Compact Monomial Involutive Bases

Vladimir P. Gerdt and Yury A. Blinkov

Abstract. Based on the minimal Gröbner basis G of a monomial ideal $\mathcal{I}$ in the commutative polynomial ring $\mathcal{K}[x_1, x_2, \ldots, x_n]$ over a field $\mathcal{K}$ and a total monomial ordering $\succ$, we define another monomial ordering $\succ_G$ such that pairwise involutive partition of variables $\{x_1, \ldots, x_n\}$ for monomials in $\mathcal{I}$ generated by $\succ_G$ yields more compact involutive basis than that generated by $\succ$. In particular, for $\succ_{\text{alex}}$, the antigraded lexicographic ordering, the involutive basis for $\succ_{\text{alex}_G}$ and $n \gg 1$ is much more compact then involutive basis for $\succ_{\text{alex}}$. We illustrate this by computer experiments.

The notion of involutive monomial division introduced in our paper [1] is a cornerstone of theory of involutive bases and their algorithmic construction. The basic idea behind this notion goes back to Janet [2] and consists in a proper partition of variables for every element in a finite monomial set into the two subsets called multiplicative and nonmultiplicative. Given a polynomial set and an admissible monomial order, the partition of variables is defined in terms of the leading monomial set. Each such partition generates a monomial division [3] called involutive, if it is defined for an arbitrary monomial set and satisfies the axioms given in Definition 1 [1]. For more definitions and proofs see [3] and book [4]).

Definition 1. [9] An *involutive division* $\mathcal{L}$ is defined on $\mathcal{M}$ if for any nonempty set $U \subset \mathcal{M}$ and for any $u \in U$ a subset $M_\mathcal{L}(u, U) \subseteq X$ is defined that generates submonoid $\mathcal{L}(u, U) \subset \mathcal{M}$ of power products in $M_\mathcal{L}(u, U)$ and the following holds

1. $v \in U \ \wedge \ u\mathcal{L}(u, U) \cap v\mathcal{L}(v, U) \neq \emptyset \Longrightarrow u \in v\mathcal{L}(v, U) \ \vee \ v \in u\mathcal{L}(u, U)\,,$
2. $v \in U \ \wedge \ v \in u\mathcal{L}(u, U) \Longrightarrow \mathcal{L}(v, U) \subseteq \mathcal{L}(u, U)$ (transitivity),
3. $u \in V \wedge \ V \subseteq U \Longrightarrow \mathcal{L}(u, U) \subseteq \mathcal{L}(u, V)$ (filter axiom).

Variables in $M_\mathcal{L}(u, U)$ are $\mathcal{L}$*-multiplicative* for u and those in $NM_\mathcal{L}(u, U) = X \setminus M_\mathcal{L}(u, U)$ are $\mathcal{L}$*-nonmultiplicative.* If $w \in u\mathcal{L}(u, U)$, then u is $\mathcal{L}$*-(involutive) divisor* of w (denotation: $u \mid_\mathcal{L} w$).

In an involutive algorithm the nonmultiplicative variables of a polynomial are used for its prolongation, that is, for the multiplication by these variables, whereas the multiplicative variables of other polynomials in the set are used for reduction

The work is supported in part by the Russian Foundation for Basic Research (grants No. 18-51-18005).

of the nonmultiplicative prolongations. An involutive basis is a polynomial set such that all its nonmultiplicative prolongations are multiplicatively reducible to zero. If an involutive algorithm terminates it outputs an involutive basis which is a Gröbner basis of the special structure determined by properties of underlying involutive division. In our approach, a reduced Gröbner basis is always a well defined subset of the involutive basis and can be extracted from the last one without any extra computation [3].

In the talk we consider pair divisions introduced in [5] which are pairwise generated by total monomial orderings and studied in [6] - [9]. They are called $\prec$ *−divisions*, where $\prec$ is a total monomial ordering compatible with multiplication, i.e. $a \succ b \rightarrow m \cdot a \succ m \cdot b$ for all m. In [9], from this class of divisions we singled out the $\succ_{\mathrm{alex}}$-division generated the antigraded lexicographic ordering $\succ_{\mathrm{alex}}$ and shown, by computer experimentation, that in the vast majority of cases $\succ_{\mathrm{alex}}$-division yields much more compact monomial involutive bases than Janet division which is pairwise generated by the pure lexicographic ordering $\succ_{\mathrm{lex}}$.

Definition 2. [9]. Let U be a finite set of monomials in $\mathcal{K}[x_1,\ldots,x_n]$, $\prec$ a total monomial ordering compatible with multiplication and σ a permutation of variables $x_1,\ldots,x_n$. Then a (pairwise) $\succ$*-division* is defined as

$$(\ \forall u \in U \ ) \ \ [\ NM_{\mathcal{L}}(u,U) = \bigcup_{v\in U\setminus\{u\}} NM_{\mathcal{L}}(u,\{u,v\}) \ ] \,, \tag{1}$$

where

$$NM_{\mathcal{L}}(u,\{u,v\}) := \begin{cases} \text{if } u \succ v \text{ or } (u \prec v \wedge v \mid u) \text{ then } \emptyset \\ \text{else } \{x_{\sigma(i)}\},\ i = \min\{j \mid \deg_{\sigma(j)}(u) < \deg_{\sigma(j)}(v)\}\,. \end{cases} \tag{2}$$

Definition 3. For a monomial $u \in U$ and a total monomial ordering $\succ$, the element $v \in G$ where $G(U)$ is the reduced Gröbner basis of U is said to be an *ancestor* of u in U w.r.t. $\succ$ (denotation: $v = \mathrm{anc}_{\succ}(u)$) if

$$v := \max_{\succ}\{\, w \in G(U) \ \mid \ w \mid u \,\}\,.$$

Given a $\prec$ −division defined in (1)-(2) and a finite monomial set U, one can further compactify its involutive basis if to define the total ordering $\succ_G$ of elements in the monomial ideal $\mathcal{I}$ generated by U as follows

$$u \succ_{\mathrm{alex}_G} v \ \ \textbf{if} \ \ \mathrm{anc}_{\succ}(u) \succ \mathrm{anc}_{\succ}(v) \ \ \textbf{or} \ \ (\mathrm{anc}_{\succ}(u) = \mathrm{anc}_{\succ}(v) \ \ \textbf{and} \ \ u \succ w) \tag{3}$$

and to use Eqs. (1)-(2) for the involutive completion of G.

Another possibility of the compactification of $\prec$ −divisions is to use the total orderings

$$\begin{aligned} u \succ_G v \qquad & \textbf{if} \ \ \deg(\mathrm{anc}_{\succ}(u)) \succ \deg(\mathrm{anc}_{\succ}(v)) \\ & \textbf{or} \ \ (\deg(\mathrm{anc}_{\succ}(u)) = \deg(\mathrm{anc}_{\succ}(v)) \ \ \textbf{and} \ \ u \succ w) \ . \end{aligned} \tag{4}$$

For several pairwise divisions, we generated randomly monomial sets for different numbers of variables and averaged the cardinalities of their involutive bases over the permutations σ of variables occurring in Eq. (2). Clearly, Gröbner bases for Eqs. (3)-(4) are much more compact and computed much faster then those for $\prec$ −divisions.

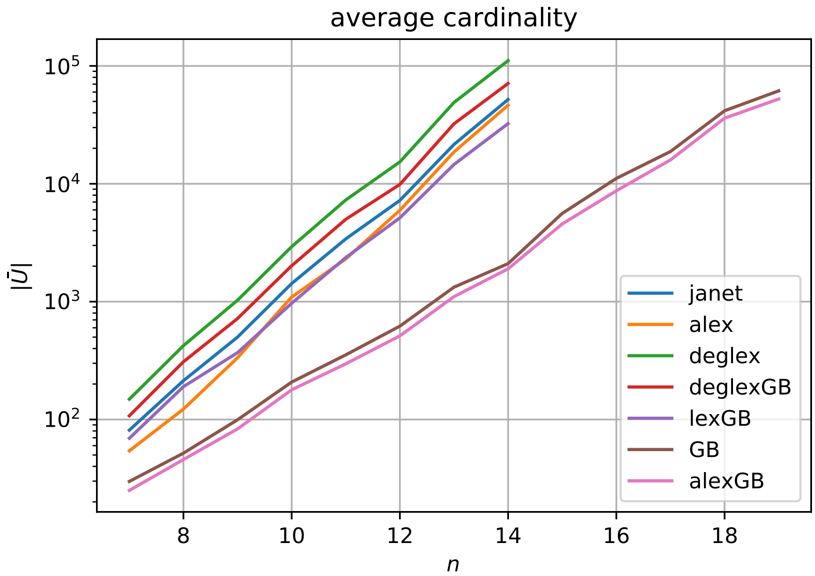

FIGURE 1. Cardinality growth with the number of variables

References

[1] V.P.Gerdt and Yu.A.Blinkov. *Involutive Bases of Polynomial Ideals*. Mathematics and Computers in Simulation, 45, 519–542, 1998; *Minimal Involutive Bases*, ibid. 543–560.

[2] M.Janet. *Leçons sur les Systèmes d'Equations aux Dérivées Partielles*. Cahiers Scientifiques, IV, Gauthier-Villars, Paris, 1929.

[3] V.P.Gerdt. *Involutive Algorithms for Computing Gröbner Bases*. Computational Commutative and Non-Commutative Algebraic Geometry. IOS Press, Amsterdam, 2005, pp.199–225.

[4] W.M.Seiler. *Involution: The Formal Theory of Differential Equations and its Applications in Computer Algebra*. Algorithms and Computation in Mathematics, 24, Springer, 2010.

[5] V.P.Gerdt. *Involutive Division Technique: Some Generalizations and Optimizations*. Journal of Mathematical Sciences, 108, 6, 1034–1051, 2002.

[6] A.S.Semenov. *On Connection Between Constructive Involutive Divisions and Monomial Orderings*. In: "Computer Algebra in Scientific Computing CASC 2006", LNCS 4194, Springer-Verlag, Berlin, 2007, pp. 261-278.

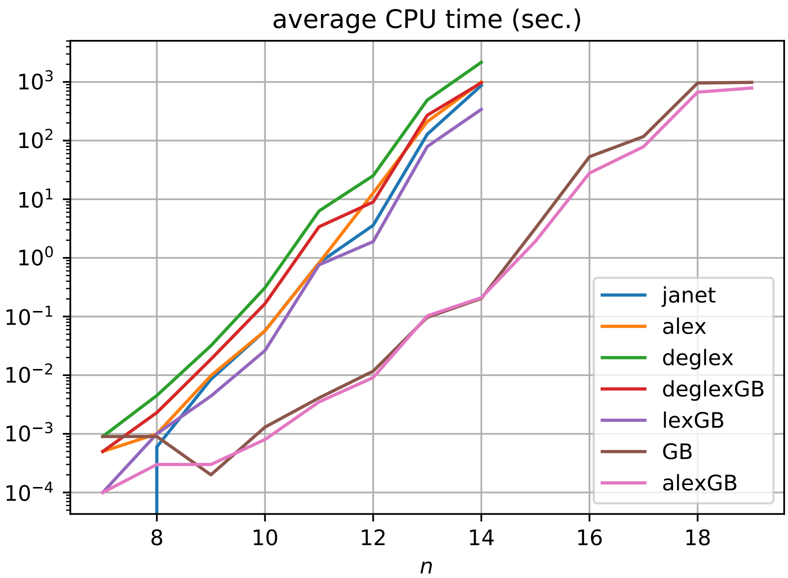

FIGURE 2. CPU time growth with the number of variables

[7] A.S.Semenov. *Constructivity of Involutive Divisions*. Programming and Computer Software, 32, 2, 96–102, 2007.

[8] A.S.Semenov and P.A.Zyuzikov. *Involutive Divisions and Monomial Orderings*. Programming and Computer Software, 33, 3, 139–146, 2007; *Involutive Divisions and Monomial Orderings: Part II*. Programming and Computer Software, 34, 2, 107–111.

[9] V.P.Gerdt and Yu.A.Blinkov. *Involutive Division Generated by an Antigraded Monomial Ordering*. In: "Computer Algebra in Scientific Computing / CASC 2011", V.P.Gerdt, W.Koepff, E.W.Mayr, E.V.Vorozhtsov (Eds.), LNCS 6885, Springer-Verlag, Berlin, 2011, pp.158–174.

Vladimir P. Gerdt
Laboratory of Information Technologies, Joint Institute for Nuclear Research
141980 Dubna, Russia
e-mail: `gerdt@jinr.ru`

Yury A. Blinkov
Department of Mathematics and Mechanics, Saratov State University
410071 Saratov, Russia
e-mail: `blinkovua@info.sgu.ru`