Available online at www.sciencedirect.com
SCIENCE DIRECT®

Nuclear Instruments and Methods in Physics Research A 559 (2006) 211–214

NUCLEAR INSTRUMENTS & METHODS IN PHYSICS RESEARCH
Section A

www.elsevier.com/locate/nima

On computation of Gröbner bases for linear difference systems

Vladimir P. Gerdt*

Laboratory of Information Technologies, Joint Institute for Nuclear Research, 141980 Dubna, Russia

Available online 15 December 2005

Abstract

In this paper, we present an algorithm for computing Gröbner bases of linear ideals in a difference polynomial ring over a ground difference field. The input difference polynomials generating the ideal are also assumed to be linear. The algorithm is an adaptation to difference ideals of our polynomial algorithm based on Janet-like reductions.

PACS: 02.10.Hh; 02.70.Bf; 11.15.Bt

Keywords: Difference algebra; Janet-like Grobner bases; Computer algebra; Difference schemes; Recurrence relations; Feynman integrals

1. Introduction

Being invented 40 years ago by Buchberger [1] for algorithmic solving of the membership problem in the theory of polynomial ideals, the Gröbner bases method has become a powerful universal algorithmic tool for solving various mathematical problems arising in science and engineering.

Though overwhelming majority of the Gröbner bases applications is still found in commutative polynomial algebra, over the last decade a substantial progress has also been achieved in application of Gröbner bases to non-commutative polynomial algebra, to algebra of differential operators and to linear partial differential equations (see, for example, Ref. [2]). As to the difference algebra, i.e. algebra of difference polynomials, in spite of its conceptual algorithmic similarity to differential algebra, only a few efforts have been done to extend the theory of Gröbner - bases to difference algebra and to exploit their algorithmic power [3,4].

Recently, two promising applications of difference Gröbner bases were revealed: generation of difference schemes for numerical solving of PDEs [5,6] and reduction of multiloop Feynman integrals to the minimal set of basis integrals [7].

In this note we describe an algorithm (Section 4) for constructing Gröbner bases for linear difference systems that is an adaptation of our polynomial algorithm [8] to linear difference ideals. We construct a Gröbner basis in its Janet-like form (Section 3), since this approach has shown its computational efficiency in the polynomial case [8,9]. We briefly outline these efficiency issues in Section 5. The difference form of the algorithm exploits some basic notions and concepts of difference algebra (Section 2) as well as the definition of Janet-like Gröbner bases and Janet-like reductions together with the algorithmic characterization of Janet-like bases (Section 3). We conclude in Section 6.

2. Elements of difference algebra

Let $\{y^1, \ldots, y^m\}$ be the set of *indeterminates*, for example, functions of n-variables $\{x_1, \ldots, x_n\}$, and $\theta_1, \ldots, \theta_n$ be the set of mutually commuting *difference operators* (*differences*), e.g.

$$\theta_i \circ y^j = y^j(x_1, \ldots, x_i + 1, \ldots, x_n).$$

A *difference ring* R *with differences* $\theta_1, \ldots, \theta_n$ is a commutative ring R such that $\forall f, g \in R,\ 1 \leqslant i,\ j \leqslant n$

$$\theta_i\theta_j = \theta_j\theta_i,\ \theta_i \circ (f+g) = \theta_i \circ f + \theta_i \circ g,$$
$$\theta_i \circ (f\, g) = (\theta_i \circ f)(\theta_i \circ g).$$

Similarly, one defines a *difference field*.

*Tel.: +7 09621 63437.
E-mail address: gerdt@jinr.ru.

0168-9002/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.nima.2005.11.141

Let $\mathbb{K}$ be a difference field, and $\mathbb{R} := \mathbb{K}\{y^1, \ldots, y^m\}$ be the difference ring of polynomials over $\mathbb{K}$ in variables

$$\{\theta^\mu \circ y^k \mid \mu \in \mathbb{Z}^n_{\geqslant 0},\ k = 1, \ldots, m\}.$$

Hereafter, we denote by $\mathbb{R}_{\mathrm{L}}$ the set of linear polynomials in $\mathbb{R}$ and use the notations:

$$\Theta = \{\theta^\mu \mid \mu \in \mathbb{Z}^n_{\geqslant 0}\}, \quad \deg_i(\theta^\mu \circ y^k) = \mu_i,$$

$$\deg(\theta^\mu \circ y^k) = |\mu| = \sum_{i=1}^{n} \mu_i.$$

A *difference ideal* is an ideal $I \subseteq \mathbb{R}$ closed under the action of any operator from Θ. If $F := \{f_1, \ldots, f_k\} \subset \mathbb{R}$ is a finite set, then the smallest difference ideal containing F will be denoted by $\mathrm{Id}(F)$. If for an ideal I there is $F \subset \mathbb{R}_{\mathrm{L}}$ such that $I = \mathrm{Id}(F)$, then I is a *linear difference ideal*.

A total ordering $\succ$ on the set of $\theta^\mu \circ y^j$ is a *ranking* if $\forall i, j, k, \mu, \nu$ the following hold:

$$\theta_i \theta^\mu \circ y^j \succ \theta^\mu \circ y^j,$$

$$\theta^\mu \circ y^j \succ \theta^\nu \circ y^k \Longleftrightarrow \theta_i \theta^\mu \circ y^j \succ \theta_i \theta^\nu \circ y^k.$$

If $\mu \succ \nu \Longrightarrow \theta^\mu \circ y^j \succ \theta^\nu \circ y^k$ the ranking is *orderly*. If $j \succ k \Longrightarrow \theta^\mu \circ y^j \succ \theta^\nu \circ y^k$ the ranking is *elimination*.

Given a ranking $\succ$, a linear polynomial $f \in \mathbb{R}_{\mathrm{L}} \setminus \{0\}$ has the *leading term* $a\vartheta \circ y^j$, $\vartheta \in \Theta$, where $\vartheta \circ y^j$ is maximal w.r.t. $\succ$ among all $\theta^\mu \circ y^k$ which appear with nonzero coefficient in f. $\mathrm{lc}(f) := a \in \mathbb{K} \setminus \{0\}$ is the *leading coefficient* and $\mathrm{lm}(f) := \vartheta \circ y^j$ is the *leading monomial*.

A ranking acts in $\mathbb{R}_{\mathrm{L}}$ as a *monomial order*. If $F \subseteq \mathbb{R}_{\mathrm{L}} \setminus \{0\}$, $\mathrm{lm}(F)$ will denote the set of the leading monomials and $\mathrm{lm}_j(F)$ will denote its subset for indeterminate y^j. Thus, $\mathrm{lm}(F) = \cup_{j=1}^{m} \mathrm{lm}_j(F)$.

3. Janet-like Gröbner bases

Given a non-zero linear difference ideal $I = \mathrm{Id}(G)$ and a ranking $\succ$, the ideal generating set $G = \{g_1, \ldots, g_s\} \subset \mathbb{R}_{\mathrm{L}}$ is a *Gröbner basis* [2,4] of I if $\forall f \in I \cap \mathbb{R}_{\mathrm{L}} \setminus \{0\}$:

$$\exists g \in G, \theta \in \Theta : \mathrm{lm}(f) = \theta \circ \mathrm{lm}(g). \tag{1}$$

It follows that $f \in I \setminus \{0\}$ *is reducible modulo* G:

$$f \underset{g}{\to} f' := f - \mathrm{lc}(f)\, \theta \circ (g/\mathrm{lc}(g)), \quad f' \in I.$$

If $f' \neq 0$, then it is again reducible modulo G, and, by repeating the reduction, in finitely many steps we obtain

$$f \underset{G}{\to} 0.$$

Similarly, a non-zero polynomial $h \in \mathbb{R}_{\mathrm{L}}$, whose terms are reducible (if any) modulo a set $F \subset \mathbb{R}_{\mathrm{L}}$, can be reduced to an irreducible polynomial $\bar{h}$, which is said to be in the *normal form modulo* F (denotation: $\bar{h} = NF(h, F)$).

In our algorithmic construction of Gröbner bases we shall use a restricted set of reductions called *Janet-like* (cf. [8]) and defined as follows.

For a finite set $F \subseteq \mathbb{R}_{\mathrm{L}}$ and a ranking $\succ$, we partition every $\mathrm{lm}_k(F)$ into groups labeled by $d_0, \ldots, d_i \in \mathbb{Z}_{\geqslant 0}$, $(0 \leqslant i \leqslant n)$. Here $[0]_k := \mathrm{lm}_k(F)$ and for $i > 0$ the group $[d_0, \ldots, d_i]_k$ is defined as

$$\{u \in \mathrm{lm}_k(F) \mid d_0 = 0, d_j = \deg_j(u), 1 \leqslant j \leqslant i\}.$$

Denote by $h_i(u, \mathrm{lm}_k(F))$ the non-negative integer

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

If $h_i(u, \mathrm{lm}_k(F)) > 0$, then $\theta_i^{s_i}$ such that

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

is called a *difference power* for $f \in F$ with $\mathrm{lm}(f) = u$.

Let $DP(f, F)$ be the set of difference powers for $f \in F$, and $\mathscr{J}(f, F) := \Theta \setminus \bar{\Theta}$ be the subset of Θ with

$$\bar{\Theta} := \{\theta^\mu \mid \exists\, \theta^\nu \in DP(f, F) : \mu - \nu \in \mathbb{Z}^n_{\geqslant 0}\}.$$

A Gröbner basis G of $I = \mathrm{Id}(G)$ is called Janet-like [8] if $\forall f \in I \cap \mathbb{R}_{\mathrm{L}} \setminus \{0\}$:

$$\exists\, g \in G, \theta \in \mathscr{J}(g, G) \ :\ \mathrm{lm}(f) = \theta \circ \mathrm{lm}(g). \tag{2}$$

This implies $\mathscr{J}$-reductions and the $\mathscr{J}$-normal form $NF_{\mathscr{J}}(f, F)$. It is clear that condition (2) implies (1). Note, however, that the converse is generally not true. Therefore, not every Gröbner basis is Janet-like.

The properties of a Janet-like basis are very similar to those of a Janet basis [9], but the former is generally more compact than the latter. More preciously, let GB be a reduced Gröbner basis [2], JB be a minimal Janet basis, and JLB be a minimal Janet-like basis of the same ideal for the same ranking. Then their cardinalities satisfy

$$\mathrm{Card}(GB) \leqslant \mathrm{Card}(JLB) \leqslant \mathrm{Card}(JB) \tag{3}$$

where Card abbreviates *cardinality*, that is, the number of elements.

Whereas the algorithmic characterization of a Gröbner basis is zero redundancy of all its S-polynomials [1,2], the algorithmic characterization of a Janet-like basis G is the following condition (cf. [8]):

$$\forall g \in G, \vartheta \in DP(g, G) :\ NF_{\mathscr{J}}(\vartheta \circ g, G) = 0. \tag{4}$$

This condition is at the root of the algorithmic construction of Janet-like bases as described in the next section.

4. ALGORITHM

Algorithm: Janet-like Gröbner Basis$(F, \succ)$

Input: $F \subseteq \mathbb{R}_{\mathrm{L}} \setminus \{0\}$, a finite set; $\succ$, a ranking
Output: G, a Janet-like basis of $\mathrm{Id}(F)$
choose $f \in F$ with the lowest $\mathrm{lm}(f)$ w.r.t. $\succ$
$G := \{f\}$
$Q := F \setminus G$
do
  $h := 0$
  while $Q \neq \emptyset$ and $h = 0$ **do**
    choose $p \in Q$ with the lowest $\mathrm{lm}(p)$ w.r.t. $\succ$
    $Q := Q \setminus \{p\}$
    $h :=$ **Normal Form**$(p, G, \succ)$

10: **od**
11: **if** $h \neq 0$ **then**
12: **for all** $g \in G$ such that $\mathrm{lm}(g) = \theta^{\mu} \circ \mathrm{lm}(h)$, $|\mu| > 0$ **do**
13: $Q := Q \cup \{g\}$; $G := G \setminus \{g\}$
14: **od**
15: $G := G \cup \{h\}$
16: $Q := Q \cup \{\, \theta^{\beta} \circ g \mid g \in G, \theta^{\beta} \in DP(g, G) \,\}$
17: **fi**
18: **od while** $Q \neq \emptyset$
19: **return** G

This algorithm is an adaptation of the polynomial version [8] to linear difference ideals. It outputs a minimal Janet-like Gröbner basis which (if monic, that is, normalized by division of each polynomial by its leading coefficient) is uniquely defined by the input set F and ranking $\succ$. Correctness and termination of the algorithm follow from the proof given in Ref. [8]; in so doing the displacement of some elements of the intermediate sets G into Q at step 13 provides minimality of the output basis. The algorithm terminates when the set Q becomes empty in accordance with (4).

The subalgorithm **Normal Form**$(p, G, \succ)$ performs the Janet-like reductions (Section 3) of the input difference polynomial p modulo the set G and outputs the Janet-like normal form of p. As long as the intermediate difference polynomial h has a term Janet-like reducible modulo G, the elementary reduction of this term is done at step 4. As usually in the Gröbner bases techniques [2], the reduction is terminated in finitely many steps due to the properties of the ranking (Section 2).

Algorithm: Normal Form$(p, G, \succ)$

Input: $p \in \mathbb{R}_{\mathrm{L}} \setminus \{0\}$, a polynomial; $G \subset \mathbb{R}_{\mathrm{L}} \setminus \{0\}$, a finite set; $\succ$, a ranking
Output: $h = NF_{\mathscr{J}}(p, G)$, the $\mathscr{J}$-normal form of p modulo G
1: $h := p$
2: **while** $h \neq 0$ **and** h has a monomial u with coefficient $b \in \mathbb{K}$ $\mathscr{J}$-reducible modulo G **do**
3: **take** $g \in G$ such that $u = \theta^{\gamma} \circ \mathrm{lm}(g)$ with $\theta^{\gamma} \in \mathscr{J}(\mathrm{lm}(g), \mathrm{lm}(G))$
4: $h := h/b - \theta^{\gamma} \circ (g/\mathrm{lt}(g))$
5: **od**
6: **return** h

An improved version of the above algorithm can easily be derived from the one for the involutive algorithm [9] if one replaces the input involutive division by a Janet-like monomial division [8] and then translates the algorithm into linear difference algebra. In particular, the improved version includes Buchberger's criteria adjusted to Janet-like division and avoids the repeated prolongations $\theta^{\beta} \circ g$ at step 16 of the algorithm.

5. Computational aspects

The polynomial version of algorithm **Janet-like Gröbner Basis** implemented in its improved form in C++ [8] has disclosed its high computational efficiency for the standard set of benchmarks.[1] If one compares this algorithm with the involutive one [9] specialized in Janet division, then all the computational merits of the latter algorithm are retained, namely:

- Automatic avoidance of some useless reductions.
- Weakened role of the criteria: even without applying any criteria the algorithm is reasonably fast. By contrast, Buchberger's algorithm without applying the criteria becomes unpractical even for rather small problems.
- Smooth growth of intermediate coefficients.
- Fast search of a polynomial reductor which provides an elementary Janet-like reduction of the given term. It should be noted that as well as in the involutive algorithm such a reductor, if it exists, is unique. The fast search is based on the special data structures called Janet trees [9].
- Natural and effective parallelism.

Though one needs intensive benchmarking for linear difference systems, we have solid grounds to believe that the above listed computational merits hold also for the difference case.

As this takes place, computation of a Janet-like basis is more efficient than computation of a Janet basis by the involutive algorithm [9]. The inequality (3) for monic bases is a consequence of the inclusion [8]:

$$GB \subseteq JLB \subseteq JB. \tag{5}$$

There are many systems for which the cardinality of a Janet-like basis is much closer to that of the reduced Gröbner basis than the cardinality of a Janet basis. Certain binomial ideals called toric form an important class of such problems. Toric ideals arise in a number of problems of algebraic geometry and closely related to integer programming. For this class of ideals the cardinality of Janet bases is typically much larger than that of reduced Gröbner - bases [8]. For illustrative purposes consider a difference analogue of the simple toric ideal [8,11] generated in the ring of difference operators by the following set:

$$\{\theta_x^7 - \theta_y^2\theta_z, \theta_x^4\theta_w - \theta_y^3, \theta_x^3\theta_y - \theta_z\theta_w\}.$$

The reduced Gröbner basis for the degree-reverse-lexicographic ranking with $\theta_x \succ \theta_y \succ \theta_z \succ \theta_w$ is given by

$$\{\theta_x^7 - \theta_y^2\theta_z, \theta_x^4\theta_w - \theta_y^3, \theta_x^3\theta_y - \theta_z\theta_w, \theta_y^4 - \theta_x\theta_z\theta_w^2\}.$$

[1] See Web page http://invo.jinr.ru.

The Janet-like basis computed by the above algorithm contains one more element $\theta_x^4\theta_w - \theta_y^3$ whereas the Janet basis adds another six extra elements to the Janet-like basis [8].

The presence of extra elements in a Janet basis in comparison with a Janet-like basis is obtained because of certain additional algebraic operations. That is why the computation of a Janet-like basis is more efficient than the computation of a Janet basis. Both bases, however, contain the reduced Gröbner basis as the internally fixed [9] subset of the output basis.[2] Hence, having any of the bases computed, the reduced Gröbner basis is easily extracted without any extra computational costs.

6. Conclusion

The above presented algorithm is implemented, in its improved form, as a Maple package [10], and already applied to generation of difference schemes for PDEs and to reduction of some loop Feynman integrals (see some examples in [10]). The last problem for more than 3 internal lines with masses is computationally hard for the current version of the package.

One reason for this is that the Maple implementation does not support Janet trees since Maple does not provide efficient data structures for trees.

Another reason is that in the improved version of the algorithm there is still some freedom in the selection strategy for elements in Q to be reduced modulo G. Though our algorithms are much less sensitive to the selection strategy than Buchberger's algorithm, the running time still depends substantially on the selection strategy: mainly because of dependence of the intermediate coefficients growth on the selection strategy. To find a heuristically good selection strategy one needs to do intensive benchmarking with difference systems. In turn, this requires an extensive data base of various benchmarks that, unlike polynomial benchmarks, up to now is missing for difference systems.

In addition to our further research on improvements of the Maple package, we are going to implement the difference algorithm in C++ as a module of the open source software GINV available on the Web site http://invo.jinr.ru.

The comparison of implementations of polynomial involutive algorithms for Janet bases in Maple and in C++ [12] shows that the C++ code is of two or three order faster than its Maple counterpart. Together with efficient parallelization of the algorithm this gives a real hope for its practical applicability to problems of current interest in reduction of loop integrals.

Acknowledgements

This work was partially supported by grants 04-01-00784 and 05-02-17645 from the Russian Foundation for Basic Research and by grant 2339.2003.2 from the Russian Ministry of Science and Education. The author thanks the organizers of ACAT 2005 for financial support.

References

[1] B. Buchberger, An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal, Ph.D. Thesis, University of Innsbruck, 1965 (in German).
[2] B. Buchberger, F. Winkler (Eds.), Gröbner Bases and Applications, Cambridge University Press, Cambridge, 1998.
[3] F. Chyzak, Gröbner bases, symbolic summation and symbolic integration, in: B. Buchberger, F. Winkler (Eds.), Gröbner Bases and Applications, Cambridge University Press, Cambridge, 1998, pp. 32–60.
[4] A.V. Mikhalev, A.B. Levin, E.V. Pankratiev, M.V. Kondratieva, Differential and Difference Dimension Polynomials, Mathematics and Its Applications, Kluwer, Dordrecht, 1999.
[5] V.V. Mozzhilkin, Yu.A. Blinkov, Trans. Saratov Univ. 1 (2) (2001) 145 (in Russian).
[6] V.P. Gerdt, Yu.A. Blinkov, V.V. Mozzhilkin, Linear difference ideals and generation of difference schemes for PDEs, Symmetry, Integrability and Geometry: Methods and Applications (SIGMA), Institute of Mathematics, Kiev, 2005, submitted.
[7] V.P. Gerdt, Nucl. Phys. B (Proc. Suppl.) 135 (2004) 232 arXiv:/hep-ph/0501053.
[8] V.P. Gerdt, Yu.A. Blinkov, Janet-like monomial division, Janet-like Gröbner bases, in: V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov (Eds.), Computer Algebra in Scientific Computing/CASC 2005, Springer, Berlin, 2005, pp. 174–195.
[9] V.P. Gerdt, Involutive algorithms for computing Gröbner bases, in: Computational Commutative and Non-commutative Algebraic Geometry, IOS Press, Amsterdam, 2005, pp. 199–225 arXiv:-math.AC/0501111, 2005.
[10] V.P. Gerdt, D. Robertz, A maple package for computing Gröbner bases for linear recurrence relations, Nucl. Instr. and Meth. A, this volume, doi:10.1016/j.nima.2005.11.171.
[11] A.M. Bigatti, R. La Scala, L. Robbiano, J. Symb. Comput. 27 (1999) 351.
[12] Yu.A. Blinkov, V.P. Gerdt, C.F. Cid, W. Plesken, D. Robertz, The maple package "Janet": I. polynomial systems, in: V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov (Eds.), Computer Algebra in Scientific Computing/CASC 2003, Institute of Informatics, Technical University of Munich, Garching, 2003, pp. 31–40.

[2] In the improved versions of the algorithms.