Trisymmetric multiplication formulae in finite fields

Hugues Randriambololona, Édouard Rousseau

July 4, 2020

Motivation

- Computations in an algebra $\mathcal{A}$

Motivation

- Computations in an algebra $\mathcal{A}$
  - multiplications: **expensive** ☹
  - additions, scalar multiplications: **cheap** ☺

Motivation

- Computations in an algebra $\mathcal{A}$
  - multiplications: **expensive** ☹
  - additions, scalar multiplications: **cheap** ☺
- we want to study/reduce the cost of multiplication

Motivation

- Computations in an algebra $\mathcal{A}$
  - multiplications: **expensive** ☹
  - additions, scalar multiplications: **cheap** ☺
- we want to study/reduce the cost of multiplication
- Lot of litterature on the subject

MOTIVATION

- Computations in an algebra $\mathcal{A}$
  - multiplications: **expensive** ☹
  - additions, scalar multiplications: **cheap** ☺
- we want to study/reduce the cost of multiplication
- Lot of litterature on the subject
  - **Karatsuba** (1962)

MOTIVATION

- Computations in an algebra $\mathcal{A}$
  - multiplications: **expensive** ☹
  - additions, scalar multiplications: **cheap** ☺
- we want to study/reduce the cost of multiplication
- Lot of litterature on the subject
  - **Karatsuba** (1962)
  - Toom-Cook (1963), **evaluation-interpolation** techniques

Motivation

- Computations in an algebra $\mathcal{A}$
  - multiplications: **expensive** ☹
  - additions, scalar multiplications: **cheap** ☺
- we want to study/reduce the cost of multiplication
- Lot of litterature on the subject
  - **Karatsuba** (1962)
  - Toom-Cook (1963), **evaluation-interpolation** techniques
  - **Schönhage-Strassen** (1971)

Motivation

- Computations in an algebra $\mathcal{A}$
  - multiplications: **expensive** ☹
  - additions, scalar multiplications: **cheap** ☺
- we want to study/reduce the cost of multiplication
- Lot of litterature on the subject
  - **Karatsuba** (1962)
  - Toom-Cook (1963), **evaluation-interpolation** techniques
  - **Schönhage-Strassen** (1971)
  - ...

MOTIVATION

- Computations in an algebra $\mathcal{A}$
  - multiplications: **expensive** ☹
  - additions, scalar multiplications: **cheap** ☺
- we want to study/reduce the cost of multiplication
- Lot of litterature on the subject
  - **Karatsuba** (1962)
  - Toom-Cook (1963), **evaluation-interpolation** techniques
  - **Schönhage-Strassen** (1971)
  - ...
  - $O(n \log n)$ algorithm [Harvey, Van Der Hoeven '19]

Bilinear complexity: intuition

- $\mathcal{A}$ an algebra over $\mathbb{K}$
- **bilinear complexity:** number of subproduct in $\mathbb{K}$ needed to compute a product in $\mathcal{A}$

Karatsuba:

$$(a_0 + a_1 X)(b_0 + b_1 X) =$$

$$a_0 b_0 + (a_0 b_1 + a_1 b_0)X + a_1 b_1 X^2$$

BILINEAR COMPLEXITY: INTUITION

- $\mathcal{A}$ an algebra over $\mathbb{K}$
- **bilinear complexity:** number of subproduct in $\mathbb{K}$ needed to compute a product in $\mathcal{A}$

Karatsuba:

$$(a_0 + a_1 X)(b_0 + b_1 X) =$$

$$a_0 b_0 + (a_0 b_1 + a_1 b_0) X + a_1 b_1 X^2$$

Bilinear complexity: intuition

- $\mathcal{A}$ an algebra over $\mathbb{K}$
- **bilinear complexity:** number of subproduct in $\mathbb{K}$ needed to compute a product in $\mathcal{A}$

Karatsuba:

$$(a_0 + a_1 X)(b_0 + b_1 X) =$$

$$c_0 + (c_2 - c_1 - c_0)X + c_1 X^2$$

with

$$\begin{cases} c_0 &= a_0 b_0 \\ c_1 &= a_1 b_1 \\ c_2 &= (a_0 + a_1)(b_0 + b_1) \end{cases}$$

Bilinear complexity: intuition

- $\mathcal{A}$ an algebra over $\mathbb{K}$
- **bilinear complexity:** number of subproduct in $\mathbb{K}$ needed to compute a product in $\mathcal{A}$

Karatsuba:

$$(a_0 + a_1 X)(b_0 + b_1 X) =$$

$$c_0 + (c_2 - c_1 - c_0)X + c_1 X^2$$

with

$$\begin{cases} c_0 & = & a_0 b_0 \\ c_1 & = & a_1 b_1 \\ c_2 & = & (a_0 + a_1)(b_0 + b_1) \end{cases}$$

Bilinear complexity: intuition

- $\mathcal{A}$ an algebra over $\mathbb{K}$
- **bilinear complexity:** number of subproduct in $\mathbb{K}$ needed to compute a product in $\mathcal{A}$

Karatsuba:

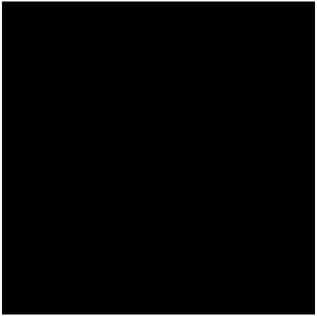
$$(a_0 + a_1X)(b_0 + b_1X) =$$
$$c_0 + (c_2 - c_1 - c_0)X + c_1X^2$$

with

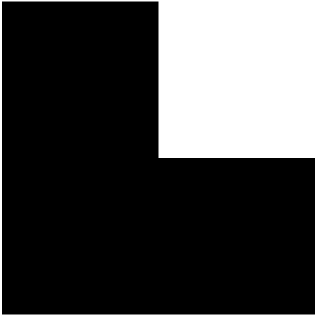
$$\begin{cases} c_0 & = & a_0b_0 \\ c_1 & = & a_1b_1 \\ c_2 & = & (a_0 + a_1)(b_0 + b_1) \end{cases}$$

- ☹ **Hard** to compute the bilinear complexity of a product: unkwown even for the 3×3 matrix product

Complexity of Karatsuba's algorithm

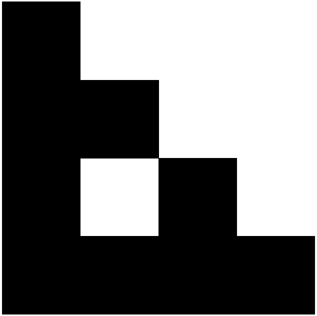


Complexity of Karatsuba's algorithm



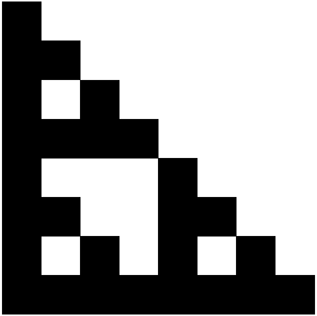
- Degree 2: 3 **multiplications instead of** 4

Complexity of Karatsuba's algorithm



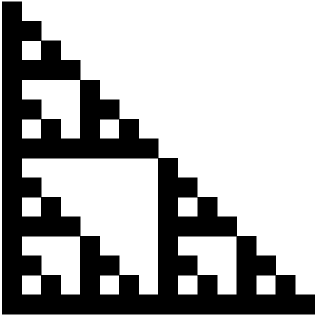
- Degree 2: 3 **multiplications instead of** 4
- Higher degrees: reccursive strategy

Complexity of Karatsuba's algorithm



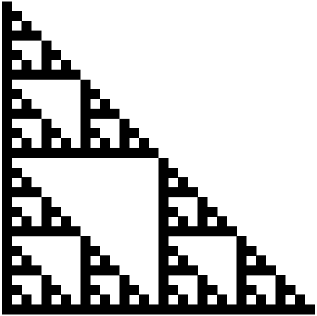
- Degree 2: 3 **multiplications instead of** 4
- Higher degrees: reccursive strategy
- Assymptotically: $O(n^{1.58})$ instead of $O(n^2)$

COMPLEXITY OF KARATSUBA'S ALGORITHM



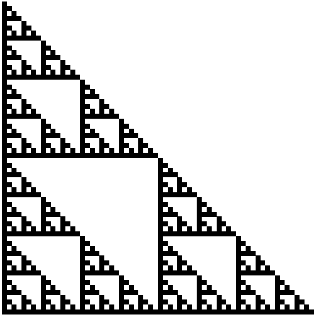
- Degree 2: 3 **multiplications instead of** 4
- Higher degrees: reccursive strategy
- Assymptotically: $O(n^{1.58})$ instead of $O(n^2)$

Complexity of Karatsuba's algorithm



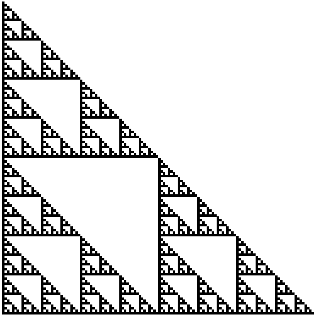
- Degree 2: 3 **multiplications instead of** 4
- Higher degrees: reccursive strategy
- Assymptotically: $O(n^{1.58})$ instead of $O(n^2)$

Complexity of Karatsuba's algorithm



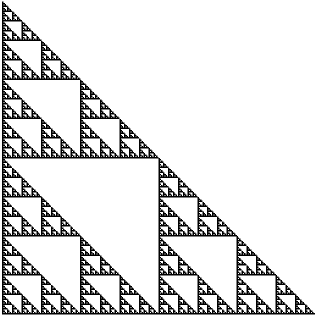
- Degree 2: 3 **multiplications instead of** 4
- Higher degrees: reccursive strategy
- Assymptotically: $O(n^{1.58})$ instead of $O(n^2)$

COMPLEXITY OF KARATSUBA'S ALGORITHM



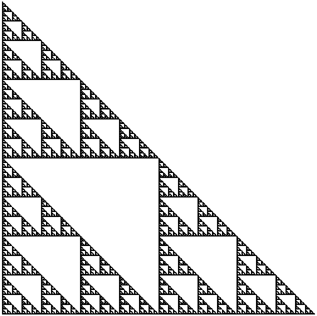
- Degree 2: 3 **multiplications instead of** 4
- Higher degrees: reccursive strategy
- Assymptotically: $O(n^{1.58})$ instead of $O(n^2)$

Complexity of Karatsuba's algorithm



- Degree 2: 3 **multiplications instead of** 4
- Higher degrees: reccursive strategy
- Assymptotically: $O(n^{1.58})$ instead of $O(n^2)$

Complexity of Karatsuba's algorithm



- Degree 2: 3 **multiplications instead of** 4
- Higher degrees: reccursive strategy
- Assymptotically: $O(n^{1.58})$ instead of $O(n^2)$

Bilinear complexity: definition

Definition

The **bilinear complexity** of the product in $\mathcal{A}$ is the minimal integer $r \in \mathbb{N}$ such that you can write, for all $x, y \in \mathcal{A}$

$$xy = \sum_{j=1}^{r} \varphi_j(x)\psi_j(y) \cdot \alpha_j$$

with φ_j, ψ_j linear forms and α_j elements of $\mathcal{A}$.

Bilinear complexity: definition

Definition

The **bilinear complexity** of the product in $\mathcal{A}$ is the minimal integer $r \in \mathbb{N}$ such that you can write, for all $x, y \in \mathcal{A}$

$$xy = \sum_{j=1}^{r} \varphi_j(x)\psi_j(y) \cdot \alpha_j$$

with φ_j, ψ_j linear forms and α_j elements of $\mathcal{A}$.

- $\varphi_j(x)$: linear combination of the coordinates x_i of x
- $\psi_j(y)$: linear combination of the coordinates y_i of y

Bilinear complexity: definition

Definition

The **bilinear complexity** of the product in $\mathcal{A}$ is the minimal integer $r \in \mathbb{N}$ such that you can write, for all $x, y \in \mathcal{A}$

$$xy = \sum_{j=1}^{r} \varphi_j(x)\psi_j(y) \cdot \alpha_j$$

with φ_j, ψ_j linear forms and α_j elements of $\mathcal{A}$.

- $\varphi_j(x)$: linear combination of the coordinates x_i of x
- $\psi_j(y)$: linear combination of the coordinates y_i of y

Notations and questions

- $\mu_q(m)$ = bilinear complexity of the product in $\mathcal{A} = \mathbb{F}_{q^m}$

Two independent questions:

- What is the asymptotic comportment of $\mu_q(m)$?

- Can we find values $\mu_q(m)$ for small m?

Notations and questions

- $\mu_q(m)$ = bilinear complexity of the product in $\mathcal{A} = \mathbb{F}_{q^m}$

Two independent questions:

- What is the asymptotic comportment of $\mu_q(m)$?
  - $\mu_q(m)$ is **linear** in m
- Can we find values $\mu_q(m)$ for small m?

Notations and questions

- $\mu_q(m) =$ bilinear complexity of the product in $\mathcal{A} = \mathbb{F}_{q^m}$

Two independent questions:

- What is the asymptotic comportment of $\mu_q(m)$?
  - $\mu_q(m)$ is **linear** in m
  - **Evaluation-interpolation** techniques:
- Can we find values $\mu_q(m)$ for small m?

Notations and questions

- $\mu_q(m)$ = bilinear complexity of the product in $\mathcal{A} = \mathbb{F}_{q^m}$

Two independent questions:

- What is the asymptotic comportment of $\mu_q(m)$?
  - $\mu_q(m)$ is **linear** in m
  - **Evaluation-interpolation** techniques:
    - [Chudnovsky-Chudnovsky '87]
    - [Shparlinski-Tsfasman-Vladut '92]
    - [Randriambololona '12]
    - ...
- Can we find values $\mu_q(m)$ for small m?

NOTATIONS AND QUESTIONS

- $\mu_q(m) =$ bilinear complexity of the product in $\mathcal{A} = \mathbb{F}_{q^m}$

Two independent questions:

- What is the asymptotic comportment of $\mu_q(m)$?
  - $\mu_q(m)$ is **linear** in m
  - **Evaluation-interpolation** techniques:
    - [Chudnovsky-Chudnovsky '87]
    - [Shparlinski-Tsfasman-Vladut '92]
    - [Randriambololona '12]
    - ...
- Can we find values $\mu_q(m)$ for small m?
  - Clever exhaustive search [BDEZ '12] [Covanov '18]

EVALUATION-INTERPOLATION SCHEMES

Karatsuba again:

- $P(X) = a_0 + a_1 X, Q(X) = b_0 + b_1 X$

Evaluation-interpolation schemes

Karatsuba again:

- $P(X) = a_0 + a_1 X, Q(X) = b_0 + b_1 X$

Big news! Karatsuba is an evaluation-interpolation scheme!

Evaluation-interpolation schemes

Karatsuba again:

- $P(X) = a_0 + a_1X, Q(X) = b_0 + b_1X$

Big news! Karatsuba is an evaluation-interpolation scheme!

- $c_0 = P(0)Q(0) = PQ(0) = a_0b_0$

Evaluation-interpolation schemes

Karatsuba again:

- $P(X) = a_0 + a_1 X, Q(X) = b_0 + b_1 X$

Big news! Karatsuba is an evaluation-interpolation scheme!

- $c_0 = P(0)Q(0) = PQ(0) = a_0 b_0$
- $c_1 = P(1)Q(1) = PQ(1) = (a_0 + a_1)(b_0 + b_1)$

EVALUATION-INTERPOLATION SCHEMES

Karatsuba again:

- $P(X) = a_0 + a_1X, Q(X) = b_0 + b_1X$

Big news! Karatsuba is an evaluation-interpolation scheme!

- $c_0 = P(0)Q(0) = PQ(0) = a_0b_0$
- $c_1 = P(1)Q(1) = PQ(1) = (a_0 + a_1)(b_0 + b_1)$
- $c_2 = c_\infty = P(\infty)Q(\infty) = PQ(\infty) = a_1b_1$

with $R(\infty)$ = leading coefficient of R

Evaluation-interpolation schemes

Karatsuba again:

- $P(X) = a_0 + a_1 X, Q(X) = b_0 + b_1 X$

Big news! Karatsuba is an evaluation-interpolation scheme!
(on the **projective line** $\mathbb{P}^1$)

- $c_0 = P(0)Q(0) = PQ(0) = a_0 b_0$
- $c_1 = P(1)Q(1) = PQ(1) = (a_0 + a_1)(b_0 + b_1)$
- $c_2 = c_\infty = P(\infty)Q(\infty) = PQ(\infty) = a_1 b_1$

with $R(\infty)$ = leading coefficient of R

Evaluation-interpolation schemes

Karatsuba again:

- $P(X) = a_0 + a_1 X, Q(X) = b_0 + b_1 X$

Big news! Karatsuba is an evaluation-interpolation scheme! (on the **projective line** $\mathbb{P}^1$)

- $c_0 = P(0)Q(0) = PQ(0) = a_0 b_0$
- $c_1 = P(1)Q(1) = PQ(1) = (a_0 + a_1)(b_0 + b_1)$
- $c_2 = c_\infty = P(\infty)Q(\infty) = PQ(\infty) = a_1 b_1$

with $R(\infty) =$ leading coefficient of R

- When studying $\mathcal{A} = \mathbb{F}_{q^m}$ for $m \to \infty$, one needs **many points** of evaluation

$\rightsquigarrow$ use a **curve** on $\mathbb{F}_q$ with **many points** for evaluations

Symmetric decompositions

- $\mathcal{A}$ **commutative** algebra

Classic decompositions	**Symmetric** decompositions
$xy = \sum_{j=1}^{r} \varphi_j(x)\psi_j(y) \cdot \alpha_j$	$yx = xy = \sum_{j=1}^{r} \varphi_j(x)\varphi_j(y) \cdot \alpha_j$

Symmetric decompositions

- $\mathcal{A}$ **commutative** algebra

Classic decompositions	**Symmetric** decompositions
$xy = \sum_{j=1}^{r} \varphi_j(x)\psi_j(y) \cdot \alpha_j$	$yx = xy = \sum_{j=1}^{r} \varphi_j(x)\varphi_j(y) \cdot \alpha_j$

SYMMETRIC DECOMPOSITIONS

- $\mathcal{A}$ **commutative** algebra

Classic decompositions	**Symmetric** decompositions
$xy = \sum_{j=1}^{r} \varphi_j(x)\psi_j(y) \cdot \alpha_j$	$yx = xy = \sum_{j=1}^{r} \varphi_j(x)\varphi_j(y) \cdot \alpha_j$

Notation: for $\mathcal{A} = \mathbb{F}_{q^m}$, we note $\mu_q^{\text{sym}}(m)$ the minimal length r in a **symmetric** decomposition

SYMMETRIC DECOMPOSITIONS

- $\mathcal{A}$ **commutative** algebra

Classic decompositions	**Symmetric** decompositions
$xy = \sum_{j=1}^{r} \varphi_j(x)\psi_j(y) \cdot \alpha_j$	$yx = xy = \sum_{j=1}^{r} \varphi_j(x)\varphi_j(y) \cdot \alpha_j$

Notation: for $\mathcal{A} = \mathbb{F}_{q^m}$, we note $\mu_q^{\text{sym}}(m)$ the minimal length r in a **symmetric** decomposition

- **Assymptotics:** $\mu_q^{\text{sym}}(m)$ is **linear** in m

SYMMETRIC DECOMPOSITIONS

- $\mathcal{A}$ **commutative** algebra

Classic decompositions	**Symmetric** decompositions
$xy = \sum_{j=1}^{r} \varphi_j(x)\psi_j(y) \cdot \alpha_j$	$yx = xy = \sum_{j=1}^{r} \varphi_j(x)\varphi_j(y) \cdot \alpha_j$

Notation: for $\mathcal{A} = \mathbb{F}_{q^m}$, we note $\mu_q^{\text{sym}}(m)$ the minimal length r in a **symmetric** decomposition

- **Assymptotics:** $\mu_q^{\text{sym}}(m)$ is **linear** in m
- **Small values: smaller** search space $\rightsquigarrow$ **faster** algorithms

Even more symmetric decompositions

- $\mathcal{A} = \mathbb{F}_{q^m}$
- every linear form φ can be written $x \mapsto \mathrm{Tr}(\alpha x)$ for some $\alpha \in \mathbb{F}_{q^m}$, with Tr the trace of $\mathbb{F}_{q^m}/\mathbb{F}_q$
- we can rewrite the formula

$$xy = \sum_{j=1}^{r} \varphi_j(x)\varphi_j(y) \cdot \beta_j$$

Even more symmetric decompositions

- $\mathcal{A} = \mathbb{F}_{q^m}$
- every linear form φ can be written $x \mapsto \mathrm{Tr}(\alpha x)$ for some $\alpha \in \mathbb{F}_{q^m}$, with Tr the trace of $\mathbb{F}_{q^m}/\mathbb{F}_q$
- we can rewrite the formula

$$xy = \sum_{j=1}^{r} \mathrm{Tr}(\alpha_j x)\,\mathrm{Tr}(\alpha_j y) \cdot \beta_j$$

Even more symmetric decompositions

- $\mathcal{A} = \mathbb{F}_{q^m}$
- every linear form φ can be written $x \mapsto \mathrm{Tr}(\alpha x)$ for some $\alpha \in \mathbb{F}_{q^m}$, with Tr the trace of $\mathbb{F}_{q^m}/\mathbb{F}_q$
- we can rewrite the formula, and even ask $\beta_j = \lambda_j \alpha_j$

$$xy = \sum_{j=1}^{r} \lambda_j \,\mathrm{Tr}(\alpha_j x)\,\mathrm{Tr}(\alpha_j y) \cdot \alpha_j$$

with $\lambda_j \in \mathbb{F}_q$ scalars

Even more symmetric decompositions

- $\mathcal{A} = \mathbb{F}_{q^m}$
- every linear form φ can be written $x \mapsto \mathrm{Tr}(\alpha x)$ for some $\alpha \in \mathbb{F}_{q^m}$, with Tr the trace of $\mathbb{F}_{q^m}/\mathbb{F}_q$
- we can rewrite the formula, and even ask $\beta_j = \lambda_j \alpha_j$

$$xy = \sum_{j=1}^{r} \lambda_j \, \mathrm{Tr}(\alpha_j x) \, \mathrm{Tr}(\alpha_j y) \cdot \alpha_j$$

with $\lambda_j \in \mathbb{F}_q$ scalars

- we call these formulae **trisymmetric** decompositions

Even more symmetric decompositions

- $\mathcal{A} = \mathbb{F}_{q^m}$
- every linear form φ can be written $x \mapsto \mathrm{Tr}(\alpha x)$ for some $\alpha \in \mathbb{F}_{q^m}$, with Tr the trace of $\mathbb{F}_{q^m}/\mathbb{F}_q$
- we can rewrite the formula, and even ask $\beta_j = \lambda_j \alpha_j$

$$xy = \sum_{j=1}^{r} \lambda_j \,\mathrm{Tr}(\alpha_j x)\,\mathrm{Tr}(\alpha_j y) \cdot \alpha_j$$

with $\lambda_j \in \mathbb{F}_q$ scalars

- we call these formulae **trisymmetric** decompositions
- we note $\mu_q^{\mathrm{tri}}(m)$ the minimal r in such formulae

Example of trisymmetric decomposition

- $\mathcal{A} = \mathbb{F}_{3^2} \cong \mathbb{F}_3[z]/(z^2 - z - 1) \cong \mathbb{F}_3(\zeta)$
- $x, y \in \mathcal{A}$, $x = x_0 + x_1\zeta$ and $y = y_0 + y_1\zeta$

EXAMPLE OF TRISYMMETRIC DECOMPOSITION

- $\mathcal{A} = \mathbb{F}_{3^2} \cong \mathbb{F}_3[z]/(z^2 - z - 1) \cong \mathbb{F}_3(\zeta)$
- $x, y \in \mathcal{A}$, $x = x_0 + x_1\zeta$ and $y = y_0 + y_1\zeta$

$$(x_0 + x_1\zeta)(y_0 + y_1\zeta) = (x_0y_0 + x_1y_1) + (x_0y_1 + x_1y_0 + x_1y_1)\zeta$$

Example of trisymmetric decomposition

- $\mathcal{A} = \mathbb{F}_{3^2} \cong \mathbb{F}_3[z]/(z^2 - z - 1) \cong \mathbb{F}_3(\zeta)$
- $x, y \in \mathcal{A}$, $x = x_0 + x_1\zeta$ and $y = y_0 + y_1\zeta$

$$(x_0 + x_1\zeta)(y_0 + y_1\zeta) = (x_0y_0 + x_1y_1) + (x_0y_1 + x_1y_0 + x_1y_1)\zeta$$

$$\begin{aligned} xy \quad = \quad & -\operatorname{Tr}(1 \times x)\operatorname{Tr}(1 \times y) \cdot 1 - \operatorname{Tr}(\zeta \times x)\operatorname{Tr}(\zeta \times y) \cdot \zeta \\ & + \operatorname{Tr}((\zeta - 1) \times x)\operatorname{Tr}((\zeta - 1) \times y) \cdot (\zeta - 1) \end{aligned}$$

Example of trisymmetric decomposition

- $\mathcal{A} = \mathbb{F}_{3^2} \cong \mathbb{F}_3[z]/(z^2 - z - 1) \cong \mathbb{F}_3(\zeta)$
- $x, y \in \mathcal{A}$, $x = x_0 + x_1\zeta$ and $y = y_0 + y_1\zeta$

$$(x_0 + x_1\zeta)(y_0 + y_1\zeta) = (x_0y_0 + x_1y_1) + (x_0y_1 + x_1y_0 + x_1y_1)\zeta$$

$$\begin{aligned} xy \quad = \quad & -\operatorname{Tr}(1 \times x)\operatorname{Tr}(1 \times y) \cdot 1 - \operatorname{Tr}(\zeta \times x)\operatorname{Tr}(\zeta \times y) \cdot \zeta \\ & + \operatorname{Tr}((\zeta - 1) \times x)\operatorname{Tr}((\zeta - 1) \times y) \cdot (\zeta - 1) \end{aligned}$$

with

$$\begin{cases} \operatorname{Tr}(x)\operatorname{Tr}(y) & = & (x_0 - x_1)(y_0 - y_1) \\ \operatorname{Tr}((\zeta - 1)x)\operatorname{Tr}((\zeta - 1)y) & = & (x_0 + x_1)(y_0 + y_1) \\ \operatorname{Tr}(\zeta x)\operatorname{Tr}(\zeta y) & = & x_0y_0 \end{cases}$$

About trisymmetric decompositions

Link with other decompositions:

$$\mu_q(m) \leq \mu_q^{\mathrm{sym}}(m) \leq \mu_q^{\mathrm{tri}}(m)$$

About trisymmetric decompositions

Link with other decompositions:

$$\mu_q(m) \underset{?}{\leq} \mu_q^{\text{sym}}(m) \underset{?}{\leq} \mu_q^{\text{tri}}(m)$$

About trisymmetric decompositions

Link with other decompositions:

$$\mu_q(m) \underset{?}{\leq} \mu_q^{\text{sym}}(m) \underset{?}{\leq} \mu_q^{\text{tri}}(m)$$

Proposition (Randriambololona, '14)

Tri-symmetric decompositions always exist, except for $q = 2, m \geq 3$.

About trisymmetric decompositions

Link with other decompositions:

$$\mu_q(m) \underset{?}{\leq} \mu_q^{\text{sym}}(m) \underset{?}{\leq} \mu_q^{\text{tri}}(m)$$

Proposition (Randriambololona, '14)

Tri-symmetric decompositions always exist, except for $q = 2, m \geq 3$.

- **Assymptotics:** linearity in m can be obtained for **symmetric** decomposition in $\mathbb{F}_{q^m}$ in **higher dimensions**

About trisymmetric decompositions

Link with other decompositions:

$$\mu_q(m) \underset{?}{\leq} \mu_q^{\text{sym}}(m) \underset{?}{\leq} \mu_q^{\text{tri}}(m)$$

Proposition (Randriambololona, '14)

Tri-symmetric decompositions always exist, except for $q = 2, m \geq 3$.

- **Assymptotics:** linearity in m can be obtained for **symmetric** decomposition in $\mathbb{F}_{q^m}$ in **higher dimensions**
  - Corollary: $\mu_q^{\text{tri}}(m)$ is also **linear** in m

About trisymmetric decompositions

Link with other decompositions:

$$\mu_q(m) \underset{?}{\leq} \mu_q^{\text{sym}}(m) \underset{?}{\leq} \mu_q^{\text{tri}}(m)$$

Proposition (Randriambololona, '14)

Tri-symmetric decompositions always exist, except for $q = 2, m \geq 3$.

- **Assymptotics:** linearity in m can be obtained for **symmetric** decomposition in $\mathbb{F}_{q^m}$ in **higher dimensions**
  - Corollary: $\mu_q^{\text{tri}}(m)$ is also **linear** in m
- **Small values:** usual algorithms do not work

About trisymmetric decompositions

Link with other decompositions:

$$\mu_q(m) \underset{?}{\leq} \mu_q^{\text{sym}}(m) \underset{?}{\leq} \mu_q^{\text{tri}}(m)$$

Proposition (Randriambololona, '14)

Tri-symmetric decompositions always exist, except for $q = 2, m \geq 3$.

- **Assymptotics:** linearity in m can be obtained for **symmetric** decomposition in $\mathbb{F}_{q^m}$ in **higher dimensions**
  - Corollary: $\mu_q^{\text{tri}}(m)$ is also **linear** in m
- **Small values:** usual algorithms do not work
  - We provide an *ad hoc* exhaustive search algorithm

Conclusion

Bilinear complexity:

- important notion in symbolic computation
- any bilinear map can be studied

Conclusion

Bilinear complexity:

- important notion in symbolic computation
- any bilinear map can be studied

Symmetric complexity:

- Generalization to the case of t-variable products, $t \geq 3$

Conclusion

Bilinear complexity:

- important notion in symbolic computation
- any bilinear map can be studied

Symmetric complexity:

- Generalization to the case of t-variable products, $t \geq 3$

Trisymmetric complexity:

- is **linear** in the extension degree
- small values can be found through exhaustive search

Conclusion

Bilinear complexity:

- important notion in symbolic computation
- any bilinear map can be studied

Symmetric complexity:

- Generalization to the case of t-variable products, $t \geq 3$

Trisymmetric complexity:

- is **linear** in the extension degree
- small values can be found through exhaustive search

Future work:

- distinguish μ_q^{tri} from μ_q^{sym} for $q \geq 3$
- find better bounds than those already known

CONCLUSION

Bilinear complexity:

- important notion in symbolic computation
- any bilinear map can be studied

Symmetric complexity:

- Generalization to the case of t-variable products, $t \geq 3$

Trisymmetric complexity:

- is **linear** in the extension degree
- small values can be found through exhaustive search

Future work:

- distinguish μ_q^{tri} from μ_q^{sym} for $q \geq 3$
- find better bounds than those already known

Thank you!