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

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)

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)

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 $\mathbb{N} \simeq \mathbb{Q}$. (Stern, 1858)

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 $\mathbb{N} \simeq \mathbb{Q}$. (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

$$\begin{cases} u_{2n} = 2v_{n-1} - n \\ u_{2n+1} = u_n + v_{n+1} \\ v_{2n} = u_{2n+1} \\ v_{2n+1} = 2v_n + u_{n+1} \end{cases}$$

$$\Downarrow$$

$$\begin{cases} u_{2n} = 2v_{n-1} - n \\ u_{2n+1} = u_n + v_{n+2} \\ v_{2n} = u_{2n+1} \\ v_{2n+1} = 2v_n + u_{n+1} \end{cases}$$

$$\Downarrow$$

Higher-Order Recurrences, Well-Foundedness

$$\begin{cases} u_{2n} = 2v_{n-1} - n \\ u_{2n+1} = u_n + v_{n+2} \\ v_{2n} = u_{2n+1} \\ v_{2n+1} = 2v_n + u_{n+1} \end{cases}$$

$$\Downarrow$$

$$1 = 0$$

$$\begin{cases} u_{2n} = 2v_{n-1} - n \\ u_{2n+1} = u_n + v_{n+1} \\ v_{2n} = u_{2n+1} \\ v_{2n+1} = 2v_n + u_{n+1} \end{cases}$$

$$\Downarrow$$

$$\begin{cases} u_n = v_{2n} - v_{n+1} \\ v_{4n+4} = v_{2n+4} - v_{n+3} \\ \qquad + 2v_{n+1} + 2v_n - n - 1 \\ v_{2n+1} = v_{2n+2} - v_{n+2} + 2v_n \\ v_{4n+2} = v_{2n+2} + v_{2n} \\ v_0 = v_1 = 0 \quad v_2 = C \\ v_3 = -1 \qquad v_4 = -2 \end{cases}$$

Whole theory (in progress) based on a Gröbner-basis theory (here).

Section Operators and Skew Polynomials

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

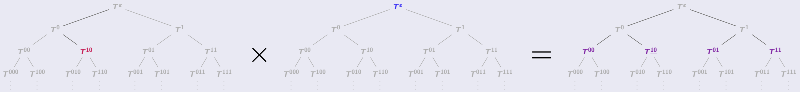
$$T^w \cdot \sum_{n\in\mathbb{N}} u_n x^n = \sum_{n\in\mathbb{N}} u_{b^\ell n+r} x^n \text{ where } \ell = |w| \text{ and } r = \sum_{i=0}^{\ell-1} w_i b^i$$

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

$k(x)\langle T_0, \dots, T_{b-1}\rangle$ with noncommutative monomials T^w

Noncommutative product

$$T^w T^v = T^{wv}, \quad T^w c(x) = T^w \left(c(x) T^\varepsilon\right) = \sum_{|w'|=|w|} d_{w'}(x) T^{w'}$$



$$d_{w'}(x) = \text{some suitable section of } c(x)$$

Section Operators and Skew Polynomials

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

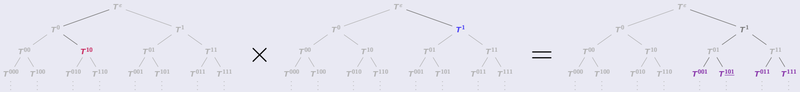
$$T^w \cdot \sum_{n \in \mathbb{N}} u_n x^n = \sum_{n \in \mathbb{N}} u_{b^\ell n + r} x^n \text{ where } \ell = |w| \text{ and } r = \sum_{i=0}^{\ell-1} w_i b^i$$

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

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

Noncommutative product

$$T^w T^v = T^{wv}, \qquad T^w (c(x) T^v) = \sum_{|w'|=|w|} d_{w'}(x) T^{w'v}$$



$d_{w'}(x) =$ some suitable section of $c(x)$

Earlier Works on Noncommutative Gröbner-Basis Theories

Noncommutative monomials, commuting with coefficients

Free noncommutative algebras (Mora, 1986, 1988, 1989). Path algebras (Ufnarovskiĭ, 1991; Green, 1993).

Monomials with commutation rules, commuting with coefficients

Weyl algebras (Galligo, 1985). Enveloping algebras of Lie algebras (Apel, Lassner, 1993). Polynomial rings of solvable type (Kandri-Rody, Weispfenning, 1990; Levandovskyy, Schönemann, 2003).

Monomials commuting with one another, but not with coefficients

Rings of difference-differential operators (Takayama, 1989). Ore algebras (Chyzak, Salvy, 1998).

Our need: *noncommutative monomials with commutation rules!*

Earlier Works on Noncommutative Gröbner-Basis Theories

Noncommutative monomials, commuting with coefficients

Free noncommutative algebras (Mora, 1986, 1988, 1989). Path algebras (Ufnarovskiĭ, 1991; Green, 1993). *Nonnoetherian.*

Monomials with commutation rules, commuting with coefficients

Weyl algebras (Galligo, 1985). Enveloping algebras of Lie algebras (Apel, Lassner, 1993). Polynomial rings of solvable type (Kandri-Rody, Weispfenning, 1990; Levandovskyy, Schönemann, 2003). *Noetherian.*

Monomials commuting with one another, but not with coefficients

Rings of difference-differential operators (Takayama, 1989). Ore algebras (Chyzak, Salvy, 1998). *Noetherian.*

Our need: *noncommutative monomials with commutation rules!*

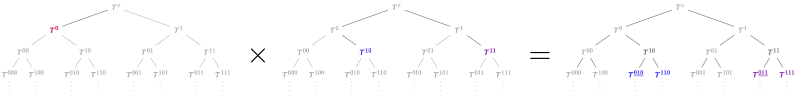
We restrict to finitely-presented ideals.

Monomial Ordering and Compatibility with Product

Breadth-first ordering

- Def.: $w < w'$ if either $|w| < |w'|$
  or $|w| = |w'|$ and $\mathrm{rev}(w) <_{\mathrm{lex}} \mathrm{rev}(w')$.
- Prop.: BFO guarantees the termination of division and a compatibility lemma crucial to the correctness of algorithms.

$$T^{w}\,(c_1(x)\,T^{v_1} + c_2(x)\,T^{v_2}) = \cdots$$



Compatibility lemma

For any skew polynomials H, K_1 and K_2 from $k(x)\langle T\rangle$, if $H \neq 0$ and $\mathrm{Im}(K_1) < \mathrm{Im}(K_2)$, then $\mathrm{Im}(HK_1) < \mathrm{Im}(HK_2)$.

Division of Skew Polynomials

Division theorem

Given divisors $B_1, \dots, B_s$, 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 $\mathrm{lm}(B_i)$;
- for each i, $\mathrm{lm}(Q_i B_i) \leq \mathrm{lm}(A)$.

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 $B_1, \dots, B_s$, 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 $\mathrm{lm}(B_i)$;
- for each i, $\mathrm{lm}(Q_i B_i) \leq \mathrm{lm}(A)$.

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

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 $F \in \mathcal{I}$, $\operatorname{lm}(F)$ is divisible by $\operatorname{lm}(G)$ 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 $\operatorname{lm}(H_2) = T^w \operatorname{lm}(H_1)$ 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 $\operatorname{lm}(Q_i F_i) \leq \operatorname{lm}(H)$.

Criterion: all S-polynomials have a standard representation $\implies$ $\mathcal{F}$ is a Gröbner basis.

Linear Algebra Approach and a Variant F4 Algorithm

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.

Linear Algebra Approach and a Variant F4 Algorithm

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.

problem	01	35	38	14	39	42	18	15	43
radix	2	2	3	2	3	2	3	2	2
deg/dim	3/14	6/127	4/161	5/63	5/485	4/31	4/161	6/127	5/63
#in/#out	7/2	5/5	5/5	5/5	5/5	24/1	4/4	6/6	48/1
Buchberger	0.29	1.89	2.09	0.46	9.10	4.90	1.64	1.98	69.95
F4	0.26	0.65	0.77	2.76	2.86	5.39	9.68	25.50	77.41
speed-up	1.09	2.91	2.70	0.17	3.18	0.91	0.17	0.08	0.90

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.