Trisymmetric multiplication formulas in finite fields

Hugues Randriambololona, Édouard Rousseau

October 22, 2020
Séminaire CRYPTO

FINITE FIELDS IN CRYPTOGRAPHY

Finite fields are (almost) everywhere in **public key** cryptography:

- discrete logarithm
- elliptic curves
- isogenies
- code-based cryptography
- multivariate cryptography

Finite fields in cryptography

Finite fields are (almost) everywhere in **public key** cryptography:

- discrete logarithm
- elliptic curves
- isogenies
- code-based cryptography
- multivariate cryptography
- used in 3 of the 4 main families of **post-quantum** protocols

Finite fields in cryptography

Finite fields are (almost) everywhere in **public key** cryptography:

- discrete logarithm
- elliptic curves
- isogenies
- code-based cryptography
- multivariate cryptography
- used in 3 of the 4 main families of **post-quantum** protocols
  - bright future!

Other applications

Finite fields are also widely used in

- coding theory
- algebraic geometry
- number theory

Other applications

Finite fields are also widely used in

- coding theory
- algebraic geometry
- number theory
- motivates their study
  - **algorithmic** study: a part of **computer algebra**

Finite field arithmetic

Notation: $\mathbb{F}_{q^m}$ denotes *the* finite field with q^m elements

$$\mathbb{F}_{q^m} \cong \mathbb{F}_q[X]/(P(X))$$

- $P \in \mathbb{F}_q[X]$ is an **irreducible** polynomial of degree m

Some possible **representations**:

- **Zech's logarithm**: elements are represented as generator powers
- **normal** basis: $(\alpha, \alpha^{\sigma}, \dots, \alpha^{\sigma^{m-1}})$
- **monomial** basis: $(1, \bar{X}, \dots, \bar{X}^{m-1})$

Finite field arithmetic

Notation: $\mathbb{F}_{q^m}$ denotes *the* finite field with q^m elements

$$\mathbb{F}_{q^m} \cong \mathbb{F}_q[X]/(P(X))$$

- $P \in \mathbb{F}_q[X]$ is an **irreducible** polynomial of degree m

Some possible **representations**:

- **Zech's logarithm**: elements are represented as generator powers
  - fast, but only possible for small fields
- **normal** basis: $(\alpha, \alpha^\sigma, \ldots, \alpha^{\sigma^{m-1}})$
- **monomial** basis: $(1, \bar{X}, \ldots, \bar{X}^{m-1})$

Finite field arithmetic

Notation: $\mathbb{F}_{q^m}$ denotes *the* finite field with q^m elements

$$\mathbb{F}_{q^m} \cong \mathbb{F}_q[X]/(P(X))$$

- $P \in \mathbb{F}_q[X]$ is an **irreducible** polynomial of degree m

Some possible **representations**:

- **Zech's logarithm**: elements are represented as generator powers
  - fast, but only possible for small fields
- **normal** basis: $(\alpha, \alpha^\sigma, \ldots, \alpha^{\sigma^{m-1}})$
  - fast Frobenius evaluation but slow multiplication
- **monomial** basis: $(1, \bar{X}, \ldots, \bar{X}^{m-1})$

Finite field arithmetic

Notation: $\mathbb{F}_{q^m}$ denotes *the* finite field with q^m elements

$$\mathbb{F}_{q^m} \cong \mathbb{F}_q[X]/(P(X))$$

- $P \in \mathbb{F}_q[X]$ is an **irreducible** polynomial of degree m

Some possible **representations**:

- **Zech's logarithm**: elements are represented as generator powers
  - fast, but only possible for small fields
- **normal** basis: $(\alpha, \alpha^\sigma, \dots, \alpha^{\sigma^{m-1}})$
  - fast Frobenius evaluation but slow multiplication
- **monomial** basis: $(1, \bar{X}, \dots, \bar{X}^{m-1})$
  - commonly used representation, easy to construct
  - multiplication slower than addition

Motivations

- Computations in an algebra $\mathcal{A}$ over $\mathbb{F}_q$
  - typically $\mathbb{F}_{q^m}$ with the **monomial** basis

Motivations

- Computations in an algebra $\mathcal{A}$ over $\mathbb{F}_q$
  - typically $\mathbb{F}_{q^m}$ with the **monomial** basis
  - multiplications: **expensive** ☹
  - additions, scalar multiplications: **cheap** ☺

Motivations

- Computations in an algebra $\mathcal{A}$ over $\mathbb{F}_q$
  - typically $\mathbb{F}_{q^m}$ with the **monomial** basis
  - multiplications: **expensive** ☹
  - additions, scalar multiplications: **cheap** ☺
- we want to study/reduce the cost of multiplication

Motivations

- Computations in an algebra $\mathcal{A}$ over $\mathbb{F}_q$
  - typically $\mathbb{F}_{q^m}$ with the **monomial** basis
  - multiplications: **expensive** ☹
  - additions, scalar multiplications: **cheap** ☺
- we want to study/reduce the cost of multiplication
- Lot of litterature on the subject

MOTIVATIONS

- Computations in an algebra $\mathcal{A}$ over $\mathbb{F}_q$
  - typically $\mathbb{F}_{q^m}$ with the **monomial** basis
  - multiplications: **expensive** ☹
  - additions, scalar multiplications: **cheap** ☺
- we want to study/reduce the cost of multiplication
- Lot of litterature on the subject
  - **Karatsuba** (1962)

Motivations

- Computations in an algebra $\mathcal{A}$ over $\mathbb{F}_q$
  - typically $\mathbb{F}_{q^m}$ with the **monomial** basis
  - 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

Motivations

- Computations in an algebra $\mathcal{A}$ over $\mathbb{F}_q$
  - typically $\mathbb{F}_{q^m}$ with the **monomial** basis
  - 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)

MOTIVATIONS

- Computations in an algebra $\mathcal{A}$ over $\mathbb{F}_q$
  - typically $\mathbb{F}_{q^m}$ with the **monomial** basis
  - 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)
  - ...

MOTIVATIONS

- Computations in an algebra $\mathcal{A}$ over $\mathbb{F}_q$
  - typically $\mathbb{F}_{q^m}$ with the **monomial** basis
  - 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)
  - ...
  - $O(m \log m)$ 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:

$$(a_0 + a_1X)(b_0 + b_1X) =$$

$$a_0b_0 + (a_0b_1 + a_1b_0)X + a_1b_1X^2$$

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:

$$(a_0 + a_1X)(b_0 + b_1X) =$$

$$c_0 + (c_2 - c_1 - c_0)X + c_1X^2$$

with

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

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:

$$(a_0 + a_1X)(b_0 + b_1X) =$$

$$c_0 + (c_2 - c_1 - c_0)X + c_1X^2$$

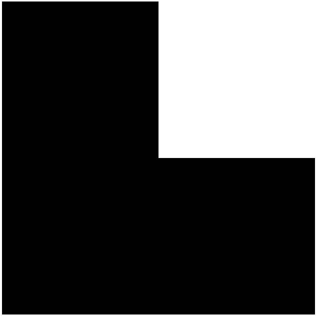
with

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

Complexity of Karatsuba's algorithm

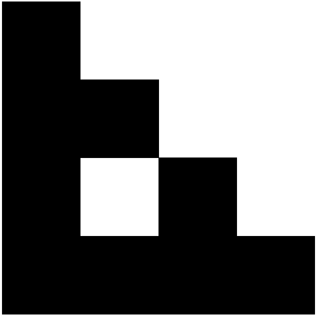
[redacted]

Complexity of Karatsuba's algorithm



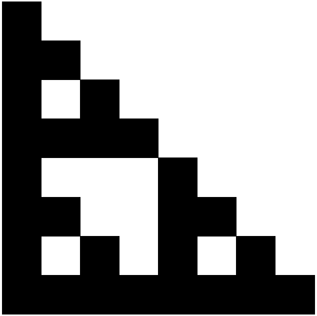
- Degree 2: 3 **multiplications instead of** 4

Complexity of Karatsuba's algorithm



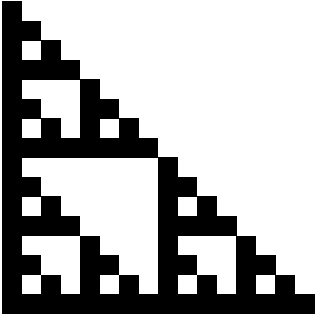
- Degree 2: 3 **multiplications instead of** 4
- Higher degrees: reccursive strategy

COMPLEXITY OF KARATSUBA'S ALGORITHM



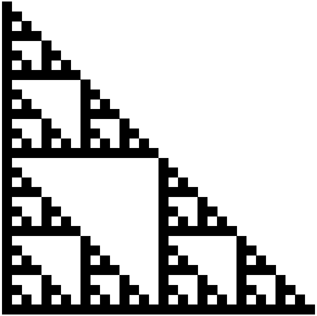
- Degree 2: 3 **multiplications instead of** 4
- Higher degrees: reccursive strategy
- Assymptotically: $O(n^{1.58})$ instead of $O(n^2)$

COMPLEXITY OF KARATSUBA'S ALGORITHM



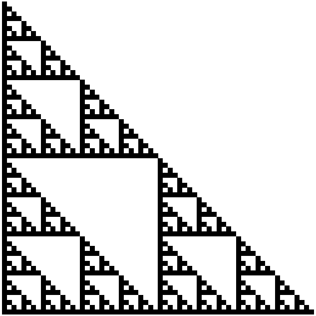
- Degree 2: 3 **multiplications instead of** 4
- Higher degrees: reccursive strategy
- Assymptotically: $O(n^{1.58})$ instead of $O(n^2)$

Complexity of Karatsuba's algorithm



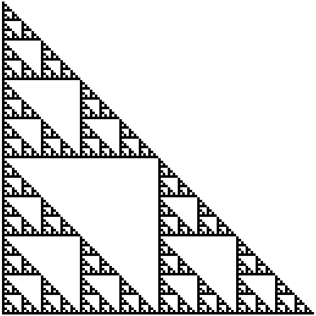
- Degree 2: 3 **multiplications instead of** 4
- Higher degrees: reccursive strategy
- Assymptotically: $O(n^{1.58})$ instead of $O(n^2)$

COMPLEXITY OF KARATSUBA'S ALGORITHM



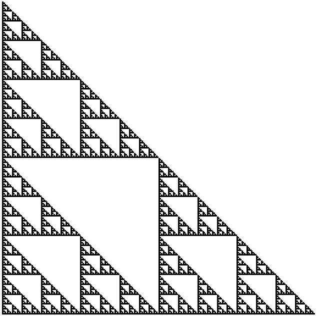
- Degree 2: 3 **multiplications instead of** 4
- Higher degrees: reccursive strategy
- Assymptotically: $O(n^{1.58})$ instead of $O(n^2)$

Complexity of Karatsuba's algorithm



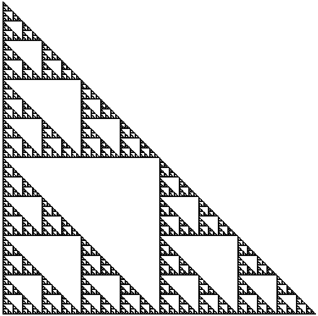
- Degree 2: 3 **multiplications instead of** 4
- Higher degrees: reccursive strategy
- Assymptotically: $O(n^{1.58})$ instead of $O(n^2)$

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: intuition

2×2 matrix multiplication:

$$\begin{pmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{pmatrix} \begin{pmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{pmatrix} = \begin{pmatrix} a_{0,0}b_{0,0} + a_{0,1}b_{1,0} & a_{0,0}b_{0,1} + a_{0,1}b_{1,1} \\ a_{1,0}b_{0,0} + a_{1,1}b_{1,0} & a_{1,0}b_{0,1} + a_{1,1}b_{1,1} \end{pmatrix}$$

Bilinear complexity: intuition

2×2 matrix multiplication:

$$\begin{pmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{pmatrix} \begin{pmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{pmatrix} = \begin{pmatrix} a_{0,0}b_{0,0} + a_{0,1}b_{1,0} & a_{0,0}b_{0,1} + a_{0,1}b_{1,1} \\ a_{1,0}b_{0,0} + a_{1,1}b_{1,0} & a_{1,0}b_{0,1} + a_{1,1}b_{1,1} \end{pmatrix}$$

Bilinear complexity: intuition

2×2 matrix multiplication:

$$\begin{pmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{pmatrix} \begin{pmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{pmatrix} = \begin{pmatrix} a_{0,0}b_{0,0} + a_{0,1}b_{1,0} & a_{0,0}b_{0,1} + a_{0,1}b_{1,1} \\ a_{1,0}b_{0,0} + a_{1,1}b_{1,0} & a_{1,0}b_{0,1} + a_{1,1}b_{1,1} \end{pmatrix}$$

- **Strassen's** algorithm: you only need 7 multiplications!

Bilinear complexity: intuition

2×2 matrix multiplication:

$$\begin{pmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{pmatrix} \begin{pmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{pmatrix} = \begin{pmatrix} a_{0,0}b_{0,0} + a_{0,1}b_{1,0} & a_{0,0}b_{0,1} + a_{0,1}b_{1,1} \\ a_{1,0}b_{0,0} + a_{1,1}b_{1,0} & a_{1,0}b_{0,1} + a_{1,1}b_{1,1} \end{pmatrix}$$

- **Strassen's** algorithm: you only need 7 multiplications!
  - that is **optimal**

Bilinear complexity: intuition

2×2 matrix multiplication:

$$\begin{pmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{pmatrix} \begin{pmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{pmatrix} = \begin{pmatrix} a_{0,0}b_{0,0} + a_{0,1}b_{1,0} & a_{0,0}b_{0,1} + a_{0,1}b_{1,1} \\ a_{1,0}b_{0,0} + a_{1,1}b_{1,0} & a_{1,0}b_{0,1} + a_{1,1}b_{1,1} \end{pmatrix}$$

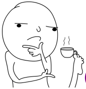
- **Strassen's** algorithm: you only need 7 multiplications!
  - that is **optimal**
  - the **bilinear complexity** of the 2×2 matrix multiplication is 7

Bilinear complexity: intuition

2×2 matrix multiplication:

$$\begin{pmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{pmatrix} \begin{pmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{pmatrix} = \begin{pmatrix} a_{0,0}b_{0,0} + a_{0,1}b_{1,0} & a_{0,0}b_{0,1} + a_{0,1}b_{1,1} \\ a_{1,0}b_{0,0} + a_{1,1}b_{1,0} & a_{1,0}b_{0,1} + a_{1,1}b_{1,1} \end{pmatrix}$$

- **Strassen's** algorithm: you only need 7 multiplications!
  - that is **optimal**
  - the **bilinear complexity** of the 2×2 matrix multiplication is 7



Open question: what is the bilinear complexity of the 3×3 matrix multiplication?

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 $\mathcal{A}$.

- $\varphi_j(x) = a_{1,j}x_1 + \cdots + a_{n,j}x_n$
- $\psi_j(y) = b_{1,j}y_1 + \cdots + b_{n,j}y_n$
- linear combinations of the coordinates x_i and y_i

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 $\mathcal{A}$.

- $\varphi_j(x) = a_{1,j}x_1 + \cdots + a_{n,j}x_n$
- $\psi_j(y) = b_{1,j}y_1 + \cdots + b_{n,j}y_n$
- linear combinations of the coordinates x_i and y_i

Notations and questions

- $\mathbb{K} = \mathbb{F}_q$
- $\mu_q(m)$ = 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?

Asymptotics

Lower bound from coding theory

- $2m - 1 \leq \mu_q(m)$

Asymptotics

Lower bound from coding theory

- $2m - 1 \leq \mu_q(m)$

Upper bounds, from **evaluation-interpolation** schemes

- [Chudnovsky-Chudnovsky '87]
- [Shparlinski-Tsfasman-Vladut '92]
- [Ballet '08]
- [Randriambololona '12]
- …

Asymptotics

Lower bound from coding theory

- $2m - 1 \leq \mu_q(m)$

Upper bounds, from **evaluation-interpolation** schemes

- [Chudnovsky-Chudnovsky '87]
- [Shparlinski-Tsfasman-Vladut '92]
- [Ballet '08]
- [Randriambololona '12]
- …
- $\mu_q(m)$ is **linear** in m

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:

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

Big news! Karatsuba is an evaluation-interpolation scheme!

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

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

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 of evaluation

HOW TO FIND SMALL VALUES?

Possibilities:

- tighten the theoretical bounds (hard ☹)
- find all formulas
  - clever **algorithms** for **exhaustive search**
  - [BDEZ '12]
  - [Covanov '18]

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 $\mu_q^{\mathrm{sym}}(m)$ the minimal length r in a **symmetric** decomposition

About symmetric decompositions

Two questions:

About symmetric decompositions

Two questions:

- **Assymptotics:**

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

About symmetric decompositions

Two questions:

- **Assymptotics:**

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

- $\mu_q^{\mathrm{sym}}(m)$ still **linear** in m

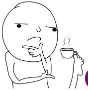
About symmetric decompositions

Two questions:

- **Assymptotics:**

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

- $\mu_q^{\text{sym}}(m)$ still **linear** in m



Open question: find q and m with

$$\mu_q(m) \neq \mu_q^{\text{sym}}(m)$$

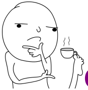
About symmetric decompositions

Two questions:

- **Assymptotics:**

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

- $\mu_q^{\text{sym}}(m)$ still **linear** in m



Open question: find q and m with

$$\mu_q(m) \neq \mu_q^{\text{sym}}(m)$$

- **Small values:**

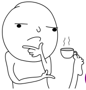
About symmetric decompositions

Two questions:

- **Assymptotics:**

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

- $\mu_q^{\mathrm{sym}}(m)$ still **linear** in m



Open question: find q and m with

$$\mu_q(m) \neq \mu_q^{\mathrm{sym}}(m)$$

- **Small values:**
  - **Smaller** search space $\rightsquigarrow$ **faster** exhaustive search

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

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 $y = y_0 + y_1\zeta$

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

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

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

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

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:

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

About trisymmetric decompositions

Link with other decompositions:

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

Proposition (Randriambololona, '14)

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

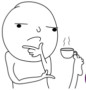
About trisymmetric decompositions

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 $q = 2, m \geq 3$.



Open question: find $q \geq 3$ and $m \geq 2$ with

$$\mu_q^{\text{sym}}(m) \neq \mu_q^{\text{tri}}(m)$$

Finding decompositions

Symmetric decompositions:

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

- [BDEZ '12]
- [Covanov '18])

Finding decompositions

Symmetric decompositions:

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

- [BDEZ '12]
- [Covanov '18])
  - rely on the fact that the α_j and β_j are independent

Finding decompositions

Symmetric decompositions:

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

- [BDEZ '12]
- [Covanov '18])
  - rely on the fact that the α_j and β_j are independent
  - no longer the case for trisymmetric decompositions

Finding decompositions

Symmetric decompositions:

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

- [BDEZ '12]
- [Covanov '18])
  - rely on the fact that the α_j and β_j are independent
  - no longer the case for trisymmetric decompositions

Trisymmetric decompositions:

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

- **ad hoc** algorithm

Computing trisymmetric decompositions

- choose a basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$

$$xy = (b_1(x,y), \ldots, b_m(x,y))$$

with b_j bilinear forms

COMPUTING TRISYMMETRIC DECOMPOSITIONS

- choose a basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$

$$xy = (b_1(x,y), \ldots, b_m(x,y))$$

with b_j bilinear forms

- find (exhaustive search) elements in $\mathbb{F}_{q^m}$ of the form $(1, *, \ldots, *)$ such that

$$b_1(x,y) = \sum_{j=1}^{r_1} \lambda_j \operatorname{Tr}(\alpha_j x) \operatorname{Tr}(\alpha_j y)$$

Computing trisymmetric decompositions

- choose a basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$

$$xy = (b_1(x,y), \ldots, b_m(x,y))$$

with b_j bilinear forms

- find (exhaustive search) elements in $\mathbb{F}_{q^m}$ of the form $(1, *, \ldots, *)$ such that

$$b_1(x,y) = \sum_{j=1}^{r_1} \lambda_j \operatorname{Tr}(\alpha_j x) \operatorname{Tr}(\alpha_j y)$$

$$xy - \sum_{j=1}^{r_1} \lambda_j \operatorname{Tr}(\alpha_j x) \operatorname{Tr}(\alpha_j y) \alpha_j = (0, b'_2(x,y), \ldots, b'_m(x,y))$$

Computing trisymmetric decompositions

- choose a basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$

$$xy = (b_1(x,y), \ldots, b_m(x,y))$$

with b_j bilinear forms

- find elements in $\mathbb{F}_{q^m}$ of the form $(0, 1, *, \ldots, *)$ such that

$$b_2'(x,y) = \sum_{j=r_1+1}^{r_2} \lambda_j \operatorname{Tr}(\alpha_j x) \operatorname{Tr}(\alpha_j y)$$

Computing trisymmetric decompositions

- choose a basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$

$$xy = (b_1(x,y), \ldots, b_m(x,y))$$

with b_j bilinear forms

- find elements in $\mathbb{F}_{q^m}$ of the form $(0, 1, *, \ldots, *)$ such that

$$b'_2(x,y) = \sum_{j=r_1+1}^{r_2} \lambda_j \operatorname{Tr}(\alpha_j x) \operatorname{Tr}(\alpha_j y)$$

$$xy - \sum_{j=1}^{r_2} \lambda_j \operatorname{Tr}(\alpha_j x) \operatorname{Tr}(\alpha_j y) \alpha_j = (0, 0, b''_3(x,y) \ldots, b''_m(x,y))$$

COMPUTING TRISYMMETRIC DECOMPOSITIONS

- choose a basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$

$$xy = (b_1(x, y), \dots, b_m(x, y))$$

with b_j bilinear forms

- find elements in $\mathbb{F}_{q^m}$ of the form $(0, 0, 1, *, \dots, *)$ such that

$$b_3''(x, y) = \sum_{j=r_2+1}^{r_3} \lambda_j \operatorname{Tr}(\alpha_j x) \operatorname{Tr}(\alpha_j y)$$

COMPUTING TRISYMMETRIC DECOMPOSITIONS

- choose a basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$

$$xy = (b_1(x,y), \ldots, b_m(x,y))$$

with b_j bilinear forms

- find elements in $\mathbb{F}_{q^m}$ of the form $(0, 0, 1, *, \ldots, *)$ such that

$$b_3''(x,y) = \sum_{j=r_2+1}^{r_3} \lambda_j \operatorname{Tr}(\alpha_j x) \operatorname{Tr}(\alpha_j y)$$

- and so on

Computing trisymmetric decompositions

- choose a basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$

$$xy = (b_1(x,y), \ldots, b_m(x,y))$$

with b_j bilinear forms

- find elements in $\mathbb{F}_{q^m}$ of the form $(0, 0, 1, *, \ldots, *)$ such that

$$b_3''(x,y) = \sum_{j=r_2+1}^{r_3} \lambda_j \operatorname{Tr}(\alpha_j x) \operatorname{Tr}(\alpha_j y)$$

- and so on
- in the end, we obtain

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

SOME RESULTS FOR $q = 3$

field	μ_q	μ_q^{sym}	μ_q^{tri}
$\mathbb{F}_{3^2}$	3	3	3
$\mathbb{F}_{3^3}$	6	6	6
$\mathbb{F}_{3^4}$	9	9	9
$\mathbb{F}_{3^5}$	$9 \leq \star \leq 11$	11	11
$\mathbb{F}_{3^6}$	$11 \leq \star \leq 15$	$13 \leq \star \leq 15$	$13 \leq \star \leq 15$

SOME RESULTS FOR $q = 3$

field	μ_q	μ_q^{sym}	μ_q^{tri}
$\mathbb{F}_{3^2}$	3	3	3
$\mathbb{F}_{3^3}$	6	6	6
$\mathbb{F}_{3^4}$	9	9	9
$\mathbb{F}_{3^5}$	$9 \leq \star \leq 11$	11	11
$\mathbb{F}_{3^6}$	$11 \leq \star \leq 15$	$13 \leq \star \leq 15$	$13 \leq \star \leq 15$

Experimental results and conjectures

Proposition

For any odd q, we have $\mu_q(2) = \mu_q^{tri}(2) = 3$.

Experimental results and conjectures

Proposition

For any odd q, we have $\mu_q(2) = \mu_q^{tri}(2) = 3$.

Experimental results:

- $\mu_3^{\mathrm{tri}}(3) = 6$
- $\mu_p^{\mathrm{tri}}(3) = 5$ for all primes $5 \leq p \leq 257$

Experimental results and conjectures

Proposition

For any odd q, we have $\mu_q(2) = \mu_q^{tri}(2) = 3$.

Experimental results:

- $\mu_3^{\text{tri}}(3) = 6$
- $\mu_p^{\text{tri}}(3) = 5$ for all primes $5 \leq p \leq 257$
- $\mu_3^{\text{tri}}(4) = 9$, $\mu_5^{\text{tri}}(4) = 8$
- $\mu_p^{\text{tri}}(4) = 7$ for all primes $7 \leq p \leq 23$

Experimental results and conjectures

Proposition

For any odd q, we have $\mu_q(2) = \mu_q^{tri}(2) = 3$.

Experimental results:

- $\mu_3^{\text{tri}}(3) = 6$
- $\mu_p^{\text{tri}}(3) = 5$ for all primes $5 \leq p \leq 257$
- $\mu_3^{\text{tri}}(4) = 9$, $\mu_5^{\text{tri}}(4) = 8$
- $\mu_p^{\text{tri}}(4) = 7$ for all primes $7 \leq p \leq 23$

Proposition

We have $\mu_q(n) \geq 2n - 1$ *with* ***equality*** *if and only if* $n < \frac{q}{2} + 1$.

EXPERIMENTAL RESULTS AND CONJECTURES

Proposition

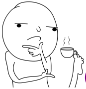
For any odd q, we have $\mu_q(2) = \mu_q^{tri}(2) = 3$.

Experimental results:

- $\mu_3^{\text{tri}}(3) = 6$
- $\mu_p^{\text{tri}}(3) = 5$ for all primes $5 \leq p \leq 257$
- $\mu_3^{\text{tri}}(4) = 9$, $\mu_5^{\text{tri}}(4) = 8$
- $\mu_p^{\text{tri}}(4) = 7$ for all primes $7 \leq p \leq 23$

Proposition

We have $\mu_q(n) \geq 2n - 1$ *with* ***equality*** *if and only if* $n < \frac{q}{2} + 1$.



Open question: is it true for $\mu_q^{\text{tri}}(n)$?

Asymptotics for trisymmetric decompositions

We know:

- $\mu_q(m)$ is **linear** in m
- $\mu_q^{\mathrm{sym}}(m)$ is **linear** in m

Asymptotics for trisymmetric decompositions

We know:

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

Question:

- is it true for $\mu_q^{\text{tri}}(m)$?

Asymptotics for trisymmetric decompositions

We know:

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

Question:

- is it true for $\mu_q^{\text{tri}}(m)$?
  - we have to study symmetry in **higher dimension** to answer!

Symmetry in higher dimensions

- What happens with the product of t variable $x_1, \ldots, x_t$, for $t \geq 3$?

Classic decompositions	**Symmetric** decompositions
$\prod_{i=1}^{t} x_i = \sum_{j=1}^{r} \varphi_j^{(1)}(x_1) \ldots \varphi_j^{(t)}(x_t) \cdot \alpha_j$	$\prod_{i=1}^{t} x_i = \sum_{j=1}^{r} \varphi_j(x_1) \ldots \varphi_j(x_t) \cdot \alpha_j$

Symmetry in higher dimensions

- What happens with the product of t variable $x_1, \ldots, x_t$, for $t \geq 3$?

Classic decompositions	**Symmetric** decompositions
$\prod_{i=1}^{t} x_i = \sum_{j=1}^{r} \varphi_j^{(1)}(x_1) \ldots \varphi_j^{(t)}(x_t) \cdot \alpha_j$	$\prod_{i=1}^{t} x_i = \sum_{j=1}^{r} \varphi_j(x_1) \ldots \varphi_j(x_t) \cdot \alpha_j$

Symmetry in higher dimensions

- What happens with the product of t variable $x_1, \ldots, x_t$, for $t \geq 3$?

Classic decompositions	**Symmetric** decompositions
$\prod_{i=1}^{t} x_i = \sum_{j=1}^{r} \varphi_j^{(1)}(x_1) \ldots \varphi_j^{(t)}(x_t) \cdot \alpha_j$	$\prod_{i=1}^{t} x_i = \sum_{j=1}^{r} \varphi_j(x_1) \ldots \varphi_j(x_t) \cdot \alpha_j$

Theorem

Let $\mathcal{A} = \mathbb{F}_{q^m}$. If $t \leq q$, the ***symmetric multilinear complexity*** *of the product of t variables is* ***linear*** *in m. If $t > q$, then there is no symmetric decomposition.*

Symmetry in higher dimensions

- What happens with the product of t variable $x_1, \dots, x_t$, for $t \geq 3$?

Classic decompositions	**Symmetric** decompositions
$\prod_{i=1}^t x_i = \sum_{j=1}^r \varphi_j^{(1)}(x_1) \dots \varphi_j^{(t)}(x_t) \cdot \alpha_j$	$\prod_{i=1}^t x_i = \sum_{j=1}^r \varphi_j(x_1) \dots \varphi_j(x_t) \cdot \alpha_j$

Theorem

*Let $\mathcal{A} = \mathbb{F}_{q^m}$. If $t \leq q$, the **symmetric multilinear complexity** of the product of t variables is **linear** in m. If $t > q$, then there is no symmetric decomposition.*

Proof.

Generalization of the Chudnovsky-Chudnovsky method: evaluation-interpolation on curves with many points. □

Back on trisymmetry

Corollary

Let $\mathcal{A} = \mathbb{F}_{q^m}$ and $q \geq 3$. Then the ***trisymmetric complexity*** $\mu_q^{tri}(m)$ *is* ***linear*** *in m.*

BACK ON TRISYMMETRY

Corollary

Let $\mathcal{A} = \mathbb{F}_{q^m}$ and $q \geq 3$. Then the ***trisymmetric complexity*** $\mu_q^{tri}(m)$ *is* ***linear*** *in m.*

Proof.

Taking the trace on a **symmetric** decomposition for the 3 variable product xyz gives a **trisymmetric** decompositon for the product xy. □

Conclusion

Bilinear complexity:

- important notion in computer algebra
- any bilinear map can be studied, not just multiplication

Conclusion

Bilinear complexity:

- important notion in computer algebra
- any bilinear map can be studied, not just multiplication

Symmetric complexity:

- Generalization to the case of t-variable products

Conclusion

Bilinear complexity:

- important notion in computer algebra
- any bilinear map can be studied, not just multiplication

Symmetric complexity:

- Generalization to the case of t-variable products

Trisymmetric complexity:

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

CONCLUSION

Bilinear complexity:

- important notion in computer algebra
- any bilinear map can be studied, not just multiplication

Symmetric complexity:

- Generalization to the case of t-variable products

Trisymmetric complexity:

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

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 computer algebra
- any bilinear map can be studied, not just multiplication

Symmetric complexity:

- Generalization to the case of t-variable products

Trisymmetric complexity:

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

Future work:

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

Thank you!