On Factoring Differential Operators in n Variables

*A*pplications of *C*omputer *A*lgebra 2014, New York

Albert Heinle

Symbolic Computation Group
University of Waterloo

July 8, 2014

Joint work with Mark Giesbrecht and Viktor Levandovskyy

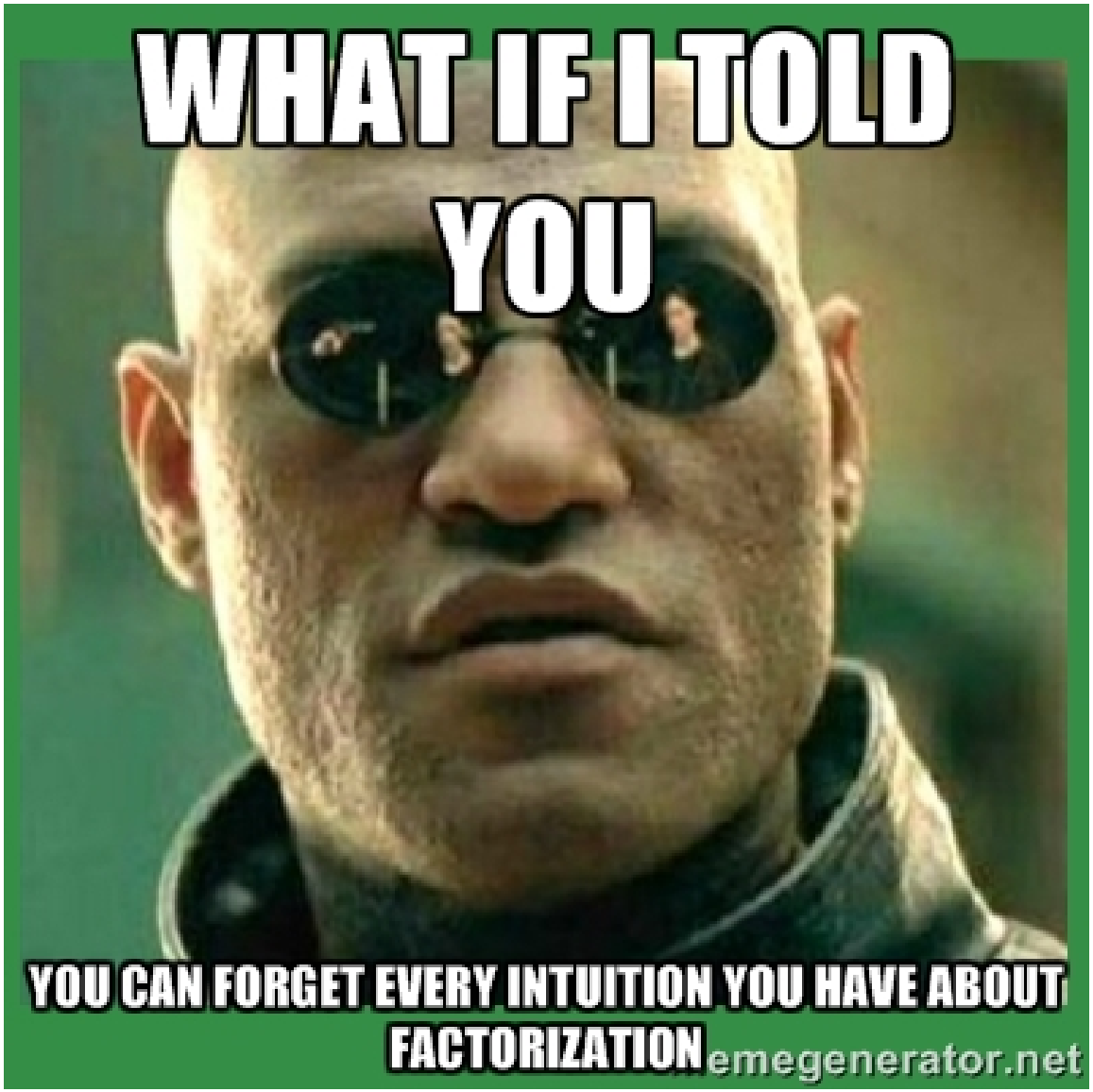


Figure: Generated on memegenerator.net

Section 1

Introduction and Motivation

Basics

- $\mathbb{K}$ always denotes a field of characteristic zero. (most of the results also applicable for finite fields)
- For $n \in \mathbb{N}$, we write $\underline{n}$ for the set $\{1, \ldots, n\}$.
- We occasionally abbreviate a selection of variables $v_1, \ldots, v_n$ by $\underline{v}$.

The Weyl Algebra

Definition

The ***n*th Weyl algebra** A_n for $n \in \mathbb{N}$ is defined as

$$A_n := \mathbb{K}\Big\langle x_1, \ldots, x_n, \partial_1, \ldots, \partial_n | \text{ for } (i,j) \in \underline{n} \times \underline{n} : \partial_i x_j = \begin{cases} x_j \partial_i, & \text{if } i \neq j \\ x_j \partial_i + 1, & \text{if } i = j \end{cases}, \partial_i \partial_j - \partial_j \partial_i = x_i x_j - x_j x_i = 0 \Big\rangle.$$

Definition

If we allow the x_i in A_1 to appear as rational arguments, we call the resulting algebra the **rational *n*th Weyl algebra**.

Factorization in Non-Commutative Rings

- Factors unique only up to a weak notion of similarity (a and b in A_n are similar : $\iff$ $A_n/A_n a \cong A_n/A_n b$; more in [BGTV03]).
- There are infinitely many distinct factorizations possible (example: $\partial_1^2 \in A_1$ in the rational Weyl algebra).
- Decision needs to be made about which factorization is more "useful" than another.

Factorization in Non-Commutative Rings

- Factors unique only up to a weak notion of similarity (a and b in A_n are similar : $\iff$ $A_n/A_n a \cong A_n/A_n b$; more in [BGTV03]).
- There are infinitely many distinct factorizations possible (example: $\partial_1^2 \in A_1$ in the rational Weyl algebra).
- Decision needs to be made about which factorization is more "useful" than another.

Example

The polynomial

$$x_1^6\partial_1^6+40x_1^5\partial_1^5+550x_1^4\partial_1^4+3200x_1^3\partial_1^3+7800x_1^2\partial_1^2+6720x_1\partial_1+1200 \in A_1$$

has 3547 distinct factorizations.

Section 2

Structuring the Weyl Algebras

Structuring A_n

Biggest problem: Structure needs to be congruent with the non-commutative relations

$$\partial_i x_i = x_i \partial_i + 1.$$

Structuring A_n

Biggest problem: Structure needs to be congruent with the non-commutative relations

$$\partial_i x_i = x_i \partial_i + 1.$$

Solution: Introduce $\mathbb{Z}^n$-grading on A_n (weight vector $[-v, v]$ for $v \in \mathbb{Z}^n$; for simplicity we choose $v = [1, \ldots, 1]$).
We view $\mathbb{Z}^n$ as ordered monoid via the absolute graded lexicographical ordering.

Structuring A_n

Biggest problem: Structure needs to be congruent with the non-commutative relations

$$\partial_i x_i = x_i \partial_i + 1.$$

Solution: Introduce $\mathbb{Z}^n$-grading on A_n (weight vector $[-v, v]$ for $v \in \mathbb{Z}^n$; for simplicity we choose $v = [1, \ldots, 1]$).
We view $\mathbb{Z}^n$ as ordered monoid via the absolute graded lexicographical ordering.

Remark: For $n = 1$, the same grading lies behind the Kashiwara and Malgrange V-filtration ([Kas83],[Mal83]).

Gaining Intuition with the $\mathbb{Z}^n$-grading

Example

We have in A_1

$$\deg(x_1\partial_1) = \deg(\partial_1 x_1 - 1) = 0.$$

In A_3, the element $x_1x_2\partial_1\partial_3 + x_1x_2^2x_3\partial_1\partial_2\partial_3^2$ is homogeneous of degree $[0, -1, 1]$.

Gaining Intuition with the $\mathbb{Z}^n$-grading

Example

We have in A_1

$$\deg(x_1\partial_1) = \deg(\partial_1 x_1 - 1) = 0.$$

In A_3, the element $x_1x_2\partial_1\partial_3 + x_1x_2^2x_3\partial_1\partial_2\partial_3^2$ is homogeneous of degree $[0, -1, 1]$.

Definition

We denote by $A_n^{(z)}$ for $z \in \mathbb{Z}^n$ the set of **homogeneous** polynomials of degree z.

Gaining Intuition with the $\mathbb{Z}^n$-grading

Example

We have in A_1

$$\deg(x_1\partial_1) = \deg(\partial_1 x_1 - 1) = 0.$$

In A_3, the element $x_1x_2\partial_1\partial_3 + x_1x_2^2x_3\partial_1\partial_2\partial_3^2$ is homogeneous of degree $[0, -1, 1]$.

Definition

We denote by $A_n^{(z)}$ for $z \in \mathbb{Z}^n$ the set of **homogeneous** polynomials of degree z.

Definition

We define the so called i**th Euler Operator** for $i \in \underline{n}$ by $\theta_i := x_i\partial_i$. Clearly $\mathbb{K}[\theta_1, \ldots, \theta_n] \subseteq A_1^{(0)}$.

And this is why we "$(x^2+y^2-1)^3-x^2y^3=0$" $\mathbb{Z}^n$-grading

- $A_n^{(\underline{0})}$, where $\underline{0} := [0,\ldots,0]$, is a ring and isomorphic to $\mathbb{K}[\theta_1,\ldots,\theta_n]$.
- θ_i and θ_i+1 for $i \in \underline{n}$ are the only irreducible monic polynomials in $\mathbb{K}[\underline{\theta}]$, that are reducible in A_n.
- $A_n^{(z)}$ for $z \in \mathbb{Z}^n$ is a cyclic $A_n^{(\underline{0})}$-bi-module.

And this is why we "$(x^2+y^2-1)^3-x^2y^3=0$" $\mathbb{Z}^n$-grading

- $A_n^{(\underline{0})}$, where $\underline{0} := [0,\ldots,0]$, is a ring and isomorphic to $\mathbb{K}[\theta_1,\ldots,\theta_n]$.
- θ_i and θ_i+1 for $i \in \underline{n}$ are the only irreducible monic polynomials in $\mathbb{K}[\underline{\theta}]$, that are reducible in A_n.
- $A_n^{(z)}$ for $z \in \mathbb{Z}^n$ is a cyclic $A_n^{(\underline{0})}$-bi-module.

This is why factorization of homogeneous polynomials can be reduced to commutative factorization in $\mathbb{K}[\underline{\theta}]$ and simple combinatorics!!!

And this is why we "$(x^2+y^2-1)^3-x^2y^3=0$" $\mathbb{Z}^n$-grading

- $A_n^{(\underline{0})}$, where $\underline{0} := [0,\ldots,0]$, is a ring and isomorphic to $\mathbb{K}[\theta_1,\ldots,\theta_n]$.
- θ_i and θ_i+1 for $i \in \underline{n}$ are the only irreducible monic polynomials in $\mathbb{K}[\underline{\theta}]$, that are reducible in A_n.
- $A_n^{(z)}$ for $z \in \mathbb{Z}^n$ is a cyclic $A_n^{(\underline{0})}$-bi-module.

This is why factorization of homogeneous polynomials can be reduced to commutative factorization in $\mathbb{K}[\underline{\theta}]$ and simple combinatorics!!!

Some more secrets:

- Any irreducible homogeneous polynomial in A_n stays irreducible in the rational Weyl algebra.
- The number of different factorizations of homogeneous polynomials in $A_n^{(z)}$ can be bounded with respect to the number of factors of the $A_n^{(\underline{0})}$-coefficients and the euclidean norm of z.

Another Example: The Weyl Hydra

$$(10x_1^4\partial_1^3 + 26x_1^3\partial_1^3 + 47x_1^4 - 117x_1^3\partial_1 - 78x_1^2\partial_1^2 + 117x_1^2 + 156x_1\partial_1 - 156) \qquad x_1$$

Another Example: The Weyl Hydra

Let

$$f = 10x_1^4\partial_1^3+26x_1^3\partial_1^3+47x_1^4-117x_1^3\partial_1-78x_1^2\partial_1^2+117x_1^2+156x_1\partial_1-156 \in A_1.$$

It is irreducible as element in A_1 (this also holds for the rational Weyl algebra).

Another Example: The Weyl Hydra

Let

$$f = 10x_1^4\partial_1^3+26x_1^3\partial_1^3+47x_1^4-117x_1^3\partial_1-78x_1^2\partial_1^2+117x_1^2+156x_1\partial_1-156 \in A_1.$$

It is irreducible as element in A_1 (this also holds for the rational Weyl algebra). We have the following surprising identity:

$$f \cdot x_1 = x_1 \cdot x_1 \cdot x_1 \cdot x_1 \cdot (10x_1\partial_1^3 + 26\partial_1^3 + 30\partial_1^2 + 47x_1 - 117\partial_1)$$

???WHY???

Another Example: The Weyl Hydra

Let

$$f = 10x_1^4\partial_1^3 + 26x_1^3\partial_1^3 + 47x_1^4 - 117x_1^3\partial_1 - 78x_1^2\partial_1^2 + 117x_1^2 + 156x_1\partial_1 - 156 \in A_1.$$

It is irreducible as element in A_1 (this also holds for the rational Weyl algebra).
We can rewrite f with respect to its homogeneous summands:

$$\begin{aligned} f = \quad & 26x_1^3\partial_1^3 - 78x_1^2\partial_1^2 + 156x_1\partial_1 - 156 && \text{(degree 0)} \\ & + 10x_1^4\partial_1^3 && \text{(degree } -1\text{)} \\ & + 117x_1^2 - 117x_1^3\partial_1 && \text{(degree } -2\text{)} \\ & + 47x_1^4 && \text{(degree } -4\text{)} \end{aligned}$$

Another Example: The Weyl Hydra

Let

$$f = 10x_1^4\partial_1^3 + 26x_1^3\partial_1^3 + 47x_1^4 - 117x_1^3\partial_1 - 78x_1^2\partial_1^2 + 117x_1^2 + 156x_1\partial_1 - 156 \in A_1.$$

It is irreducible as element in A_1 (this also holds for the rational Weyl algebra).
We can rewrite f with respect to its homogeneous summands:

$$\begin{aligned} f = \quad & 26(\theta_1 - 1)(\theta_1 - 2)(\theta_1 - 3) && \text{(degree 0)} \\ & + 10(\theta_1 - 1)(\theta_1 - 2)(\theta_1 - 3) \cdot x_1 && \text{(degree } -1\text{)} \\ & - 117(\theta_1 - 3) \cdot x_1^2 && \text{(degree } -2\text{)} \\ & + 47 \cdot x_1^4 && \text{(degree } -4\text{)} \end{aligned}$$

Another Example: The Weyl Hydra

Let

$$f = 10x_1^4\partial_1^3 + 26x_1^3\partial_1^3 + 47x_1^4 - 117x_1^3\partial_1 - 78x_1^2\partial_1^2 + 117x_1^2 + 156x_1\partial_1 - 156 \in A_1.$$

It is irreducible as element in A_1 (this also holds for the rational Weyl algebra).
And now multiplying x_1 from the right:

$$\begin{aligned} f \cdot x_1 = \quad & 26(\theta_1 - 1)(\theta_1 - 2)(\theta_1 - 3) \cdot x_1 && \text{(degree } -1) \\ & +10(\theta_1 - 1)(\theta_1 - 2)(\theta_1 - 3) \cdot x_1^2 && \text{(degree } -2) \\ & -117(\theta_1 - 3) \cdot x_1^3 && \text{(degree } -3) \\ & +47 \cdot x_1^5 && \text{(degree } -5) \end{aligned}$$

Another Example: The Weyl Hydra

Let

$$f = 10x_1^4\partial_1^3 + 26x_1^3\partial_1^3 + 47x_1^4 - 117x_1^3\partial_1 - 78x_1^2\partial_1^2 + 117x_1^2 + 156x_1\partial_1 - 156 \in A_1.$$

It is irreducible as element in A_1 (this also holds for the rational Weyl algebra).
Switching the positions of x_1 to the left:

$$\begin{aligned} f \cdot x_1 = \quad & x_1 \cdot 26(\theta_1)(\theta_1 - 1)(\theta_1 - 2) && \text{(degree } -1) \\ & + x_1^2 \cdot 10(\theta_1 + 1)(\theta_1)(\theta_1 - 1) && \text{(degree } -2) \\ & + x_1^3 \cdot (-117\theta_1) && \text{(degree } -3) \\ & + x_1^5 \cdot 47 && \text{(degree } -5) \end{aligned}$$

Another Example: The Weyl Hydra

Let

$$f = 10x_1^4\partial_1^3 + 26x_1^3\partial_1^3 + 47x_1^4 - 117x_1^3\partial_1 - 78x_1^2\partial_1^2 + 117x_1^2 + 156x_1\partial_1 - 156 \in A_1.$$

It is irreducible as element in A_1 (this also holds for the rational Weyl algebra).
Rewriting the θ_1 and $\theta_1 + 1$ plus switching:

$$\begin{aligned} f \cdot x_1 = \quad & 26x_1^4\partial_1^3 && \text{(degree } -1\text{)} \\ & + x_1^2 \cdot 10(x_1^3\partial_1^3 + 3x_1^2\partial_1^2) && \text{(degree } -2\text{)} \\ & + x_1^3 \cdot (-117x_1\partial_1) && \text{(degree } -3\text{)} \\ & + x_1^5 \cdot 47 && \text{(degree } -5\text{)} \end{aligned}$$

Another Example: The Weyl Hydra

Let

$$f = 10x_1^4\partial_1^3 + 26x_1^3\partial_1^3 + 47x_1^4 - 117x_1^3\partial_1 - 78x_1^2\partial_1^2 + 117x_1^2 + 156x_1\partial_1 - 156 \in A_1.$$

It is irreducible as element in A_1 (this also holds for the rational Weyl algebra).
Rewriting the θ_1 and $\theta_1 + 1$ plus switching:

$$\begin{aligned} f \cdot x_1 = \quad & x_1^4 \cdot 26\partial_1^3 && \text{(degree } -1\text{)} \\ & + x_1^4 \cdot 10(x_1\partial_1^3 + 3\partial_1^2) && \text{(degree } -2\text{)} \\ & + x_1^4 \cdot (-117\partial_1) && \text{(degree } -3\text{)} \\ & + x_1^4 \cdot 47x_1 && \text{(degree } -5\text{)} \end{aligned}$$

Section 3

Factoring Elements in the Weyl Algebras

Example

Let

$$\begin{aligned} p &:= \underbrace{\theta_1\partial_2}_{=p_{[0,1]}} + \underbrace{(\theta_1+3)\theta_2}_{=p_{[0,0]}} + \underbrace{x_2}_{=p_{[0,-1]}}, \\ q &:= \underbrace{(\theta_1+4)x_1\partial_2}_{=q_{[-1,1]}} + \underbrace{x_1}_{=q_{[-1,0]}} + \underbrace{(\theta_1+1)x_1x_2}_{=q_{[-1,-1]}} \in A_2 \text{ and} \end{aligned}$$

$$\begin{aligned} h &:= pq = \theta_1(\theta_1+4)x_1\partial_2^2 \\ &+ (\theta_1(\theta_1-1)\theta_2 + 8\theta_1\theta_2 + \theta_1 + 12\theta_2)x_1\partial_2 \\ &+ (\theta_1(\theta_1-1)\theta_2 + \theta_1^2 - \theta_1 + 4\theta_1\theta_2 + 2\theta_1 + 7\theta_2)x_1 \\ &+ (\theta_1(\theta_1-1)\theta_2 + 5\theta_1\theta_2 + 3\theta_2 + 1)x_1x_2 \\ &+ (\theta_1+1)x_1x_2^2. \end{aligned}$$

Continuing Example

- Knowledge:

$$p_{[0,1]} = p_{\eta_1} = \theta_1 \partial_2 \quad , \quad p_{[0,-1]} = p_{\eta_3} = x_2,$$
$$q_{[-1,1]} = q_{\mu_1} = (\theta_1 + 4) x_1 \partial_2 \quad , \quad q_{[-1,1]} = q_{\mu_3} = (\theta_1 + 1) x_1 x_2$$

  We set $k := l := 3$, and it remains to solve for $\tilde{q}_{[-1,0]}$ and $\tilde{p}_{[0,0]}$.
- Degree-bounds for $p_{[0,0]}$ and $q_{[0,0]}$ in θ_1 and θ_2 via h: **2**.

Continuing Example

The product of $(p_{\eta_1} + p_{\eta_2} + p_{\eta_3})(q_{\mu_1} + q_{\mu_2} + q_{\mu_3})$ with known values inserted is

$$\begin{aligned} pq &= \theta_1(\theta_1+4)x_1\partial_2^2 \\ &+ (\theta_1\tilde{q}_{\mu_2}(\theta_1,\theta_2+1) + \tilde{p}_{\eta_2}(\theta_1+4))x_1\partial_2 \\ &+ (\theta_1(\theta_1+1)(\theta_2+1) + (\theta_1+4)\theta_2 + \tilde{p}_{\eta_2}\tilde{q}_{\mu_2})x_1 \\ &+ (\tilde{q}_{\mu_2}(\theta_1,\theta_2-1) + \tilde{p}_{\eta_2}(\theta_1+1))x_1x_2 \\ &+ (\theta_1+1)x_1x_2^2. \end{aligned}$$

It must be equal to:

$$\begin{aligned} h &= \theta_1(\theta_1+4)x_1\partial_2^2 \\ &+ (\theta_1(\theta_1-1)\theta_2 + 8\theta_1\theta_2 + \theta_1 + 12\theta_2)x_1\partial_2 \\ &+ (\theta_1(\theta_1-1)\theta_2 + \theta_1^2 - \theta_1 + 4\theta_1\theta_2 + 2\theta_1 + 7\theta_2)x_1 \\ &+ (\theta_1(\theta_1-1)\theta_2 + 5\theta_1\theta_2 + 3\theta_2 + 1)x_1x_2 \\ &+ (\theta_1+1)x_1x_2^2. \end{aligned}$$

Continuing Example

The equations that we are looking at:

$$
\begin{array}{lcl}
\theta_1(\theta_1+4) & = & \theta_1(\theta_1+4), \\
(\theta_1 \tilde{q}_{\mu_2}(\theta_1,\theta_2+1)+\tilde{p}_{\eta_2}(\theta_1+4)) & = & (\theta_1(\theta_1-1)\theta_2+8\theta_1\theta_2+\theta_1+12\theta_2), \\
(\theta_1(\theta_1+1)(\theta_2+1)+(\theta_1+4)\theta_2+\tilde{p}_{\eta_2}\tilde{q}_{m_2}) & = & (\theta_1(\theta_1-1)\theta_2+\theta_1^2-\theta_1+4\theta_1\theta_2+2\theta_1+7\theta_2), \\
(\tilde{q}_{\mu_2}(\theta_1,\theta_2-1)+\tilde{p}_{\eta_2}(\theta_1+1)) & = & (\theta_1(\theta_1-1)\theta_2+5\theta_1\theta_2+3\theta_2+1), \\
(\theta_1+1) & = & (\theta_1+1).
\end{array}
$$

At the top and at the bottom, we can transform the equations such that $\tilde{p}_{\eta_2}$ is on the left hand side. This leads to two identities of $\tilde{p}_{\eta_2}$:

$$
\begin{aligned}
\tilde{p}_{\eta_2} &= \frac{\theta_1(\theta_1-1)\theta_2+8\theta_1\theta_2+\theta_1+12\theta_2-\theta_1\tilde{q}_{\mu_2}(\theta_1,\theta_2+1)}{\theta_1+4} \\
&= \frac{\theta_1(\theta_1-1)\theta_2+5\theta_1\theta_2+3\theta_2+1-\tilde{q}_{\mu_2}(\theta_1,\theta_2-1)}{\theta_1+1}.
\end{aligned}
$$

The polynomial $\tilde{q}_{\mu_2}$ has to fulfill both identities.

The solution in this case is unique: $\tilde{q}_{\mu_2}=1$.

Section 4

Implementation

About the Implementation in SINGULAR

- Library `ncfactor.lib`

About the Implementation in SINGULAR

- Library `ncfactor.lib`
- For the
  - first Weyl,
  - the first Shift
  - and homogeneous polynomials in the first q-Weyl algebra,

  factorization algorithms are implemented and distributed with SINGULAR since version 3-1-3 (major changes in 3-1-6).

About the Implementation in SINGULAR

- Library `ncfactor.lib`
- For the
  - first Weyl,
  - the first Shift
  - and homogeneous polynomials in the first q-Weyl algebra,

  factorization algorithms are implemented and distributed with SINGULAR since version 3-1-3 (major changes in 3-1-6).
- For the
  - nth Weyl,
  - the nth Shift
  - and homogeneous polynomials in the nth q-Weyl algebra,

  an implementation is submitted to the SINGULAR team and will appear with the next version ($>$3-1-6).

Remark: The implementation is experimental; there is lots of room to increase the performance.

About the Implementation in SINGULAR

- Library `ncfactor.lib`
- For the
  - first Weyl,
  - the first Shift
  - and homogeneous polynomials in the first q-Weyl algebra,

  factorization algorithms are implemented and distributed with SINGULAR since version 3-1-3 (major changes in 3-1-6).
- For the
  - nth Weyl,
  - the nth Shift
  - and homogeneous polynomials in the nth q-Weyl algebra,

  an implementation is submitted to the SINGULAR team and will appear with the next version ($>$3-1-6).

Remark: The implementation is experimental; there is lots of room to increase the performance.

DEMO

Section 5

Conclusion/Future Work/Summary

$\mathbb{Z}^n$-grading seems useful... What else can we do?

Directly related to the factorization problem:

- Finding (better?) bounds for numbers of different factorizations.
- Proving finite factorization property for several non-commutative algebras.

$\mathbb{Z}^n$-grading seems useful... What else can we do?

Directly related to the factorization problem:

- Finding (better?) bounds for numbers of different factorizations.
- Proving finite factorization property for several non-commutative algebras. Properties of homogeneous polynomials play a central role.

$\mathbb{Z}^n$-grading seems useful... What else can we do?

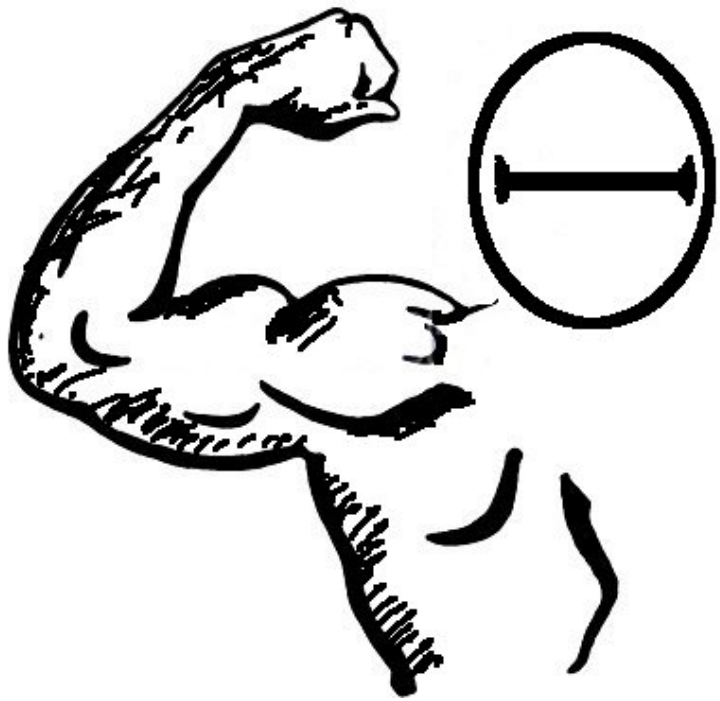
Directly related to the factorization problem:

- Finding (better?) bounds for numbers of different factorizations.
- Proving finite factorization property for several non-commutative algebras. Properties of homogeneous polynomials play a central role.

Unrelated to the factorization problem:

- Generating syzygy elements for a set of polynomials.
- Finding bounds for the sizes of the generators of a syzygy module.
- Finding necessary conditions for two polynomials to be similar.

Message To Take Home



Summary, Conclusions and Future Work

- Utilization of $\mathbb{Z}^n$-graded structure on A_n.
- Factoring homogeneous elements in A_n simple.
- Factoring arbitrary elements in A_n via an ansatz using factorization of the highest and the lowest homogeneous summand works well.
- Implementation in SINGULAR available.
- Factoring non-commutative polynomial rings is still a hard problem. Utilize it for cryptography?
- For more details on the factorization technique, publication in ISSAC'14 proceedings.
- Future Work: Adapting technique for factoring in rational Weyl algebra.
- Future Work: Utilizing $\mathbb{Z}^n$ grading when approaching other algorithmic problems.


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


M. Kashiwara.
Vanishing cycle sheaves and holonomic systems of differential equations.
In *Algebraic Geometry*, pages 134–142. Springer, 1983.


B. Malgrange.
Polynômes de Bernstein-Sato et cohomologie evanescente.
Astérisque, 101-102:243–267, 1983.