Bull. Math. Soc. Sci. Math. Roumanie
Tome 60 (108) No. 1, 2017, 67–81

Standard Bases with Special generators of the leading ideal
by
Shamsa Kanwal, Gerhard Pfister

Abstract

Let $I \subseteq K[x]$ be an ideal, K a field, $x = (x_1, \ldots, x_n)$ and $>$ a monomial ordering (not necessarily a well-ordering). Let $L(I)$ be the leading ideal of I with respect to $>$. A standard basis (in case of a well-ordering a Gröbner basis) $G = \{f_1, \ldots, f_m\}$ is defined by the property that $L(I)$ is generated by the leading monomials $LM(f_1), \ldots, LM(f_m)$ of G. Usually one considers a standard basis associated to the uniquely determined minimal system of monomials generating $L(I)$, a minimal standard basis. In case of border bases, Janet bases or Pommaret bases (usually only defined for well-orderings but we generalize the concept to any ordering) the underlying standard bases have as leading monomials special (non minimal) generators of $L(I)$. We describe an algorithm which computes these bases using a minimal standard bases and the corresponding special generators of $L(I)$. We have implemented these algorithms in Singular (cf. [DGPS16]) including modular and parallel implementations and give timings to compare them (cf.[KP17]). We also discuss the verification of the modular algorithm to compute border bases and Janet bases.

Key Words: Gröbner basis, standard basis, Janet Basis, Border Basis, modular computation
2010 Mathematics Subject Classification: Primary 13P99, 13E05

1 Introduction

Gröbner bases are in our days a very powerful tool for symbolic computations in mathematics and its applications. The ideas go back to Gordan (cf. [Go99]), Macaulay (cf. [M39]) and Gröbner (cf. [Gr39]). For ideals in a polynomial ring they are special generators with many good properties. 1965 Buchberger (cf. [Bu65]) gave his famous algorithm to compute them. For ideals in power series rings the corresponding theory goes back to Hironaka (cf. [H64]) and Grauert (cf. [Gr72]), called standard bases. Mora (cf. [Mo82], [Mo92]) gave the first algorithm to compute standard bases. Now we have a unified theory: Gröbner bases are standard bases in case of global orderings (all monomials are greater than 1) and the standard bases of Hironaka and Grauert correspond to local orderings (all monomials are smaller than 1), cf. [GP07]. Involutive bases or more general r-standard bases are Gröbner bases with additional properties. They were introduced by Gerdt and Blinkov (cf. [Ger05], [GB98], [GBY01]) influenced by ideas studying partial differential equations.
Let K be a field, $x = (x_1, \ldots, x_n)$ and $I \subseteq K[x]$ an ideal, let $>$ be a monomial ordering and $L(I)$ the leading ideal of I. In [Ger05] V.Gerdt defined a restricted division r on the set of monomials $Mon(x)$ to be a transitive relation

$$u|_r v,\ u, v \in Mon(x) \text{ such that } u|_r v \text{ implies } u|v.$$

Special choices of r lead to involutive division and involutive bases of I including Janet bases and Pommaret bases. The definition implies that an r-standard basis of I is a standard basis of I. An r-standard basis may be an infinite set. There exist always finite Janet bases and Pommaret bases (cf. [Ger05]).

Example 1. *We give the following examples for restricted divisions.*

1. *The ordinary division of monomials is a restricted division.*
2. *The Pommeret division is defined as follows. Let $u = x_1^{e_1} \dots x_n^{e_n}$ and $v \in Mon(x)$ we define the restricted division $u|_r v$ by the conditions $u|v$ and $v/u \in K[x_1, \dots, x_i]$ with i minimal such that $e_i > 0$.*
3. *More general assume that for any monomial $u \in Mon(x)$ there is associated a subset $x(u) \subset x$ of so-called multiplicative variables [1]. Let $u = x_1^{e_1} \dots x_n^{e_n}$ and $v \in Mon(x)$ we define the restricted division $u|_r v$ by the conditions $u|v$. and $v/u \in K[x(u)]$.*
4. *The Janet division is defined as follows. Let U be a finite set of monomials[2]. If $u \notin U$ we define $x(u) = \emptyset$. For $u = x_1^{e_1} \dots x_n^{e_n} \in U$ we define $[\emptyset] = U$ and for and $1 \leq k \leq n$*

   $$[e_{k+1}, \dots, e_n] = \{x_1^{v_1} \dots x_n^{v_n} \in U | e_{k+1} = v_{k+1}, \dots, e_n = v_n\}.$$

   The variable x_k is multiplicative for u (with respect to U) if

   $$e_k = max\{v_k | x_1^{v_1} \dots x_n^{v_n} \in [e_{k+1}, \dots, e_n]\}.$$

5. *As a special example for the Janet division consider $U = \{x^5, x^2y^2, y^6\} \subset K[x, y]$. The multiplicative variables for x^5 and x^2y^2 are $\{x\}$ and for y^6 are $\{x, y\}$.*

Such a restricted division leads to a special system $\{m_j\}_{j \in J}$ of monomials of $L(I)$ with the following property [3].

$$\text{For every } m \in L(I) \text{ there is a } j \in J \text{ such that } m_j|_r m.$$

The set $\{m_j\}_{j \in J}$ is a special set of monomials generating $L(I)$ with respect to the restricted division, so-called r-generators of $L(I)$.

Definition 1. *A subset $G \subseteq I$ is called an r-standard basis of I if the leading monomials of the elements of G form a set of r-generators of $L(I)$. If especially the restricted division is a Pommeret (resp. Janet) division the corresponding r-standard basis is called Pommeret (resp. Janet) basis.*

Border bases (cf. [KK05],[KK06], [KKR05]) can also be interpreted as special r-standard bases.

[1] In the previous example $x(u) = \{x_1, \dots, x_i\}$.

[2] In the applications U will be a finite set of generators of the leading ideal $L(I)$ of an ideal I with respect to the fixed ordering.

[3] Note, that the restricted division may depend on the ideal $L(I)$ as we will see for the Janet-division.

Definition 2. *Let* $O := Mon(x) \setminus Mon(x) \cap L(I)$ *and* $\partial O := x_1O \cup \ldots \cup x_nO \setminus O$ *the border of* O *then* $L(I) = \langle \partial O \rangle$. *A subset* $G \subset I$ *is called border basis if* ∂O *is the set of leading monomials of* G.

The elements of the border have the following property:

Let m, n, t be monomials, $m, t \in \partial O$ and $n \notin \partial O$. If $m|n$ then $n \nmid t$.

This implies that the following relation r is transitive:

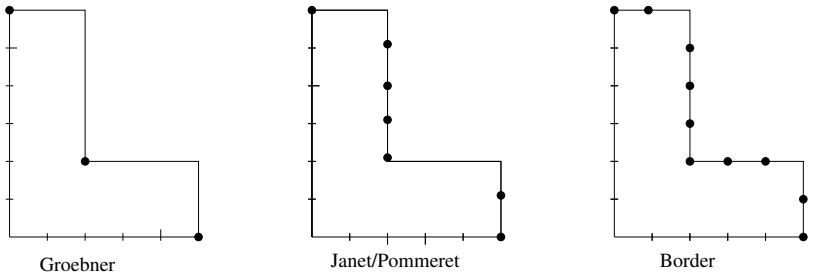
If $(m, n) \in \partial O \times \partial O$ then $m \nmid_r n$. If $(m, n) \notin \partial O \times \partial O$ then $m|_r n$ if and only if $m|n$.

Using this restricted division a border basis is an r-standard basis. If $dimK[x]/I = 0$ then a border basis is finite.
Let us consider the following example:

Example 2. *Let* $I =< x^5, x^2y^2, y^6 > \subset K[x, y]$ *then*

1. $\{x^5, x^2y^2, y^6\}$ *is a Gröbner basis of* I.
2. $\{x^5, x^2y^2, y^6, x^5y, x^2y^3, x^2y^4, x^2y^5\}$ *is a Janet basis and also a Pommaret basis of* I *since* $x^5, x^2y^2, x^5y, x^2y^3, x^2y^4, x^2y^5$ *have* $\{x\}$ *as multiplicative variable and* y^6 *has* $\{x, y\}$ *as multiplicative variables.*
3. *A border basis of* I *is given by the set* $\{x^5, x^2y^2, y^6, x^5y, x^2y^3, x^2y^4, x^2y^5, xy^6, x^3y^2, x^4y^2\}$ *since* $O = \{1, y, y^2, y^3, y^4, y^4, x, xy, xy^2, xy^3, xy^4, xy^5, x^2, x^2y, x^3, x^3y, x^4, x^4y\}$.

The following diagrams visualize the bases in 1. to 3. in the example [4].



Next we want to explain the idea of modular computations. We refer to [A03], [NY17], [BDFG15], [GY03] and [IPS11] for a detailed description and analysis of the modular approach. We describe here how to compute a standard basis using modular methods. We use the following notations.

Definition 3. *Let* $K = \mathbb{Q}$ *and* $S \subset \mathbb{Q}[x]$ *be a set of polynomials, then*

1. $LM(S) := \{LM(f) \mid f \in S\}$ *is the set of leading monomials of* S.

[4] The dots correspond to the exponents of the monomials in the corresponding basis.

2. *If $I = \langle f_1, \ldots, f_r \rangle \subset \mathbb{Q}[x]$ and p is a prime number which does not divide any denominator of the coefficients of $f_1, \ldots, f_r$. We write $I_p := \langle f_1 mod\, p, \ldots, f_r mod\, p \rangle \subset \mathbb{F}_p[x]$.*

The idea of the algorithm is as follows.

1. We choose a set of prime numbers P and compute for $p \in P$ a standard basis G_p of $I_p \subset \mathbb{F}_p[x]$.

2. Then we lift these modular standard bases to a set of polynomials $G \subset \mathbb{Q}[x]$.

The lifting process consists of the two steps. The set

$$GP = \{G_p \mid p \in P\} \text{ is lifted to } G_N \subset \mathbb{Z}/N\mathbb{Z}[x] \text{ with } N = \prod_{p \in P} p$$

using Chinese remainder theorem (here N should be larger than the moduli of all coefficients in the expected standard basis). We obtain

$$G \subset \mathbb{Q}[x] \text{ applying the Farey rational map to the coefficients in } G_N$$

(here we need that $\sqrt{N/2}$ is larger than the moduli of all coefficients of G). Since we do not have good bounds for N to guarantee the correct lifting, we enlarge the set of primes as long as the lifting stabilizes. Then the result is a standard basis of the ideal I with high probability (a so-called probabilistic standard basis). To guarantee a correct result, we need a final test in $\mathbb{Q}[x]$.

$$\text{We test if } I =< G > \text{ and } G \text{ is a standard basis of } < G >.$$

If the test fails we enlarge the set of primes and continue. The test is usually very time consuming. In many cases one can prove that it is enough to test that

$$I \subset< G > \text{ and } G \text{ is a standard basis of } < G >.$$

This is the so-called verification theorem (cf. [A03], [P07]). We will prove such a verification theorem for r-standard bases.

Finally, we recall the classical approach to rational reconstruction which is based on the lifting of modular to rational results by computing Farey preimages via Euclidean division with remainder ([BDFG15], [C94], [KG83]). Let

$$F_B = \{\frac{a}{b} \in \mathbb{Q} | \gcd(a,b) = 1, 0 \leq a \leq B, 0 < |b| \leq B\}$$

and

$$\mathbb{Q}_N = \{\frac{a}{b} \in \mathbb{Q} | \gcd(a,b) = \gcd(b,N) = 1\}.$$

Let $\varphi_N : \mathbb{Q}_N \to \mathbb{Z}/N$ defined by $\varphi_N\left(\frac{a}{b}\right) = (a \mod N)(b \mod N)^{-1} := (\frac{a}{b})_N$.

If $2B^2 < N$ then the Farey map $\varphi_{B,N} : F_B \cap \mathbb{Q}_N \to \mathbb{Z}/N$ is injective. The following algorithm computes the preimage of the Farey map.

Algorithm 1 FAREY(N)

Require: Integers $N \geq 2$ and $0 \leq r \leq N-1$.
Ensure: `false` or a rational a/b with $\gcd(a,b) = \gcd(b,N) = 1$, $a/b \equiv r \bmod N$, $0 \leq a, |b| \leq \sqrt{(N-1)/2}$,
$(a_0, b_0) := (N, 0)$, $(a_1, b_1) := (r, 1)$, $i := -1$
while $2a_{i+2}^2 \geq N-1$ **do**
$i := i+1$
divide a_i by a_{i+1} to find q_i, a_{i+2}, b_{i+2} such that

$$(a_i, b_i) = q_i(a_{i+1}, b_{i+1}) + (a_{i+2}, b_{i+2})$$

and $0 \leq a_{i+2} < a_{i+1}$
if $2b_{i+2}^2 < N$ and $\gcd(a_{i+2}, b_{i+2}) = 1$ **then**
return $\frac{a_{i+2}}{b_{i+2}}$
return `false`

The aim of this paper is to define and compute border basis and Janet bases also for non-well orderings in a general setting, analyze the modular and parallel algorithms to compute them and compare the results with other implementations. We also compare our implementation of Janet bases with the implementation in SINGULAR based on the algorithm of V. Gerdt (cf. [Ger05]).

2 r-Standard Bases

To explain our approach to compute r-standard bases let us recall the properties of a weak normal form (cf. [GP07]).

Let $G = \{g_1, \ldots, g_m\}$ be a standard basis of I with respect to $>$. For any $f \in K[x]$ there exist polynomials $u, a_1, \ldots, a_m \in K[x]$ such that

$$uf = \Sigma_{i=1}^m a_i g_i + h.$$

satisfying

1. If $h \neq 0$ then $LM(h)$ is not divisible by $LM(g_i), i = 1, \ldots, m$.
2. $LM(\Sigma_{i=1}^m a_i g_i) \geq LM(a_i g_i)$ for all i with $a_i g_i \neq 0$.
3. $LM(u) = 1$, if $>$ is a global ordering(i.e. a well-ordering), then u can be choosen to be 1.

The polynomial h is called weak normal form of f with respect to G. There exist algorithms to compute a weak normal form. We fix now such an algorithm computing uniquely (unique by using the algorithm) u, h such that $uf - h \in I$ and write $(h, u) = NF(f \mid G)$ i.e., $h = NF(f \mid G)[1]$ and $u = NF(f \mid G)[2]$.

Using the normal form we can construct an r-standard basis as described in the following proposition.

Proposition 1. *Let $M = \{m_1, \ldots, m_k\}$ be a set of r-generators of $L(I)$ and $G = \{g_1, \ldots, g_m\}$ a standard basis of I. Let $(h_i, u_i) = NF(m_i \mid G)$ and $f_i := u_i m_i - h_i, i = 1, \ldots, k$. Then $\{f_1, \ldots, f_k\}$ is an r-standard basis of I.*

Proof. $LM(f_i) = LM(u_i m_i)$ using property (2) of the weak normal form,
$LM(u_i m_i) = m_i$ since $LM(u_i) = 1$. □

On the basis of Proposition 1 we have implemented algorithms to compute Janet bases and border bases. They can be used to compute this bases using modular and parallel methods.

3 Modular Computations of r-Standard Bases

In this chapter we fix a monomial ordering $>$ and a restricted division r on $Mon(x)$. We also assume that we have an algorithm rMon which associates to every monomial ideal I in a unique way a finite set of r-generators of I (rMon returns the empty set if there is no finite set of r-generators). Examples for rMon are algorithms to compute a border basis for a zero-dimensional monomial ideal or to compute a Janet basis (more general an involutive basis) for a monomial ideal.

We describe now an algorithm to compute an r-standard basis using modular methods. We use the notations used in the introduction.

The idea of the algorithm is as follows. We choose a set of prime numbers P and compute for $p \in P$ a standard basis G_p of $I_p \subset \mathbb{F}_p[x]$. Then we lift these modular standard bases $GP = \{G_p \mid p \in P\}$ to a set of polynomials $G \subset \mathbb{Q}[x]$. We obtain a probabilistic standard basis of I or after a verification process a standard basis of I. Now we apply the algorithm rMon to the leading ideal $L(G)$ of G and consider the monomials $J := \text{rMon}(L(G)) \setminus \text{LM}(G)$, the "extra" generators coming from the restricted division. Using the normal form we obtain for every monomial $m \in J$ the normal form $(u_p, h_p) = NF(m \mid G_p)$. For $p \in P$ let $R_p = \{u_p m - h_p \mid m \in J\}$. As before we lift $RP = \{R_p \mid p \in P\}$ to $R \subset \mathbb{Q}[x]$. $G \cup R$ is the r-standard basis we wanted to compute.

We want to use only primes p such that $\text{LM}(G) = \text{LM}(G_p)$, so-called lucky primes. The set of unlucky primes is finite. The following procedure tries to avoid the unluky primes.

deleteUnluckyPrimesSB: *We define an equivalence relation on (GP, P) by $(G_p, p) \sim (G_q, q) :\Longleftrightarrow \text{LM}(G_p) = \text{LM}(G_q)$. Then the equivalence class of largest cardinality is stored in (GP, P), the others are deleted.*

Since we do not know if the number of lucky primes we have choosen is big enough, we test from time to time whether the lifting gives the correct result, i.e. G is a standard basis and $I = \langle G \rangle$. This test is very expensive. In case of a local ordering or a homogeneous ideal in case of a global ordering Theorem 1 simplifies the test. In all cases the following test in

positive characteristic accelerates the algorithm very much.

pTestSB: *We randomly choose a prime number $p \notin P$ such that p does not divide the numerator and denominator of any polynomial of the input. The test is positive if and only if $(G \mod p)$ is a standard basis of I_p.*

For the verification of the r-standard basis we use the following theorem.

Theorem 1. *Let $I \subset \mathbb{Q}[x]$ be an ideal, $>$ a monomial ordering, we assume that either $>$ is global and I is homogeneous*[5] *or $>$ is a local ordering*[6]*. Let $R \subset \mathbb{Q}[x]$ be a set of polynomials such that $LM(R) = LM(R_p)$ where R_p is an r-standard basis of I_P for some prime p. If R is a standard basis of $\langle R\rangle$ and $I \subset \langle R\rangle$ then $I = \langle R\rangle$ and R is an r-standard basis of I.*

Proof. Since R_p is a standard basis of I_p it follows from [A03] resp. [P07] that $I = \langle R\rangle$. Since R_p is a standard basis of I_p and $LM(R) = LM(R_p)$ it follows that R is an r-standard basis. □

We obtain the following algorithms (pseudo-code without the optimization used in the implementation in Singular).

Algorithm 2 rStandard(G, J)

Require: G a standard basis, $J \subseteq \mathrm{LM}(G)$ a finite set.
Ensure: R a set of polynomials of G such that $\mathrm{LM}(R) = J$.

```
R = ∅;
for m ∈ J do
  (u, h) = NF(m | G);
  R = R ∪ {um − h};
return R;
```

The main algorithm will be Algorithm 3.

Remark 1. *Algorithm 3 can easily parallelized as follows:*

1. *The standard bases G_p can be computed in parallel.*
2. *The verification can be parallelized:*
   - *$R \subset \langle G\rangle$ can be checked in parallel for every generator of R.*
   - *The check for G being a standard basis can be done reducing every $s-$polynomial with respect to G in parallel.*

[5] If the ideal is not homogeneous and the ordering is not local the theorem is wrong. K. Yokoyama(cf. [Y12]) gave an example that Theorem 2.4 in [IPS11] fails. The correct statement can be found in [NY17].

[6] For the definition of a local ordering cf. [GP07].

Algorithm 3 rStandardBasis

Require: $I \subseteq \mathbb{Q}[x]$ an ideal given by generators, $>$ a monomial ordering, s an integer.
Ensure: $R \subseteq \mathbb{Q}[x]$ r-standard basis of I(with verification if $s = 1$ and $>$ is local or I is homogeneous).

```
if If s = 1 and > is not local and I is not homogeneous then
  s = 0;
choose P, a list of random primes;
GP = ∅, RP = ∅;
loop
  for p ∈ P do
    compute a standard basis G_p of I_p;
    GP = GP ∪ {G_p};
  (GP, P) = deleteUnluckyPrimesSB(GP, P);
  lift (GP, P) to G ⊆ Q[x] by applying Chinese remainder and Farey fraction rational
  map;
  if pTestSB(I, G, P) then
    if s = 1 then
      if I ⊆ ⟨G⟩ then
        if G is a standard basis of ⟨G⟩ then
          compute J := rMon(L(G)) \ LM(G);
          for p ∈ P do
            R_p = rStandard(G_p, J);
            RP = RP ∪ {R_p};
            lift (RP, P) to R ⊂ Q[x] by applying Chinese remainder and Farey fraction
            rational map;
            if R ⊂ ⟨G⟩ then
              R = R ∪ G;
              return R;
    else
      compute J := rMon(L(G)) \ LM(G);
      for p ∈ P do
        R_p = rStandard(G_p, J);
        RP = RP ∪ {R_p};
        lift (RP, P) to R ⊂ Q[x] by applying Chinese remainder and Farey fraction
        rational map;
        if R ⊂ ⟨G⟩ then
          R = R ∪ G;
          return R;
  enlarge P;
```

4 Examples, timings and conclusions

In this chapter we study examples computing border bases and Janet bases.
We use the following examples 1-19 which can be found in the SymbolicData project of

H.-G. Gräbe (cf.[Gr16]), using the link http://symbolicdata.org/XMLResources/IntPS/.

1. Cyclic_7.xml
2. Milnor1.xml
3. Tjurina1.xml
4. random1.xml
5. random2.xml
6. Singular.schwarz_6.xml (dehomogenized: h=1)
7. Twomat3.xml
8. Klein.xml
9. Meintjes.xml
10. Wilfred.xml
11. Behnke.xml
12. Paris.ilias13.xml
13. Pfister_2.xml
14. Singular.gerhard_3.xml
15. Singular.gerhard_1.xml (dehomogenized w=1)
16. Milnor3.xml
17. Tjurina1.xml
18. Milnor4.xml
19. Steidel_1.xml

In Table 1 (resp. Table 2) we compare timings to compute the border bases (resp. Janet bases) with Algorithm 1 using as rMon an algorithm to compute the border of the order ideal associated to the ordering (degrevlex in examples 1-13 and local degrevlex in examples 14-19) (resp. a Janet basis of the leading ideal).
borderbasisP, rJanetP (resp. borderBasis0, rJanet0) are the timings in characteristic 32003 (resp. 0). modBorder1, modJanet1 (resp. modBorder0, modJanet0) give the timings for the parallel and modular computation with (resp. without) verification of the result. In the second table JanetP (resp. Janet0) are the timings using the Singular implementation of V. Gerdt's algorithm for computing Janet bases in characteristic 32003 (resp. 0) which is implemented only for well–orderings.

Example	borderBasisP	borderBasis0	modBorder1	modBorder0
1	148	–	1899	1224
3	57	–	647	416
6	31	18	414	148
11	1038	73891	83021	27758
12	37	10041	1997	1216
13	7	3617	99	66
16	782	–	–	–
17	243	–	7838	4695
18	1	6283	10	4
19	2	–	17	6

Table 1: Total running times for computing a border basis of the considered examples.

Example	JanetP	Janet0	rJanetP	rJanet0	modJanet1	modJanet0
1	4	29	1	–	71	46
3	126	–	13	–	563	373
4	10	17456	1	–	56	19
5	60	–	3	–	154	54
6	–	–	0	0	0	0
7	74555	77496	41	38	5854	2760
8	31	8885	3	–	–	382673
9	–	65982	807	3921	72639	71591
10	–	–	68452	83420	–	–
12	114	1635	4	6554	602	348
13	48	325	1	1368	30	20
14	61	87	31	239	3403	2500
15			0	–	5	2
16			91	–	–	277878
17			34	–	4015	1734
18			0	3022	2	1
19			0	–	11	4

Table 2: Total running times for computing a Janet basis of the considered examples.

The timings are given in seconds,"–" means that the computation was stopped after one day or the memory exceeded 50 GB. The timings show that our implementation of the algorithm to compute Janet basis is faster than the implementation of V. Grerdt's algorithm. They also show that the modular and parallel approach is much more powerfull than the direct computation in characteristic 0 and the verification step in the modular approach is very time consuming for difficult examples.

The computations are done using the 64-bit version of SINGULAR 4-1-0 on an Dell

PowerEdge R720 2x Intel Xeon E5-2690 2.9 -3.8 GHz 20 MB Cache, 16 Cores, 32 Threads, 192 GB RAM under the Gentoo Linux operating system.

References

[A03] E. A. Arnold: Modular algorithms for computing Gröbner bases, J. Symbolic Comput. 35 (2003), no. 4, 403-419.

[Bu65] B. Buchberger: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. PhD Thesis, University of Innsbruck, Austria (1965).

[BDFG15] J.Böhm, W.Decker, C.Fieker, G.Pfister: The use of bad primes in rational reconstruction, Math. Comp. 84, 3013-3027 (2015).

[C94] G.E. Collins, M.J. Encarnación: Efficient Rational Number Reconstruction. J. Symb. Comput. 20, 287–297 (1995).

[DGPS16] W. Decker, G.-M. Greuel, G. Pfister, H. Schönemann: 2016. SINGULAR 4-1-0. A computer algebra system for polynomial computations. http://www.singular. uni-kl.de

[Ger05] V. P. Gerdt: Involutive Algorithms for Computing Gröbner Bases, In "Computational Commutative and Non-Commutative Algebraic Geometry", S.Conjocaru, G. Pfister and V. Ufnarovski (Eds.), NATO Science Series, 105 Press 2005, 199-255.

[GB98] V. P. Gerdt, Y. A. Blinkov: Involutive bases of polynomial ideals, Mathematics and Computers in Simulation 45 (5),1998, 519-541

[GBY01] V. P. Gerdt, Y. A. Blinkov, D. A. Yanovich: Construction of Janet bases II. Polynomial bases, Computer Algebra in Scientific Computing CASC 2001, 249-263

[GY03] V. P. Gerdt, D. A. Yanovich: Parallel computation of involutive and Gröbner bases, Computer Algebra in Scientific Computing/CASC,2003, 185-194.

[Go99] P. Gordan: Neuer Beweis des Hilbert'schen Satzes über homogene Funktionen. Nachrichten königl. Ges. der Wiss. Göttingen, 240-242 (1899)

[Gr72] H. Grauert: Über die Deformationen isolierter Singularitten analytischer Mengen, Inventiones Math. 15 , 171-198 (1972)

[Gr16] H.-G. Gräbe: The SymbolicData Project Wiki - Tools and Data for Testing Computer Algebra Software. http://www.symbolicdata.org (2016)

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

[Gr39] W. Gröbner: Über die algebraischen Eigenschaften der Integrale von linearen Differentialgleichungen mit konstanten Koeffizienten, Monatsb. der Mathematik 47,247-284 (1939)

[H64] H. Hironaka: Resolution of Singularities of an Algebraic Variety over a Field of Characteristic Zero, Annals of Math. 79 , 109-326 (1964).

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

[KP17] S. Kanwal, G. Pfister: rStandard.lib, SINGULAR -liberary to compute Janet bases and border bases (2017).

[KK05] A. Kehrein, M. Kreuzer: Characterizations of Border Bases, Journal of Pure and Applied Algebra 196 (2005), 251–270.

[KKR05] A. Kehrein, M. Kreuzer, L. Robbiano: An Algebraists View on Border Bases, in: A. Dickenstein and I. Emiris (eds.), Solving Polynomial Equations: Foundations, Algorithms,and Applications, Springer, Heidelberg 2005, 169-202.

[KK06] A. Kehrein, M. Kreuzer: Computing border bases.Journal of Pure and Applied Algebra, 205(2):279-295, 2006

[KG83] P. Kornerup, R.T. Gregory: Mapping Integers and Hensel Codes onto Farey Fractions. BIT Numerical Mathematics 23(1), 9–20 (1983).

[M39] F.S. Macaulay: Some properties of Enumeration in the Theory of Modular Systems. Proc. London Math. Soc. 26, 531-555 (1939)

[Mo82] T. Mora: An algorithm to compute the equations of tangent cones. Proc. EUROCAM 82, Springer Lecture Notes in Computer Science (1982).

[Mo92] T. Mora, G. Pfister, C. Traverso: An introduction to the tangent cone algorithm . Advances in Computing research, Issues in Robotics and nonlinear geometry (**6**) 199–270 (1992).

[NY17] M. Noro, K. Yokoyama: Usage of Modular Techniques for Efficient Computation of Ideal Operations, to appear (2017).

[P07] G. Pfister: On Modular Computation of Standard Basis. An. Stiint. Univ. Ovidius Constanta Ser. Mat. 15 (2007), no. 1, 129–137.

[Y12] K. Yokoyama: Usage of Modular Techniques for Efficient Computation of Ideal Operations,(Invited Talk) in Computer Algebra in Scientific Computing CASC 2012, LNCS 7442, 361–362, 2012.

Received:
Revised:
Accepted:

(1) Abdus Salam School of Mathematical Sciences, GC University, Lahore, 68-B, New Muslim Town, Lahore 54600, Pakistan
E-mail: lotus_zone16@yahoo.com
(2) Department of Mathematics, University of Kaiserslautern, Erwin-Schrödinger-Str., 67663 Kaiserslautern, Germany
E-mail: pfister@mathematik.uni-kl.de