Bull. Math. Soc. Sci. Math. Roumanie
Tome 61 (109) No. 2, 2018, 135–146

Tangent space to the orbit of an algebraic group action

by
Deeba Afzal[(1)], Shamsa Kanwal[(2)], Gerhard Pfister[(3)]

Abstract

We give an algorithm to compute a standard basis of the tangent space to the orbit of an algebraic group action. Using this standard basis we can compute the codimension of the tangent space, an important invariant in the classification of map germs. The task is not completely trivial since the tangent space is usually described as the sum of two infinite dimensional vector spaces given by two modules over different rings. We also explain how the standard basis can be computed using modular methods.

Key Words: standard basis, tangent space at orbit, right-left equivalence, map germs.
2010 Mathematics Subject Classification: Primary 14B05. Secondary 14H20, 14J17.

1 Introduction

Let K be a field, $\mathrm{x} := (x_1, \ldots, x_n)$, let $>$ be a local ordering[1] on $K[[\mathrm{x}]]$ and denote by $>$ the extension of this ordering to the following ordering on

$$K[[\mathrm{x}]]^p = \sum_{i=1}^{p} K[[\mathrm{x}]]e_i, \quad e_i = \big(0, \ldots, 1, \ldots, 0\big) :$$

$$\mathrm{x}^\alpha e_i > \mathrm{x}^\beta e_j \quad if \quad i < j \quad or(\quad i = j \quad and \quad \mathrm{x}^\alpha > \mathrm{x}^\beta).$$

Let $A(n,p) =< \mathrm{x} > K[[\mathrm{x}]]^p$, let $\mathcal{R} := Aut_K(K[[\mathrm{x}]])$, $\mathcal{L} := Aut_K(K[[\mathrm{y}]])$, $\mathrm{y} = (y_1, \ldots, y_p)$ and $\mathcal{M} := Gl(p, K[[\mathrm{y}]])$. Define the groups $\mathcal{A} := \mathcal{R} \times \mathcal{L}$ and $\mathcal{K} := \mathcal{R} \times \mathcal{M}$. If $K = \mathbb{C}$ the field of complex numbers then $A(n,p)$ can be considered as the set of map germs $(\mathbb{C}^n, 0) \longrightarrow (\mathbb{C}^p, 0)$, $\mathcal{R}$ resp. $\mathcal{L}$ is the group of automorphism of $(\mathbb{C}^n, 0)$ resp. $(\mathbb{C}^p, 0)$.

In the classification of map germs the groups $\mathcal{A}$ and $\mathcal{K}$ resp. the tangent spaces to the orbits under the action of these groups and their codimension play an important role (cf. [BG82],[GH93],[Gi83],[Ri87],[RR91] and [Wa83]).

The group $\mathcal{A}$(resp. $\mathcal{K}$) acts on $A(n,p)$ as follows:

$$\mathcal{A} \times A(n,p) \longrightarrow A(n,p), \quad ((\phi, \psi), f) \mapsto \psi \circ f \circ \phi^{-1}$$
$$\mathcal{K} \times A(n,p) \longrightarrow A(n,p), \quad ((\phi, M), f) \mapsto Mf \circ \phi^{-1}.$$

[1] For the definition and properties see [GP07].

If we write

$$\mathcal{R} = \{\phi = \begin{pmatrix}\phi_1\\ \vdots \\ \phi_n\end{pmatrix}, \phi_i \in < \mathrm{x} > K[[\mathrm{x}]], det(\frac{\partial \phi_j}{\partial x_l}(0)) \neq 0\}$$

$$\mathcal{L} = \{\psi = \begin{pmatrix}\psi_1\\ \vdots \\ \psi_p\end{pmatrix}, \psi_i \in < \mathrm{y} > K[[\mathrm{y}]], det(\frac{\partial \psi_j}{\partial y_i}(0)) \neq 0\}$$

and

$$\mathcal{M} = \{\psi = (\psi_{ij}), \psi_{ij} \in K[[\mathrm{y}]], \quad det(\psi_{ij}) \text{ a unit}\},$$

then the action of $\mathcal{A}$ can be written explicitly as

$$\psi \circ f \circ \phi^{-1} = \begin{pmatrix}\psi_1(f_1(\bar{\phi_1}, \ldots, \bar{\phi_n}), \ldots, f_p(\bar{\phi_1}, \ldots, \bar{\phi_n}))\\ \vdots \\ \psi_p(f_1(\bar{\phi_1}, \ldots, \phi_n), \ldots, f_n(\bar{\phi_1}, \ldots, \bar{\phi_n}))\end{pmatrix}, \phi^{-1} = \begin{pmatrix}\bar{\phi_1}\\ \vdots \\ \bar{\phi_n}\end{pmatrix}.$$

Similarly we obtain a formula for the $\mathcal{K}$-action:

$$Mf \circ \phi^{-1} = M\begin{pmatrix}f_1(\bar{\phi_1}, \ldots, \bar{\phi_n})\\ \vdots \\ f_n(\bar{\phi_1}, \ldots, \bar{\phi_n})\end{pmatrix}.$$

We assume now (only for the introduction) that K is a field of characteristic 0. Given $f \in A(n,p)$ we define the orbit map $\theta_f : \mathcal{A} \longrightarrow A(n,p)$ by $\theta_f(\phi, \psi) = \psi \circ f \circ \phi^{-1}$. Especially we have $\theta_f(id) = f$. The image of θ_f is the orbit of f under the action of $\mathcal{A}$, let $\mathcal{A}_f := Im(\theta_f)$.

The corresponding tangent map

$$T_{\mathcal{A}_f,id} : T_{\mathcal{A},id} \longrightarrow T_{A(n,p),f}$$

has an image the tangent space to the orbit at f, $T_{\mathcal{A}_f,f}$. This follows from the fact that we are in characteristic 0 and therefore the orbit map is separable (cf. [Bo98] and [Sp98]).

It is not difficult to see that

$$T_{\mathcal{A}_f,f} = < \mathrm{x} >_{K[[\mathrm{x}]]} < \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n} >_{K[[\mathrm{x}]]} + < f_1, \ldots, f_p >_{K[[f_1,\ldots,f_p]]} K[[f_1, \ldots, f_p]]^p.$$

Note, this is a sum of K-vector spaces.

Since $T_{\mathcal{A}_f,f}$ is not an $K[[\mathrm{x}]]-$ module we cannot use ordinary standard bases to compute the codimension

$$cod_{\mathcal{A}}(f) := dim_K A(n,p)/T_{\mathcal{A}_f,f}.$$

Similarly we obtain a formula for the tangent space to the orbit at f under the action of $\mathcal{K}$ replacing the automorphism ψ by a matrix $\psi = (\psi_{ij})$:

$$T_{\mathcal{K}_f,f} = < \mathrm{x} >_{K[[x]]} < \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n} >_{K[[\mathrm{x}]]} + < f_1, \ldots, f_p >_{K[[\mathrm{x}]]} K[[\mathrm{x}]]^p$$

Here the situation is different. $T_{\mathcal{K}_f,f}$ is an $K[[x]]$-module and we can compute the codimension

$$cod_{\mathcal{K}}(f) := dim_K A(n,p)/T_{\mathcal{K}_f,f}$$

computing a standard basis of $T_{\mathcal{K}_f,f}$. We define the extended tangent space with respect to the action of $\mathcal{A}$(resp. $\mathcal{K}$) by

$$T_{\mathcal{A}_f^e,f} :=< \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n} >_{K[[x]]} + K[[f_1, \ldots, f_p]]^p$$

resp.

$$T_{\mathcal{K}_f^e,f} :=< \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n} >_{K[[x]]} + < f_1, \ldots, f_p >_{K[[x]]} K[[x]]^p$$

Mather proved (cf. [Ma69]) that f is finitely $\mathcal{A}$-determined if and only if $cod_{\mathcal{A}}(f) < \infty$.

Definition 1. *$f \in A(n,p)$ is $\mathcal{A}$-finitely determined if there exists $k > 0$ such that for all $g \in A(n,p)$ with $jet(f,k) = jet(g,k)$ it follows that g is in the orbit of f under the action of $\mathcal{A}$.*

The following theorem of Du Plessis (cf. [Du80]) gives a sufficient condition for $f \in A(n,p)$ to be finitely determined:

Theorem 1. *Let $f \in A(n,p)$ and suppose that*

$$< x >^l K[[x]]^p \subseteq T_{\mathcal{K}^e,f} + < x >^{l+1} K[[x]]^p$$

$$< x >^k K[[x]]^p \subseteq T_{A^e,f} + < x >^{k+l} K[[x]]^p$$

Then f is $k+l$ determined and $< x >^k K[[x]]^p \subseteq T_{\mathcal{A}^e,f}$.

From now on we assume that f is k-determined. Let $\mathcal{A}^{(k)} = jet(\mathcal{A},k)$ and $A^{(k)}(n,p) = jet(A(n,p),k)$. Then $\mathcal{A}^{(k)}$ acts smoothly on $A^{(k)}(n,p)$.

We obtain

$$T_{A_f^{(k)},f} = T_{\mathcal{A}_f,f} / < x >^{k+1} K[[x]]^p$$

and

$$cod_{\mathcal{A}}(f) = dim_K A(n,p) / < x >^{k+1} K[[x]]^p - dim_K T_{\mathcal{A}_f^{(k)},f}.$$

We define the notion of a standard basis for a K-vector space contained in $K[[x]]^p$.

Definition 2. *Let $U \subseteq K[[x]]^p$ be a subspace of the K-vector space $K[[x]]^p$ and $>$ a local monomial ordering. A subset $W \subseteq U$ is called standard basis of U if $L(U) = L(W)$. Here $L(U)$ is the K-vector space generated by the leading monomials of U with respect to the ordering $>$.*

The aim of the paper is to give an algorithm to compute a standard basis of the vector space $T_{\mathcal{A}_f,f}$ resp. $T_{\mathcal{A}_f^{(k)},f}$. In Section 2 we will generalize this problem and give a solution. As in the case of Gröbner bases it is easy to see that $dim_K K[[x]]^p/U = dim_K K[[x]]^p/L(U)$. In Section 3 we will describe a modular version of the algorithms of Section 2 and give timings in Section 4.

2 Standard bases of special subspaces of $K[[\mathrm{x}]]^p$

Let $R = K[[\mathrm{x}]]$, $\mathrm{x} =< x_1, x_2, \ldots, x_n >$, let $M \subseteq R^p$ be an R-module such that $< \mathrm{x} >^k R^p \subseteq M$ for some k.[2] Let $N =< w_1, \ldots, w_s >_K \subseteq R^p$ be a finite dimensional K-vector space. The aim is to compute a standard basis for the K-vector space $M + N$ with respect to a given local monomial ordering $>$. We choose an extension of the ordering $>$ to R^p as defined in Section 1. By assumption $dim_K R^p/M < \infty$. Let $\{m_1, m_2, \ldots, m_l\}$ be the set of monomials of R^p not being in $L(M)$. Assume that $m_1 > \ldots > m_l$. Using a standard basis G of M (as R-module) we can compute the normal form of the generators w_i of N with respect to M, $NF(w_i|M) = NF(w_i|G) = \sum_{j=1}^{l} c_{ij} m_j$, $c_{ij} \in K$.

Let $(\bar{c}_{ij})$ be the matrix obtained from (c_{ij}) in reduced row echelon form, i.e. the $\bar{c}_{ij}$ have the following properties: $\exists \quad j_1, \ldots, j_a$ such that $\bar{c}_{ij_i} = 1$, $\bar{c}_{ij} = 0$ if $j < j_i$, $i = 1, \ldots, a$ and $\bar{c}_{ij} = 0$ if $i > a$.

Proposition 1. *$L(M+N)$ is the K-vector space generated by the monomials of $L(M)$ and $\{m_{j_1}, \ldots, m_{j_a}\}$.*

Proof. Let $f \in M + N$, $f = f_M + f_N$, $f_M \in M$, $f_N \in N$. If the leading monomial of f, $LM(f)$ is in $L(M)$ we are done. If $LM(f) \notin L(M)$ then
$NF(f|M) = NF(f_N|M) \in < m_1, \ldots, m_l >_K$ and $LM(f) = LM(NF(f|M))$.
Let $f_N = \sum_{i=1}^{t} c_i w_i + f_T$, $f_T \in < \mathrm{x} >^k R^p \subseteq M$, $c_i \in K$. This implies
$NF(f_N|M) = \sum_{i=1}^{t} c_i NF(w_i|M)$. All together we obtain
$NF(f|M) = \sum_{i=1}^{t} c_i NF(w_i|M)$. According to the definition of $j_1, j_2, \ldots, j_a$ we find b such that $LM(NF(f|M)) = m_{j_b}$. □

Corollary 1. *Let G be a standard basis of M as R-module and $H := \{\mathrm{x}^\alpha g | g \in G, \alpha \in \mathbb{Z}^n_{\geq 0}\}$ and $L := \{\sum_{j=1}^{\mathrm{l}} \bar{c_{ij}} m_j, i = 1, \ldots, a\}$. Then $H \cup L$ is a standard basis of $M+N$ as K-vector space.*

Corollary 2.

$$dim_K R^p/(M + N) = dim_K(R^p/M) - a$$

Definition 3. *With the notations of corollary 1 we will call the pair (G, L) a standard basis of $M + N$, if G is a standard basis of M (as R-module) and $\{\mathrm{x}^\alpha g | g \in G, \alpha \in \mathbb{Z}^n_{\geq 0}\} \cup L$ is a standard basis for $M + N$ (as K-vector space).*

We call the pair (G, L) a reduced standard basis, if G is a reduced standard basis of M, L is a set of monic polynomials, no monomial of a polynomial in L is in $L(M)$ and L is in reduced row echelon form.

Remark 1. *A reduced standard basis of $M + N$ exists and is uniquely determined. This is a consequence of the fact that M is zero-dimensional. The behavior with respect to local orderings in this situation the same as for global orderings.*

[2] This implies $dim_K R^p/M < \infty$.

We obtain the following algorithms to compute a standard basis and the codimension of a submodule in $K[[x]]^p$. [3]

Algorithm 1 vStd

Input: $M \subseteq K[[x]]^p$ $K[[x]]$-module, $N \subseteq K[[x]]^p$ finite dimensional K-vector space , bound an integer

Output: (G, L) a standard basis of $M + N + < x >^{bound} K[[x]]^p$

1: compute G a standard basis of $M + < x >^{bound} K[[x]]^p$;
2: use Gaussian algorithm to compute a reduced row echelon form of $L := \{L_1, \ldots, L_t\}$ of $NF(N|G) :=< N_1, \ldots, N_s >$ with respect to the ordering.
3: **return**(G, L);

Algorithm 2 codimMod

Input: $f = \langle f_1, \ldots, f_p \rangle \subseteq K[[x]]^p$, $M \subseteq K[[x]]^p$ an $K[[x]]$-module, $N =< N_1, \ldots, N_s > \subseteq S^p$ an $S = K[[f]]$ module and bound an integer

Output: codimension of $M + N + < x >^{bound} K[[x]]^p$

1: compute $N := \{f_1^{i_1} \ldots f_p^{i_p}.N_i | f_1^{i_1} \ldots f_p^{i_p}.N_i \notin < x >^{bound} K[[x]]^p, \quad i = 1, \ldots, s\}$
2: $(G, L) := vStd(M, N, bound)$;
3: **return** $dim(K[[x]]^p/L(G)) - \#L$;

Remark 2. *One important application is the following. Let $f = (f_1, f_2, \ldots, f_p) \in R^p$ and $S = K[[f]]$. Let $M \subseteq R^p$ be an R-module, and $N = < n_1, n_2, \ldots, n_s >_S \subseteq S^p$ a finitely generated S-module.*

The aim is to compute a standard bases of the K-vector space $M + < x >^k R^p + N$. Let $W = \{f_1^{i_1} \ldots f_m^{i_m}.n_i | f_1^{i_1} \ldots f_m^{i_m}.n_i \notin < x >^k R^p, i = 1, \ldots, s\} =: \{w_1, \ldots, w_t\}$ and $N_0 =< w_1, \ldots, w_t >_K$ then

$$M + < x >^k R^p + N = M + < x >^k R^p + N_0.$$

We obtain the following algorithm to compute the codimension of the tangent space of the orbit of a map germ under the action of $\mathcal{A}$.

We use the local reverse lexicographic ordering for $\mathbb{Q}[[x, y]]$ resp. $\mathbb{Q}[[t]]$ and with the extension to modules as defined in Section 1.

[3] These algorithms are implemented in the SINGULAR library classifyMapGerms.lib (cf. [AKP16]).

Algorithm 3 codimMap

Input: $f = \langle f_1, \ldots, f_p \rangle \subseteq K[[\mathrm{x}]]$,

Output: extended codimension of $< \frac{\partial f}{\partial x_j} > + K[[f]]^p$

1: compute $M :=< \frac{\partial f}{\partial x_j} >$;
2: $N := K[[f]]^p$;
3: $bound = computeBound(M, N, f)$;
4: **return**$codimMod(M, N, f, bound)$;

The algorithm *computeBound* computes an estimate for the determinacy of f. It is based on Theorem 1 and computes l such that $< \mathrm{x} >^l K[[\mathrm{x}]]^p \subseteq T_{\mathcal{K}^e,f} + < \mathrm{x} >^{l+1} K[[\mathrm{x}]]^p$ by computing a standard basis of $T_{\mathcal{K}^e,f}$ and checking case by case if $< \mathrm{x} >^l K[[\mathrm{x}]]^p \subseteq T_{\mathcal{K}^e,f} + < \mathrm{x} >^{l+1} K[[\mathrm{x}]]^p$. It uses $k = 10$ as initial bound and increases the bound k as long as $< \mathrm{x} >^k K[[\mathrm{x}]]^p \subseteq T_{\mathcal{A}^e,f} + < \mathrm{x} >^{k+l} K[[\mathrm{x}]]^p$. Then by using Theorem 1 f is $k + l$ determined.

In the following examples we want to compute the codimension to the orbit for the action of $\mathcal{A}$. We give explicitly the standard basis (G, L) and the codimension.

Example 1. $R = \mathbb{Q}[[x, y]]$, $f = (x, xy + y^4)$, $S = \mathbb{Q}[[x, xy + y^4]]$

$M =< x, y > . < \begin{pmatrix} 1 \\ y \end{pmatrix}, \begin{pmatrix} 0 \\ x + 4y^3 \end{pmatrix} >_R$

$N =< x, xy + y^4 > S^2$. *We obtain as standard basis for* $M + < x >^{10} R^2$ *(as R-module)*

$G = \{ \begin{pmatrix} x \\ 0 \end{pmatrix}, \begin{pmatrix} y \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ x^2 \end{pmatrix}, \begin{pmatrix} 0 \\ xy \end{pmatrix}, \begin{pmatrix} 0 \\ y^{10} \end{pmatrix} \}$ *and*

$L = \{ \begin{pmatrix} 0 \\ x \end{pmatrix}, \begin{pmatrix} 0 \\ y^4 \end{pmatrix}, \begin{pmatrix} 0 \\ y^5 \end{pmatrix}, \begin{pmatrix} 0 \\ y^6 \end{pmatrix}, \begin{pmatrix} 0 \\ y^7 \end{pmatrix}, \begin{pmatrix} 0 \\ y^8 \end{pmatrix}, \begin{pmatrix} 0 \\ y^9 \end{pmatrix} \}$

Especially

$$dim_{\mathbb{Q}} R^2/(M + < x >^{10} R^2 + N) = dim_{\mathbb{Q}} R^2/M - 7 = 5.$$

Example 2. $R = \mathbb{Q}[[t]]$, $f = (t^4, t^7 + t^9, t^{17})$, $S = \mathbb{Q}[[t^4, t^7 + t^9, t^{17}]]$

$M =< \begin{pmatrix} 4t^3 \\ 7t^6 + 9t^8 \\ 17t^{16} \end{pmatrix} >_R$, *and* $N = S^3$.

We obtain a standard basis for $M + < t >^{14} R^3$ *(as R-module)*

$G = \{ \begin{pmatrix} 4t^3 \\ 7t^6 + 9t^8 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ t^{14} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ t^{14} \end{pmatrix} \}$ *and*

$L = \{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ t^4 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ t^7 + 9/7t^9 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ t^8 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ t^9 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ t^{10} + 16/7t^{12} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ t^{11} + 9/7t^{13} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ t^{12} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ t^{13} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ t^4 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ t^7 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ t^8 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ t^{11} \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ t^{12} \end{pmatrix} \}.$

Especially

$$dim_{\mathbb{Q}} R^3/(M + < t >^{14} R^3 + N) = dim_{\mathbb{Q}} R^3/(M + < t >^{14} R^3) - 16 = 15.$$

3 Modular Computations

Modular computation reduces the computation of standard basis to the case of finite fields, when we apply in Section 2. In this section we describe how to compute the standard basis for the vector spaces described in Section 2 with modular methods. Let $K = \mathbb{Q}$ be the field of rational numbers. As before we fix a local monomial ordering $>$ on $R := K[[\mathrm{x}]]$ and extend it to a module ordering on R^q. Let $M \subseteq R^q$ be an R-module such that

1. $M \supseteq < \mathrm{x} >^k R^q$ for some k.
2. $M =< f_1, \ldots, f_r >_R$ with $f_i \in K[\mathrm{x}]$.

Let $N =< w_1, \ldots, w_s >_K$ be a finitely generated sub space in R^q, $w_i \in K[x]$. The aim is to compute a standard basis (G, L) of $M + N$ using modular methods.

The idea is as follows. Choose P, a finite set of primes which do not divide any denominator of the coefficients of the f_i and w_j, compute a reduced standard basis (G_p, L_p) of $M_p + N_p \subseteq \mathbb{F}_p[[\mathrm{x}]]^q$, for every $p \in P$. Here $M_p :=< f_1 \mod p, \ldots, f_r \mod p >$ and $N_p =< w_1 \mod p, \ldots, w_s \mod p >$. Then lift these modular standard basis to a standard basis (G, L) of $M + N$. The lifting process consists of two steps. Using Chinese remainder algorithm we can lift $\{(G_p, L_p)\}_{p \in P}$ to (G_a, L_a) over $\mathbb{Z}/a[[\mathrm{x}]]^q$ with $a := \prod_{p \in P} p$. Since (G_a, L_a) is uniquely determined modulo a, we need a to be larger then the moduli of all coefficients occurring in a standard basis over $\mathbb{Q}$. The problem is that we do not know this in advance. The second step uses the Farey rational map (cf. [KG83]). This map gives a unique result provided $\sqrt{a/2}$ is larger than the moduli of all coefficients in (G, L). This motivates the following definition (cf. [IPS11]) :

Definition 4. *Let (G, L) be a standard basis of $M + N$.*

1. *If (G_p, L_p) is a standard basis of $M_p + N_p$ then p is called lucky for $M + N$ if G and G_p have the same leading monomials, $LM(G) = LM(G_p)$, and L and L_p have the same leading monomials, $LM(L) = LM(L_p)$. If p is not lucky for $M + N$ it is called unlucky.*
2. *A set P of lucky primes for $M + N$ is called sufficiently large for $M + N$ if*

$$\prod_{p \in P} p \geq max\{2|c|^2 |\ c \text{ a coefficient in } G \text{ or } L\}.$$

Since we do not know the standard basis we cannot test a single prime for being unlucky (for more details see [BDFP15]. Therefore we fix a set of primes P. After having computed the set of standard bases $B := \{(G_p, L_p) | p \in P\}$ we delete unlucky primes as follows by majority vote.

DeleteUnluckyPrimes. *We define an equivalence relation on (B, P) by*

$$(G_p, L_p) \sim (G_{p'}, L_{p'}) \Leftrightarrow LM(G_p) = LM(G_{p'}) \quad \text{and} \quad LM(L_p) = LM(L_{p'}).$$

The equivalence class of largest cardinality is stored in (B, P), the others are deleted.

Similarly to [Pf07] and [IPS11] we obtain the following algorithm.

Assume $>$ is a local ordering.

Algorithm 4 modVStd

Input: $M \subseteq \mathbb{Q}[[x]]^q$, $\mathbb{Q}[[x]]$-module, $N \subseteq \mathbb{Q}[[x]]^q$ finite dimensional $\mathbb{Q}$-vector space, bound an integer

Output: (G, L) a standard basis of $M + N + < x >^{bound} \mathbb{Q}[[x]]^q$

choose P, a list of random primes;
$B := \emptyset$; $M := M + < x >^{bound} \mathbb{Q}[[x]]^q$
loop
  for $p \in P$ **do**
    compute the reduced standard basis (G_p, L_p) of $M_p + N_p$
    $B := B \bigcup \{(G_p, L_p)\}$
    $(B, P) = DeleteUnluckyPrimes(B, P)$;
  lift (B, P) to (G, L) , G, $L \subseteq \mathbb{Q}[x]^q$ using Chinese remainder algorithm and Farey rational map;
  if $M \subseteq < G >_{\mathbb{Q}[[x]]}$ and $M + N \subseteq < G >_{\mathbb{Q}[[x]]} + < L >_{\mathbb{Q}}$ **then**
    if G is a standard basis of M as $\mathbb{Q}[[x]]$-module **then**
      return(G, L);
  enlarge P;

The algorithm terminates by construction and its correctness follows by the next theorem which goes back to E. Arnold (cf. [Ar03]) for homogenous ideals and was proved in [GP07] for ideals and local orderings.

Theorem 2. *Let M, N be as above, let p be a prime and G, $L \subseteq \mathbb{Q}[x]^q$ such that $LM(G) = LM(G_p)$ and $LM(L) = LM(L_p)$. Assume that (G_p, L_p) is a reduced standard basis of $M_p + N_p$ and G is a standard basis of $< G >_{\mathbb{Q}[[x]]}$. Assume that $M \subseteq < G >_{\mathbb{Q}[[x]]}$ and $M + N \subseteq < G >_{\mathbb{Q}[[x]]} + < L >_{\mathbb{Q}}$ then (G, L) is a reduced standard basis [4] of $M + N$.*

Proof. Since G_p is a reduced standard basis of M_p and $M \subseteq < G >_{\mathbb{Q}[[x]]}$ and G is a standard basis of $< G >$ we obtain from [Pf07] (which can be proved for modules similarly to the case of ideals) that $M = < G >_{\mathbb{Q}[[x]]}$. The lifting G of G_p is a reduced standard basis since G is a standard basis and G_p is a reduced standard basis. Since L_p is in reduced echelon form the lifting L is also in reduced echelon form. Since L_p is a set of monic vectors and no monomial of a vector in L_p is in $L(M_p)$ the same holds for L. This implies that (G, L) is a reduced standard basis of $< G >_{\mathbb{Q}[[x]]} + < L >_{\mathbb{Q}}$.

It remains to prove that $M + N = < G >_{\mathbb{Q}[[x]]} + < L >_{\mathbb{Q}} = M + < L >_{\mathbb{Q}}$. We know that $M + N \subseteq < G >_{\mathbb{Q}[[x]]} + < L >_{\mathbb{Q}}$. This implies that

$$dim_{\mathbb{Q}} M + N / < x >^k R^q \leq dim_{\mathbb{Q}} M + < L >_{\mathbb{Q}} / < x >^k R^q.$$

[4] We do not assume that the prime is lucky, but it is a consequence of the theorem.

On the other hand we have for $p \in P$ that

$$dim_{\mathbb{Q}} M + N/ < \mathrm{x} >^k R^q \geq dim_{\mathbb{F}_p} M_p + N_p/ < \mathrm{x} >^k \mathbb{F}_p[[\mathrm{x}]]^q.$$

But

$$dim_{\mathbb{Q}} M + < L >_{\mathbb{Q}} / < \mathrm{x} >^k R^q = dim_{\mathbb{F}_p} M_p + N_p/ < \mathrm{x} >^k \mathbb{F}_p[[\mathrm{x}]]^q$$

implies the result we were looking for. □

4 Examples and timings

We create the examples (coming from the classification of map germs) as follows:

Given $f = (f_1, f_2)$, $f_i \in \mathbb{C}[[\mathrm{x}]]$ and ϕ, $\psi : \mathbb{C}[[\mathrm{x}]] \longrightarrow \mathbb{C}[[\mathrm{x}]]$. We construct the $\mathcal{A}$-equivalent map germ F defined by (ϕ, ψ), i.e. $F = \psi \circ f \circ \phi^{-1}$.

Let $M =< \mathrm{x} >< \frac{\partial F}{\partial \mathrm{x}} >$ and $N = F\mathbb{C}[[F]]^2$(tangent space) in case of two variables x resp. $M =< \frac{\partial F}{\partial \mathrm{x}} >$, $N = \mathbb{C}[[F]]^2$(extended tangent space) in case of one variable x. Given a bound b we compute $vStd(M, N, b)$, its modularized version and the parallel modular version and give the corresponding timings.

Example 3.

$bound$= 15, $f_1 = x$, $f_2 = xy + y^5 + y^7$, $g_1 = f_1 + f_1 f_2$, $f =< g_1, g_2 >$

$\phi(x, y) = (x + y + x^3 + xy^3 + y^{11} + y^{14} + xy^{17}, y + y^2 + x^3 + 2x^3y + x^6 + y^{14} + 2y^{15} + 2x^3y^{14} + xy^{17} + 2xy^{18} + 2x^4y^{17} + y^{28} + 2xy^{31} + x^2y^{34})$

$F = \phi(f)$, $M =< x, y >< \frac{\partial F}{\partial x}, \frac{\partial F}{\partial y} >$, $N = F\mathbb{C}[[F]]^2$

Example 4.

$bound$= 15, $f_1 = x$,$f_2 = xy^2 + y^5 + y^9$, $f =< f_1, f_2 >$

$\phi(x, y) = (x + xy^4, y + x^2 + y^{11})$

$F = \phi(f)$, $M =< x, y >< \frac{\partial F}{\partial x}, \frac{\partial F}{\partial y} >$, $N = F\mathbb{C}[[F]]^2$

Example 5.

$bound$= 15, $f =< x, x^2y + y^4 >$, $\phi(x, y) = (x + xy^4, y + x^2 + y^{11})$

$F = \phi(f)$, $M =< x, y >< \frac{\partial F}{\partial x}, \frac{\partial F}{\partial y} >$, $N = F\mathbb{C}[[F]]^2$

Example 6.

$bound$= 250, $f_1 = t^{56}$, $f_2 = t^{70} + t^{91}$, $f_3 = t^{84} + 2t^{105}$, $f_4 = t^{101}$

$g_1 = f_1 + 231f_2f_1 + 311f_1f_3 + 71f_1^2 + 611f_1f_2f_3$, $g_2 = f_2 + 911f_1^2 + 511f_2f_3 + f_1^2f_2^2$, $g_2 = f_2 + 911f_1^2 + 511f_2f_3 + f_1^2f_2^2$, $g_3 = f_3 + 731f_1f_2f_3 + 1171f_3^2 + f_2^3$

$\phi(t) = t + 22t^2 + 323t^3 + 555t^4 + 777t^6$

$F = \phi(f)$, $M =< \frac{\partial F}{\partial t} >$, $N = \mathbb{C}[[F]]^2$

Example 7.

bound$= 300$, $f_1 = t^{80}$, $f_2 = t^{120} + t^{140} + t^{150} + t^{175}$, $f_3 = t^{181}$

$g_1 = f_1 + 231 f_2 f_1 + 71 f_1^2$, $g_2 = f_2 + 911 f_1^2 + f_1^2 f_2^2$, $g_3 = f_3 + f_1 f_2$, $f =< g_1, g_2, g_3 >$

$\phi(t) = t + 55t^2 + 366t^3 + 577t^4 + 788t^6$, $F = \phi(f)$, $M =< \frac{\partial F}{\partial t} >$, $N = \mathbb{C}[[F]]^2$

Example 8.

bound$= 350$, $f_1 = t^{84}$, $f_2 = t^{140} + t^{210} + t^{245}$, $f_3 = t^{139}$

$g_1 = f_1 + 231 f_2 f_1 + 715 f_1^2$, $g_2 = f_2 + 911 f_1^2 + 4567 f_1^2 f_2^2$, $g_3 = f_3 + 333 f_1 f_2$

$f =< g_1, g_2 >$, $\phi(t) = t + 22t^2 + 333t^3 + 544t^4 + 755t^6 + 567t^7$, $F = \phi(f)$

$M =< \frac{\partial F}{\partial t} >$, $N = \mathbb{C}[[F]]^2$

We summarize the results in the table below where modVStd0 denotes the parallelized version of modVStd computing the characteristic p results in parallel. All timings are given in seconds. The computation are made on a Dell PowerEdge R720 with two Intel(R) Xeon(R) CPU E5 − 2690 @ 2.90GHz, 20 MB Cache, 16 Cores, 32 Threads, 192 GB RAM with a Linux operating system (Gentoo). "–" means that the task did not finish because of memory overflow.

The timings show that as expected for complicated examples the parallel modular version of vStd is more successful. For simple examples the overhead dominates the computation.

Example	vStd	modVStd	modVStd0
3	4123	2942	52
4	–	532	324
5	–	3	8
6	2258	36	24
7	56	19	12
8	864	4	14

Acknowledgement. This research was partly supported by the DAAD and ASSMS. We would like to thank the referee for giving several hints improving the presentation of the results.

References

[AKP16] Afzal, D.; Pfister, G.; Kanwal, S., classifyMapGerms.lib. A Singular 4-0-2 library for computing the standard basis of the tangent space at the orbit of an algebraice group action and classifying simple singularities given by Riegers(2016). https://github.com/Singular/Sources/blob/spielwiese/ Singular/ LIB/classifyMapGerms.lib.

[Ar03] Arnold, E. A, Modular Algorithms for Computing Gröbner Basis, *J. Symbolic Comput.* **35**, 403-419 (2003).

[BG82] Bruce, J. W.; Gaffney T. J., Simple Singularities of Mappings $(\mathbb{C},0) \to (\mathbb{C}^2,0)$, *J. London. Math. Soc.* **2**, 465-474 (1982).

[Bo98] Bongartz, K., Some Geometric Aspets in Representation Theory, *In Reiten, I., Smalø, S.O., Selberg, ø. Algebras and Modules I, Workshop in Represtation of Algebras and Related Topics, July 29- August 3, 1996 Trondkeim Norway CMS Conference Proc.*, **23**, 1-27 (1998).

[BDFP15] Böhm, J.; Decker, W.; Fieker, C.; Pfister, G., The Use of Bad Primes in Rational Reconstruction, *Math. Comp.*, **84**, 3013-3027 (2015).

[DGPS16] Decker, W.; Greuel, G.-M.; Pfister, G.; Schönemann, H., Singular *4-0-2 – A computer algebra system for polynomial computations*, `http://www.singular.uni-kl.de` (2016).

[Du80] Du Plessis, A., On the Determinancy of Smooth Map Germs, *Invent. Math.*, **58**, 107-160 (1980).

[GH93] Gibson, C. G; Hobbs, C. A., Simple Singularities of Space Curves, *Mathematics. Proc. Cambridge Philos. Soc.*, **113**, 297-310 (1993).

[Gi83] Giusti, M., Classification Des Singularités Isolées Simples D'Intersections Complètes, *Proc. Symp. Pure Math.* **40**, 457-494 (1983).

[GP07] Greuel, G.-M.; Pfister, G., A Singular Introduction to Commutative Algebra, Second edition, Springer (2007).

[IPS11] Idrees, N.; Pfister, G.; Steidel, S., Parallelization of Modular Algorithms, *J. Symbolic Comput.*, **46**, 672-684 (2011).

[KG83] Kornerup, P.; Gregory, R. T., Mapping Integers and Hensel Codes onto Farey Fractions, *BIT Numerical Mathematics*, **23**, 9-20 (1983).

[Ma69] Mather, J. N.,Stability of $\mathbb{C}^\infty$-mappings III. Finitely Determined Map-germs, *Publ. Math. IHES*, **35**, 127-156 (1969).

[Pf07] Pfister, G., On Modular Computation of Standard Basis. *An. Stiint. Univ. Ovidius Constanta Ser. Mat.*, **15**, 129-137 (2007).

[Ri87] Rieger, J. H., Families of Maps from the Plane to the Plane, *J. London Math. Soc.*, **(2)36**, 351-369 (1987).

[RR91] Rieger, J. H.; Ruas, M. A. S., Classification of $A-$germs from K^n to K^2, *Compositio Mathematica*, **79**, 99-108 (1991).

[Sp98] Springer, T. A., Linear Algebraic Groups, Second edition, Birkhäuser, (1998).

[Wa83] Wall, C.T.C. Classification of Unimodal Isolated Singularities of Complete Intersections, *Proc. Symp. Pure Math. Part2, Amer. Math. Soc.*, **40**, 625-640 (1983).

Received: 21.03.2017
Revised: 26.05.2017
Accepted: 30.05.2017

(1) (i) Department of Mathematics, University of Kaiserslautern
Erwin-Schrödinger-Str., 67663 Kaiserslautern, Germany
(ii) Department of Mathematics, University of Lahore
Near Raiwind Road, 54000 Lahore, Pakistan
E-mail: deebafzal@gmail.com

(2) Abdus Salam School of Mathematical Sciences, GC University
Lahore, 68-B New Muslim Town, 54000 Lahore, Pakistan
E-mail: lotus_zone16@yahoo.com

(3) Department of Mathematics, University of Kaiserslautern
Erwin-Schrödinger-Str., 67663 Kaiserslautern, Germany
E-mail: pfister@mathematik.uni-kl.de