A Factorization Algorithm for G-Algebras and Applications

ACA 2016 – Kassel – Germany

Albert Heinle

Symbolic Computation Group
David R. Cheriton School of Computer Science
University of Waterloo
Canada

2016–08–04

Introduction

Factorization Properties of Integral Domains

For integral domains (in the literature commonly assumed to be commutative rings) many factorization properties have been defined. (c.f. (Anderson et al., 1990; Anderson and Anderson, 1992; Anderson and Mullins, 1996; Anderson, 1997))

$$
\begin{tikzcd}
 & \mathrm{HFD} \arrow[dr, Rightarrow] & & & \\
\mathrm{UFD} \arrow[ur, Rightarrow] \arrow[r, Rightarrow] \arrow[dr, Rightarrow] & \mathrm{FFD} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \mathrm{BFD} \arrow[r, Rightarrow] & \mathrm{ACCP} \arrow[r, Rightarrow] & \text{atomic.} \\
 & \text{idf-domain} & & &
\end{tikzcd}
$$

Figure : from (Anderson et al., 1990)

Factorization Properties of Integral Domains

For integral domains (in the literature commonly assumed to be commutative rings) many factorization properties have been defined. (c.f. (Anderson et al., 1990; Anderson and Anderson, 1992; Anderson and Mullins, 1996; Anderson, 1997))

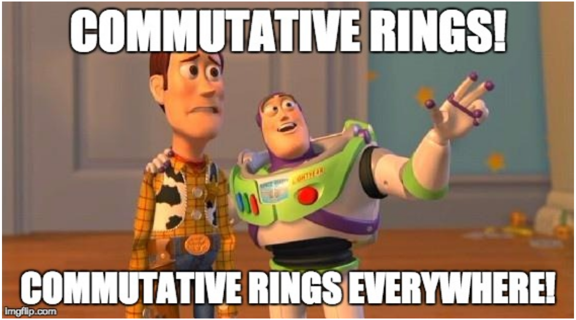

Figure : Created on `https://imgflip.com/`

What has been done for Non-Commutative Rings?

- Free associative algebras are unique factorization domains (Cohn, 1963).
- Certain Ore domains (like the Weyl algebra) are unique factorization domains (e.g. (Bueso et al., 2003)).

What has been done for Non-Commutative Rings?

- Free associative algebras are unique factorization domains (Cohn, 1963).
- Certain Ore domains (like the Weyl algebra) are unique factorization domains (e.g. (Bueso et al., 2003)).

STOP

What has been done for Non-Commutative Rings?

- Free associative algebras are unique factorization domains (Cohn, 1963).
- Certain Ore domains (like the Weyl algebra) are unique factorization domains (e.g. (Bueso et al., 2003)).

STOP

The factors are only unique up to similarity!

What has been done for Non-Commutative Rings?

- Free associative algebras are unique factorization domains (Cohn, 1963).
- Certain Ore domains (like the Weyl algebra) are unique factorization domains (e.g. (Bueso et al., 2003)).

STOP

The factors are only unique up to similarity!

Definition

Let R be a ring. Two elements $a, b \in R$ are said to be **similar**, if R/Ra and R/Rb are isomorphic as left R-modules.

However, similarity is a very weak property, as one can e.g. see in (Giesbrecht and Heinle, 2012).

On Non-Commutative Finite Factorization Domains

Definitions

Definition (Commutative FFD, cf. (Anderson et al., 1990))

Let R be a commutative integral domain. Then R is a finite factorization domain (FFD) if each nonzero non-unit of R has only a finite number of non-associate divisors and hence, only a finite number of factorizations up to order and associates.

Definition (Non-Commutative FFD, cf. (Bell et al., 2014))

Let A be a (not necessarily commutative) domain. We say that A is a finite factorization domain (FFD, for short), if every nonzero, non-unit element of A has at least one factorization into irreducible elements and there are at most finitely many distinct factorizations into irreducible elements up to multiplication of the irreducible factors by central units in A.

Definitions

Definition (Commutative FFD, cf. (Anderson et al., 1990))

Let R be a commutative integral domain. Then R is a finite factorization domain (FFD) if each nonzero non-unit of R has only a finite number of non-associate divisors and hence, only a finite number of factorizations up to order and associates.

Definition (Non-Commutative FFD, cf. (Bell et al., 2014))

Let A be a (not necessarily commutative) domain. We say that A is a finite factorization domain (FFD, for short), if every nonzero, non-unit element of A has at least one factorization into irreducible elements and there are at most finitely many distinct factorizations into irreducible elements up to multiplication of the irreducible factors by central units in A.

Necessary Conditions for Non-Commutative FFDs

Theorem (cf. (Bell et al., 2014))

Let $\mathbb{K}$ be an algebraically closed field and let A be a $\mathbb{K}$-algebra. If there exists a finite-dimensional filtration $\{V_n \colon n \in \mathbb{N}\}$ on A such that the associated graded algebra $B = \mathrm{gr}_V(A)$ is a (not necessarily commutative) domain over $\mathbb{K}$, then A is a finite factorization domain over $\mathbb{K}$.

Necessary Conditions for Non-Commutative FFDs

Theorem (cf. (Bell et al., 2014))

Let $\mathbb{K}$ be an algebraically closed field and let A be a $\mathbb{K}$-algebra. If there exists a finite-dimensional filtration $\{V_n \colon n \in \mathbb{N}\}$ on A such that the associated graded algebra $B = \mathrm{gr}_V(A)$ is a (not necessarily commutative) domain over $\mathbb{K}$, then A is a finite factorization domain over $\mathbb{K}$.

Corollary (cf. (Bell et al., 2014))

Let $\mathbb{K}$ be a field and let A be a $\mathbb{K}$-algebra. If there exists a finite-dimensional filtration $\{V_n \colon n \in \mathbb{N}\}$ on A such that the associated graded algebra $B = \mathrm{gr}_V(A)$ has the property that $B \otimes_{\mathbb{K}} \overline{\mathbb{K}}$ is a (not necessarily commutative) domain, then A is a finite factorization domain.

Example for a Commutative Non-FFD

Example

Let $\mathbb{K} = \mathbb{R}$ and $A = \mathbb{R} + \mathbb{C}[t] \cdot t \subseteq \mathbb{C}[t]$. We consider the filtration induced by the degree in t on this algebra. Then the associated graded algebra of A is A itself again, i.e. a domain. But we have infinitely many factorizations of t^2 of the form

$$t^2 = (\cos(\theta) + i\sin(\theta))t \cdot (\cos(\theta) - i\sin(\theta))t$$

for any $\theta \in [0, 2\pi)$. Notice that the units of A are precisely the nonzero real numbers and hence for $\theta \in [0, \pi)$ these factorizations are distinct.

Example for a Noncommutative Non-FFD

Let $\mathbb{K}(x)\langle\partial \mid \partial \cdot f(x) = f(x)\partial + f'(x)\rangle$. Then there are infinitely many factorizations of ∂^2 of the form

$$\partial^2 = \left(\partial + \frac{b}{x+c}\right)\left(\partial - \frac{b}{x+c}\right), \quad b, c \in \mathbb{K}.$$

G-Algebras

Definition

For $n \in \mathbb{N}$ and $1 \leq i < j \leq n$ consider the units $c_{ij} \in \mathbb{K}^*$ and polynomials $d_{ij} \in \mathbb{K}[x_1, \ldots, x_n]$. Suppose, that there exists a monomial total well-ordering $\prec$ on $\mathbb{K}[x_1, \ldots, x_n]$, such that for any $1 \leq i < j \leq n$ either $d_{ij} = 0$ or the leading monomial of d_{ij} is smaller than $x_i x_j$ with respect to $\prec$. The $\mathbb{K}$-algebra $A := \mathbb{K}\langle x_1, \ldots, x_n \mid \{x_j x_i = c_{ij} x_i x_j + d_{ij} \colon 1 \leq i < j \leq n\}\rangle$ is called a G-**algebra**, if $\{x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} : \alpha_i \in \mathbb{N}_0\}$ is a $\mathbb{K}$-basis of A.

Remark

- *Also known as "algebras of solvable type" and "PBW (Poincaré Birkhoff Witt) Algebras"*

Examples for G-Algebras

- Weyl algebras ($\mathbb{K}\langle x_1, \ldots, x_n, \partial_1, \ldots, \partial_n \mid \forall i : \partial_i x_i = x_i \partial_i + 1\rangle$)
- Shift algebras ($\mathbb{K}\langle x_1, \ldots, x_n, s_1, \ldots, s_n \mid \forall i : s_i x_i = (x_i + 1) s_i\rangle$)
- q-Weyl algebras ($\mathbb{K}\langle x_1, \ldots, x_n, \partial_1, \ldots, \partial_n \mid \forall i \exists q_i \in \mathbb{K}^* : \partial_i x_i = q_i x_i \partial_i + 1\rangle$)
- q-Shift algebras ($\mathbb{K}\langle x_1, \ldots, x_n, s_1, \ldots, s_n \mid \forall i \exists q_i \in \mathbb{K}^* : s_i x_i = q_i x_i s_i\rangle$)
- Universal enveloping algebras of finite dimensional Lie algebras.
- $\ldots$

G-Algebras are FFD

Theorem (cf. (Bell et al., 2014))

Let $\mathbb{K}$ be a field. Then G-algebras over $\mathbb{K}$ and their subalgebras are finite factorization domains.

Consequences

- We have now more than just the similarity property to characterize factorizations in G-algebras.
- New algorithmic problem: Calculate all factorizations of an element in a given G-algebra.
- With this knowledge, study how algorithms from commutative algebra can be generalized to certain non-commutative algebras.

Non-Commutative Factorized Gröbner Bases

Factorized Gröbner bases – Commutative

- The factorized Gröbner approach has been studied extensively for the commutative case (Czapor, 1989b,a; Davenport, 1987; Gräbe, 1995a,b).
- Application: Obtaining triangular sets.
- Possible extension: Allowing constraints on the solutions.
- Implementations: e.g. in SINGULAR and REDUCE.
- Idea: For each factor $\tilde{g}$ of a reducible element g during a Gröbner computation, recursively call algorithm on the same generator set, with g being replaced by $\tilde{g}$.

Generalization to Non-Commutative Rings

- Ideals in commutative ring $\leftrightarrow$ Varieties
- Ideals in Non-Commutative ring $\leftrightarrow$ Solutions
- Formal notion of solutions: Let $\mathcal{F}$ be a left A-module for a $\mathbb{K}$-algebra A (space of solutions). Let a left A-module M be finitely presented by an $n \times m$ matrix P. Then

$$\mathrm{Sol}_A(P, \mathcal{F}) = \{f \in \mathcal{F}^m : Pf = 0\}$$

- Divisors for commutative rings $\leftrightarrow$ Right divisors for non-commutative rings.

Picking the Right Right Divisors

There are different strategies:

- Split Gröbner computation with respect to different irreducible right divisors.

Picking the Right Right Divisors

There are different strategies:

- Split Gröbner computation with respect to different irreducible right divisors. $\Rightarrow$ This approach may cause lost of possible solutions to the whole system.

Picking the Right Right Divisors

There are different strategies:

- Split Gröbner computation with respect to different irreducible right divisors. $\Rightarrow$ This approach may cause lost of possible solutions to the whole system.
- Split Gröbner computation with respect to all possible maximal right divisors.

Picking the Right Right Divisors

There are different strategies:

- Split Gröbner computation with respect to different irreducible right divisors. $\Rightarrow$ This approach may cause lost of possible solutions to the whole system.
- Split Gröbner computation with respect to all possible maximal right divisors. $\Rightarrow$ Less possible solutions may be lost.

Picking the Right Right Divisors

There are different strategies:

- Split Gröbner computation with respect to different irreducible right divisors. $\Rightarrow$ This approach may cause lost of possible solutions to the whole system.
- Split Gröbner computation with respect to all possible maximal right divisors. $\Rightarrow$ Less possible solutions may be lost.
- Split Gröbner computation with respect to all possible non-unique maximal right divisors.

Picking the Right Right Divisors

There are different strategies:

- Split Gröbner computation with respect to different irreducible right divisors. $\Rightarrow$ This approach may cause lost of possible solutions to the whole system.
- Split Gröbner computation with respect to all possible maximal right divisors. $\Rightarrow$ Less possible solutions may be lost.
- Split Gröbner computation with respect to all possible non-unique maximal right divisors. $\Rightarrow$ Our choice!

Remark

This methodology also appears in the context of semifirs, where the concept of so called block factorizations or cleavages has been introduced to study the reducibility of a principal ideal (Cohn, 2006, Chapter 3.5).

Main Difference

In the commutative case, for an ideal I and the output $B_1, \ldots, B_m$ of the factorized Gröbner basis algorithm, one has

$$\sqrt{I} = \bigcap_{i=1}^{m} \sqrt{B_i}.$$

We would like to have something similar for the non-commutative case.
However, as the next example depicts, we do not have it in our setting.

Example I

Let

$$p = (x^6 + 2x^4 - 3x^2)\partial^2 - (4x^5 - 4x^4 - 12x^2 - 12x)\partial + (6x^4 - 12x^3 - 6x^2 - 24x - 12)$$

in the polynomial first Weyl algebra. This polynomial appears in (Tsai, 2000, Example 5.7) and has two different factorizations, namely

$$\begin{aligned} p =& (x^4\partial - x^3\partial - 3x^3 + 3x^2\partial + 6x^2 - 3x\partial - 3x + 12) \cdot \\ & (x^2\partial + x\partial - 3x - 1) \\ =& (x^4\partial + x^3\partial - 4x^3 + 3x^2\partial - 3x^2 + 3x\partial - 6x - 3) \cdot \\ & (x^2\partial - x\partial - 2x + 4). \end{aligned}$$

Example II

A reduced Gröbner basis of
$\langle x^2\partial + x\partial - 3x - 1\rangle \cap \langle x^2\partial - x\partial - 2x + 4\rangle$, computed with SINGULAR, is given by

$$\begin{aligned}\{&3x^5\partial^2 + 2x^4\partial^3 - x^4\partial^2 - 12x^4\partial + x^3\partial^2 - 2x^2\partial^3 + 16x^3\partial \\ &+ 9x^2\partial^2 + 18x^3 + 4x^2\partial + 4x\partial^2 - 42x^2 - 4x\partial - 12x - 12, \\ &2x^4\partial^4 - 2x^4\partial^3 + 11x^4\partial^2 + 12x^3\partial^3 - 2x^2\partial^4 - 2x^3\partial^2 \\ &+ 10x^2\partial^3 - 44x^3\partial - 17x^2\partial^2 + 64x^2\partial + 12x\partial^2 + 66x^2 \\ &+ 52x\partial + 4\partial^2 - 168x - 16\partial - 60\}.\end{aligned}$$

Remark

The space of holomorphic solutions of the differential equation associated to p in fact coincides with the union of the solution spaces of the two generators of the intersection.

Last Definition before the Algorithm

Definition

Let B, C be finite subsets in $\mathcal{G}$. We call the tuple (B, C) a **constrained Gröbner tuple**, if B is a Gröbner basis of $\langle B \rangle$, and $\mathrm{NF}(g, B) \neq 0$ for every $g \in C$. We call a constrained Gröbner tuple **factorized**, if every $f \in B$ is either irreducible or has a unique irreducible left divisor.

Factorized Gröbner bases Algorithm for G-Algebras (FGBG)

- **Input:** $B := \{f_1, \ldots, f_k\} \subset \mathcal{G}$, $C := \{g_1, \ldots, g_l\} \subset \mathcal{G}$.
- **Output:** $R := \{(\tilde{B}, \tilde{C}) \mid (\tilde{B}, \tilde{C})$ is factorized constrained Gröbner tuple$\}$ with $\langle B \rangle \subseteq \bigcap_{(\tilde{B}, \tilde{C}) \in R} \langle \tilde{B} \rangle$
- **Assumption:** We can find all factorizations of an element in $\mathcal{G}$.
- **Algorithm:**
  - If one of the f_i is reducible and has more than one distinct factorization, set $M := \{(f_i^{(1)}, f_i^{(2)} \mid f_i^{(1)}, f_i^{(2)} \in \mathcal{G} \setminus \mathbb{K}, \mathrm{lc}(f_i^{(1)}) = \mathrm{lc}(f_i^{(2)}) = 1, f_i^{(1)} \cdot f_i^{(2)} = f_i, f_i^{(1)}$ is irreducible$\}$ and return
  $$\bigcup_{(a,b) \in M} \mathrm{FGBG}\left((B \setminus \{f_i\}) \cup \{b\}, C \cup \bigcup_{\substack{(\tilde{a}, \tilde{b}) \in M \\ b \neq \tilde{b}}} \{\tilde{b}\} \right)$$
  - $P := \{(f_i, f_j) \mid i, j \in \{1, \ldots, k\}, i < j\}$
  - While $P \neq \emptyset$:
    - Pick $(f, g) \in P$ and remove it from P, compute the S-polynomial of f and g and its normal form h with respect to B.
    - If $h \neq 0$ and h is reducible, return $\mathrm{FGBG}(B \cup \{h\}, C)$.
    - If $h \neq 0$ and h is irreducible, $P := P \cup \{(h, f) \mid f \in B\}$ and $B := B \cup \{h\}$
    - If there exists $i \in \{1, \ldots, l\}$ with $\mathrm{NF}(g_i, B) = 0$, return $\emptyset$.
  - Return (B, C)

Example I

We consider the first Weyl algebra. Let

$$B := \{\partial^4 + x\partial^2 - 2\partial^3 - 2x\partial + \partial^2 + x + 2\partial - 2, \\ x\partial^3 + x^2\partial - x\partial^2 + \partial^3 - x^2 + x\partial - 2\partial^2 - x + 1\}$$

and $C := \{\partial - 1\}$. Each element factors separately as

$$\begin{aligned} f_1 :=& \partial^4 + x\partial^2 - 2\partial^3 - 2x\partial + \partial^2 + x + 2\partial - 2 \\ =& (\partial^3 + x\partial - \partial^2 - x + 2) \cdot (\partial - 1) \\ =& (\partial - 1) \cdot (\partial^3 + x\partial - \partial^2 - x + 1), \end{aligned}$$

respectively

$$\begin{aligned} f_2 :=& x\partial^3 + x^2\partial - x\partial^2 + \partial^3 - x^2 + x\partial - 2\partial^2 - x + 1 \\ =& (x\partial^2 + x^2 + \partial^2 + x - \partial - 1) \cdot (\partial - 1) \\ =& (x\partial - x + \partial - 2) \cdot (\partial^2 + x). \end{aligned}$$

Example II

Hence, FGBG will return two recursive calls of itself, namely

- $\cancel{\mathrm{FGBG}(\{\partial - 1, f_2\}, \{\partial - 1, \partial^3 + x\partial - \partial^2 - x + 1\})}$
- $\mathrm{FGBG}(\{\partial^3 + x\partial - \partial^2 - x + 1, f_2\}, C)$

$\partial^3 + x\partial - \partial^2 - x + 1$ has only one possible factorization.
Considering factorizations of f_2, we get two further recursive calls:

- $\cancel{\mathrm{FGBG}(\{b_1, \partial - 1\}, \{\partial - 1, \partial^2 + x\})}$
- $\mathrm{FGBG}(\{\partial^3 + x\partial - \partial^2 - x + 1, \partial^2 + x\}, C)$

Since $\partial^2 + x$ divides $\partial^3 + x\partial - \partial^2 - x + 1$ from the right, our algorithm returns $\{(\{\partial^2 + x\}, C)\}$ as final output.

Conclusion and Future Work

Beer Challenge

- Let $p_1, p_2 \in \mathbb{Q}$ be non-square numbers, which are negative and have either 1,2 or 4 in the denominator.
- Define

$$\begin{aligned} A := \mathbb{Q}\langle x, y, z, u \,| & xy + yx = xz + zx = yz + zy = 0, \\ & ux + xu = 0, uy + yu = y^2, uz + zu = z^2, \\ & x^2 = p_1 y^2 + p_2 z^2 \rangle. \end{aligned}$$

Beer Challenge

- Let $p_1, p_2 \in \mathbb{Q}$ be non-square numbers, which are negative and have either 1,2 or 4 in the denominator.
- Define

$$\begin{aligned} A := \mathbb{Q}\langle x, y, z, u \,|\, & xy + yx = xz + zx = yz + zy = 0, \\ & ux + xu = 0, uy + yu = y^2, uz + zu = z^2, \\ & x^2 = p_1 y^2 + p_2 z^2 \rangle. \end{aligned}$$

Proof that A is a finite factorization domain.

Future Work

- FFDs are generalized... What about BFDs, HFDs, etc.?
- More non-commutative FFDs are to be identified.
- More efficient algorithms to factor (certain) G-algebras.
- Study the output of non-commutative factorized Gröbner basis algorithm. What does it say about the ideal structure? What is the connection to the solution space?
- Implementation of all the algorithms (partly done). Latest `ncfactor.lib` can be found in the SINGULAR GitHub repository[1].

[1] `https://github.com/Singular/Sources/blob/spielwiese/Singular/LIB/ncfactor.lib`

Bibliography I

Anderson, D. (1997). *Factorization in integral domains*, volume 189. CRC Press.

Anderson, D. and Anderson, D. (1992). Elasticity of factorizations in integral domains. *Journal of pure and applied algebra*, 80(3):217–235.

Anderson, D., Anderson, D., and Zafrullah, M. (1990). Factorization in integral domains. *Journal of pure and applied algebra*, 69(1):1–19.

Anderson, D. and Mullins, B. (1996). Finite factorization domains. *Proceedings of the American Mathematical Society*, 124(2):389–396.

Bell, J. P., Heinle, A., and Levandovskyy, V. (2014). On noncommutative finite factorization domains. *To Appear in the Transactions of the American Mathematical Society; arXiv preprint arXiv:1410.6178*.

Bueso, J., Gómez-Torrecillas, J., and Verschoren, A. (2003). *Algorithmic methods in non-commutative algebra. Applications to quantum groups.* Dordrecht: Kluwer Academic Publishers.

Cohn, P. (1963). Noncommutative unique factorization domains. *Transactions of the American Mathematical Society*, 109(2):313–331.

Cohn, P. M. (2006). *Free ideal rings and localization in general rings*, volume 3. Cambridge University Press.

Czapor, S. R. (1989a). Solving algebraic equations: combining Buchberger's algorithm with multivariate factorization. *Journal of Symbolic Computation*, 7(1):49–53.

Czapor, S. R. (1989b). Solving algebraic equations via Buchberger's algorithm. In *Eurocal'87*, pages 260–269. Springer.

Davenport, J. H. (1987). Looking at a set of equations. *Technical report, School of Mathematical Sciences, The University of Bath.*

Giesbrecht, M. and Heinle, A. (2012). A Polynomial-Time Algorithm for the Jacobson Form of a Matrix of Ore Polynomials. In *Computer Algebra in Scientific Computing*, pages 117–128. Springer.

Giesbrecht, M., Heinle, A., and Levandovskyy, V. (2015). Factoring linear partial differential operators in n variables. *Journal of Symbolic Computation*.

Gräbe, H.-G. (1995a). On factorized Gröbner bases. In *Computer algebra in science and engineering, pages 77–89. World Scientific*. Citeseer.

Bibliography II

Gräbe, H.-G. (1995b). *Triangular systems and factorized Gröbner bases*. Springer.

Lazard, D. (1991). A new method for solving algebraic systems of positive dimension. *Discrete Applied Mathematics*, 33(1-3):147–160.

Lazard, D. (1992). Solving zero-dimensional algebraic systems. *Journal of symbolic computation*, 13(2):117–131.

Möller, H. M. (1993). On decomposing systems of polynomial equations with finitely many solutions. *Applicable Algebra in Engineering, Communication and Computing*, 4(4):217–230.

Tsai, H. (2000). Weyl closure of a linear differential operator. *Journal of Symbolic Computation*, 29:747–775.