the degrees of g and h could be arbitrarily high. Consider the following two transformations:

$$T_1\colon (x_1, \ldots, x_n) \Rightarrow (x_1 + p, x_2 \ldots, x_n)$$
$$T_2\colon (x_1, \ldots, x_n) \Rightarrow (x_1 - p, x_2 \ldots, x_n)$$

where p is a polynomial in $x_2, \ldots, x_n$ of any degree. Then $T_1 \circ T_2 = (x_1, \ldots, x_n)$. For any decomposition $f = g \circ h$, $f = (g \circ T_1) \circ (T_2 \circ h)$ is also a decomposition of f. Therefore, one way to solve Problem 7.1 is to find the smallest possible degrees of g and h if a decomposition exists.

The second problem is about the computational complexity of FDP. In this aspect, even the simplest case is not resolved.

Problem 7.2 *Let $f \in \mathcal{R}^n$ be a set of quartic polynomials. Estimate the complexity of computing an FDP of f over a finite field $K = F_q$. In particular, does there exist a polynomial-time algorithm for Boolean polynomials?*

Remark: Faugère et al [11] also proved the correctness of section 4 of our paper, but the corresponding part of our work was independently finished and used a different method.

References

[1] E.W. Chionh, X.S. Gao, and L.Y. Shen, Inherently improper surface parametric supports. *Computer Aided Geometric Design*, **23**, 629-639, 2006.

[2] D. Coppersmitha and S. Winograda, Matrix multiplication via arithmetic progressions. *Journal of Symbolic Computation*, **9**(3), 251-280, 1990.

[3] D. Cox, J. Little and D. O'Shea, *Ideals, Variaties, and Algorithms*, second edition, Springer-Verlag, 1996.

[4] M. Dickerson, The functional Decomposition of Polynomials, Ph.D Thesis, TR 89-1023, Department of Compupter Science, Cornell University, Ithaca, NY, July 1989.

[5] J.Gutierre, R.Rubio, J. von zur Gathen. Multivariate polynomial Decomposition. *Algebra in Engeering, Communication and Computing* , **14**(1), 11-31, 2003.

[6] J. von zur Gathen, Functional decomposition of polynomials: the tame case. *Journal of Symbolic Computation*, **9**, 281-299, 1990.

[7] J. von zur Gathen, Functional Decomposition of Polynomials: the Wild Case. *Journal of Symbolic Computation*, **10**, 437-452, 1990.

[8] J.-C. Faugère, L.Perret, Cryptanalysis of $2R^-$ schemes. *Advances in Cryptology-CRYPTO 2006*, Lecture Notes in Computer Science, **4117**, 357-372, 2006.

[9] J.-C. Faugère, L.Perret, An Efficient Algorighm for Decomposing Multivariate Ploynomials and its applications to Cryptography. *Special Issue of JSC, "Gröbner Bases techniques in Coding Theorey and Cryptography"*, 2008.

[10] J.-C. Faugère, L.Perret, High order derivatives and decomposition of multivariate polynomials. *Proc. ISSAC 2009*, 151-158, ACM Press, 2009.

[11] J.-C. Faugère, J. von zur Gathen and L.Perret, Decompostion of generic multivariate polynomials. *ISSAC 2010,* 25-28, 2010.

[12] T.Y. Lam, *The algebraic theory of quadratic forms*, Benjamin 1973.

[13] J. Li, L. Shen, X.S. Gao, Proper Reparametrization of Rational Ruled Surface, *Journal of Computer Science and Technology*, **23**(2), 290-297, 2008.

[14] J. Li and X.S. Gao, The Proper Parametrization of a Special Class of Rational Parametric Equations, *J. of Sys. Sci. and Complexity*, 19, 331-339, 2006.

[15] R. Lidl and H. Niederreiter, *Finite fields.* Addison-Wesley Publishing Company, 1983.

[16] J. Patarin and L.Goubin, Asymmetric cryptography with S-boxes. *Proceedings of ICICS'97*, Lecture Notes in Computer Science, **1334**, springer, 1997.

[17] J. Patarin and L.Goubin, Asymmetric cryptography with S-boxes-extended version. Available at http://citeseer.ist.psu.edu/patarin97asymmetric.html.

[18] A. Schinzel, *Polynomials wih Special Regard to Reducibility.* Cambridge University Press, 2000.

[19] D.F. Ye, K.Y. Lam and Z.D. Dai, Cryptanalysis of "2R" Schemes. *Advances in Cryptology-CRYPTO 1999*, Lecture Notes in Computer Science, **1666**, Springer, 315-325, 1999.