Gröbner Bases Specialization through Hilbert Functions: The Homogeneous Case

M.–J. Gonzalez–Lopez*† and L. Gonzalez–Vega*†
Dpto. Matemáticas, Estadística y Computación
Universidad de Cantabria, Santander, Spain

C. Traverso* and A. Zanoni*
Dipartimento di Matematica
Università di Pisa, Pisa, Italy

Abstract

In this paper it is shown how to deal with homogeneous polynomial system solving involving parameters by using the Hilbert function in order to check that the specialization of a "generic" Gröbner Basis of the parametric homogeneous polynomial system (computed in a polynomial ring containing the parameters and the unknowns as variables) is a Gröbner Basis of the specialized homogeneous polynomial system. A preliminary implementation of these algorithms into the PoSSoLib is also reported.

Introduction.

Many practical problems can be easily solved if we are able to find the solution of an algebraic system of equations with parametric coefficients for any (or for many) values of the parameters. In these problems the use of Gröbner Bases techniques to rewrite the given equations in easier ways (for example, in triangular form) have to be completed with other techniques to determine which are the values of the parameters that preserve the good properties of the Gröbner bases computations. In this paper we address this question, for the case of homogeneous polynomial systems, by focusing our attention to the using of the already available tools inside the FRISCO framework [5] such as the PoSSoLib. As a final result it is obtained an efficient implementation dealing with the problem of solving a homogeneous polynomial system of equations containing parameters when using Gröbner Bases as the main tool.

*Partially supported by FRISCO (European Union, LTR 21.024).
†Partially supported by DGICYT PB 95/0563-A (Sistemas de Ecuaciones Algebraicas: Resolución y Aplicaciones).

Let $\underline{T}$ be the parameters $(T_1, \ldots, T_s)$ and $\underline{X} = (X_1, \ldots, X_n)$ the unknowns. The problem to solve is the determination (whatever it means and to be clarified later) of the solution set of the polynomial system of equations:

$$\begin{array}{ll} F_1(\underline{T}, X_1, \ldots, X_n) & = 0 \\ F_2(\underline{T}, X_1, \ldots, X_n) & = 0 \\ \vdots & \vdots \\ F_m(\underline{T}, X_1, \ldots, X_n) & = 0 \end{array}$$

where the F_i's are homogeneous polynomials in the variables $\underline{X}$. Two different questions arise naturally in this context: first, to get the conditions the parameters must verify in order the considered homogeneous system has a solution and, second, to describe, in some way, the solutions, i.e., the dependency between every unknown and the parameters.

Different methods can be found in the Computer Algebra literature addressing this problem in general (not only for the homogeneous case). Mainly:

- To use Comprehensive Gröbner Bases (see [14]).
  - The notion of Comprehensive Gröbner Bases (see [14]) is exactly, if it is easy to compute, what we want to obtain: an explicit partition of the parameter space together with a Gröbner Basis of the considered ideal, already specialized, for every subset in such partition. The main problem with this approach is that, in its general version, is highly inefficient due mainly to the big number of sets appearing in such partition.
- To use the Dynamic Evaluation Method (see [4]).
  - By using only "well parametrized" gcd computations and a "case by case" methodology, a complete description of the solution set is obtained in terms of conditions on the parameters.
- To use multivariate resultants (see [13]).
  - The usual techniques based upon resultants work only when the numbers of equations and unknowns are equal, they require the computation of determinants of matrices with a very big size and polynomial entries and, initially, they only provide the conditions on the parameter space in order the considered system has a solution.
- To use triangular sets (see [8]and the references contained there) .
  - It is close in spirit to the Dynamic Evaluation Method before mentioned but stronger algebraic techniques are used in order to remove multiplicities from the different solution sets which helps to improve the efficiency of the method.
- To use specific Linear Algebra tools for parametric linear systems (see [11]).

– An ad–hoc using of Cramer's rule together with a parameter dependent rank computation of matrices with polynomial entries provide a specific solution for this case.

In this paper our goal is to show how, with a not very expensive cost, the using of Gröbner Bases can help to get answers when trying to describe the solution set of the considered homogeneous system in terms of the parameters. Since the tool chosen to be used is the computation of Gröbner Bases, the first section presents, in an unified way, the behaviour of Gröbner Bases under specialization. Two strategies can be initially adopted:

- To compute a Gröbner Basis of the ideal generated by the polynomials $F_1, \ldots, F_m$ in $\mathbb{Q}(\underline{T})[X_1, \ldots, X_n]$ (with respect to any monomial ordering) together with the "good" specialization conditions on $\underline{T}$ (see [3]).
- To compute a Gröbner Basis of the ideal generated by the polynomials $F_1, \ldots, F_m$ in $\mathbb{Q}[\underline{T}, X_1, \ldots, X_n]$ (with respect to any monomial ordering) together with the "good" specialization conditions on $\underline{T}$. Anyway, the new system is always equivalent to the first one, even if it is not a Gröbner Basis (see [7] or [9]).

and their analysis is done is the first section. This section shows also how to adapt the strategy in [6] to avoid the growing the coefficients in the Gröbner Basis in order to get a list of open conditions on the parameter space where a Gröbner Basis is available after specialization.

The second section contains the main result of this paper: it is shown, when working in $\mathbb{Q}[\underline{T}, X_1, \ldots, X_n]$, how to use the Hilbert Function in order to obtain a set of conditions on the parameters providing that the specialization of a "generic" Gröbner Basis in such polynomial ring is again a Gröbner Basis of the specialized homogeneous polynomial system. Last two sections are devoted, first, to indicate to use these techniques to deal with polynomial system solving involving parameters and homogeneous polynomials and, second, to present the implementation of these algorithms in the PoSSoLib.

1 Gröbner bases under specializations.

This section is devoted to present the state of the art in this kind of techniques. Let $\mathbb{K}$ be a field and $\underline{X} = (X_1, \ldots, X_n)$, $\underline{T} = (T_1, \ldots, T_m)$ sets of variables. We call *specialization* any ring homomorphism $\varphi : \mathbb{K}[\underline{T}, \underline{X}] \to \mathbb{K}[\underline{X}]$ such that $\varphi(\mathbb{K}[\underline{T}]) = \mathbb{K}$ and $\varphi(X_i) = X_i, i = 1, \ldots, n$. The *specialization associated to* a point $t^{(0)} \in \mathbb{K}^m$ is the one defined by $\varphi^{(0)}(p(\underline{T}, \underline{X})) := p(t^{(0)}, X)$, for $p(\underline{T}, \underline{X}) \in \mathbb{K}[\underline{T}, \underline{X}]$.

Let $I =< F_1(\underline{T}, \underline{X}), \ldots, F_m(\underline{T}, \underline{X}) >\subseteq \mathbb{K}[\underline{T}, \underline{X}]$ be an ideal, $>$ a monomial ordering in $\mathbb{K}[\underline{T}, \underline{X}]$ and $G = \{g_1(\underline{T}, \underline{X}), \ldots, g_s(\underline{T}, \underline{X})\}$ a Gröbner basis of I with respect to $>$.

The most practical question that we would like to solve is to determine the subset W of $\mathbb{K}^m$ such that $t^{(0)} \in W$ if and only if its associated specialization

$\varphi^{(0)}$ verifies that $\varphi^{(0)}(G)$ is a Gröbner basis of $\varphi^{(0)}(I)$. From a computational point of view this is the most interesting aspect, as once we have computed W, every time that we are given a value to the parameters we just have to test if it belongs or not to W to determine if we have or not a Gröbner basis.

There are two possibilities to deal with this problem: to perform the initial Gröbner Bases computation in $\mathbb{K}(\underline{T})[\underline{X}]$ or in $\mathbb{K}[\underline{T},\underline{X}]$.

1.1 Working in $\mathbb{K}(\underline{T})[\underline{X}]$.

The best result, when working in $\mathbb{K}(\underline{T})[\underline{X}]$, that we have found appears in [3] (pp. 277, Exercises 5 to 9), where it is proposed an algorithmic method to compute a subset $\tilde{W} \subset \mathbb{K}^m$ such that if $\tilde{G} = \{\tilde{g}_1(\underline{X}), \dots, \tilde{g}_s(\underline{X})\} \subset \mathbb{K}(\underline{T})[\underline{X}]$ is a Gröbner basis of the ideal $\tilde{I} =< \tilde{F}_1(\underline{X}), \dots, \tilde{F}_m(\underline{X}) >\subset \mathbb{K}(\underline{T})[\underline{X}]$, and $t^{(0)} \in \tilde{W}$, then $\varphi^{(0)}(\tilde{G})$ is a Gröbner basis of $\varphi^{(0)}(\tilde{I})$. This set $\tilde{W}$ of sufficient conditions on the parameters is defined by:

a) none of the denominators of $\tilde{F}_i$ are 0, $i = 1, \dots, m$,

b) none of the denominators of $\tilde{g}_j$ are 0, $j = 1, \dots, s$,

c) let B_{ij} be the polynomials in $\mathbb{K}(\underline{T})[\underline{X}]$ such that $\tilde{g}_j = \sum_{i=1}^{m} B_{ij}\tilde{F}_i$; none of the denominators of B_{ij} are 0.

Although the computation of the denominators appearing in the $\tilde{F}_i$'s and the $\tilde{g}_j$'s is easy, the computation of the denominators in the B_{ij}'s can lead to lengthy calculations: we have to compute one quotient ideal $(\tilde{I} : \tilde{g}_j)$ and one elimination ideal $(\tilde{I} : \tilde{g}_j \cap \mathbb{K}[\underline{T}])$ for every polynomial $\tilde{g}_j$ in the basis.

1.2 Working in $\mathbb{K}[\underline{T},\underline{X}]$.

The approaches to be considered here treat the specialization aspect for particular orderings (block or lexicographical orderings), particular ideals (zero dimensional and univariate ideals) and *particular specializations*. The most important difference between these approaches and the previous one is that some computations have to be made for every given specialization in order to check if the specialized Gröbner Basis is actually a Gröbner Basis of the specialized ideal. In the following we present the details of these two approaches.

1.2.1 Gianni's approach.

Given a specialization φ, we will say that an ordering $>$ on the monomials of $\mathbb{K}[\underline{T},\underline{X}]$ is *φ-admissible* if it is a block ordering with respect to $\underline{T}$ and $\underline{X}$, and $\underline{X} > \underline{T}$, i.e., if $>_1$ (resp. $>_2$) is the restriction of $>$ to the $\underline{X}$-variables (resp. to the $\underline{T}$-variables), then:

$$\mathbf{T^B X^A} > \mathbf{T^D X^C} \iff \begin{array}{c} \mathbf{X^A} >_1 \mathbf{X^C} \\ \text{or} \\ \mathbf{X^A} = \mathbf{X^C} \text{ and } \mathbf{T^B} >_2 \mathbf{T^D} \end{array}$$

for all $A, C \in \mathbb{N}^n$ and for all $B, D \in \mathbb{N}^m$.

For a subset H of $\mathbb{K}[\underline{T}, \underline{X}]$, $Lt(H)$ denotes the ideal generated by $\{lt(f)/f \in H\}$, where $lt(f)$ denotes the leading term of f. If φ is a specialization then $lt_\varphi(f)$ ($f \in \mathbb{K}[\underline{T}, \underline{X}]$) will denote $U(\underline{T})\mathbf{X}^A$ where $\mathbf{X}^A$ is the biggest $\underline{X}$–monomial in f. Thus $Lt_\varphi(H)$ will denote the ideal generated by $\{lt_\varphi(f)/f \in H\}$.

Theorem 1 *([7]) Let $I \subset \mathbb{K}[\underline{T}, \underline{X}]$ be an ideal, φ a specialization and G a Gröbner basis for I with respect to a φ-admissible ordering. If*

$$Lt(\varphi(I)) = \varphi(Lt_\varphi(I)) \tag{1}$$

then $\varphi(G)$ is a Gröbner basis for $\varphi(I)$

Remark that, as G is a Gröbner basis of I, we can write

$$Lt(I) = < lt(g_1), \ldots, lt(g_s) >$$

, and, therefore, we know the generators of the ideal to the right of the equality (1), $\varphi(Lt_\varphi(I))$:

$$\varphi(Lt_\varphi(I)) = < \varphi(lt_\varphi(g_1)), \ldots, \varphi(lt_\varphi(g_s)) > .$$

However, we do not have a finite representation of the ideal to the left $Lt(\varphi(I))$ — unless we know a priori a Gröbner basis of $\varphi(I)$ — but finding this is the purpose of our computations.

In the zero–dimensional and univariate case ($\dim(\langle F_1, \ldots, F_m \rangle) = 0$ and $n = 1$) the results here described can be stated in a very practical way, avoiding any test.

Theorem 2 *([7]) Let $I \subset \mathbb{K}[\underline{T}, \underline{X}]$ be a zero dimensional ideal and $n = 1$, i.e. $\underline{X} = (X_1)$. Let φ be a specialization. If G is a Gröbner basis for I with respect to a φ–admissible ordering then $\varphi(G)$ is a Gröbner basis for $\varphi(I)$.*

1.3 Kalkbrener's approach.

M. Kalkbrener (see [9]) proposes a slightly different approach, as he considers that the specialization map has the following domain and image:

$$\varphi : R \to \mathbb{K}$$

where R is a Noetherian commutative ring ($\mathbb{K}[\underline{T}]$ in our case) and $\mathbb{K}$ is a field, and a Gröbner basis G of I in $R[\underline{X}]$ with respect to any ordering in the monomials of $R[\underline{X}]$ (note that in this case Kalkbrener's approach requires the computation of a Gröbner Basis in $\mathbb{K}[\underline{T}][\underline{X}]$). The question to answer is: when is $\varphi(G)$ a Gröbner basis of $\varphi(I)$?, and the answer is similar to Gianni's one: in [9] it is shown that this is is equivalent to the following:

> *assume that the g_i's are ordered in such a way that there exists one $r \in \{0, \ldots, s\}$ with $\varphi(lt(g_i)) \neq 0$ for $i \in \{1, \ldots, r\}$, and $\varphi(lt(g_i)) = 0$ for $i \in \{r+1, \ldots, s\}$. Then, for every $i \in \{r+1, \ldots, s\}$ the polynomial $\varphi(g_i)$ is reducible to 0 modulo $\{\varphi(g_1), \ldots, \varphi(g_r)\}$.*

But remark that in order to test this condition, we need to compute a Gröbner basis of $\{\varphi(g_1), \ldots, \varphi(g_r)\}$, but this can be, in the worst case, similar to compute a Gröbner basis of $\varphi(G)$, unless in the case in which $r = s$, where we can directly conclude that $\varphi(G)$ is a Gröbner basis.

Although this approach seems to contain in particular Gianni's one, remark that G is a Gröbner basis in $R[\underline{X}]$ with $R = \mathbb{K}[\underline{T}]$, which implies that it requires the computation of a Gröbner Basis over an integral domain ($\mathbb{K}[\underline{T}]$) and not over a field which is the usual case: in [1] or in [2] it is described how to compute such Gröbner Bases.

1.4 GPT Strategy.

The strategy, here denoted GPT, was introduced in [6] in order to avoid the growth of the coefficients when using Buchberger algorithm to compute a Gröbner Basis of a multivariate polynomial ideal. The main idea is to keep track, into the different steps of Buchberger algorithm, of a list of potential factors (presented in factored form) such that in many cases simplification is posible by dividing by the "greatest between the common divisors that are easy to compute" and in this way to avoid gcd computations.

In our case, it seems that to apply this strategy is even more natural than to apply it to avoid the growing of the integers as it was the initial motivation in [6]. In fact the list of potential factors, in our case and working in $\mathbb{K}(\underline{T})[\underline{X}]$, is going to give us a set of open conditions on the parameters such that if they are verified it is clear that the specialization of the generic Gröbner Basis is going to give us a Gröbner Basis of the specialized ideal.

The example in [6] is very clear about how to proceed: if the initial system is

$$g_0 = ax^3 + byz + c, \quad g_1 = dxy + ez^2, \quad g_2 = fxz + gy$$

then the list of open conditions is given by

$$\{a, d, f, g, c, b^2e^2, b^2e\}$$

and when all these polynomials in the parameters are different from 0, the specialization of the generic Gröbner Basis is a Gröbner Basis of the specialized ideal.

In fact this is no more that a lazy application of the "Dynamic Evaluation Method" of D. Duval (see [4]) but following only one **open** branch. The decision to make at this point is how much do we want to have simplified the list of open conditions.

The case of only one parameter is especially suited to apply the so called GPT strategy since all the computations with the parameters reduce to compute gcd's of univariate polynomials which is not very expensive.

1.5 Conclusion.

As a final conclusion of this section, all the results ([7, 3, 9]) give just sufficient conditions for the specialization of a Gröbner basis to be a Gröbner basis:

- The approach in [3] searches a set of "good specializations" verifying this condition. Although from a practical point of view this is the most interesting question, it *"can lead to lengthy calculations which may be too much for some computer algebra systems", [3].*

- In [7] and [9] we find a test to decide if a given specialization is good or not. The computations needed to realize these tests are efficient only in particular cases or when the specialization is such that no leading terms of the polynomials in the Gröbner basis vanishes. (In the other cases one more Gröbner basis computation is needed, which can be, in the worst case, the Gröbner basis of the specialization). Remark that the approach in [9] requires the computation of a Gröbner Basis over an integral domain which is usually harder that when the computations are done with polynomials with coefficients in a field.

2 Using Hilbert Function.

Let J be an ideal in $\mathbb{K}[X_0, \ldots, X_n] = \mathbb{K}[\underline{X}]$. J is said homogeneous if the relation $F \in J$ implies that all the homogeneous components of F are in J. Let $\mathbb{K}[\underline{X}]_s$ denote the set of homogeneous polynomials of total degree s (including the zero polynomial) which is a $\mathbb{K}$–vector space of dimension $\theta(n,s) = \binom{n+s}{s}$. If J is a homogeneous ideal, we let

$$J_s = J \cap \mathbb{K}[\underline{X}]_s.$$

Then the *Hilbert function of J* is defined by

$$H_J(s) = \dim_{\mathbb{K}} \mathbb{K}[\underline{X}]_s / J_s.$$

It is also possible to define the Hilbert Function for inhomogeneous ideals: it is enough to replace $\mathbb{K}[X_0, \ldots, X_n]_s$ by $\mathbb{K}[X_1, \ldots, X_n]_{\leq s}$, the set of polynomials in $\mathbb{K}[X_1, \ldots, X_n]$ of total degree at most s (including the zero polynomial).

Following the ideas in [12] it is posible to use the Hilbert function, to check if the specialisation of a Gröbner Basis of a homogeneous (with respect to $\underline{X} = (X_0, \ldots, X_n)$) ideal J in $\mathbb{K}[\underline{T}, \underline{X}]$ with respect to a block ordering is a Gröbner Basis of the specialised homogeneous ideal. The main tool is the following theorem appearing in [12] and its corollary to the situation we are dealing with.

Theorem 3 *([12]) Let J be an ideal in $\mathbb{K}[\underline{X}]$ and σ a degree–compatible term ordering. Let $G = \{g_1, \ldots, g_k\}$ be a set of elements of J. If*

$$H_{Lt_\sigma(J)} = H_{Lt_\sigma(G)}$$

then G is a Gröbner basis of J with respect to σ.

Corollary 1 *Let J be a homogeneous ideal in $\mathbb{K}[\underline{T}, \underline{X}]$, G its Gröbner basis with respect to a block $\underline{X}$–degree–compatible ordering σ in $\mathbb{K}[\underline{T}, \underline{X}]$ and ϕ the* *specialization map giving values to the parameters in* $\underline{T}$. *Let* $\overline{\sigma}$ *be the restriction of* σ *to* $\mathbb{K}[\underline{X}]$, $H_{Lt_{\overline{\sigma}}(G)}$ *the Hilbert function of the ideal generated by the* $\underline{X}$-*leading power products of* G *and* $H_{Lt_{\overline{\sigma}}(\phi(G))}$ *the Hilbert function of the ideal generated by the leading power products of* $\phi(G)$. *If*

$$H_{Lt_{\overline{\sigma}}(G)} = H_{Lt_{\overline{\sigma}}(\phi(G))}$$

then $\phi(G)$ *is a Gröbner basis of* $\phi(J)$ *with respect to* $\overline{\sigma}$.

Proof: Any specialization ψ producing $Lt_{\overline{\sigma}}(G)$ as set of leading terms for $\psi(J)$ verifies that $\psi(G)$ is a Gröbner Basis of $\psi(J)$ and thus $H_{\text{generic}} := H_{\psi(J)}$ is equal to $H_{Lt_{\overline{\sigma}}(G)}$. But if our specialization ϕ verifies that $H_{Lt_{\overline{\sigma}}(\phi(G))}$ is equal to the "generic" Hilbert function H_{generic} then, by applying Theorem 3, $\phi(G)$ is a Gröbner Basis of $\phi(J)$. ∎

The key point here is to compute a "generic" Gröbner Basis of the ideal J regarded in $\mathbb{K}[\underline{T}, \underline{X}]$ with respect to a degree–compatible monomial ordering and to use this Gröbner Basis to derive the "generic" Hilbert function of J considered as ideal in $\mathbb{K}[\underline{X}]$. For a given specialization of the parameters, the specialization of the "generic" Gröbner Basis is a Gröbner Basis if the "generic" Hilbert function agrees with the Hilbert function of the monomial ideal generated by the leading power products of the specialized Gröbner Basis. To remark finally that the Hilbert function of a monomial ideal is very easy to compute and thus it seems to be an immediate tool to use in order to check the correctness of the specialization process.

2.1 Computing a set of good specialization parameter conditions.

Let J be a homogeneous ideal in $\mathbb{K}[\underline{T}, \underline{X}]$, $G = \{g_1, \ldots, g_s\}$ its Gröbner basis with respect to a block $\underline{X}$–degree–compatible ordering σ in $\mathbb{K}[\underline{T}, \underline{X}]$. Every polynomial g_j has the structure

$$g_j(\underline{T}, \underline{X}) = \sum_{i=1}^{m_j} u_{i,j}(\underline{T})\mathbf{X}^{\alpha_{i,j}}, \qquad \alpha_{1,j} >_{\overline{\sigma}} \alpha_{2,j} >_{\overline{\sigma}} \ldots$$

with $\overline{\sigma}$ the restriction of σ to $\mathbb{K}[\underline{X}]$.

For a list of s nonnegative integers $L = [n_1, \ldots, n_s]$ with $0 \leq n_j \leq m_j$, the specialization condition defined by L is given by

$$u_{j,1}(\underline{T}) = 0, \ldots, u_{j,n_j-1}(\underline{T}) = 0, u_{j,n_j}(\underline{T}) \neq 0, \qquad 1 \leq j \leq s$$

By using corollary 1, it is clear that, for any specialization verifying the conditions indicated by L, if the Hilbert Function of the monomial ideal generated by $\{\mathbf{X}^{\alpha_{j,n_i}} : 1 \leq j \leq s\}$ agrees with the Hilbert Function of the monomial ideal generated by $\{\mathbf{X}^{\alpha_{j,1}} : 1 \leq j \leq s\}$ then the specialization of G is a Gröbner Basis of the specialization of J (with respect to $\overline{\sigma}$).

This consequence of corollary 1 provides a nice way of computing a set of conditions which are good for specializing the Gröbner Basis of J already computed in $\mathbb{K}[\underline{T},\underline{X}]$: i.e. those whose Hilbert function computed with the leading terms already present agrees with the "generic" Hilbert function. In order to avoid the consideration of all the possible cases $((m_1+1)\cdot\ldots\cdot(m_s+1))$ the following lemma and its remarks show how to know in advance that such a condition list is bad once one such list has been previously classified as bad.

Lemma 1 *Let $\geq$ be the ordering introduced in the set of conditions lists for G defined by*

$$[n_1,\ldots,n_s] \geq [k_1,\ldots,k_s] \quad \Longleftrightarrow \quad n_1 \geq k_1,\ldots,n_s \geq k_s.$$

If L is a condition list for G bad for specialization then every condition list L' for G with $L < L'$ is also bad for specialization

Proof: It is enough to take into account that if $L < L'$ then the dimension (as a vector space) of the monomial ideal generated by the condition L is smaller than or equal to the dimension of the one generated by L' and thus the corresponding Hilbert functions verify that $H'_L \leq H_L$. Since, by hypothesis, $H_L < H_{\text{generic}}$ then L' is bad for specialization: its Hilbert function is different from the generic one. ∎

First, it is clear that the list $\mathbf{0} = [0,\ldots,0]$ provides a good specialization condition. Next, it is analyzed the case of the vanishing of some $\underline{T}$–coefficients into only one g_j polynomial: for every $j \in \{1,\ldots,s\}$ the biggest (for $\geq$) conditions lists for G with only one non zero element which are good for specialization. Once these lists have been determined, we know, by the previous lemma that we do not need to consider any conditions list for G strictly bigger than one of such lists. Proceeding in a similar way with the case of only two, three, etc non–zero elements and with conditions lists not strictly bigger than those already located in the previous step, we exhaust all the possibilities.

Graphically this means that, for this Gröbner Basis,

$$\begin{array}{cccccc}
g_1(\underline{T},\underline{X}) \rightarrow & u_{11}(\underline{T}) & u_{12}(\underline{T}) & u_{13}(\underline{T}) & \ldots & u_{1m_1}(\underline{T}) \\
g_2(\underline{T},\underline{X}) \rightarrow & u_{21}(\underline{T}) & u_{22}(\underline{T}) & u_{23}(\underline{T}) & \ldots & u_{2m_2}(\underline{T}) \\
g_3(\underline{T},\underline{X}) \rightarrow & u_{31}(\underline{T}) & u_{32}(\underline{T}) & u_{33}(\underline{T}) & \ldots & u_{3m_3}(\underline{T}) \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
g_s(\underline{T},\underline{X}) \rightarrow & u_{s1}(\underline{T}) & u_{s2}(\underline{T}) & u_{s3}(\underline{T}) & \ldots & u_{sm_s}(\underline{T})
\end{array}$$

if we consider the set $\mathcal{A}$ of all lists $[n_1,\ldots,n_s]$ with $0 \leq n_j \leq m_j$ (the different specialization conditions), we are looking for the maximal elements of the subset:

$$\mathcal{S} = \{[n_1,\ldots,n_s] \in \mathcal{A} : [n_1,\ldots,n_s] \text{ good for specialization}\}$$

with respect to the order relation $\geq$ in $\mathcal{A}$ defined in Lemma 1. If $L_1,\ldots,L_k$ are these maximal elements of $\mathcal{S}$ we have obtained that if, for some i, $L = [n_1,\ldots,n_s] \leq L_i$ then the verification of the conditions

$$u_{j,1}(\underline{T}) = 0,\ldots,u_{j,n_j-1}(\underline{T}) = 0, u_{j,n_j}(\underline{T}) \neq 0, \qquad 1 \leq j \leq s \tag{2}$$

implies that the specialization of the considered Gröbner Basis G gives a Gröbner Basis of the specialized ideal.

In conclusion, every maximal element $L_i = [k_1, \dots, k_s]$ of $\mathcal{S}$ provides a set of $(k_1+1)\cdot \ldots \cdot (k_s+1)$ conditions with each one having the structure showed in 2. This procedure, as it has been explained taking only into account the set $\mathcal{A}$, can be easily optimized if we take also into account the structure of the polynomials $g_j(\underline{T}, \underline{X})$'s: for example, if it is known that the coefficient $u_{ji}(\underline{T})$ is a non zero constant then we can discard directly from the set $\mathcal{A}$ those lists whose j–th element is bigger than i.

2.2 Simplification of the set of conditions.

As described in the previous section, we have obtained a set of good specialization conditions. Each condition different from the first one, ie that corresponding to the list $[0, \dots, 0]$, is presented in the following way:

$$p_1(\underline{T}) = 0, \dots, p_k(\underline{T}) = 0, q_1(\underline{T}) \neq 0, \dots, q_m(\underline{T}) \neq 0 \tag{3}$$

where $k \geq 1$, $m \geq 1$ and the p_i's and the q_i's are polynomials in $\mathbb{Z}[\underline{T}]$ non constant. In what follows it is showed how the description of every condition can be simplified.

In the case of one parameter, $\underline{T} = t$, if

$$p(t) = \gcd(p_1(t), \dots, p_k(t))$$

the considered condition (3), with $\underline{T} = t$, is equivalent to

$$p(t) = 0, q_1(t) \neq 0, \dots, q_m(t) \neq 0 \tag{4}$$

If $p(t) = 1$, ie the p_i's are coprime, then this condition is directly discarded since it would be never verified. If $\deg(p(t)) \geq 1$ then by defining iteratively

$$Q_0(t) = p(t), \qquad Q_{i+1}(t) = \frac{Q_i(t)}{\gcd(Q_i(t), q_i(t))}, \quad \text{if } i \geq 0$$

it is easy to verify that the condition (4) is equivalent to

$$Q_{m+1}(t) = 0 \tag{5}$$

In the case of several parameters, it is clear that the same approach can not be further followed but several heuristics can be adopted in order to simplify the output:

- To check for emptyness with respect to the equalities: if the Grobner Basis of $p_1(\underline{T}), \dots, p_k(\underline{T})$ with respect to any monomial ordering is equal to 1 then the corresponding condition is discarded.
- To apply a "lazy factorization" approach as in the GPT strategy (see [6] or subsection 1.4).

3 What to do with a "parametric" Gröbner Basis?

It is worth to remark that in many cases, when the methods considered here are applied, then other algorithms are to be applied too: for example once it is known a set of specializations (through a set of conditions into the parameters) such that the specialised Gröbner Basis for any of these values of the parameters is indeed a Gröbner Basis then one could ask, if for these specializations, if the considered ideal is zero dimensional ideal. Note moreover that in this case, since the leading monomials do not change after the considered specializations, we have also a basis of the quotient (involving only $\underline{X}$)–monomials) which can be very useful to get several informations about the properties of the set of $\underline{X}$–zeros of the considered ideal when the parameters live inside the set determined by the set of considered conditions.

If we consider the polynomials:

$$\begin{array}{l} F_1 = axt^2 + byzt - x(x^2 + cy^2 + dz^2) \\ F_2 = ayt^2 + bzxt - x(y^2 + cz^2 + dx^2)\,, \\ F_3 = azt^2 + bxyt - x(z^2 + cx^2 + dy^2) \end{array}$$

with x, y, z the unknowns and a, b, c, d the parameters, first we compute the Gröbner Basis of the ideal generated by F_1, F_2 and F_3 in $\mathbb{Q}[a, b, c, d, x, y, z, t]$ with respect the grevlex (graded reverse lexicographical) ordering. It has 23 polynomials whose leading terms and monomials are:

- leading terms:

  $[c, d, 1, d^2 - c, c^2 - d, cd - 1, c^4d + cd^4 - 2c^2d^2 - c^3 - d^3 + 2cd, c^3 + d^3 - 3cd + 1, d^2, cd - 1, c^2 - d, cd - 1, 1, 4cd - d^3 - 1 + c^4d + cd^4 - 3c^2d^2 - c^3, 4cd - d^3 - 1 + c^4d + cd^4 - 3c^2d^2 - c^3, c^3 - 2cd + 1, d^3 - 2cd + 1, 1, 4cd - d^3 - 1 + c^4d + cd^4 - 3c^2d^2 - c^3, cd^3 - c^2d - d^2 + c, c^2d^2 - 2cd + 1, c^3d - c^2 - cd^2 + d, 1]$

- leading monomials:

  $[x^2z, x^2y, x^3, zy^3, xy^2z, xy^3, y^2z^3, xyz^3, x^2z^3, y^4z, y^4z, y^5, x^2y^3, yz^5, xz^5, y^3z^3, xy^2z^3, x^2yz^3, z^7, y^2z^5, y^2z^5, y^2z^5, x^2z^5]$

The "generic" Hilbert function is in this case

$$\frac{n^6 + 3\,n^5 + 6\,n^4 + 7\,n^3 + 6\,n^2 + 3\,n + 1}{1 - n}$$

and since, for example, the condition $[c = 0, d = 1]$ (with any value for a and b) conveys to the same Hilbert Function, it is concluded that such condition is good for specialization. Nevertheless the condition $[c = 0, d = 0]$ (with any value for a and b) conveys to the Hilbert Function

$$\frac{2\,n^8 + 5\,n^7 + 5\,n^6 + n^5 - 5\,n^4 - 7\,n^3 - 6\,n^2 - 3\,n - 1}{1 - n}$$

and thus is not good for specialization.

For the first case, we have computed a Grobner Basis that specializes correctly for any value of the parameters verifying $[c = 0, d = 1]$. This allows to get information about the solution set of the considered system by performing, for example, parametric computations into the quotient ring $\mathbb{Q}[x, y, z, t]/ < F_1, F_2, F_3 >$ (no need of taking care about the values of a and b).

4 Implementation and Experimentation.

We used the `PoSSoLib` library to write the code used for tests; it is a C++ library developed (and still developing) within the ESPRIT projects PoSSo and FRISCO. It permits a complete customization of many algebraic structures (rings, polynomials, monoids, orderings, etc.) and provides many functions to deal with all the main operations within these structures in a very flexible way, and not available in such a way in other symbolic computation packages. Gröbner bases and Hilbert function computations are also available, together with many other low– and high–level features.

The code consisted in some new specific functions and a C++ program organizing all the computations: the specification of the polynomial ring $\mathbb{K}[\underline{T}, \underline{X}]$ and the polynomials under consideration are read from an input file. There are two operative modes, and the user must choose:

1. Check a particular specialization; a list of values for the parameters is read from the input file, and the computation is done just for that single case (see the example).

2. Compute conditions: the general analysis (section 2) is performed.

In the first case the direct computation and Hilbert function testing is performed, in the second one the rings $\mathbb{K}[\underline{T}]$, $\mathbb{K}[\underline{X}]$ are constructed, the polynomials converted and the monomials $\mathbf{X}^\alpha$ taken, for the computation of the Hilbert functions to be compared, while the "coefficients" $u_{i,j}(\underline{T})$ play their role in cutting the condition tree (when they are constant) and in the final simplification of obtained conditions. The code is currently being expanded to obtain a clean and clear output, and to make the whole analysis completely automatic.

Next it is shown how the performed implementation works over the homogeneous polynomial system of equations coming from the modelling of a neural network. In this case there is only one parameter c and four unknowns u, v, w, t:

$$\begin{aligned} t^3 - cut^2 - uv^2 - uw^2 = 0 \\ t^3 - cvt^2 - vu^2 - vw^2 = 0 \\ t^3 - cwt^2 - wu^2 - wv^2 = 0 \end{aligned}$$

The input file, which is included below, contains first the definition of the polynomial ring (with the corresponding ordering) where the computations are to be performed and then the list of polynomials. The final line, which is optional, contains the values of the parameters under consideration (to be used if we are only interested about these concrete values).

```
{5,
 {N, {c,  u,v,w,t}},
 {C, {0,  1,1,1,1}},
 {V, {0,  1,1,1,1}},
 {C, {1,  0,0,0,1}}
}
{
 {1t3, -1cut2, -1uv2, -1uw2}
 ,
 {1t3, -1cvt2, -1vu2, -1vw2}
 ,
 {1t3, -1cwt2, -1wu2, -1wv2}
}
{-1}
```

In this example the current implementation returns that, for any c such that $c \neq 0$, the "generic" Gröbner Basis specializes well.

Next example is more complicated (see [10]) and it was already used in section 3. It contains four parameters (a, b, c and d) and four unknowns (x, y, z and t):

$$\begin{aligned} F_1 &= axt^2 + byzt - x(x^2 + cy^2 + dz^2) \\ F_2 &= ayt^2 + bzxt - x(y^2 + cz^2 + dx^2) \\ F_3 &= azt^2 + bxyt - x(z^2 + cx^2 + dy^2) \end{aligned}$$

and in this case the Gröbner Basis (computed in $\mathbb{Q}[a, b, c, d, x, y, z, t]$) contains 23 polynomials and the computation, which is to be shown below, provided in less than 1 second (including the Gröbner Basis computation) the following good conditions for specialization (which are later further simplified):

- $c \neq 0, d \neq 0, d^2 - c \neq 0, c^2 - d \neq 0, cd - 1 \neq 0, c^4d + cd^4 - 2c^2d^2 - c^3 - d^3 + 2cd \neq 0, c^3 + d^3 - 3cd + 1 \neq 0, d^3 - 2cd + 1 \neq 0, cd^3 - c^2d - d^2 + c \neq 0, c^2d^2 - 2cd + 1 \neq 0, c^3d - cd^2 - c^2 + d \neq 0.$

- $c^4d + cd^4 - 2c^2d^2 - c^3 - d^3 + 2cd = 0, c \neq 0, d \neq 0, d^2 - c \neq 0, c^2 - d \neq 0, cd - 1 \neq 0, cd^3 - c^2d - d^2 + c \neq 0, c^3 + d^3 - 3cd + 1 \neq 0, c^2d^2 - 2cd + 1 \neq 0, d^3 - 2cd + 1 \neq 0, c^3d - cd^2 - c^2 + d \neq 0.$

- $c = 0, d \neq 0, d^2 \neq 0, d^3 \neq 0.$

A simplification through factorization provides the following final result:

- $c \neq 0, d \neq 0, d^2 - c \neq 0, c^2 - d \neq 0, cd - 1 \neq 0, c^3 - 2cd + d^3 \neq 0, c + d + 1 \neq 0, d^2 + 1 - d + c^2 - c - cd \neq 0, d^3 - 2cd + 1 \neq 0.$

- $c^3 - 2cd + d^3 = 0, c \neq 0, d \neq 0, d^2 - c \neq 0, c^2 - d \neq 0, cd - 1 \neq 0, c + d + 1 \neq 0, d^2 + 1 - d + c^2 - c - cd \neq 0, d^3 - 2cd + 1 \neq 0.$

- $c = 0, d \neq 0.$

Next it is shown how the computations are performed: first the file containing the polynomials (and the corresponding ring) is read and a Grobner Bases computation is performed.

```
frisco% ./paramCond test.in
Homogenous system.
File : test.in
Initial basis:
{
-(x^3 + c*x*y^2 + d*x*z^2 - b*y*z*t - a*x*t^2),
 -(d*x^2*y + y^3 + c*y*z^2 - b*x*z*t - a*y*t^2),
 -(c*x^2*z + d*y^2*z + z^3 - b*x*y*t - a*z*t^2)
}

GroebnerBasis is :
{
 c*x^2*z + d*y^2*z + z^3 - b*x*y*t - a*z*t^2,
 d*x^2*y + y^3 + c*y*z^2 - b*x*z*t - a*y*t^2,
 ........................................
 ........................................,

 x^2*z^5 - c^2*d*y^2*z^5 + d^2*y^2*z^5 + c*y^2*z^5
 - c*d^2*z^7 + 2*d*z^7 - b*d^2*x*y*z^4*t
 + b*c*x*y*z^4*t - b*d*x*y*z^4*t + a*d*x^2*z^3*t^2
 - 2*a*x^2*z^3*t^2 + a*c^2*d*y^2*z^3*t^2
 + a*c*d*y^2*z^3*t^2 - a*d^2*y^2*z^3*t^2
 - b^2*y^2*z^3*t^2 - 2*a*c*y^2*z^3*t^2
 + a*c*d^2*z^5*t^2 + b^2*d*z^5*t^2 + a*c*d*z^5*t^2
 + a*d^2*z^5*t^2 - 4*a*d*z^5*t^2 - a*z^5*t^2
 + a*b*d^2*x*y*z^2*t^3 - a*b*c*x*y*z^2*t^3
 + a*b*d*x*y*z^2*t^3 - a^2*d*x^2*z*t^4
 + a^2*x^2*z*t^4 - a^2*c*d*y^2*z*t^4
 + a*b^2*y^2*z*t^4 + a^2*c*y^2*z*t^4
 - a*b^2*d*z^3*t^4 - a^2*c*d*z^3*t^4
 - a^2*d^2*z^3*t^4 + a^2*d*z^3*t^4 + 2*a^2*z^3*t^4
 + a^3*d*z*t^6 - a^3*z*t^6
}
```

Next, the user is asked if he wants to compute the good conditions for specialization (our case) or to check a particular set of values. Then, for every polynomial in the Grobner Basis already computed, it is performed the separation between the $\underline{X}$–monomials and their coefficients.

```
What do you want to use ?
1) isGoodSpecialization          2) conditions
Make your choice :  2
Phase 2: testing conditions.     list length = 23
```

```
lengths = [5 5 5 5 5 5 7 9 9 9 11 8 9
           9 11 9 10 10 11 13 11 10 12]
varList = {
 { x^2*z, y^2*z, z^3, x*y*t, z*t^2},
 { x^2*y, y^3, y*z^2, x*z*t, y*t^2},
 .....................................
 .....................................,
 { x^2*z^5, y^2*z^5, z^7, x*y*z^4*t, x^2*z^3*t^2,
   y^2*z^3*t^2, z^5*t^2, x*y*z^2*t^3, x^2*z*t^4,
   y^2*z*t^4, z^3*t^4, z*t^6}
}

parList = {
 { c, d, 1,  - b,  - a},
 { d, 1, c,  - b,  - a},
 .....................................,
 { 1,  - c^2*d + d^2 + c,  - c*d^2 + 2*d,
   - b*d^2 + b*c - b*d, a*d - 2*a,
   a*c^2*d + a*c*d - a*d^2 - b^2 - 2*a*c,
   a*c*d^2 + b^2*d + a*c*d + a*d^2 - 4*a*d - a,
   a*b*d^2 - a*b*c + a*b*d,  - a^2*d + a^2,
   - a^2*c*d + a*b^2 + a^2*c,
   - a*b^2*d - a^2*c*d - a^2*d^2 + a^2*d + 2*a^2,
   a^3*d - a^3}
}
```

Now the algorithm presented in section 2 is applied: the different Hilbert Functions arising after specializations are compared with the generic Hilbert Function. The final result is the set of maximal elements of the set $\mathcal{S}$ introduced in the subsection 2.1. After lemma 1, all the lists (called below *list of exploded indexes*) smaller than those which are maximal give the set of good specialization conditions.

```
originalHFunction = {1,0,0,-3,0,0,3,0,0,-1}
Result : list of indexes.

[0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 2, 2, 2, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 1, 2, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 2, 0, 2, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Result : list of ‘‘exploded’’ indexes.

[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
```

```
[0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 2, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
.....................................................................
[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
```

Finally, after a initial simplification, three conditions are obtained. Every condition has two parts: the first correspond to "$= 0$" conditions and the second to "$\neq 0$" conditions.

```
Result : list of ‘‘simplified’’ conditions.
( { 0 }
  { c, d, d^2 - c, c^2 - d, c*d - 1, c^4*d + c*d^4
    - 2*c^2*d^2 - c^3 - d^3 +  2*c*d, c^3 + d^3
    - 3*c*d + 1, d^3 - 2*c*d + 1, c*d^3 - c^2*d
    - d^2 + c, c^2*d^2 - 2*c*d + 1, c^3*d - c*d^2
    - c^2 + d },

  { c^4*d + c*d^4 - 2*c^2*d^2 - c^3 - d^3 + 2*c*d}
  { c, d, d^2 - c, c^2 - d, c*d - 1, c*d^3 - c^2*d
    - d^2 + c, c^3 + d^3 - 3*c*d + 1,
    c^2*d^2 - 2*c*d + 1, d^3 - 2*c*d + 1, c^3*d
    - c*d^2 - c^2 + d },

  { c }
  { d, d^2, d^3 }
)
```

A more complicated example is the one defined by the following homogeneous polynomial system of equations (where m is the only parameter):

$$\begin{aligned}
F_1 &= 2mt^3 - 7xt^2 + mx^2y + mzt^2 \\
F_2 &= 3mxt^2 + u^2t - 2mytu \\
F_3 &= 2mt^3 - 2t^3 + z^2u + xyt - mz^2t \\
F_4 &= 2t^3 + z^2u + m^2xyt - mzyt
\end{aligned}$$

In this case a "generic" Grobner Basis with 50 elements is obtained and the good conditions for specialization are:

$$[m \neq 0, m^2 - 1 \neq 0, 2m^2 - 7 \neq 0, 5m^2 + 4m - 7 \neq 0]$$

Note that this condition is obtained after a big number of Hilbert Series computations according to the algorithm presented in section 2.

5 Conclusions.

It has been shown how to deal with polynomial system solving involving parameters, in the homogeneous case, by using as main tool the properties of Gröbner

Bases under specialization. In conclusion, the most promising techniques are those based upon the using of the Hilbert function plus a simplification of the result "á la GPT" and a future complete automatization of the algorithm already implemented will provide, in a very efficient way, a set of "good specialization conditions" together with a Gröbner Basis of the considered homogeneous polynomial system for every one of those conditions.

References

[1] W. W. Adams, P. Loustaunau. *An Introduction to Grobner Bases.* Graduate Studies in Mathematics, Volume 3, AMS, 1994.

[2] T. Becker, V. Weispfenning *Grb̈ner Bases: A Computational Approach to Commutative Algebra.* Graduate Studies in Mathematics, Volume 141, Springer Verlag, 1993 (second edition, 1998).

[3] D. Cox, J. Little, D. O'Shea. *Ideals, Varieties, and Algorithms.* Springer–Verlag, 1991 (second corrected edition, 1998).

[4] D. Duval. *Evaluation dynamique et clôture algébrique.* Journal of Pure and Applied Algebra 99, 267–295, 1995.

[5] FRISCO. *A Framework for Integrated Symbolic/Numeric Computation.* ESPRIT Project LTR 21024, 1996–1999, European Union.

[6] A. Galligo, L. Poittier, C. Traverso. *Greatest Easy Common Divisor and standard basis completion algorithms.* ISSAC'98. Lecture Notes in Computer Science 358, 162–176, 1988.

[7] P. Gianni. *Properties of Gröbner basis under specializations.* European Conference on Computer Algebra, Leipzig, GDR, 1987 (J. H. Davenport, ed.). Lecture Notes in Computer Science 378, 293–297, 1987.

[8] M. Moreno–Maza. *Calculs de Pgcd au–dessus des Tours d'Extensions Simples et Résolution des Systèmes d'Équations Algébriques.* Doctoral Thesis, Université Paris 6, 1997.

[9] M. Kalkbrener. *On the stability of Gröbner basis under specializations.* Journal of Symbolic Computation 24 (1), 51–58, 1997.

[10] K. Rimey. *A system of polynomial equations and a solution by an unusual method.* ACM SIGSAM Bulletin, 1, 18, 1984.

[11] W. Y. Sit. *An algorithm for solving parametric linear systems.* Journal of Symbolic Computation 13, 353–394, 1992.

[12] C. Traverso. *Hilbert Functions and the Buchberger Algorithm.* Journal of Symbolic Computation 22 (4), 355–376, 1996.

[13] B. L. van der Waerden. *Modern Algebra II.* Third edition. F. Ungar Publishing Co., NY, 1950.

[14] V. Weispfenning. *Comprehensive Gröbner Bases.* Journal of Symbolic Computation, 14 (1), 1–30, 1992.