Programming and Computer Software, Vol. 27, No. 3, 2001, pp. 139–141.

Method of Separative Monomials for Involutive Divisions

Yu. A. Blinkov
Department of Mechanics and Mathematics, Saratov State University, Saratov, 410071 Russia
Received May 20, 2000

Abstract—A method of separative monomials is presented for constructing a partition of a set of monomials associated with a certain involutive division. Given a particular set, the method is capable of constructing a search tree of an involutive divisor with various balancing criteria.

1. INTRODUCTION

A general algorithmic approach to construction of involutive polynomial Gröbner bases can be developed on the basis of properties of involutive division discussed in [1–3]. The involutive approach came to commutative algebra [4] from theory of partial differential equations. The verification of the compatibility conditions in involutive algorithms is similar to calculation of S-polynomials in the Buchberger algorithm [5] for construction of Gröbner bases. Based on the form of leading monomials of involutive bases, explicit formulas for the Hilbert function and polynomial [6, 7] are easily constructed.

In what follows, we use the following notation: $\deg_i(u)$ is the degree of variable x_i in the monomial u, $\gcd(u, v)$ is the greatest common divisor of the monomials u and v, and $\mathrm{lcm}(u, v)$ is the least common multiple of u and v.

Definition 1. [1] An *involutive division L* is said to be defined on a set of monomials $\mathbb{M}$ if, for any finite subset $U \subset \mathbb{M}$ and for any $u \in U$, a submonoid $L(u, U)$ of the monoid $\mathbb{M}$ is given that satisfies the following conditions:

(i) $w \in L(u, U)$ and $v \mid w$ imply that $v \in L(u, U)$;

(ii) $u, v \in U$ and $uL(u, U) \cap vL(v, U) \neq \varnothing$ imply that $u \in vL(v, U)$ or $v \in uL(u, U)$;

(iii) $v \in U$ and $v \in uL(u, U)$ imply that $L(v, U) \subseteq L(u, U)$; and

(iv) $V \subseteq U$ implies that $L(u, U) \subseteq L(u, V)$ for all $u \in V$.

The elements $L(u, U)$ ($u \in U$) are called *multiplicative* for all u. If $w \in uL(u, U)$, then u is referred to as an (L–) *involutive divisor* of w, which is denoted as $u|_L w$. In this case, the monomial w is called an (L–) *multiple* of u.

For every $u \in U$, Definition 1 results in the partition ([1])

$$\{x_1, \ldots, x_n\} = M_L(u, U) \cup NM_L(u, U),$$
$$M_L(u, U) \cap NM_L(u, U) = \varnothing$$

of the set of variables into two disjoint subsets of *multiplicative*, $M_L(u, U) \subset L(u, U)$, and *nonmultiplicative*, $NM_L(u, U) \cap L(u, U) = \varnothing$, variables.

By now, a number of involutive divisions have been constructed and examined [1, 2, 6, 8, 9].

2. METHOD OF SEPARATIVE MONOMIALS

It follows from condition (ii) of Definition 1 that, if the set is involutively autoreduced [1], there may exist only one involutive divisor for an arbitrary monomial. This makes it possible to construct a search tree with different balancing for the Janet division [10]. The following definition generalizes this approach for other involutive divisions.

Definition 2. A monomial w is called *separative* for a subset $V \subseteq U$ and a given involutive division L if it satisfies the following conditions:

(i) $V = V_1 \cup V_2$, $V_1 \neq \varnothing$ and $V_2 \neq \varnothing$;

(ii) $\forall u \in V_1$, $\nexists\, v$ such that $w \nmid v$ and $v \in uL(u, U)$;

(iii) $\forall u \in V_2$, $\nexists\, v$ such that $w \mid v$ and $v \in uL(u, U)$.

Since condition (iii) is negation of condition (ii) for the sets V_1 and V_2, it follows from Definition 2 that $V_1 \cap V_2 = \varnothing$. Consider examples of partitioning for various divisions.

Definition 3. *The Thomas division* [11]. A variable x_i is multiplicative for $u \in U$ if $\deg_i(u) = \max\{\deg_i(v) \mid v \in U\}$ and nonmultiplicative otherwise.

Definition 4. *The Janet division* [12]. For every value of index i, $1 \le i \le n$, of a variable, let us divide elements of U into the subgroups determined by a set of nonnegative integers $d_1, \ldots, d_i$:

$$[d_1, \ldots, d_i] = \{u \in U \mid d_j = \deg_j(u),\ 1 \le j \le i\}.$$

Then, the variable x_i is multiplicative for $u \in U$ if either $i = 1$ and $\deg_1(u) = \max\{\deg_1(v) \mid v \in U\}$ or $i > 1$, $u \in [d_1, \ldots, d_{i-1}]$, and $\deg_i(u) = \max\{\deg_i(v) \mid v \in [d_1, \ldots, d_{i-1}]\}$.

Example 1. Consider the set $U = \{x^2y, xz, y^2, yz, z^3\}$ with the order of variables ($x > y > z$) for the Thomas

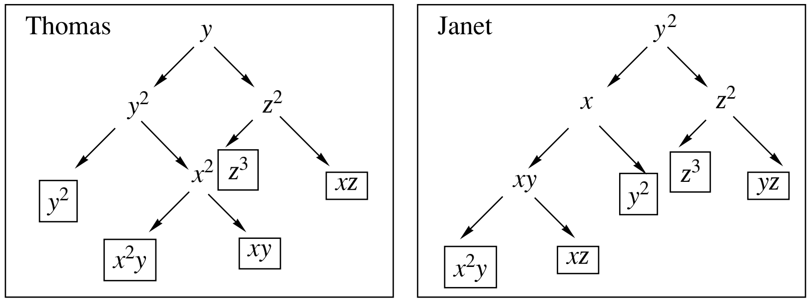

Figure.

and Janet divisions. The separative monomials for these divisions and the set U are shown in the figure. The monomials located in the leaves and enclosed into the rectangles belong to the original set. In accordance with Definition 2, the monomial located in the root is separative. For all monomials located in the leaves, the right subtree cannot contain an involutive divisor of the monomial the divisor of which (in the common sense) is the monomial located in the root.

Theorem. If assumptions of Definition 2 are fulfilled, the two following assertions are equivalent:

(1) $\forall u \in V_2$ and $\nexists\, v$ such that $w \mid v$ and $v \in uL(u, U)$;

(2) $\forall u \in V_2$ and $(\forall w_1, w_2) w = w_1 w_2$ imply that $w_1 \notin L(u, U)$ and $w_2 \nmid u$.

Proof. $1 \Rightarrow 2$. Suppose that $\forall u \in V_2$ and $(\exists w_1, w_2) w = w_1 w_2$ imply that $w_1 \in L(u, U)$ and $w_2 \mid u$. Then, in accordance with the first assertion, for the monomial $u \in V_2$, consider $v = (u/w_2)w$. By construction, $w \mid v$ and $v = uw_1 \in uL(u, U)$, and we arrive at the contradiction.

$2 \Rightarrow 1$. Let $\forall u \in V_2$ and $\exists v$ such that $w \mid v$ and $v \in uL(u, U)$. Hence, $u \mid v$ and $(v/u) \in L(u, U)$. According to the second assertion, since $w \mid v$, consider w_1 and w_2 such that $w_1 = \gcd(v/u, w)$ and $w_2 = \gcd(u, w)$. On the other hand,

$$\begin{aligned} w &= \gcd(v, w) = \frac{\gcd(v, w)}{\gcd(u, w)}\gcd(u, w) \\ &= \gcd(v/u, w)\gcd(u, w) = w_1 w_2. \end{aligned}$$

and we arrive at the contradiction since $w_1 \in L(u, U)$ and $w_2 \mid u$.

This theorem provides us with a constructive method of finding separative monomials. Let us introduce the following notation: $\gcd(uL(u, U), w) = v$ if $(v \in uL(u, U), v \mid w)$ and $(\forall s \in uL(u, U), s \mid w)$ implies that $s \mid v$.

Corollary. Under the assumptions of Definition 2, the following conditions are necessary and sufficient for a monomial be separative:

(1) $(\forall u \in V_1)\gcd(uL(u, U), w) = w$;

(2) $(\forall u \in V_2)\gcd(uL(u, U), w) \neq w$.

Proof. The necessity and sufficiency of the first condition is evident since, if $w \nmid v$, it immediately follows that $v \notin uL(u, U)$. In view of the above notation, the second condition was proved in the theorem.

The following example shows that a separative monomial may not exist for an arbitrary partition and involutive division.

Example 2. For the Thomas division, the set $U = \{x^2, y^2, z^2, t^2, xy, zt\}$ cannot be partitioned into $\{x^2, y^2, z^2, t^2\}$ and $\{xy, zt\}$. In accordance with the above corollary, only $1_{\mathbb{M}}$ can be a separative monomial. Indeed, for $\{x^2, y^2, z^2, t^2\}$, each monomial for the Thomas division can divide only the degree of a variable that is greater than two, of which it is composed. As a result, the only candidate on the place of a separative monomial is the unit one, and the second condition is violated.

ACKNOWLEDGMENTS

This work was supported in part by the Russian Foundation for Basic Research, project nos. 98-01-00101 and 00-15-96691, and by INTAS, project no. 99-1222.

REFERENCES

1. Gerdt, V.P. and Blinkov, Yu.A., Involutive Bases of Polynomial Ideals, *Math. Comp. Simul.*, 1998, vol. 45, pp. 519–542.
2. Gerdt, V.P. and Blinkov, Yu.A., Minimal Involutive Bases, *Math. Comp. Simul.*, 1998, vol. 45, pp. 543–560.
3. Gerdt, V.P. and Blinkov, Yu.A., Involutive Divisions of Monomials, *Programmirovanie*, 1998, no. 6, pp. 22–24.
4. Zharkov, A.Yu. and Blinkov, Yu.A., Involutive Systems of Algebraic Equations, *Programmirovanie*, 1994, no. 1, pp. 53–56.
5. Buchberger, B., Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory, *Symbolic and Algebraic*

Computations, Buchberger, B., Collins, G., and Loos, R., Eds., Wien: Springer, 1982. Translated under the title *Komp'yuternaya algebra. Simvol'nye i algebraicheskie vychisleniya*, Moscow: Mir, 1986.

6. Apel, J., Theory of Involutive Divisions and an Application to Hilbert Function, *J. Symol. Comp.*, 1998, vol. 25, pp. 683–704.
7. Gerdt, V.P., Completion of Linear Differential Systems to Involution, *Computer Algebra in Scientific Computing, CASC'99* Ganzha, V.G., Mayr, E.W., and Vorozhtsov, E.V., Eds., Berlin: Springer, 1999, pp. 115–137.
8. Gerdt, V.P., Involutive Division Technique: Some Generalizations and Optimizations, *Notes of SPOMI*, St. Petersburg, 1999, vol. 258, pp. 115–137.
9. Chen, Yu-Fu and Gao, X.-S., Vector Representation of Involutive Divisions, *Mathematics–Mechanization Research Preprints*, Beijing, 1999, no. 18, pp. 9–22.
10. Gerdt, V.P., Yanovich, D., and Blinkov, Yu.A., Fast Search of the Janet Divisor, *Programmirovanie*, 2000.
11. Thomas, J., *Differential Systems*, New York: AMS, 1937.
12. Janet, M., *Leçons sur les Systèmes d'Equations aux Dérivées Partielles*, Cahiers Scientifiques, IV, Paris: Gauthier-Villars, 1929.