Dynamic Properties of Involutive Divisions: Facts and Examples

Alexander Semenov, Petr Zyuzikov

Moscow State University
Department of Mechanics and Mathematics

February 20, 2007
References


1 Axioms

Let $U$ be a finite monomial set. For all $u \in U$ $L(u, U) \subset M$ is a submonoid satisfying following axioms [1, 2]:

- if $w \in L(u, U)$ and $v|w \implies v \in L(u, U)$
- if $u, v \in U$ and $uL(u, U) \cap vL(v, U) \neq \emptyset \implies u \in vL(v, U)$ or $v \in uL(u, U)$
- if $v \in U$ and $v \in uL(u, U) \implies L(v, U) \subseteq L(u, U)$
- For $U \subseteq V$ and $\forall u \in U$ $L(u, V) \subseteq L(u, U)$

Elements in $L(u, U)$ are multiplicative for $u$. If $w \in uL(u, U)$ then $u$ is the involutive divisor of $w$, and it is denoted as $u|_{Lw}$.

The equality $w = uv$ is written as $w = u \times v$, if $u|_{Lw}$, and $w = u \cdot v$, otherwise.
For all $u$ in $U$ exists the separation of variables into multiplicative ($M_L(u, U) \subset L(u, U)$) and non-multiplicative ($NM_L(u, U) \not\in L(u, U)$).

$$C_L(u, U) = uL(u, U), C_L(U) = \bigcup_{u\in U} C_L(u, U)$$

**Example 1 (Janet division).** Consider a finite set $U$ of monomials. For each $1 \leq i \leq n$, we divide $U$ into groups labeled by non-negative integers $d_1, \ldots, d_i$:

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

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

- Description of all involutive divisions admissible for algorithmic use.

- Improving of Janet division or rigorous proof of its excellence.

None of the problems have been solved yet.
Example 2 ($\succ$-division). Let $U$ be a finite monomial set with distinct elements and $L$ be an involutive division. A variable $x_i$ ($1 \leq i \leq n$) is non-multiplicative for $u \in U$, if exists $u_1 \in U$, $u_1 \succ u$, $i = \min\{j | \deg_j(u) < \deg_j(u_1)\}$.

Janet division is lex-division, where lex is a lexicographic ordering for which $x_1 \succ x_2 \succ \ldots x_n$.

Compare:

Example 3 (Induced $\succ$-division [3]). Let $U$ be a finite monomial set with distinct elements and $L$ be an involutive division. A variable $x_i$ ($1 \leq i \leq n$) is non-multiplicative for $u \in U$, if exists $u_1 \in U$, $u_1 \prec u$ and $\deg_i(u) < \deg_i(u_1)$. 
3 Dynamic Properties of Involutive Divisions

**Axiom 1.** (Reformulation of filter property) For all $U, V$ and $\forall u \in U \cap V$

$$ML(u, U \cup V) \subseteq ML(u, U) \cap ML(u, V).$$

**Definition 1.** (Reformulation of pair property) For all $U, V$ and $\forall u \in U \cap V$

$$ML(u, U \cup V) = ML(u, U) \cap ML(u, V).$$

**Theorem 1.** If $\succ$ is an admissible monomial ordering then $\succ$-division is pairwise.
Janet division is:

- disjoint: \( \forall u, v \in U, v \neq u, v \in uL(u, U) \),
- homothetic: \( NM_L(u, U) = NM_L(mu, mU) \),
- pairwise,
- continuous,
- “widest” on two-element sets.

So are all \( \succ \)-divisions.

Which \( \succ \)-divisions are admissible for algorithmic use?
4 Constructivity

Definition 2. [1, 2] Continuous involutive division $L$ is constructive on $U$, if for all $u \in U$, $x_i \in NM_L(u, U)$, such that $u \cdot x_i$ has no involutive divisions in $U$ and

$$(\forall v \in U)(\forall x_j \in NM_L(v, U))(v \cdot x_j \mid u \cdot x_i, v \cdot x_j \neq u \cdot x_i) \implies v \cdot x_j \in C_L(U)$$

the following is true:

$$\forall w \in C_L(U)[u \cdot x_i \not\in C_L(U \cup \{w\})].$$
Constructivity of an involutive division $L$ assures that:

- all minimal non-multiplicative prolongations lie in monomial basis,

- minimal involutive monomial basis exists for every $U$,

- whole theory of [1, 2] is applicable to this involutive division $L$. 
Theorem 2. Consider the $\succ$-division $L$. If ordering $\succ$ satisfies the condition: $\exists i < j < k < l$ and $\exists s \in \mathbb{N}, s > 0$ s.t. $x_j x_l \succ x_k^s \succ x_i x_l$ then $L$ is non-constructive.

Proof. The relation $x_j x_l \succ x_k^s \succ x_i x_l$ implies $x_j^2 x_j x_l \succ x_k^2 x_k^s$ and $x_i x_j x_k^s \succ x_j^2 x_j x_l$. Also, $x_j^2 x_j x_l \succ x_i x_k^s$ is valid.

Consider $U = \{x_i x_k^s, x_i^2 x_k^s, x_j^2 x_j x_l\}$, $w = x_i x_k^s \times x_j$. The main relation is $x_i^2 x_k^s \cdot x_j = x_i x_j x_k^s \times x_i$.

<table>
<thead>
<tr>
<th>$U$</th>
<th>$NM_L(U)$</th>
<th>$U \cup {x_i x_j x_k^s}$</th>
<th>$NM_L(U \cup {x_i x_j x_k^s})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_i x_k^s$</td>
<td>$x_i$</td>
<td>$x_i x_k^s$</td>
<td>$x_i, x_j$</td>
</tr>
<tr>
<td>$x_i^2 x_k^s$</td>
<td>$x_j$</td>
<td>$x_i^2 x_k^s$</td>
<td>$x_j$</td>
</tr>
<tr>
<td>$x_j^2 x_j x_l$</td>
<td>$-$</td>
<td>$x_j^2 x_j x_l$</td>
<td>$x_k$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$x_i x_j x_k^s$</td>
<td>$-$</td>
</tr>
</tbody>
</table>

That proves the theorem.
Non-existence of the minimal involutive basis:

Let $s = 1$ (for example, ordering lex$\{j,k,i,l\}$) and $U$ be an autoreduced set $\{x_i^2x_jx_l, x_ix_k\}$.

Both sets $U_1 = \{x_i x_j x_k, x_i^2 x_j x_l, x_i^2 x_k, x_ix_k\}$ and $U_2 = \{x_i^2 x_j x_k, x_i^2 x_j x_l, x_i^2 x_k, x_i x_k\}$ are involutive monomial bases.

$U_1 \cap U_2 = \{x_i x_k, x_i^2 x_k, x_i^2 x_j x_l\}$.

Neither $U_1 \cap U_2$ nor its subsets cannot be involutive bases of $U$.

The minimal involutive basis should be contained in every involutive basis, what is impossible here.
The following examples show that there exist many non-constructive divisions in three-variable case.

**Theorem 3.** Consider the $\succ$-division $L$. If for the ordering $\succ$ one of four conditions

1. $\exists i < j < k$ s.t. $x_j < x_i < x_k$,
2. $\exists i < j < k$ s.t. $x_i < x_j < x_k$,
3. $\exists i < j < k, p \in \mathbb{N}$ s.t. $x_i < x_k < x_j < x_k^{p-1}$,
4. $\exists i < j < k < l$ s.t. $x_j \succ x_k \succ x_i$, $x_j \succ x_k \succ x_l$

is satisfied, $L$ is non-constructive.
A very important theorem:

The permutation $\xi \in S_n$ is associated with $\succ$, if $x_{\xi(1)} \succ \cdots \succ x_{\xi(n)}$. Ordering $\text{lex}(\prec)$ is the lexicographic ordering with respect to the permutation $\xi$.

**Theorem 4.** Let $L$ be an involutive $\succ$-division, $U$ be an arbitrary finite monomial set with distinct elements, and $u_1, u_2$ be such elements, that $u_1 \cdot x \in u_2 L(u_2, U)$, where $x$ is a non-multiplicative variable for $u_1$ and $U$. Then $u_1 \prec u_2$, $u_1 \prec_{\text{lex}(\prec)} u_2$. 
Definition 3. Let $L$ be an involutive $\succ$-division. A set of distinct monomials $\{u_1, u, w, \hat{u}\}$ is $\gamma$-configuration, if it satisfies the following conditions:

1. $u \prec \hat{u}$,

2. $w = u_1 \times v$, $v \in L(u_1, \{u_1, u, \hat{u}\})$,

3. $u \cdot x_i \in wL(w, \{\hat{u}, u, u_1, w\})$, where $x_i = NML(u, \{u, \hat{u}\})$. 

Lemma 1. Let $L$ be an involutive $\succ$-division which is non-constructive. Then it exists a $\gamma$-configuration $\{u_1, u, w, \hat{u}\}$ for which relations $u_1 \prec u$, and $u_1 <_{\text{lex}(\prec)} u$ are valid.

The indices $i, j, k$ are used in following sense:

- $x_i = N M_L(u, \{u, \hat{u}\})$,
- $x_j = N M_L(u_1, \{u_1, u\})$,
- $x_k = N M_L(u_1, \{u_1, \hat{u}\})$.

Lemma 2. For every $\gamma$-configuration $\{u_1, u, w, \hat{u}\}$ corresponding to $\succ$-division, where $u_1 \prec u$, the relation $x_i \succ x_j$ is valid.
Theorem 5. Let $\succ$ be an admissible monomial ordering, such that $x_1 \succ x_2 \succ \ldots \succ x_n$. There is no $\gamma$-configurations with $u_1 \prec u$ and $u_1 \prec_{\text{lex}(\prec)} u$ and involutive $\succ$-division $L$ is constructive.

Theorem 6. Consider an involutive $\succ$-division $L$ and a finite monomial set $U$ with distinct elements, which is involutive with respect to $L$, and for $\succ$ the relation $x_1 \succ x_2 \succ \ldots \succ x_n$ is valid. Then $U$ is involutive with respect to $\text{lex}(\prec)$-division, namely, Janet division.

In this case every monomial involutive basis is Janet basis but may be not the minimal Janet basis.
Theorem 7. Consider the two-variable case i.e. when \( n = 2 \) and all the monomials are formed by variables \( x_1, x_2 \). Then for every \( \succ \)-division \( L \) no \( \gamma \)-configurations with \( u_1 \prec u \) and \( u_1 <_{\text{lex}(\succ)} u \) exist and involutive \( \succ \)-division \( L \) is constructive.

Theorem 8. Let \( L \) be a \( \succ \)-division on three variables. It is constructive in and only in the following cases:

- \( x_1 \succ x_2 \succ x_3 \),
- \( x_2 \succ x_1 \succ x_3 \),
- \( x_2 \succ x_3 \succ x_1, \forall p, q \in \mathbb{M} \quad \deg_2(p) > \deg_2(q) \Rightarrow p \succ q \),
- \( x_1 \succ x_3 \succ x_2, \forall s, k \in \mathbb{N} \text{ s.t. } x_3^k \succ x_1^s \succ x_2 x_3^{k-1} \).
And for the four and more variables:

**Theorem 9.** Consider the $\succ$-division $L$. If for the ordering $\succ$ the condition is satisfied: $\exists i < j < k < l$ and $\exists s, m, q \in \mathbb{N}$ s.t. $x_j^{m+1} x_l^q \succ x_k^s \succ x_i x_j^m x_l^q$, then $L$ is non-constructive.
Variable set $x_1, \ldots, x_n$ is divided into 2 groups, each consisting of $r_i$ variables:

$$x_{1,1}, \ldots, x_{1,r_1}, x_{2,1}, \ldots, x_{2,r_2}.$$ 

Degree of variable $x_{s,p}$ in a monomial $m$ is denoted as $\deg_{s,p}(m)$.

Monomials $[u]_s, 1 \leq s \leq 2$ are defined the following way:

$$\deg_{h,p}([u]_s) = \begin{cases} 
0, & h \neq s \\
\deg_{h,p}(u), & h = s 
\end{cases}$$
≺_s (1 ≺ s ≺ 2): admissible orderings on sets of monomials of type 
\{ x_{s,1}^{n_s}, \ldots, x_{s,r_s}^{n_s} \}.

On \mathbb{M} = \{ x_1, \ldots, x_n \} = \{ x_{1,1} \ldots x_{1,r_1}, x_{2,1} x_{2,r_2} \} the admissible
ordering ≺_{1,2} is defined as:

\[ u ≺_{1,2} v \iff \exists 1 ≤ s ≤ 2, \forall p < s, [u]_p = [v]_p, [u]_s ≺_s [v]_s. \]

**Theorem 10.** Let \( L_k \) — be a finite set of ≻_k-divisions
(1 ≤ k ≤ 2), where ≻_k are admissible orderings. For every division
\( L_k \) no \( \gamma \)-configurations with \( u_1 ≺_k u, u_1 <_{\text{lex}(≺_k)} u \) exist. Then
≻ = (≻_1, ≻_2) is an admissible ordering, for ≻-division \( L \) no
\( \gamma \)-configurations with \( u_1 ≺ u, u_1 <_{\text{lex}(≺)} u \) exist, and \( L \) is
constructive.
Two interesting facts:

1. The $\text{lex}_{\{2,3,1\}}$-division is constructive, but the $\text{lex}_{\{2,3,1,4\}}$ is non-constructive.

Explanation: $\text{lex}_{\{2,3,1\}}$-division do not satisfy the conditions of theorem 10 because it allows $\gamma$-configurations with $u_1 \prec u$ and $u_1 <_{\text{lex}(\prec)} u$.

2. Relation $\succ$ on variables does not define whether $\succ$-division is constructive.

Let $x_2 \succ x_1 \succ x_3 \succ x_4$.

The $\text{lex}_{\{2,1,3,4\}}$-division is constructive due to the theorem 10.

But if $\succ$ is such that $x_2x_4 \succ x_3^2 \succ x_1x_4$, then division is non-constructive according to the theorem 9.
For the constructive involutive divisions, for which relations $x_1 \succ x_2 \succ \ldots \succ x_n$ do not hold, the minimal involutive basis can contain less elements than minimal Janet basis.

**Example 4.** Consider the set $U = \{x_1^2, x_2\}$. This set is autoreduced. Let $J$ be a Janet involutive division, and $L$ be a $\text{lex}\{2,1\}$-division. Both divisions are constructive, so the Minimal Involutive Basis algorithm gives correct results. It is clear to see, that $MB_J(U) = \{x_2, x_1 x_2, x_1^2\}$, and $MB_L(U) = \{x_1^2, x_2\}$. So, the size of $MB_J(U)$ exceeds that of $MB_L(U)$. 
5 Monotonicity

Theorem 11. Let $\succ$ be such an admissible ordering, for which the following holds: $\forall i, j \in \mathbb{N} : i \neq j \exists \varphi, \psi \in \mathbb{N} :$

$$
\begin{cases}
  x_j^{\psi} \prec x_i^{\varphi}, \\
  x_i^{\varphi - 1} \prec x_j^{\psi - 1}.
\end{cases}
$$

Then $\succ$-division $L$ is non-monotone.

As every $\succ$-division in two variables is constructive, the theorem gives examples of constructive and non-monotone involutive divisions.