A Gröbner-Basis Theory for Divide-and-Conquer Recurrences

Frédéric Chyzak

INRIA

July 2020 — ISSAC ’20

Joint work with Ph. Dumas
### Divide-and-Conquer Recurrences

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Description</th>
<th>Initial Conditions</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>A064194</td>
<td>Number of ring multiplications in Karatsuba’s algorithm</td>
<td>( u_n = 2u_{\lceil n/2 \rceil} + u_{\lfloor n/2 \rfloor} ), ( u_1 = 1 )</td>
<td>Karatsuba, Ofman, 1962</td>
</tr>
<tr>
<td>A020985</td>
<td>Golay-Rudin-Shapiro sequence in functional analysis</td>
<td>( u_{2n} = u_n ), ( u_{2n+1} = (-1)^n u_n ), ( u_0 = 1 )</td>
<td>Golay, 1951</td>
</tr>
<tr>
<td>A002487</td>
<td>Stern-Brocot sequence in number theory</td>
<td>( u_{n+1} = (2k + 1)u_n - u_{n-1} ), ( k = \lfloor u_{n-1}/u_n \rfloor )</td>
<td>Stern, 1858</td>
</tr>
</tbody>
</table>
**Divide-and-Conquer Recurrences**

**A064194, Number of ring multiplications in Karatsuba’s algorithm**

\[ u_n = 2u_{\lceil n/2 \rceil} + u_{\lfloor n/2 \rfloor}, \quad u_1 = 1 \]

Algorithm / Complexity analysis. (Karatsuba, Ofman, 1962)

\[ u_{2n} = 3u_n, \quad u_{2n+1} = 2u_{n+1} + u_n, \quad u_1 = 1 \]

**A020985, Golay-Rudin-Shapiro sequence in functional analysis**

\[ u_{2n} = u_n, \quad u_{2n+1} = (-1)^n u_n, \quad u_0 = 1 \]

Spectroscopy in infrared ray / Extremal function. (Golay, 1951)

\[ u_{2n} = u_n, \quad u_{4n+1} = u_{2n}, \quad u_{4n+3} = -u_{2n+1}, \quad u_0 = 1 \]

**A002487, Stern-Brocot sequence in number theory**

\[ u_{n+1} = (2k + 1)u_n - u_{n-1}, \quad k = \lfloor u_{n-1}/u_n \rfloor \]

Design of clocks / Explicit bijection \( \mathbb{N} \sim \mathbb{Q} \). (Stern, 1858)

\[ u_{2n} = u_n, \quad u_{2n+1} = u_n + u_{n+1}, \quad u_0 = 0, \quad u_1 = 1 \]
Higher-Order Recurrences, Well-Foundedness

\[
\begin{align*}
    u_{2n} &= 2v_{n-1} - n \\
    u_{2n+1} &= u_n + v_{n+2} \\
    v_{2n} &= u_{2n+1} \\
    v_{2n+1} &= 2v_n + u_{n+1}
\end{align*}
\]

\[
\begin{align*}
    u_{2n} &= 2v_{n-1} - n \\
    u_{2n+1} &= u_n + v_{n+1} \\
    v_{2n} &= u_{2n+1} \\
    v_{2n+1} &= 2v_n + u_{n+1}
\end{align*}
\]
Higher-Order Recurrences, Well-Foundedness

\[
\begin{align*}
\{ & u_{2n} = 2v_{n-1} - n \\
& u_{2n+1} = u_n + v_{n+2} \\
& v_{2n} = u_{2n+1} \\
& v_{2n+1} = 2v_n + u_{n+1} \\
\} \\
\downarrow \\
1 = 0
\end{align*}
\]

\[
\begin{align*}
\{ & u_{2n} = 2v_{n-1} - n \\
& u_{2n+1} = u_n + v_{n+1} \\
& v_{2n} = u_{2n+1} \\
& v_{2n+1} = 2v_n + u_{n+1} \\
\} \\
\downarrow \\
\begin{align*}
& u_n = v_{2n} - v_{n+1} \\
& v_{4n+4} = v_{2n+4} - v_{n+3} \\
& + 2v_{n+1} + 2v_n - n - 1 \\
& v_{2n+1} = v_{2n+2} - v_{n+2} + 2v_n \\
& v_{4n+2} = v_{2n+2} + v_{2n} \\
& v_0 = v_1 = 0 \\
& v_2 = C \\
& v_3 = -1 \\
& v_4 = -2
\end{align*}
\]

Whole theory (in progress) based on a Gröbner-basis theory (here).
Section Operators and Skew Polynomials

**Action of section operators (fixed integer \( b \geq 2 \))**

\[
T^w \cdot \sum_{n \in \mathbb{N}} u_n x^n = \sum_{n \in \mathbb{N}} u_{b^\ell n + r} x^n \quad \text{where} \quad \ell = |w| \quad \text{and} \quad r = \sum_{i=0}^{\ell-1} w_i b^i
\]

**Nonnoetherian algebra of skew polynomials** \(( T^w = T_{w_{\ell-1}} \cdots T_{w_0} )\)

\[k(x)\langle T_0, \ldots, T_{b-1}\rangle \text{ with noncommutative monomials } T^w\]

**Noncommutative product**

\[
T^w T^v = T^{wv}, \quad T^w c(x) = T^w (c(x) T^\epsilon) = \sum_{|w'|=|w|} d_{w'}(x) T^{w'}
\]

\[d_{w'}(x) = \text{some suitable section of } c(x)\]
Section Operators and Skew Polynomials

Action of section operators (fixed integer \( b \geq 2 \))

\[
T^w \cdot \sum_{n \in \mathbb{N}} u_n x^n = \sum_{n \in \mathbb{N}} u_{b^\ell n + r} x^n \quad \text{where} \quad \ell = |w| \quad \text{and} \quad r = \sum_{i=0}^{\ell-1} w_i b^i
\]

Nonnoetherian algebra of skew polynomials (\( T^w = T_{w_{\ell-1}} \cdots T_{w_0} \))

\[
k(x)\langle T_0, \ldots, T_{b-1} \rangle \quad \text{with noncommutative monomials} \quad T^w
\]

Noncommutative product

\[
T^w T^v = T^{wv}, \quad T^w (c(x) T^v) = \sum_{|w'|=|w|} d_{w'}(x) T^{w'v}
\]

\( d_{w'}(x) = \text{some suitable section of } c(x) \)
Earlier Works on Noncommutative Gröbner-Basis Theories

Noncommutative monomials, commuting with coefficients


Monomials with commutation rules, commuting with coefficients


Monomials commuting with one another, but not with coefficients


Our need: *noncommutative monomials with commutation rules!*
Earlier Works on Noncommutative Gröbner-Basis Theories

Noncommutative monomials, commuting with coefficients


Monomials with commutation rules, commuting with coefficients


Monomials commuting with one another, but not with coefficients


Our need: noncommutative monomials with commutation rules!

We restrict to finitely-presented ideals.
Breadth-first ordering

- **Def.**: \( w < w' \) if either \(|w| < |w'|\)
  or \(|w| = |w'|\) and \(\text{rev}(w) \prec_{\text{lex}} \text{rev}(w')\).

- **Prop.**: BFO guarantees the termination of division and a compatibility lemma crucial to the correctness of algorithms.

### Compatibility lemma

For any skew polynomials \( H, K_1 \) and \( K_2 \) from \( k(x)\langle T \rangle \), if \( H \neq 0 \) and \( \text{lm}(K_1) < \text{lm}(K_2) \), then \( \text{lm}(HK_1) < \text{lm}(HK_2) \).
Division of Skew Polynomials

**Division theorem**

Given divisors $B_1, \ldots, B_s$, any dividend $A$ can be written

$$A = Q_1 B_1 + \cdots + Q_s B_s + R$$

where:
- the monomials of $R$ are not divisible by any of the $\text{lm}(B_i)$;
- for each $i$, $\text{lm}(Q_i B_i) \leq \text{lm}(A)$.

**Proof:** Obvious algorithm *provided the $B_i$ are monic*, because:

$$(cT^w + \text{lower terms}) \times (T^v + \text{lower terms}) = cT^{wv} + \text{lower terms}.$$  

Then, use: $A = QB + R \iff A = (Q \times c)(c^{-1} \times B) + R$.  

Division of Skew Polynomials

Division theorem

Given divisors $B_1, \ldots, B_s$, any dividend $A$ can be written $A = Q_1 B_1 + \cdots + Q_s B_s + R$ where:

- the monomials of $R$ are not divisible by any of the $\text{Im}(B_i)$;
- for each $i$, $\text{Im}(Q_i B_i) \leq \text{Im}(A)$.

Proof: Obvious algorithm provided the $B_i$ are monic, because:

$$(cT^w + \text{lower terms}) \times (T^v + \text{lower terms}) = cT^{wv} + \text{lower terms}.$$  

Then, use: $A = QB + R \iff A = (Q \times c)(c^{-1} \times B) + R$.

We always present ideals by monic generators.
Gröbner Bases and a Variant Buchberger Algorithm

Gröbner basis of a left ideal $\mathcal{I}$
A finite $\mathcal{G} \subset \mathcal{I}$ of monic polynomials such that for any $F \in \mathcal{I}$, \( \text{lm}(F) \) is divisible by \( \text{lm}(G) \) for some $G \in \mathcal{G}$.

Algorithm (variant of (Buchberger, 1965))
Given a finite $\mathcal{F} \subset \mathcal{I}$ of monic polynomials, while any $H_1$ and $H_2$ from $\mathcal{F}$ are such that $\text{lm}(H_2) = T^w \text{lm}(H_1)$ for some $w$, compute the remainder of the S-polynomial $H := H_2 - T^w H_1$ under division by $\mathcal{F}$ and add its monic multiple to $\mathcal{F}$.

Correctness proof: Usual approach + Specific compatibility lemma
Standard representation: $H = \sum_{i=1}^{m} Q_i F_i$ with $\text{lm}(Q_i F_i) \leq \text{lm}(H)$.
Criterion: all S-polynomials have a standard representation $\iff \mathcal{F}$ is a Gröbner basis.
A Gröbner basis doesn’t exceed the max input monomial.

Algorithm (variant of (Faugère, 1999))

Represent polynomials by row vectors w.r.t. basis of decreasing monomials. Represent presentation of $\mathcal{I}$ by matrices in row echelon form: remove null rows, never exchange rows, always add more rows at the bottom. Add at the bottom of the matrix all multiples of $\mathcal{F}$ needed to reduce all S-polynomials, row-reduce, repeat.
A Gröbner basis doesn’t exceed the max input monomial.

Algorithm (variant of (Faugère, 1999))

Represent polynomials by row vectors w.r.t. basis of decreasing monomials. Represent presentation of $\mathcal{I}$ by matrices in row echelon form: remove null rows, never exchange rows, always add more rows at the bottom. Add at the bottom of the matrix all multiples of $\mathcal{F}$ needed to reduce all S-polynomials, row-reduce, repeat.

<table>
<thead>
<tr>
<th>problem</th>
<th>01</th>
<th>35</th>
<th>38</th>
<th>14</th>
<th>39</th>
<th>42</th>
<th>18</th>
<th>15</th>
<th>43</th>
</tr>
</thead>
<tbody>
<tr>
<td>radix</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>#in/#out</td>
<td>7/2</td>
<td>5/5</td>
<td>5/5</td>
<td>5/5</td>
<td>5/5</td>
<td>24/1</td>
<td>4/4</td>
<td>6/6</td>
<td>48/1</td>
</tr>
<tr>
<td>Buchberger</td>
<td>0.29</td>
<td>1.89</td>
<td>2.09</td>
<td>0.46</td>
<td>9.10</td>
<td>4.90</td>
<td>1.64</td>
<td>1.98</td>
<td>69.95</td>
</tr>
<tr>
<td>F4</td>
<td>0.26</td>
<td>0.65</td>
<td>0.77</td>
<td>2.76</td>
<td>2.86</td>
<td>5.39</td>
<td>9.68</td>
<td>25.50</td>
<td>77.41</td>
</tr>
<tr>
<td>speed-up</td>
<td>1.09</td>
<td>2.91</td>
<td>2.70</td>
<td>0.17</td>
<td>3.18</td>
<td>0.91</td>
<td>0.17</td>
<td>0.08</td>
<td>0.90</td>
</tr>
</tbody>
</table>
Conclusion

This work

- First Gröbner-basis theory in algebraic setting with both word monomials and skew commutations.
- Termination and correctness reduce the choice of orderings.
- Need for monic generators, special S-polynomials, predictable maximal monomial to be used.
- Implementation available from https://specfun.inria.fr/chyzak/gbdacr/.
- Impact of F4 to efficiency still unclear.

In progress

- Extension to modules motivates another specific ordering.
- Algorithm to determine well-foundedness of a general divide-and-conquer recurrence system.