Computational Aspects of Constructing Gröbner Bases by Involutive Methods

Vladimir Gerdt

Laboratory of Information Technologies

Joint Institute for Nuclear Research

141980 Dubna, Russia

`gerdt@jinr.ru`

Talk at RICAM Linz 28.02.2006

Contents

Constructive Theory of Involutivity

Cartan (1899, 1901): **Involutivity** of exterior PDEs.

Riquier (1910), Janet (1920), Thomas (1937): **Involutivity** of PDEs.

Spencer (1965), Kuranishi (1967), Goldschmidt (1969), Pommaret (1978): **Formal Theory** of differential systems.

Reid (1991): **Standard Form** of linear PDEs.

Wu (1991): **Relation** of Riquier-Janet theory **to Gröbner bases**.

Zharkov, Blinkov (1993): **Pommaret Bases** of polynomial ideals.

Reid, Wittkopf, Boulton (1996): **Reduced Involutive Form** of PDEs.

Gerdt, Blinkov (1995-1998): **Involutive Division** $\Longrightarrow$ general **Involutive Bases**.

Apel (1998): **Admissible Involutive Division** on a monomial set.

Gerdt (1999): **Involutive Systems of Linear PDEs**.

Seiler (2002): **Combinatorial Aspects of Involutivity**.

Chen, Gao (2002): **Involutive Characteristic Sets** for PDEs.

Hemmecke (2003): **Sliced Involutive Division**.

Evans (2004): **Noncommutative Involutive Bases**.

Gerdt, Blinkov (2005): **Janet-like Division**.

Implementation

Arais, Shapeev, Yanenko (1974): Cartan algorithm in **Auto-Analytik**.

Schwarz (1984): Riquier-Janet theory in **Reduce**.

Hartley, Tucker (1991): Cartan algorithm in **Reduce**.

Schwarz (1992): Linear differential Janet bases (DJB) in **Reduce**.

Reid, Wittkopf, Boulton (1993): Standard Form and Rif (2000) in **Maple**.

Seiler (1994): Formal theory in **Axiom**.

Zharkov, Blinkov (1993); G., Blinkov (1995): Pol. Pommaret bases (PPB) in **Reduce**.

Kredel (1996): PPB in **MAS**.

Nischke (1996): Polynomial JB (PJB) and PPB in **C++ (PoSSoLib)**.

Berth (1999): Polynomial and differential involutive bases in **Mathematica**.

Cid (2000)-Robertz (2002-2005): PJB, DJB and Difference JB in **Maple**.

Blinkov (2000-2005): PJB in **Reduce, C++**.

Yanovich (2001-2004): PJB in **C, Singular**.

Hausdorf, Seiler (2000-2002): DJB and DPB in **MuPAD**.

Chen, Gao (2002): Involutive Extended Characteristic Sets in **Maple**.

Hemmecke (2002): Sliced Division Algorithm in **Aldor**.

Evans (2005): Noncommutative Involutive Bases in **C**.

Involutive Division

Definition: (*G.,Blinkov'98*) An **involutive division** $\mathcal{L}$ of variables is defined on $\mathbb{M}$ if for any finite monomial set $U \subset \mathbb{M}$ and for any $u \in U$ there is defined a subset $M(u,U) \subseteq \mathbb{X} = \{x_1, \ldots, x_n\}$ of variables generating monoid $\mathcal{L}(u,U) \equiv \mathbb{M}_{M(u,U)}$ such that

1. $u, v \in U,\ u\mathcal{L}(u,U) \cap v\mathcal{L}(v,U) \neq \emptyset \Longleftrightarrow u \in v\mathcal{L}(v,U)$ or $v \in u\mathcal{L}(u,U)$.
2. $v \in U,\ v \in u\mathcal{L}(u,U) \Longleftrightarrow \mathcal{L}(v,U) \subseteq L(u,U)$.
3. $V \subseteq U \Longrightarrow \mathcal{L}(u,U) \subseteq \mathcal{L}(u,V)\ \ \forall u \in V$.

Variables in $M(u,U)$ are called ($\mathcal{L}-$)**multiplicative** for u and those in $NM(u,U) \equiv \mathbb{X} \setminus M(u,U)$ are ($\mathcal{L}-$)**nonmultiplicative** for u, respectively.

If $w \in u\mathcal{L}(u,U)$ then u is **involutive divisor** of w: $u \mid_{\mathcal{L}} w \Longrightarrow$ **involutive reduction** and **involutive normal form** $NF_{\mathcal{L}}(f,F)$ where $f \in \mathbb{R}$ and $F \subset \mathbb{R}$.

involutive separation $\Longleftrightarrow$ **involutive division** (*G., Blinkov*)

Janet Division

Definition: (*Janet'20, G.,Blinkov'98*) For each finite monomial set $U \subset \mathbb{M}$ and $0 \leq i \leq n$ partition U into groups labeled by $d_0, \ldots, d_i \in \mathbb{N}_{\geq 0}$ ($U = [0]$)

$$[d_0, d_1, \ldots, d_i] := \{u \in U \mid d_0 = 0, d_1 = \deg_1(u), \cdots, d_i = \deg_i(u)\}.$$

Variable x_i is ***J*-multiplicative** for $u \in U$ if $u \in [d_0, \ldots, d_{i-1}]$ and

$$\deg_i(u) = \max\{\deg_i(v) \mid v \in [d_0, \ldots, d_{i-1}]\}\,.$$

Notation: $\deg_i \equiv \deg_{x_i}, \quad u \sqsubset v \Longleftrightarrow u \mid v \ \wedge \ u \neq v$

Definition: (*Pommaret division*). For $v = x_1^{d_1} \cdots x_k^{d_k}$ with $d_k > 0$ $(k \leq n)$ the variables $x_j, j \geq k$ are **multiplicative** and the other variables are **nonmultiplicative**. For $v = 1$ all the variables are multiplicative.

Example: $lm(F) = \{x^2y, x^2z, xy^2, xz^2, y^3, yz, z^3\} \quad (x \succ y \succ z)$

Leading monomial	Janet separation of variables	
	nonmultiplicative	multiplicative
x^2y	$-$	x, y, z
x^2z	y	x, z
xy^2	x	y, z
xz^2	x, y	z
y^3	x	y, z
yz	x, y	z
z^3	x, y	z

Example: $U = \{x_1^2x_3, x_1x_2, x_1x_3^2\}$

Element in U	Separation of variables			
	Janet		Pommaret	
	M_J	NM_J	M_P	NM_P
$x_1^2x_3$	x_1, x_2, x_3	$-$	x_3	x_1, x_2
x_1x_2	x_2, x_3	x_1	x_2, x_3	x_1
$x_1x_3^2$	x_3	x_1, x_2	x_3	x_1, x_2

Definition: A monomial set $U \in \mathcal{M}$ is **$\mathcal{L}$-complete** or **$\mathcal{L}$-involutive** if

$$(\forall w \in \mathcal{M})\ (\forall u \in U)\ (\exists v \in U)\ \ [\ v \,|_{\mathcal{L}}\ u \cdot w\ ]$$

The corresponding J-and $P-$completion of $U = \{x_1^2x_3, x_1x_2, x_1x_3^2\}$

Janet : $\{x_1^2x_3, x_1x_2, x_1x_3^2, x_1^2x_2\}$,

Pommaret : $\{x_1^2x_3, x_1x_2, x_1x_3^2, x_1^2x_2, \ldots, x_1^{i+2}x_2, \ldots, x_1^{j+2}x_3, \ldots\}$

$\boxed{\textbf{The Pommaret division is non-Noetherian}}$

Gröbner and Involutive Bases

A finite set $F = \{f_1, \ldots, f_m\} \in \mathbb{R} := \mathcal{K}[x_1, \ldots, x_n]$ of multivariate polynomials is **a basis of the ideal** I

$$I =< F >= \{ \sum_{i=1}^{m} h_i f_i \mid h_j \in \mathbb{R} \}$$

Given a polynomial set F and **a linear monomial order** $\succ$ such that

$$(i)\ m \neq 1 \implies m \succ 1, \quad (ii)\ m_1 \succ m_2 \iff m_1 m \ \succ m_2 m$$

holds for any monomials m, m_1, m_2, one can select **the leading monomial** $lm(f)$ of any $f \in \mathbb{R}$ and define a **Gröbner basis** $G \subset \mathbb{R}$ of ideal $I =< G >$:

$$(\forall f \in I)\ (\exists g \in G)\ \ [\ lm(g) \mid lm(f)\ ]$$

Similarly, given an involutive division $\mathcal{L}$, an **involutive basis** H of I is defined as

$$(\forall f \in I)\ (\exists h \in H)\ \ [\ lm(g) \mid_{\mathcal{L}} lm(f)\ ]$$

An involutive $\mathcal{L}$-basis is a (generally redundant) **Gröbner basis with the $\mathcal{L}$-complete set of leading monomials**

Definition: Given a finite set $F \subset \mathbb{R}$, a polynomial $p \in \mathbb{R}$, and a monomial order $\succ$, a **normal form** $NF(p, F)$ of p modulo F is defined as

$$NF(p, F) = p' = p - \sum_{ij} \alpha_{ij} m_{ij} f_j$$

where $\alpha_{ij} \in \mathcal{K},\ f_j \in F,\ m_{ij} \in \mathcal{M},\ lm(m_{ij}g_j) \preceq lm(p)$ and there are no monomial in p' **multiple** of any leading monomial of elements in F.

Similarly, given an involutive division $\mathcal{L}$, an ($\mathcal{L}-$)**involutive normal form** $NF_{\mathcal{L}}(p, F)$ is defined. The only distinction is that in the latter case all the monomial factors m_{ij} must be $\mathcal{L}-$multiplicative for f_j, i.e. $m_{ij} \in \mathcal{L}(f_j, F)$, and p' cannot contain monomials $\mathcal{L}-$multiple of any leading monomials in F.

This yields another definition of a Gröbner (GB) G and an involutive (IB) basis H of ideal I:

$$\begin{aligned} \text{GB}: &\qquad p \in I \Longleftrightarrow NF(p, G) = 0\,, \\ \text{IB}: &\qquad p \in I \Longleftrightarrow NF_{\mathcal{L}}(p, H) = 0\,. \end{aligned}$$

IB can be computed by the following Involutive algorithm (*G.,Blinkov'98*) for any (noetherian) involutive division:

Buchberger algorithm:
Start with $G := F$.
For a pair of polynomials $f_1, f_2 \in G$:
  Compute $S(f_1, f_2)$.
  Compute $h := NF(S(f_1, f_2), G)$.
  If $h = 0$, consider the next pair.
  If $h \neq 0$, add h to G and iterate.

$S(f_1, f_2) = c_1 t_1 f_1 - c_2 t_2 f_2,\ c_1, c_2 \in \mathcal{K}$, $t_1, t_2 \in \mathcal{M},\ \ c_1 t_1 lm(f_1) = c_2 t_2 lm(f_2)$.

Involutive algorithm:
Start with $G := F$.
Choose a pair of $f \in G, x \in NM_{\mathcal{L}}(f, G)$ with minimal $lm(f \cdot x)$ w.r.t. $\succ$:
  Compute $h := NF_{\mathcal{L}}(f \cdot x, G)$.
  If $h = 0$, consider the next pair.
  If $h \neq 0$, add h to G and iterate.

N.B. For linear PDEs instead of $f \cdot x$ one should take $\partial_x(f)$.

Algorithm: Involutive Basis $(F, \prec, \mathcal{L})$

Input: F, a polynomial set; $\prec$, a monomial order; $\mathcal{L}$, an involutive division
Output: G, a **minimal** involutive basis of $\mathrm{Id}(F)$

choose $f \in F$ without $g \in F \setminus \{f\} \,:\, \mathrm{lm}(g) \sqsubset \mathrm{lm}(f)$; $G := \{f\}$; $Q := F \setminus G$
do
    $h := 0$
    while $Q \neq \emptyset$ and $h = 0$ **do**
        choose $p \in Q$ without $q \in Q \setminus \{f\} \,:\, \mathrm{lm}(q) \sqsubset \mathrm{lm}(p)$
        $Q := Q \setminus \{p\}$; $h := NF_{\mathcal{L}}(p, T)$
    od
    if $h \neq 0$ **then**
        for all $\{g \in G \mid lm(g) \sqsupset lm(h)\}$ **do**
            $Q := Q \cup \{g\}$; $G := G \setminus \{g\}$
        od
        $G := G \cup \{h\}$; $Q := Q \cup \{\, g \cdot x \mid g \in G,\, x \in NM_{\mathcal{L}}(g, G)\,\}$
    fi
od while $Q \neq \emptyset$ **return** G

Table 1: Computation of Janet basis for $F = \{x^2y - 1, xy^2 - 1\}$

Steps of algorithm	Sets G and Q		
	elements in G	NM_J	Q
initialization	$xy^2 - 1$	$-$	$\{x^2y - 1\}$
iteration	$x^2y - 1$ $xy^2 - 1$	$-$ x	$\{x^2y^2 - x\}$
	$x - y$	$-$	$\{xy^2 - 1, x^2y - 1\}$
	$x - y$ $y^3 - 1$	$-$ x	$\{x^2y - 1, xy^3 - x\}$
	$x - y$ $y^3 - 1$	$-$ x	$\{\ \}$

Some optimizations

To avoid useless repeated prolongations and to apply the involutive analogues of the Buchberger criteria one has to keep the history of computation.

Definition: An **ancestor** of a polynomial $f \in F \subset \mathbb{R} \setminus \{0\}$ is a polynomial $g \in F$ of the smallest $\deg(\mathrm{lm}(g))$ among those satisfying $f = g \cdot u$ modulo $\mathrm{Id}(F \setminus \{f\})$ with $u \in \mathbb{M}$. If $\deg(\mathrm{lm}(g)) < \deg(\mathrm{lm}(f))$ $(u \neq 1)$ the ancestor g of f is called **proper**.

Remark: If an intermediate polynomial h that arose in the course of a completion algorithm has a proper ancestor g, then h has been obtained from g via a sequence of $\mathcal{L}$-head irreducible non-multiplicative prolongations. For the ancestor g itself the equality $\mathrm{lm}(\mathrm{anc}(g)) = \mathrm{lm}(g)$ holds.

Let now every element $f \in F$ in the intermediate set of polynomials be endowed with the triple structure

$$p = \{f,\, g,\, vars\}$$

where

$$\begin{array}{lcl} \mathrm{pol}(p) & = & f \ \text{ is the polynomial } f \text{ itself,} \\ \mathrm{anc}(p) & = & g \ \text{ is a polynomial ancestor of } f \text{ in } F, \\ \mathrm{nmp}(p) & = & vars \ \text{ is a (possibly empty) subset of variables.} \end{array}$$

The set $vars$ associated with polynomial f accumulates those non-multiplicative variables of f have been already used in the algorithm for construction of non-multiplicative prolongations. It keeps information on non-multiplicative prolongations of polynomial f that have been already examined in the course of completion and serves to avoid useless repeated prolongations.

Remark: The reduced GB is a subset of IB containing all the polynomials which have no proper ancestors. Due to the above triple structure associated with intermediate polynomials, the reduced GB is an internally fixed subset of IB. Therefore, having IB computed, the reduced GB is extracted without any extra computational costs.

Computational Peculiarities of Janet Division Algorithm

Pro's: (*G.'05*)

Automatic avoidance of some useless critical pairs

Table 2: Example of avoidance of such a pair

Polynomial	NM_J	Prolongation	$S-$polynomial
$p_1 = xy - 1$	–	–	–
$p_2 = xz - 1$	y	$y\,p_2$	$S(p_2, p_1) = y\,p_2 - z\,p_1$
$p_3 = yz - 1$	x	$x\,p_3$	$S(p_3, p_1) = x\,p_3 - z\,p_1$

Weakened role of criteria

Table 3: Timings for C code (Opteron 242 computer)

Example	Applicability				Timing (sec.)				
	C_1	C_2	C_3	C_4	–	C_1	$C_{1\div 2}$	$C_{1\div 3}$	$C_{1\div 4}$
Cyclic6	98	2	4	–	0.18	0.14	0.13	0.13	0.12
Cyclic7	698	190	22	–	85.18	63.82	58.61	58.14	58.72
Katsura8	173	1	1	–	32.16	27.59	26.92	27.08	27.48
Katsura9	344	–	1	–	402.38	335.50	332.94	335.69	337.52
Cohn3	–	114	169	7	90.20	90.32	87.66	76.05	76.72
Assur44	89	60	171	3	12.39	12.28	11.95	10.29	10.35
Reimer6	63	235	179	12	35.49	38.56	21.93	9.42	9.69
Reimer7	327	1723	497	71	9385.17	9817.16	3290.06	714.08	719.37
Hairer2	3766	1158	256	91	2107.24	246.90	104.80	70.02	62.91

$C_1 \wedge C_2 \wedge C_3 \wedge C_4 \Longleftrightarrow$ Buchberger criteria (*Apel, Hemmecke'02*)

Smooth growth of intermediate coefficients

Example: (*Arnold'03*) Consider ideal $\mathcal{I} = Id(F)$ in $\mathbb{Q}[x, y, z]$ generated by the polynomial set:

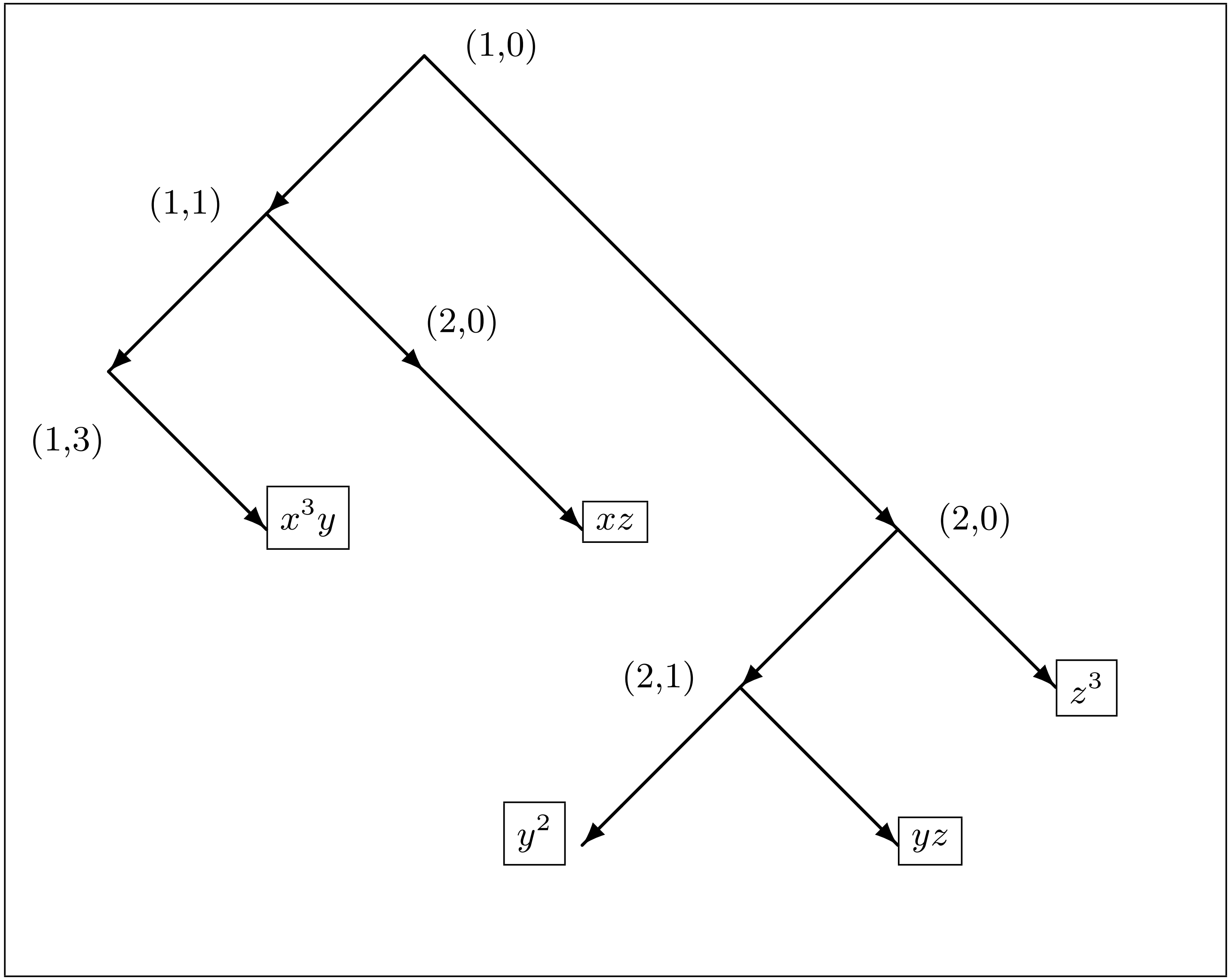
$$F = \begin{cases} 8\,x^2y^2 + 5x\,y^3 + 3x^3z + x^2y\,z, \\ x^5 + 2\,y^3z^2 + 13\,y^2\,z^3 + 5\,y\,z^4, \\ 8\,x^3 + 12\,y^3 + x\,z^2 + 3, \\ 7\,x^2y^4 + 18\,x\,y^3z^2 + y^3z^3. \end{cases}$$

Its Gröbner basis for the degree-reverse-lexicographical order with $x \succ y \succ z$ is small $G = \{x, 4\,y^3 + 1, z^2\}$ whereas in the course of Buchberger's algorithm, as it implemented in Macaulay 2, there arise intermediate coefficients with about **80,000 digits**. As to algorithm **Involutive Basis II**, it outputs Gröbner basis G or Janet basis $\{x, 4\,y^3 + 1, z^2, y\,z^2, y^2z^2\}$, with not more than **400 digits** in the intermediate coefficients.

Table 4: Coefficient size in 64 bit words

Example	Input	Intermediate	Output	Swell factor
Cyclic6	1	3	1	3.00
Cyclic7	1	11	5	2.20
Katsura8	1	5	4	1.25
Katsura9	1	8	6	1.33
Cohn3	1	168	19	8.84
Assur44	1	93	19	4.89
Reimer6	1	4	4	1.00
Reimer7	1	10	10	1.00
Hairer2	1	10	6	1.00

Fast search for Janet divisor (Janet tree)



Comparison with Binary Search

Let d be the maximal total degree of the leading monomials of polynomials in n variables which constitute the finite set F.

Then the complexity bound of the search for a Janet divisor in the Janet tree and the binary search algorithm is given by

$$\begin{aligned} t_{\mathbf{J-divisor}} &= O(d+n), \\ t_{\mathbf{BinarySearch}} &= O(n((d+n)\log(d+n) - n\log(n) - d\log(d))). \end{aligned}$$

Uniqueness of reduction sequence

By properties of an involutive division $\mathcal{L}$, any monomial may have at most one $\mathcal{L}$-devisor among the leading monomials of the intermediate basis G. Thereby, the reduction sequence is unique.

Parallelism

Table 5: Timings (in seconds) and speedup due to parallelism

Example	1 Thread	3 Threads	Speedup	$t_{1\,th}/t_{3\,th}$
Cyclic6	0.79	1.16	-0.37	0.68
Cyclic7	386.89	182.86	+294.03	2.12
Katsura8	119.92	53.72	+66.20	2.23
Katsura9	1356.37	587.82	+768.55	2.31
Cohn3	554.75	222.69	+332.06	2.49
Assur44	73.93	31.34	+42.59	2.36
Reimer6	88.99	52.56	+36.43	1.69

<u>Con's</u> (*G.,Blinkov'02*)

Example 1: Toric ideal I (*Bigatti, Scala, Robbiano'99*) $(x \succ y \succ z \succ w)$.

$$\{\ x^7 - y^2 z, x^4 w - y^3, x^3 y - zw\ \}.$$

Example 2: Polynomial ideal (*Gräbe, Hemmecke*) $(w \succ x \succ y \succ z)$.

$$\{\ z^{20} + z^{10} - x^2, z^{30} + z^{10} - x\,y^3, w^{40} x^4 - y^6\ \}.$$

Example 3: Toric ideal II (*Morales*) $(x_0 \succ x_1 \succ x_2 \succ x_3 \succ x_4)$.

$$\{\ x_0 x_1 x_2 x_3 x_4 - 1, x_2^{29} x_3^5 - x_1^{14} x_4^{20}, x_1^{39} - x_2^{25} x_3^{14}\ \}.$$

Example 4: Toric ideal III (*Morales'95*) $(x \succ y \succ z \succ w)$.

$$\{\ y^{250} - x^{239} z^{11},\ x^{150} z^{12} - y^{161} w,\ y^{89} z - x^{89} w\, x^{61} z^{13} - y^{72} w^2,$$
$$x^{33} z^{27} - y^{55} w^5,\ z^{55} - x^{23} y^{21} w^{11},\ x^5 z^{41} - y^{38} w^8,\ y^{17} z^{14} - x^{28} w^3\ \}.$$

Table 6: Cardinalities of Gröbner and Janet bases for Examples 1 - 4

Example	Cardinality	
	Gröbner basis	Janet basis
1	4	11
2	9	983
3	19	7769
4	8	37901

Janet-like Division

Definition: (*G.,Blinkov'05*) Let $U \subset \mathbb{M}$ be a monomial set and its elements be partitioned into groups as for the Janet division. For every $u \in U$ and $1 \le i \le n$ consider

$$h_i(u, U) := \max\{\deg_i(v) \mid u, v \in [d_0, \ldots, d_{i-1}]\} - \deg_i(u).$$

If $h_i(u, U) > 0$, then the power $x_i^{k_i}$ where

$$k_i := \min\{\deg_i(v) - \deg_i(u) \mid v, u \in [d_0, \ldots, d_{i-1}],\ \deg_i(v) > \deg_i(u)\}$$

is a **nonmultiplicative power** for u.

Notation: $NMP(u, U)$ is the set of all nonmultiplicative powers for $u \in U$.

Definition: (**Janet-like division**). For a set $U \subset \mathbb{M}$ and $u \in U$, elements of the monoid ideal

$$\mathcal{NM}(u, U) := \{v \in \mathbb{M} \mid \exists w \in NMP(u, U) : w \mid v\}$$

are **$\mathcal{J}$-nonmultipliers** for $u \in U$. Elements in $\mathcal{M}(u, U) := \mathbb{M} \setminus \mathcal{NM}(u, U)$ are **$\mathcal{J}$-multipliers** for u, respectively. $u \in U$ is a **Janet-like divisor or $\mathcal{J}-$divisor** of $w \in \mathbb{M}$ (denotation $u \mid_{\mathcal{J}} w$) if $w = u \cdot v$ with $v \in \mathcal{M}(u, U)$.

Example: $U = \{x_1^5, x_1^2x_2^2x_3, x_1^2x_3^2, x_2^4x_3, x_2x_3^2, x_3^5\} \subset \mathbb{K}[x_1, x_2, x_3]$.

Table 7: Comparison with Janet division

Element in U	Division		
	Janet		Janet-like
	M_J	NM_J	NMP
x_1^5	x_1, x_2, x_3	$-$	$-$
$x_1^2x_2^2x_3$	x_2, x_3	x_1	x_1^3
$x_1^2x_3^2$	x_3	x_1, x_2	x_1^3, x_2^2
$x_2^4x_3$	x_2, x_3	x_1	x_1^2
$x_2x_3^2$	x_3	x_1, x_2	x_1^2, x_2^3
x_3^5	x_3	x_1, x_2	x_1^2, x_2

Corollary: $u \,|_J\, w \Longrightarrow u \,|_{\mathcal{J}}\, w$. The converse is generally not true.

Remark: Janet-like division **is not involutive** division since $\mathcal{M}(u, U)$ is not monoid. However, this division possesses all the above listed attractive algorithmic properties of the Janet division.

Definition: (**Janet-like basis**) Let $\mathcal{I} \subset \mathbb{R}$ be a nonzero ideal and $\succ$ be a monomial order. Then a minimal $\mathcal{J}$-autoreduced subset $G \subset \mathbb{R}$ such that $\mathcal{I} = Id(G)$ is **Janet-like basis (JLB) or $\mathcal{J}-$basis of** $\mathcal{I}$ if

$$\forall f \in \mathcal{I},\ \exists g \in G\ :\ \mathrm{lm}(g) \,|_{\mathcal{J}}\, \mathrm{lm}(f)\,.$$

From the above corollary it follows

$$\mathrm{card}(GB) \leq \mathrm{card}(JLB) \leq card(JB) \quad \overset{monicity}{\Longrightarrow} \quad GB \subseteq JLB \subseteq JB$$

Table 8: Cardinalities of bases for Examples 1-4

Example	Cardinality		
	Gröbner basis	Janet-like basis	Janet basis
1	4	5	11
2	9	14	983
3	19	190	7769
4	8	18	37901

Selection Strategy

Apart from improvement of the division, there is another important source of optimization in the involutive algorithms: **selection of non-multiplicative prolongations** that (when $\mathcal{L}$-head reducible) play in the involutive approach the same role as $S-$polynomials play in Buchberger's algorithm.

Though in the involutive approach an admissible choice of a non-multiplicative prolongation is subject to certain restrictions, **for examples large enough, one can choose from many possible prolongations**. For example, in the 7th order cyclic root example at the intermediate algorithmic steps there arise several hundreds prolongations such that any of them can be chosen. By this reason it is important to investigate a heuristical efficiency of different selection strategies.

Below we present three different selection strategies which as we recently found (*G., Blinkov'06*) are computationally good for the Janet division. In so going, **we restrict ourselves with degree compatible orders**. Due to the **FGLM** and **Gröbner walk** conversion algorithms, this is a reasonable restriction.

Janet Division Algorithm: Strategy I ($F \in \mathbb{R} \setminus \{0\}$, degree compatible $\prec$)

choose $f \in F$ of the minimal $\deg(\mathrm{lm}(f))$; $G := \{f\}$; $Q := F \setminus G$
do
  $S := \{\, q \in Q \mid \deg(\mathrm{lm}(q)) = \mathrm{mindeg}(\mathrm{lm}(Q))\,\}$; $P := \emptyset$; $Q := Q \setminus S$
  for all $s \in S$ **do**
    $S := S \setminus \{s\}$; $p := HNF_J(s, G)$ /* *Head Normal Form* */
    if $p \neq 0$ **then**
      $P := P \cup \{p\}$
    fi
  od
  while $P \neq \emptyset$ **do**
    choose $p \in P$ with minimal $\mathrm{lm}(p)$ w.r.t. $\succ$; $P := P \setminus \{p\}$; $h := NF_J(p, G)$
    for all $\{g \in G \mid \mathrm{lm}(g) \sqsupset \mathrm{lm}(h)\}$ **do**
      $Q := Q \cup \{g\}$; $G := G \setminus \{g\}$
    od
    $G := G \cup \{h\}$; $Q := Q \cup \{\, g \cdot x \mid g \in G,\ x \in NM_J(\mathrm{lm}(g), \mathrm{lm}(G))\,\}$
  od
od while $Q \neq \emptyset$
return $G := \{\ g \in G\ :\ g = \mathrm{anc}(g)\ \}$ /* *reduced GB* */

Janet Division Algorithm: Strategy II ($F \in \mathbb{R} \setminus \{0\}$, degree compatible $\prec$)

choose $f \in F$ of the minimal $\deg(\mathrm{lm}(f))$; $G := \{f\}$; $Q := F \setminus G$
do
  $S := \{\, q \in Q \mid \deg(\mathrm{lm}(q)) = \mathrm{mindeg}(\mathrm{lm}(Q)) \,\}$; $P := \emptyset$; $Q := Q \setminus S$
  for all $s \in S$ **do**
    $S := S \setminus \{s\}$; $p := NF_J(s, G)$ /* *Full Normal Form* */
    if $p \neq 0$ **then**
      $P := P \cup \{p\}$
    fi
  od
  $P :=$ **Update**$(P, \prec)$
  for all $p \in P$ **do**
    for all $\{g \in G \mid \mathrm{lm}(g) \sqsupset \mathrm{lm}(p)\}$ **do**
      $Q := Q \cup \{g\}$; $G := G \setminus \{g\}$
    od
    $G := G \cup \{p\}$; $Q := Q \cup \{\, g \cdot x \mid g \in G,\ x \in NM_J(\mathrm{lm}(g), \mathrm{lm}(G)) \,\}$
  od
od while $Q \neq \emptyset$
return $G := \{\ g \in G\ :\ g = \mathrm{anc}(g)\ \}$ /* *reduced GB* */

Algorithm: Update$(P, \succ)$

Input: $P \subset \mathbb{R} \setminus \{0\}$, a finite set; $\succ$, an order
Output: $H \subset \mathbb{R} \setminus \{0\}$, an updated input set

```
 1: choose f ∈ P with the highest/lowest lm(f) w.r.t. ≻
 2: H := {f};   P := P \ {f}
 3: while P ≠ ∅ do
 4:    choose p ∈ P with the highest/lowest lm(p) w.r.t. ≻
 5:    P := P \ {p}
 6:    h := NF_J(p, H)
 7:    if h ≠ 0 then
 8:       H := H ∪ {h}
 9:    fi
10: od
11: return H
```

Benchmarking

Strategy I was implemented in C as a part of package **JB** (*Yanovich'02*) whose version is also included in the library of Singular, and in the C++ as a part of the open source software **GINV** (**G**röbner **INV**olutive) (*Blinkov'05*). The last software implements also **Strategy II** for both options in subalgorithm **Update**.

The timings in the following table were obtained on the following machines:

JB: 2xOpteron-242 (1.6 Ghz) with 4Gb of RAM running under Gentoo Linux 2004.3 with gcc-3.4.2 compiler.

GINV: Turion-3400 (1.8 Ghz) with 2Gb of RAM running under Gentoo Linux 2005.1 with gcc-3.4.4 compiler.

Magma: dual processor Pentium III (1 Ghz) with 2 GB of RAM running under SuSE Linux 8.0 (kernel 2.4.18-64GB-SMP) with gcc-2.95.3 compiler.

All timings in the table are given in seconds, and (*) shows that the example was not computed because of the memory overflow.

Timings

Example	Strategy I (JB)	Strategy I (GINV)	Strategy II high (GINV)	Strategy II low (GINV)	Magma V2.11-8	Magma V2.12-17
assur44	10.35	14.20	6.33	6.4	4.56	4.99
butcher8	1.06	1.02	0.38	0.39	4.68	5.00
chemequs	0.67	0.61	0.57	0.6	12.80	11.99
chemkin	17.83	16.87	10.95	9.95	32.34	29.83
cohn3	76.72	107.14	30.21	25.47	37.73	39.20
cpdm5	1.78	1.57	1.69	1.68	0.69	0.70
cyclic6	0.12	0.19	0.14	0.14	0.09	0.08
cyclic7	58.72	60.94	68.59	65.28	6.64	7.08
cyclic8	12056.24	14046.26	5826.18	4424.96	235.73	245.65
d1	8.77	12.58	1.99	2.08	28.49	8.29
des18_3	0.19	0.18	0.19	0.19	1.81	1.89
des22_24	0.68	0.62	0.77	0.79	1.37	1.46
discret3	23322.8	20956.31	12642.49	13521.65	33658.09	19369.53
dl	270.17	278.89	80.77	89.52	14.57	11.95
eco8	0.40	0.44	0.44	0.46	0.20	0.20
eco9	3.22	5.60	4.99	5.08	1.25	1.20
eco10	52.56	56.70	65.71	68.06	7.07	6.91
eco11	765.98	741.74	718.53	679.3	62.33	51.08
extcyc5	1.35	1.53	1.46	1.37	0.37	0.38
extcyc6	324.70	184.49	276.06	155.64	45.36	47.96

Timings (cont.)

Example	Strategy I (JB)	Strategy I (GINV)	Strategy II high (GINV)	Strategy II low (GINV)	Magma V2.11-8	Magma V2.12-17
extcyc7	*	*	*	*	8242.00	8492.13
f744	4.88	7.71	2.22	2.68	1.47	1.38
f855	132.97	139.79	37.64	38.45	48.63	37.06
fabrice24	108.52	116.77	8.2	7.7	9.45	8.70
filter9	20.97	5.76	1.13	1.6	80.04	56.67
hairer2	62.91	108.17	126.69	125.43	92.07	85.86
hairer3	1.96	0.92	0.32	1.4	*	*
hcyclic7	64.17	53.87	65.81	73.0	6.26	6.76
hcyclic8	6024.97	4316.59	*	7560.99	229.70	237.12
hf744	22.17	8.58	7.18	11.26	1.39	1.32
hf855	2157.88	534.08	806.51	988.38	48.15	36.69
hietarinta1	0.77	0.71	0.38	0.53	2.63	2.15
i1	98.24	122.36	58.29	58.21	55.07	42.35
ilias13	1167.18	5851.97	3013.1	2469.62	336.21	309.64
ilias_k_2	323.59	669.68	445.51	270.21	55.41	54.71
ilias_k_3	452.32	846.19	1162.7	622.14	90.67	89.97
jcf26	224.96	211.24	16.44	14.65	31.64	25.59
katsura7	2.15	1.77	2.08	1.98	0.72	0.79
katsura8	27.48	24.66	28.8	27.09	4.7	5.06
katsura9	337.52	294.59	340.45	311.98	33.47	34.87

Timings (cont.)

Example	Strategy I (JB)	Strategy I (GINV)	Strategy II high (GINV)	Strategy II low (GINV)	Magma V2.11-8	Magma V2.12-17
katsura10	4790.55	4983.11	7220.29	6204.95	287.38	292.02
kin1	15.18	20.32	7.11	7.11	50.56	45.33
kotsireas	6.33	37.94	4.93	4.27	3.45	3.67
noon6	0.97	1.29	1.27	1.29	0.60	0.62
noon7	28.87	32.58	37.52	38.52	4.93	4.77
noon8	1552.26	2292.84	3322.62	3152.57	43.65	42.80
pinchon1	10.37	0.04	0.01	0.01	4.09	3.54
rbpl	210.94	177.51	173.8	173.98	38.33	35.79
rbpl24	108.78	116.78	8.23	7.7	9.62	8.74
redcyc6	0.16	0.17	0.13	0.14	0.10	0.10
redcyc7	913.75	1048.69	48.19	48.61	5.73	6.36
redeco10	18.51	18.66	23.91	22.4	2.33	2.40
redeco11	178.32	187.36	253.34	228.41	14.56	14.85
redeco12	1735.95	2172.75	4666.8	3385.97	101.51	103.02
reimer5	0.22	0.36	0.34	0.38	0.74	0.70
reimer6	9.69	21.60	24.19	23.96	42.13	42.40
reimer7	719.37	3808.91	4756.4	4314.12	5216.53	5032.73
virasoro	9.69	8.90	10.96	10.68	1.72	1.77

Conclusion

- Our involutive Janet division algorithm is rather efficient in computing GB.
- Some useless critical pairs ($S-$polynomials) are automatically avoided.
- The intermediate coefficients growth is smoothed.
- The role of criteria is weakened. Even without any criteria the algorithm works reasonably fast.
- Janet trees form the data structures providing very fast search for involutive divisor which is unique.
- The algorithm admits an effective parallelization.
- Janet-like division improves the Janet division.
- Having JB computed, the reduced GB is extracted from JB without any extra computational costs.
- Experimenting with three different selection strategies shows rather good stability of the algorithm.
- Our publications, computer experiments and GINV software are available on the Web: `http://invo.jinr.ru`