JEAN-CHARLES FAUGÈRE, JOACHIM VON ZUR GATHEN & LUDOVIC PERRET (2010). Decomposition of Generic Multivariate Polynomials. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation ISSAC '10, Munich, Germany*, STEPHEN WATT, editor, 131–137. ACM Press. URL http://dx.doi.org/10.1145/1837934.1837964.

Decomposition of Generic Multivariate Polynomials

(Version : July 19, 2010)

Jean-Charles Faugère
SALSA Project INRIA Paris-Rocquencourt
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6
UFR Ingénierie 919, LIP6 Passy Kennedy
4, Place Jussieu 75252 Paris Cedex 05
Jean-Charles.Faugere@inria.fr

Joachim von zur Gathen
B-IT, Universität Bonn
D-53113 Bonn, Germany
gathen@bit.uni-bonn.de

Ludovic Perret
SALSA Project INRIA Paris-Rocquencourt
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6
UFR Ingénierie 919, LIP6 Passy Kennedy
4, Place Jussieu 75252 Paris Cedex 05
ludovic.perret@lip6.fr

ABSTRACT

We consider the composition $f = g \circ h$ of two systems $g = (g_0,\dots,g_t)$ and $h = (h_0,\dots,h_s)$ of homogeneous multivariate polynomials over a field $\mathbb{K}$, where each $g_j \in \mathbb{K}[y_0,\dots,y_s]$ has degree ℓ, each $h_k \in \mathbb{K}[x_0,\dots,x_r]$ has degree m, and $f_i = g_i(h_0,\dots,h_s) \in \mathbb{K}[x_0,\dots,x_r]$ has degree $n = \ell \cdot m$, for $0 \le i \le t$. The motivation of this paper is to investigate the behavior of the decomposition algorithm **MultiComPoly** proposed at ISSAC'09 [18]. We prove that the algorithm works correctly for generic decomposable instances – in the special cases where ℓ is 2 or 3, and m is 2 – and investigate the issue of uniqueness of a *generic* decomposable instance. The uniqueness is defined w.r.t. the "normal form" of a multivariate decomposition, a new notion introduced in this paper, which is of independent interest.

Categories and Subject Descriptors

I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms Algebraic Algorithms

General Terms

Algorithms.

Keywords

Functional Decomposition, Generic Uniqueness, Gröbner bases.

1. INTRODUCTION

Let $\mathbb{K}$ be an arbitrary field. The multivariate *Functional Decomposition Problem (FDP)* [23, 12, 30] is the problem of representing a given polynomial $f = (f_0,\dots,f_t) \in \mathbb{K}[x_0,\dots,x_r]^{t+1}$ as a functional composition:

$$(f_0,\dots,f_t) = \big(g_0(h_0,\dots,h_s),\dots,g_t(h_0,\dots,h_s)\big),$$

of polynomials $g = (g_0,\dots,g_t) \in \mathbb{K}[y_0,\dots,y_s]^{t+1}$ and $h = (h_0,\dots,h_s) \in \mathbb{K}[x_0,\dots,x_r]^{s+1}$ of smaller degree.

FDP is a classical problem in computer algebra ([26, 21, 22, 23, 10, 29]) which has been thoroughly investigated in the univariate case from an algorithmic as well as from a theoretical point of view; see [1, 5, 26, 21, 22, 20, 14, 27]. The decomposition of univariate polynomials is a standard functionality proposed by major computer algebra systems[1].

For general multivariate decomposition, the situation is different and probably more complicated. For instance, there is no multivariate equivalent of Ritt's theorem [27, 14] which is a central tool in the univariate case. Typically, this makes it delicate to define a proper notion of nontrivial decomposition (for instance see [23, 24]). In [23], von zur Gathen, Gutierrez and Rubio have investigated several variants of FDP, the so-called *uni-multivariate*, *multi-univariate* and *single-variable* decompositions, which are extensions of the univariate case. They presented algorithms to solve these variants, together with some theoretical results. It is only recently that algorithms for decomposing general multivariate polynomials have been proposed [17, 18]. The original motivation of these methods was in the cryptanalysis of multivariate cryptosystems [16]. In this paper, we focus attention on the **MultiComPoly** algorithm proposed at ISSAC'09 [18]. We are interested in the behavior of the algorithm for generic decomposable instances, in the special cases where ℓ is 2 or 3, and m is 2. These are sufficient for the cryptanalytic applications. We prove that the algorithm works correctly for generic decomposable instances, and returns a unique decomposition. The uniqueness is defined w.r.t. the "normal form" of a multivariate decomposition, a new notion introduced in this paper.

1.1 The MultiComPoly algorithm

In order to be self-contained, we briefly recall the principle of the decomposition algorithm **MultiComPoly** [18]. Some of the notation will be used in the rest of this paper. So, let $f = g \circ h$ be the composition of $g = (g_0,\dots,g_t) \in \mathbb{K}[y_0,\dots,y_s]^{t+1}$ and $h = (h_0,\dots,h_s) \in \mathbb{K}[x_0,\dots,x_r]^{s+1}$ of homogeneous multivariate polynomials. Most decomposition techniques first determine the right component h, then the left component g. The algorithm of [18] is no exception. More precisely, **MultiComPoly** recovers first the vector space $\mathscr{L}(h) = \mathrm{Span}_{\mathbb{K}}(h_0,\dots,h_s)$ spanned by the right component h. This vector space is obtained by considering the ideal generated by high order dif-

[1] For instance, `compoly` of MAPLE `http://www.maplesoft.com/`

ferentials of f:

$$\partial^k \mathscr{I}_f = \left\langle \frac{\partial^k f_i}{\partial x_{j_1} \cdots \partial x_{j_k}} \mid 0 \le i \le t, 0 \le j_1 < \cdots < j_k \le r \right\rangle,$$

for some k depending of the degree of g, where $\mathscr{I}_f$ is the ideal generated by the polynomials in f. It has been proved [18] that there exists $\delta > 0$ such that:

$$x_r^\delta h_i \subseteq \partial^{\deg(g)-1} \mathscr{I}_f, \text{ for all } i, 0 \le i \le s.$$

A basis of $\mathscr{L}(h)$ is obtained by computing a DRL (degree reverse lexicographical) Gröbner basis [6, 7, 8, 9] of $\partial^{\deg(g)-1}\mathscr{I}_f : x^\delta$, for a suitable $\delta > 0$. More precisely, we compute a truncated [11] Gröbner basis G of $\partial^{\deg(g)-1}\mathscr{I}_f : x^\delta$. If $\#G = s+1$, then $\mathrm{Span}_{\mathbb{K}}(G) = \mathscr{L}(h)$. From the knowledge of $\mathscr{L}(h)$, it is well known [28] that the left component g can be recovered by solving a linear system of equations. This is studied in more generality in Section 4.

1.2 Organization of the paper

We study in detail the behavior of **MultiComPoly** for generic decomposable instances. The paper is organized as follows. In Section 2, we introduce more precisely the decomposition problem studied here, and fix some further notation. In Section 3, we focus on the first part of **MultiComPoly** which computes the vector space $\mathscr{L}(h)$. Let the notation be as in subsection 1.1, and G be the set of polynomials computed during the first step of **MultiComPoly** in Section 3, we prove that the property:

$$\mathrm{Span}_{\mathbb{K}}(G) = \mathscr{L}(h).$$

is generic (in the sense of the Zariski topology). We first prove that the set of elements for which this property fails is contained in a closed algebraic set. The second part of the proof, which is the most difficult, consists of finding particular decomposable instances for which we can prove the property. As a side remark, we mention that the genericity of semi-regular sequences [2, 3, 4] is a well known conjecture of Fröberg [19] whose bottleneck is to simply find a semi-regular sequence. In our context, we consider in Section 3 rather simple family of decomposable instances. For this family, we prove that the equality $\mathrm{Span}_{\mathbb{K}}(G) = \mathscr{L}(h)$ indeed holds. To do that, we describe the exact structure of the truncated Gröbner basis G for the family under consideration. After that, we study in Section 4 the property of the linear system corresponding to the recovery of the left component when the right component is known. We conjecture that for a "generic" h, the system has maximal rank and thus is overdetermined. This conjecture has been proven in the previous sections for the examples considered there.

All in all, we prove that **MultiComPoly** computes a "unique" decomposition, w.r.t a normal form, for generic decomposable instances.

2. FUNCTIONAL DECOMPOSITION

Rather than the general multivariate *Functional Decomposition Problem* (FDP) problem (see [23, 12, 30]), we consider throughout this paper the homogeneous variant. Thus for any positive integers ℓ and m, we have the following problem.

FDP(ℓ, m)
Input: $f = (f_0, \ldots, f_t) \in \mathbb{K}[x_0, \ldots, x_r]^{t+1}$ homogeneous polynomials, all of the same degree.
Output: Either "no decomposition" or homogeneous polynomials $\big(g = (g_0, \ldots, g_t), h = (h_0, \ldots, h_s)\big) \in \mathbb{K}[y_0, \ldots, y_s]^{t+1} \times \mathbb{K}[x_0, \ldots, x_r]^{s+1}$ all of degree ℓ and m, respectively, such that $f = g \circ h$.

Trivial decomposition may occur when $\ell = 1$ or $m = 1$, and we assume in the rest of this paper that $\ell > 1$ and $m > 1$.

DEFINITION 1. *$f \in \mathbb{K}[x_0, \ldots, x_r]^{t+1}$ is decomposable if there exists (g,h) such that $f = g \circ h$ with $\deg(g) > 1$ and $\deg(h) > 1$. The pair (g,h) is an (ℓ, m) decomposition of f if (g,h) is a decomposition of f with $\deg(g) = \ell$ and $\deg(h) = m$.*

Linear substitutions introduce inessential nonuniquenesses of decompositions. Indeed, any invertible linear combination $A \in \mathrm{GL}_s(\mathbb{K})$ of $(h_0, \ldots, h_s)$ leads to a decomposition of f, since

$$f(x_1, \ldots, x_r) = \big(g(y_0, \ldots, y_r)A^{-1}\big) \circ \big(h(x_0, \ldots, x_r)A\big).$$

As in the univariate case, it is convenient to define a "normal form" [21, 22, 20] of a decomposition. In the univariate case, a polynomial h is said to be original if $h(0) \neq 0$. A univariate decomposition $\big(g, h\big)$ of f is called normal if h is original and monic (i.e., leading coefficient equal to 1). We introduce a similar notion for the multivariate case.

DEFINITION 2. *We consider homogeneous monic polynomials, whose leading coefficient in the DRL order equals 1. A decomposition (g,h) of such an f is in normal form if the polynomials $((g_0, \ldots, g_t), (h_0, \ldots, h_s))$ are homogeneous and monic and $(h_0, \ldots,$
$h_s)$ is an m-Gröbner basis (a Gröbner basis up to degree m) w.r.t. DRL order (i.e., degree reverse lexicographical). Two decompositions (g,h) and $(\tilde{g}, \tilde{h})$ of f are equivalent if their normal forms are equal.*

In the multivariate case, the fact that $(h_0, \ldots, h_s)$ are homogeneous implies in particular $h(\mathbf{0}) = 0$. One might view homogeneous as a natural extension of the concept of original. In addition, if the polynomials of h are an m-Gröbner basis, then the polynomials $(h_0, \ldots, h_s)$ are, in particular, monic. Note that if h is a m-Gröbner basis, then $(h_0, \ldots, h_s)$ is also a basis of the $\mathbb{K}$-vector spanned by $h_0, \ldots, h_s$; a natural and canonical representative of equivalent decompositions. Note that **MultiComPoly** actually computes the normal form of a decomposition.

We fix some notation for the remainder of this paper. For $r \ge 1$ and $\delta \ge 0$, we write:

$$P_{r,\delta} = \{f \in \mathbb{K}[x_0, \ldots, x_r] : f \text{ homogeneous, and } \deg(f) = \delta\}$$

for the vector space of homogeneous polynomials of degree δ. A basis of $P_{r,\delta}$, denoted $M_r(\delta)$, is given by the set of all monomials of degree δ. Thus $\dim(P_{r,\delta}) = \#M_r(\delta)$. We define the composition map:

$$\begin{array}{rccc} \gamma_{s,\ell,r,m}: & P_{s,\ell} \times P_{r,m} & \to & P_{r,\ell,m} \\ & (g,h) & \mapsto & g \circ h \end{array}$$

and write $D_{r,\ell,m} = \mathrm{Im}(\gamma_{s,\ell,r,m})$ for the set of (ℓ, m) decomposables. Finally, we state the framework in which we prove our results.

DEFINITION 3. *Let F be an algebraic closure of $\mathbb{K}$, and $\mathrm{E}_{\ell,m} \subset F[y_0, \ldots, y_s]^{t+1} \times F[x_0, \ldots, x_r]^{s+1}$ be the set of homogeneous polynomials $(g_0, \ldots, g_t)$ of degree ℓ, and $(h_0, \ldots, h_s)$ of degree m. We say that a property is generic if the set of elements in $\mathrm{E}_{\ell,m}$ verifying this property is a non-empty Zariski-open subset; i.e., the property is verified for all elements of $\mathrm{E}_{\ell,m}$ except for an algebraic set of codimension one.*

We recall that in order to prove that a certain property is generic, it is sufficient to show the following

1. First: show that the set of points/elements for which the property fails is the zero of a system of polynomial equations. This defines the complement of an open set with respect to Zariski topology.

2. Second: prove that the Zariski-open subset is not empty; which means that we have to prove that the property is valid at least on one specific example. The examples that we exhibit are actually defined over the ground field $\mathbb{K}$, and we avoid reference to its algebraic closure in the following.

3. GENERIC UNIQUENESS OF THE RIGHT COMPONENT

We consider here the first part of **MultiComPoly** on the set $D_{r,\ell,m}$ of (ℓ,m) decomposables. The aim of the first part is to obtain a basis of the vector space $\mathscr{L}(h)$. As explained in the introduction, this vector space is obtained from the truncated m-Gröbner basis G of $\partial^{\ell-1}\mathscr{I}_f : x_r^{\delta}$, for a suitable $\delta > 0$, w.r.t. DRL. In [18], it is proved that $\mathrm{Span}_{\mathbb{K}}(G)$ is also a basis of $\mathscr{L}(h)$ as a $\mathbb{K}$-vector space, if $\#G = s+1$. We prove here that the property

$$\mathrm{Span}_{\mathbb{K}}(G) = \mathscr{L}(h)$$

is generic for the set of $D_{r,2,2}$ of $(2,2)$ decomposables, and for the set of $D_{r,3,2}$ of $(3,2)$ decomposables.

3.1 Roadmap of the proof

In both cases $D_{r,2,2}$ and $D_{r,3,2}$, the general strategy is identical although the technical details differ. As explained previously, a proof of genericity is divided into two steps. We provide here a high level description of the strategy in our context.

1. To define the algebraic set, we will adopt a linear algebra point of view. In this context, it is not difficult to see that the condition $\mathscr{L}(h) \neq \mathrm{Span}_{\mathbb{K}}(G)$ implies a defects in the rank of a certain matrix. By considering generic polynomials, it is possible to construct an algebraic system whose variables correspond to the coefficients of a right component. This algebraic system vanishes as soon as the right component h is such that $\mathscr{L}(h) \neq \mathrm{Span}_{\mathbb{K}}(G)$.

2. We prove then that the Zariski-open set is not empty by providing suitable explicit examples. This is the most difficult part of the proof. Here, we will use use a polynomial point of view. We consider the following family $f = g\circ h \in D_{r,\ell,2}$ of $(\ell,2)$ decomposables:

   - $r = s = t$ and $g = (y_0^{\ell},\ldots,y_s^{\ell})$,
   - for all i with $0 \le i \le s$, $h_i = \sum_{j=i}^{s} x_j^2$.

3.2 $(2,2)$ decomposition

We first consider the basic case of a decomposable $f \in D_{r,2,2}$. Let then $((g_0,\ldots,g_t),(h_0,\ldots,h_s))$ be a $(2,2)$ decomposition of f. In this situation, we have to consider the ideal:

$$\partial\mathscr{I}_f = \left\langle \frac{\partial f_i}{\partial x_u} \mid 0 \le i \le t, \text{ and } 0 \le u \le r \right\rangle.$$

generated by the partial derivatives of f. This is due to the fact that for all $0,1 \le i \le t$, $f_i = g_i(h_0,\ldots,h_s) = \sum_{0\le j,k\le r} g_{j,k}^{(i)} h_j h_k$, with $g_i = \sum_{0\le j,k\le s} g_{j,k}^{(i)} y_j y_k$. Thus

$$\frac{\partial f_i}{\partial x_u} = \sum_{0\le j,k\le s} g_{j,k}^{(i)} \left(h_j \frac{\partial h_k}{\partial x_u} + h_k \frac{\partial h_j}{\partial x_u} \right).$$

Each partial derivative $\frac{\partial f_i}{\partial x_u}$ is a linear combination of elements $\{x_j \cdot h_k\}_{0\le j\le r}^{0\le k\le s}$. For the analysis, it is convenient to consider the $\big((t+1)\cdot(r+1)\big) \times \big((s+1)\cdot(r+1)\big)$ matrix:

$$A = \begin{array}{c} \\ \frac{\partial f_0}{\partial x_u} \\ \vdots \\ \frac{\partial f_i}{\partial x_u} \\ \vdots \\ \frac{\partial f_t}{\partial x_u} \end{array} \begin{array}{c} \cdots \quad \cdots \quad x_j\cdot h_k \quad \cdots \quad \cdots \\ \left(\begin{array}{c} \cdots \\ \vdots \\ \cdots \\ \cdots \\ \vdots \\ \cdots \\ \cdots \end{array} \right) \end{array} \tag{1}$$

where the $((i,u),(j,k))$-entry equals the coefficient of $x_j \cdot h_k$ in $\frac{\partial f_i}{\partial x_u}$. If $\mathrm{Rank}(A) = \#\mathrm{Columns}(A) = (s+1)\cdot(r+1)$, then each $x_j \cdot h_k$ can be expressed as a linear combination of $\frac{\partial f_i}{\partial x_u}$ leading in particular to

$$x_r h_i \in \partial\mathscr{I}_f, \text{for all } i, 0 \le i \le s. \tag{2}$$

Let G be a truncated 2-Gröbner basis of $\partial\mathscr{I}_f : x_r$. Our goal is to prove that

$$\mathrm{Span}_{\mathbb{K}}(G) = \mathscr{L}(h). \tag{3}$$

This condition (3) is clearly a necessary condition of success of **MultiComPoly**. The set of decomposable for which (3) is not fulfilled is an algebraic set. Indeed, the failure of condition (3) is due to a defect in the rank of two sub matrices of (1) (see [18]). It remains to prove that this Zariski-open set is nonempty. To do so, we consider the following particular decomposable instance $f = g\circ h \in D_{r,2,2}$:

- $r = s = t$ and $g = (y_0^2,\ldots,y_s^2)$
- for all $i, 0 \le i \le s$, $h_i = \sum_{j=i}^{s} x_j^2$.

To show that (3) is fulfilled for this family, we need several intermediate results.

LEMMA 3.1. *Let $f = g\circ h \in D_{r,2,2}$ be as defined previously. For all $i, 0 \le i \le s$, we have:*

$$\frac{\partial f_i}{\partial x_u} = \begin{cases} 4x_u h_i = 4x_u \sum_{j=i}^{s} x_j^2 & \text{if } u \ge i, \\ 0 & \text{if } u < i. \end{cases}$$

PROOF.

$$\begin{aligned} f_i &= h_i^2, \\ \frac{\partial f_i}{\partial x_u} &= 2h_i \frac{\partial h_i}{\partial x_u}. \end{aligned}$$

Due to the particular choice of h, $\frac{\partial f_i}{\partial x_u} = 0$ if $u < i$. For all $u \ge i$, $\frac{\partial f_i}{\partial x_u} = 4x_u h_i = 4x_u \sum_{j=i}^{s} x_j^2$. $\square$

From this, we deduce the following.

LEMMA 3.2. *For all $i \leq s$ and $u > i$:*

$$\frac{\partial f_i}{\partial x_u} - \frac{\partial f_{i+1}}{\partial x_u} = 4x_u x_i^2,$$

with the convention that $f_{s+1} = f_0$.

Recall that we consider the DRL ordering $\succ$ with $x_0 \succ \cdots \succ x_s$.

LEMMA 3.3. *Let $i \leq s$. Then*

$$LT_{\succ}\left(\frac{\partial f_i}{\partial x_i}\right) = x_i^3,$$

where $LT_{\succ}$ stands for the leading term.

PROOF. Here, $\frac{\partial f_i}{\partial x_i} = 4x_i \sum_{j=i}^{s} x_j^2$. Hence:

$$LT_{\succ}\left(\frac{\partial f_i}{\partial x_i}\right) = x_i LT_{\succ}\left(\sum_{j=i}^{s} x_j^2\right) = x_i^3.$$

□

We now describe explicitly the leading terms of $\partial \mathscr{I}_f$.

LEMMA 3.4. *Let $f = g \circ h \in D_{r,2,2}$ be the particular example defined previously. The leading terms of a truncated 3-Gröbner basis of $\partial \mathscr{I}_f$ are:*

$$\begin{array}{ccc} & \left[x_s^3\right] & \cup \\ & \left[x_s x_{s-1}^2, x_{s-1}^3\right] & \cup \quad \left[x_s x_{s-2}^2, x_{s-1} x_{s-2}^2, x_{s-2}^3\right] \\ & & \cup \quad \cdots \\ \cup \left[x_s x_0^2, x_{s-1} x_0^2, \cdots, x_2 x_0^2, x_0^3\right] & & . \end{array}$$

PROOF. Clearly

$$\begin{aligned} \partial \mathscr{I}_f &= \left\langle \frac{\partial f_i}{\partial x_u} \mid 0 \leq i \leq u \leq s \right\rangle \\ &= \left\langle \frac{\partial f_i}{\partial x_u} \mid 0 \leq i < u \leq s \right\rangle + \left\langle \frac{\partial f_i}{\partial x_i} \mid 0 \leq i \leq s \right\rangle \\ &= \left\langle \frac{\partial f_i}{\partial x_u} - \frac{\partial f_{i+1}}{\partial x_u} \mid 0 \leq i < u \leq s \right\rangle + \left\langle \frac{\partial f_i}{\partial x_i} \mid 0 \leq i \leq s \right\rangle \\ &= \left\langle x_u x_i^2 \mid 0 \leq i < u \leq s \right\rangle + \left\langle \frac{\partial f_i}{\partial x_i} \mid 0 \leq i \leq s \right\rangle. \end{aligned}$$

Since $LT_{\succ}\left(\frac{\partial f_i}{\partial x_i}\right) = x_i^3$, the leading terms are pairwise distinct. This proves that

$$\left[x_u x_i^2 \mid 0 \leq i < u \leq s\right] + \left[\frac{\partial f_i}{\partial x_i} \mid 0 \leq i \leq s\right],$$

is a 3-Gröbner basis of $\partial \mathscr{I}_f$. □

Finally:

COROLLARY 3.1. *Let $\mathbb{K}$ be a field of characteristic $\neq 2$, and let $f = g \circ h \in D_{r,2,2}$ be the particular example defined previously. The truncated 2-Gröbner basis of $\partial \mathscr{I}_f : x_s$ is exactly $\left[x_0^2, \ldots, x_s^2\right] = \mathscr{L}(h)$.*

PROOF. It is a well known property of the DRL ordering that for a polynomial f, $x_s | f$ iff $x_s | LT_{\succ}(f)$. Consequently, the polynomials in $\partial \mathscr{I}_f$ of degree 3 divisible by x_s are, thanks to Lemma 3.4: $\frac{\partial f_0}{\partial x_s} = 4x_s \sum_{j=0}^{s} x_j^2$ and $x_s x_i^2$ for $0 \leq i < s$. Consequently, the truncated 2-Gröbner basis of $\partial \mathscr{I}_f : x_s$ is:

$$\left\langle \sum_{j=0}^{s} x_j^2, x_0^2, \ldots, x_{s-1}^2 \right\rangle = \left\langle x_s^2, x_0^2, \ldots, x_{s-1}^2 \right\rangle.$$

Finally, is not difficult to see that a basis of $\mathscr{L}(h)$ is also $\left[x_0^2, \ldots, x_s^2\right]$. □

3.3 $(3,2)$ decomposition

We now consider a $(3,2)$ decomposable $f = (f_0, \ldots, f_t) \in D_{r,2,3}$. In this case, we start from the ideal generated by the second order partial derivatives:

$$\partial^2 \mathscr{I}_f = \left\langle \frac{\partial^2 f_i}{\partial x_u \partial x_p} \mid 0 \leq i \leq t, \text{ and } 0 \leq u, p \leq r \right\rangle.$$

According to [18], each generator of the previous ideal is a linear combination of elements $\{x_j x_k \cdot h_q\}_{1 \leq j,k \leq r}^{1 \leq q \leq s}$. As previously, it is convenient to consider the $(t \cdot r(r+1)/2) \times (s \cdot r(r+1)/2)$ matrix:

$$A = \begin{array}{c} \\ \frac{\partial^2 f_0}{\partial x_u \partial x_p} \\ \vdots \\ \frac{\partial^2 f_i}{\partial x_u \partial x_p} \\ \vdots \\ \frac{\partial^2 f_t}{\partial x_u \partial x_p} \end{array} \begin{array}{c} \cdots \quad \cdots \quad x_j x_k \cdot h_q \quad \cdots \quad \cdots \\ \left(\begin{array}{c} \cdots \\ \cdots \\ \cdots \\ \cdots \\ \cdots \end{array} \right) \end{array}$$

In a similar way, if $\mathrm{Rank}(A) = \#\mathrm{Columns}(A)$, then each $x_r^2 \cdot h_i$ can be expressed as a linear combination of $\frac{\partial^2 f_i}{\partial x_u \partial x_p}$ leading in particular to

$$x_r^2 h_i \in \partial \mathscr{I}_f^2, \text{for all } i, 0 \leq i \leq s. \tag{4}$$

Let G be truncated 2-Gröbner basis of $\partial \mathscr{I}_f^2 : x_r^2$. Again, we want to prove the necessary condition of success of **MultiComPoly**:

$$\mathrm{Span}_{\mathbb{K}}(G) = \mathscr{L}(h). \tag{5}$$

Similarly to the $(2,2)$ case, it is clear that set of h satisfying (5) is a Zariski-open set. The main task is to show that it is nonempty. We consider the same type of decomposable $f = g \circ h \in D_{r,3,2}$ as previously:

- $r = s = t$ and $g = (y_0^3, \ldots, y_s^3)$,
- for all $i, 0 \leq i \leq s, h_i = \sum_{j=i}^{s} x_j^2$.

In what follows, we set $f_{s+1} = h_{s+1} = 0$. The idea is to split the ideal $\partial^2 \mathscr{I}_f$ into several parts:

$$\partial^2 \mathscr{I}_f = \mathscr{H}_1 \cap \mathscr{H}_2 \cap \mathscr{H}_3$$

where:

$$\begin{aligned} \mathscr{H}_1 &= \left\langle \frac{\partial^2 f_{i+1}}{\partial x_u \partial x_p} - \frac{\partial^2 f_i}{\partial x_u \partial x_p} \mid i < u < p \leq s \right\rangle \\ \mathscr{H}_2 &= \left\langle \frac{\partial^2 f_{i+1}}{\partial x_u^2} - \frac{\partial^2 f_i}{\partial x_u^2} \mid 0 \leq i < s \text{ and } i \leq u \leq s \right\rangle + \left\langle \frac{\partial^2 f_s}{\partial x_s^2} \right\rangle \\ \mathscr{H}_3 &= \left\langle \frac{\partial^2 f_{i+1}}{\partial x_i \partial x_p} - \frac{\partial^2 f_i}{\partial x_i \partial x_p} \mid 0 \leq i < s \text{ and } i \leq p \leq s \right\rangle \end{aligned}$$

It turns out that we can predict accurately the leading terms of a 4-Gröbner basis of each ideals and that they are all distinct. For that, we need several technical lemmas.

LEMMA 3.5. *For $i \leq u < p \leq s$, we have:*

$$\begin{aligned} &\frac{\partial^2 f_i}{\partial x_u \partial x_p} = 24 x_u x_p h_i \\ &\frac{\partial^2 f_{i+1}}{\partial x_u \partial x_p} - \frac{\partial^2 f_i}{\partial x_u \partial x_p} = 24 x_i^2 x_u x_p \text{ if } u > i. \\ &\frac{\partial^2 f_i}{\partial x_u^2} = 6\left(h_i + 4x_u^2\right) h_i. \end{aligned} \tag{6}$$

Consequently ,if the characteristic of $\mathbb{K}$ is not 2 or 3, $\mathscr{H}_1 = \langle x_i^2 x_u x_p \mid i < u < p \leq s \rangle$.

PROOF.

$$\begin{aligned} f_i &= h_i^3, \\ \frac{\partial f_i}{\partial x_u} &= 3h_i^2 \frac{\partial h_i}{\partial x_u}. \end{aligned}$$

Due to the particular choice of h, $\frac{\partial f_i}{\partial x_u} = 0$ if $u < i$ and for all $u \geq i$, $\frac{\partial f_i}{\partial x_u} = 6 x_u h_i^2$. Now, let $i \leq u \leq p \leq s$, we have $\frac{\partial^2 f_i}{\partial x_u \partial x_p} =$

$$\begin{aligned} 12 x_u h_i \frac{\partial h_i}{\partial x_p} &= 24 x_u x_p h_i, && \text{if } u \neq p. \\ &= 6h_i^2 + 24 x_u^2 h_i, && \text{if } u = p. \end{aligned}$$

Finally, if $u \neq p$ and $u > i$, then $\frac{\partial^2 f_{i+1}}{\partial x_u \partial x_p} - \frac{\partial^2 f_i}{\partial x_u \partial x_p} = x_u x_p (h_{i+1} - h_i) = x_u x_p x_i^2$. $\square$

LEMMA 3.6. *The leading terms w.r.t a DRL ordering of a truncated 4-Gröbner basis of $\mathscr{H}_3$ have the following shape:*

$$x_i^3 x_p \text{ for } 0 \leq i < s \text{ and } i \leq p \leq s. \tag{7}$$

PROOF. We have:

$$\frac{\partial^2 f_{i+1}}{\partial x_i \partial x_p} - \frac{\partial^2 f_i}{\partial x_i \partial x_p} = 0 - \frac{\partial^2 f_i}{\partial x_i \partial x_p} = -24 x_i x_p (x_i^2 + \cdots + x_s^2).$$

Thus the leading term is $x_i^3 x_p$. $\square$

LEMMA 3.7. *We consider the following $N \times N$ integer matrix:*

$$A_N = \begin{bmatrix} 5 & 1 & \cdots & 1 & 1 \\ 1 & 5 & \cdots & 1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \cdots & 5 & 1 \\ 1 & 1 & \cdots & 1 & 5 \end{bmatrix}.$$

Then $\det(A_N) = (N+4)\, 2^{2N-2}$.

PROOF. By summing up the rows of the matrix A_N we obtain the following vector:

$$\mathbf{v} = \begin{bmatrix} (N+4) & \cdots & (N+4) \end{bmatrix}.$$

For all $1 \leq i < N$, we subtract from the i-th row of A_N the vector $\frac{1}{N+4}\mathbf{v}$. Hence:

$$\det(A_N) = \begin{vmatrix} 4 & 0 & \cdots & 0 & 0 \\ 0 & 4 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 4 & 0 \\ N+4 & N+4 & \cdots & N+4 & N+4 \end{vmatrix} = (N+4) 4^{N-1}$$

$\square$

LEMMA 3.8. *If the characteristic of $\mathbb{K}$ is larger than $s+4$, then $\mathscr{H}_2 = \langle x_j^2 h_i \mid 0 \leq i \leq s$ and $i \leq j \leq s \rangle$.*

PROOF. Clearly $\mathscr{H}_2 = \left\langle \frac{\partial^2 f_i}{\partial x_u^2} \mid 0 \leq i \leq s \text{ and } i \leq u \leq s \right\rangle$.
From the expression (6) of $\frac{\partial^2 f_i}{\partial x_u^2}$ we deduce that:

$$\begin{bmatrix} \frac{\partial^2 f_i}{\partial x_i^2} \\ \vdots \\ \frac{\partial^2 f_i}{\partial x_s^2} \end{bmatrix} = 6 A_{s-i+1} \begin{bmatrix} x_i^2 h_i \\ \vdots \\ x_s^2 h_i \end{bmatrix}$$

Since the characteristic of $\mathbb{K}$ is $> s+4$, we know from lemma 3.7 that $\det(A_{s-i+1}) \neq 0$ and thus

$$\left\langle \frac{\partial^2 f_i}{\partial x_i^2}, \cdots, \frac{\partial^2 f_i}{\partial x_s^2} \right\rangle = \langle x_i^2 h_i, \ldots, x_s^2 h_i \rangle$$

$\square$

LEMMA 3.9. *If the characteristic of $\mathbb{K}$ is $> s+4$, it holds that* $\mathscr{H}_2 = \langle x_0^4,\ x_0^2 x_1^2, x_1^4, x_0^2 x_2^2, x_1^2 x_2^2, x_2^4, \ldots,\ x_0^2 x_s^2, x_1^2 x_s^2, \ldots, x_{s-1}^2 x_s^2, x_s^4 \rangle$.

PROOF. We set $\mathscr{I}_i = \langle x_i^2 h_i, \ldots, x_s^2 h_i \rangle$. From lemma 3.8 we know that $\mathscr{H}_2 = \mathscr{I}_0 \cap \mathscr{I}_s$. We prove by induction that $\mathscr{I}_i \bmod \mathscr{I}_{i+1} \cap \cdots \cap \mathscr{I}_s = \langle x_i^2 x_i^2, \ldots, x_i^2 x_s \rangle$.
For $i' = s$ the property is true since $\mathscr{I}_s = \langle x_s^4 \rangle$.
Now we assume that the property is true for all $i' > i$. This implies that for all $j > i$:

$$x_j^2 h_i = x_j^2 x_i^2 + \sum_{k=i+1}^{s} x_j^2 x_k^2 \longrightarrow_{\mathscr{I}_{i+1} \cap \cdots \cap \mathscr{I}_s} x_j^2 x_i^2,$$

where $\longrightarrow_{\mathscr{I}}$ stands for the reduction modulo $\mathscr{I}$.
Finally $x_i^2 h_i = x_i^4 + \sum_{j=i+1}^{s} x_i^2 x_j^2 \longrightarrow_{\langle x_{i+1}^2 h_i, \cdots, x_s h_s \rangle} x_i^4$. Consequently the property is also true if $i' = i$. $\square$

We now summarize our results.

COROLLARY 3.2. *Let $f = g \circ h \in D_{r,3,2}$ be the particular example defined previously. If the characteristic of $\mathbb{K}$ is larger than $s+4$, the truncated 2-Gröbner basis of $\partial \mathscr{I}_f^2 : x_s^2$ is*

$$\left[x_0^2, \ldots, x_s^2 \right] = \mathscr{L}(h)$$

PROOF. According to the previous lemmas 3.5, 3.6, and 3.9, the leading terms of $\mathscr{H}_1$, $\mathscr{H}_2$, and $\mathscr{H}_3$ are pairwise distinct. We deduce a 4-Gröbner basis of $\partial \mathscr{I}_f^2$. Hence, the polynomials in $\partial \mathscr{I}_f^2$ of degree 4 divisible by x_s^2 are in $\mathscr{H}_3$. The result comes from the fact that these $s+1$ polynomials are the monomials $\left[x_0^2 x_s^2, \ldots, x_s^2 x_s^2 \right]$. $\square$

4. GENERIC UNIQUENESS OF THE LEFT COMPONENT

The left component of a decomposition can recovered by solving a linear system as soon as h (or any basis of $\mathscr{L}(h)$ is known. Indeed, given f and h, a solution g to $f = g \circ h$ can be described by a system of linear equations. This system has

$$\alpha = (t+1) \binom{r+n}{r}$$

equations, each corresponding to one monomial in f. The coefficients in this linear system are polynomials in the coefficients of h. The unknowns correspond to the coefficients of g are

$$\beta = (t+1) \binom{s+\ell}{s}$$

in number. When can we expect g to be uniquely determined by f and h? Generically, this corresponds to the question of whether $\alpha \geq \beta$.

THEOREM 4.1. *1. If $s \leq r + \ell(m-1)$ and $\ell \leq r$, then $\alpha \geq \beta$.*

2. If $s = r + \ell(m-1)$, $m \geq 2$, and $\ell \leq r$, then $\alpha \geq \beta$.

3. *If $s > r+\ell(m-1)$ and $r \leq \ell$, then $\alpha < \beta$.*

4. *If $s \geq (r+n)(n+1)/(\ell+1)-\ell$, $\ell, m \geq 2$, and $\ell \leq r \leq 2\ell$, then $\alpha < \beta$.*

PROOF. (1) We have

$$\alpha \geq \beta \Leftrightarrow \quad \frac{(r+n)^{\underline{r}}}{r!} = \binom{r+n}{r} \geq \binom{s+\ell}{s} = \frac{(s+l)^{\underline{\ell}}}{\ell!} \quad (8)$$

$$\Leftrightarrow \quad (r+n)^{\underline{l}}(r+n-\ell)^{\underline{r-\ell}} \geq \frac{r!}{\ell!}(s+\ell)^{\underline{\ell}} = (s+\ell)^{\underline{\ell}} r^{\underline{r-\ell}}, \quad (9)$$

where $x^{\underline{r}} = x \cdot (x-1)\cdots(x-r+1)$ is the falling factorial (or Pochhammer symbol). We have $r+n-\ell = r+\ell(m-1) \geq r$ and $r+n \geq s+\ell$, so that the inequality (9) holds.

(2) Let $k = r+n = s+\ell$. We have $n \geq m\ell \geq 2\ell$, and

$$\begin{aligned}
\alpha \geq \beta \Leftrightarrow & \quad \binom{k}{r} \geq \binom{k}{s} \\
\Leftrightarrow & \quad \frac{|r-n|}{2} = |r-\tfrac{k}{2}| \leq |s-\tfrac{k}{2}| \\
= & \quad \frac{|2r+2n-2\ell-(r+n)|}{2} = \frac{|r+n-2\ell|}{2} = \frac{r+n-2\ell}{2} \\
\Leftrightarrow & \quad |r-n| \leq n+r-2\ell.
\end{aligned}$$

If $r \geq n$, then this holds since $0 \leq 2n-2\ell = 2\ell(m-1)$, and otherwise we have $|r-n| = n-r \leq n+r-2\ell$, since $\ell \leq r$.

(3) Similarly to (1), we write

$$\alpha < \beta \Longleftrightarrow (r+n)^{\underline{\ell}}(r+n-\ell)^{\underline{n-\ell}} < (s+\ell)^{\underline{\ell}} n^{\underline{n-\ell}}.$$

Since $r \leq \ell$, the latter inequality is satisfied by assumption.

(4) We write

$$\begin{aligned}
\frac{r!}{t+1}\alpha &= (r+n)^{\underline{r}} = (r+n)\cdots(n+1), && (10)\\
\frac{r!}{t+1}\beta &= (s+\ell)^{\underline{\ell}}\frac{r!}{\ell!} = (s+\ell)^{\underline{\ell}} r^{\underline{r-\ell}} && (11)\\
&= (s+\ell)\cdots(s+1)\cdot r\cdots(\ell+1). && (12)
\end{aligned}$$

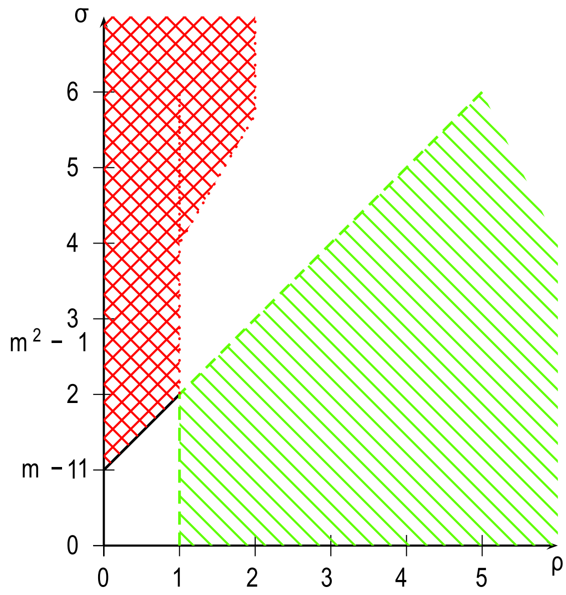
In both products, we multiply the first and last terms, the second and second last terms, etc. The resulting biproducts are $(r+n-i)(n+1+i)$ and $(s+\ell-i)(\ell+1+i)$, respectively, for $0 \leq i < r-\ell$. The assumption on s implies $s+\ell > r+n$, as in 3, since $(n+1)/(\ell+1) > 1$. In particular, we have $r < s$, and for $i \geq 0$

- $(r+n)(n+1) - \ell(\ell+1) \leq s(\ell+1)$,
- $(r+n)(n+1)-(s+\ell)(\ell+1)-i(s-r) < (r+n)(n+1)-(s+\ell)(\ell+1) \leq 0$,
- $(r+n-i)(n+1+i) \leq (s+\ell-i)(\ell+1+i)$.

Since $r-\ell \leq \ell$, the factors not absorbed in these $r-\ell$ biproducts are

- $(r+n-(r-\ell))\cdots(n+1+r-\ell) = (n+\ell)\cdots(n+r-\ell+1)$ in (10),
- $(s+\ell-(r-\ell))\cdots(s+1) = (s+2\ell-r)\cdots(s+1)$ in (12).

(These products are empty if $r = 2\ell$.) The assumption guarantees that $n+\ell-i < s+2\ell-r-i$ for $i \geq 0$, and $\alpha < \beta$ follows. $\square$



5. CONCLUSION

In order to visualize the result, we divide the variables by ℓ, obtaining $\rho = r/\ell$ and $\sigma = s/\ell$. In the figure on the opposite page, we have $\alpha \geq \beta$ in the green striped area, $\alpha < \beta$ in the red hashed area, and $\alpha = \beta$ on the diagonal line.

For our application, we think of ℓ and m (and hence n) as being fairly small, and of r and s as being substantially larger. Thus the right-hand striped area in the figure is relevant for us.

If $\alpha < \beta$, then the system for solving $f = g \circ h$ is underdetermined and has either no or many solutions. If $\alpha \geq \beta$, we have at least as many equations as unknowns. We conjecture that for a "generic" h, the system has maximal rank and thus is overdetermined. By trying to solve it, we determine whether a solution exists or not.

The central result of this paper is the proof in the preceding sections of this conjecture in the cases (2,2) and (3,2).

6. REFERENCES

[1] V. S. Alagar and M. Thanh. *Fast Polynomial Decomposition Algorithms*. In Proc. EUROCAL85, Lecture Notes in Computer Science, vol. 204, pp. 150-153, Springer–Verlag, 1985.

[2] M. Bardet. *Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie.* Thèse de doctorat, Université de Paris VI, 2004.

[3] M. Bardet, J-C. Faugère, and B. Salvy. *On the Complexity of Gröbner Basis Computation of Semi-Regular Overdetermined Algebraic Equations.* In Proc. of International Conference on Polynomial System Solving (ICPSS), pp. 71–75, 2004.

[4] M. Bardet, J-C. Faugère, B. Salvy and B-Y. Yang. *Asymptotic Behaviour of the Degree of Regularity of Semi-Regular Polynomial Systems.* In Proc. of MEGA 2005, Eighth International Symposium on Effective Methods in Algebraic Geometry, 2005.

[5] D. R. Barton and R. E. Zippel. *Polynomial decomposition algorithms.* J. Symb. Comp., 1, pp.

159–168, 1985.

[6] B. Buchberger. *An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal (German)*, PhD Thesis, University of Innsbruck, Math. Institute, Austria, 1965. (English Translation: J.S.C., Special Issue on Logic, Mathematics, and Computer Science: Interactions. Vol. 41 (3-4), pp 475-511, 2006).

[7] B. Buchberger. *Ein algorithmisches Kriterium fur die Lšsbarkeit eines algebraischen Gleichungssystems (An Algorithmical Criterion for the Solvability of Algebraic Systems of Equations)* Aequationes mathematicae 4/3, 1970, pp. 374-383. (English translation in: B. Buchberger, F. Winkler (eds.), Gröbner Bases and Applications, Proc. of the International Conference “33 Years of Gröbner Bases”, 1998, RISC, Austria, London Mathematical Society Lecture Note Series, Vol. 251, Cambridge University Press, 1998, pp. 535 -545.)

[8] B. Buchberger. *Gröbner Bases : an Algorithmic Method in Polynomial Ideal Theory.* Recent trends in multidimensional systems theory. Reider ed. Bose, 1985.

[9] B. Buchberger, G.-E. Collins, and R. Loos. *Computer Algebra Symbolic and Algebraic Computation.* Springer-Verlag, second edition, 1982.

[10] E.-W. Chionh, X.-S. Gao, L.-Y. Shen. *Inherently Improper Surface Parametric Supports.* Computer Aided Geometric Design 23 (2006),pp. 629–639.

[11] D. A. Cox, J.B. Little, and D. O’Shea. *Ideals, Varieties, and Algorithms: an Introduction to Computational Algebraic Geometry and Commutative Algebra.* Undergraduate Texts in Mathematics. Springer-Verlag. New York, 1992.

[12] M. Dickerson. *The functional Decomposition of Polynomials.* Ph.D Thesis, TR 89-1023, Departement of Computer Science, Cornell University, Ithaca, NY, July 1989.

[13] M. Dickerson. *General Polynomial Decomposition and the s-1-decomposition are NP-hard.* International Journal of Foundations of Computer Science, 4:2 (1993), pp. 147–156.

[14] F. Dorey and G. Whaples. *Prime and composite polynomials.* J. Algebra,(28), pp. 88-101, 1974.

[15] J.-C. Faugère. *A New Efficient Algorithm for Computing Gröbner Basis without Reduction to Zero:* F_5. Proceedings of ISSAC, pp. 75–83. ACM press, July 2002.

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

[17] J.-C. Faugère, L. Perret. *An Efficient Algorithm for Decomposing Multivariate Polynomials and its Applications to Cryptography.* Special Issue of JSC, “Gröbner Bases techniques in Coding Theory and Cryptography” , on-line available.

[18] J.-C. Faugère, L. Perret. *High order derivatives and decomposition of multivariate polynomials*. Proceedings of ISSAC, pp. 207-214. ACM press, July 2009.

[19] R. Fröberg. *An inequality for Hilbert series of graded algebras*. Math. Scand., 56(2) :117–144, 1985.

[20] J. von zur Gathen. *The number of decomposable univariate polynomials.* Proceedings of ISSAC, pp. 359-366. ACM press, July 2009.

[21] J. von zur Gathen. *Functional decomposition of polynomials: the tame case.* J. Symb. Comput. (9), pp. 281–299, 1990.

[22] J. von zur Gathen. *Functional decomposition of polynomials: the wild case.* J. Symb. Comput. (10), pp. 437–452, 1990.

[23] J. von zur Gathen, J. Gutierrez, R. Rubio. *Multivariate Polynomial Decomposition.* Applicable Algebra in Engineering, Communication and Computing, 14 (1), pp. 11–31, 2003.

[24] J. Gutierrez, D. Sevilla. *Computation of Unirational fields.* J. Symb. Comput. 41(11), pp. 1222–1244, 2006.

[25] J. Gutierrez, R. Rubio, D. Sevilla. *On Multivariate Rational Function Decomposition.* J. Symb. Comput. 33(5), pp. 545–562, 2002.

[26] D. Kozen, and S. Landau. *Polynomial Decomposition Algorithms.* J. Symb. Comput. (7), pp. 445–456, 1989.

[27] J. F. Ritt. *Prime and Composite Polynomials.* Trans. Amer. Math. Soc., (23), pp 51-66, 1922.

[28] M. Sweedler. *Using Gröbner Bases to Determine the Algebraic and Transcendental Nature of Field Extensions: Return of the Killer Tag Variables.* Proc. AAECC, 66–75, 1993.

[29] S. M. Watt. *Functional Decomposition of Symbolic Polynomials.* In Proc. International Conference on Computational Sciences and its Applications, (ICCSA 2008), IEEE Computer Society, pp. 353–362.

[30] D.F. Ye, Z.D. Dai and K.Y. Lam. *Decomposing Attacks on Asymmetric Cryptography Based on Mapping Compositions*, Journal of Cryptology (14), pp. 137–150, 2001.