ALCOCRYPT
02/24/2023, CIRM, Marseille.

Improving Chudnovsky-type algorithms over the projective line thanks to derivative evaluations

Bastien Pacifico

joint work with

Stéphane Ballet et **Alexis Bonnecaze**
ATI, I2M, Marseille

Aix*Marseille université

INSTITUT de MATHÉMATIQUES de MARSEILLE

Introduction

Multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$:

Let $\mathcal{B} = \{e_1, \ldots, e_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

The product of $x = \sum_{i=1}^{n} x_i e_i$ and $y = \sum_{i=1}^{n} y_i e_i$ is given by

$$z = xy = \sum_{h=1}^{n} z_h e_h = \sum_{h=1}^{n} \left(\sum_{i,j=1}^{n} t_{ijh} x_i y_j \right) e_h, \tag{1}$$

with

$$e_i e_j = \sum_{h=1}^{n} t_{ijh} e_h,$$

where $t_{ijh} \in \mathbb{F}_q$ are some constants in $\mathbb{F}_q$.

Introduction

Multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$:

Let $\mathcal{B} = \{e_1, \ldots, e_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

The product of $x = \sum_{i=1}^{n} x_i e_i$ and $y = \sum_{i=1}^{n} y_i e_i$ is given by

$$z = xy = \sum_{h=1}^{n} z_h e_h = \sum_{h=1}^{n} \left(\sum_{i,j=1}^{n} t_{ijh} x_i y_j \right) e_h, \tag{1}$$

with

$$e_i e_j = \sum_{h=1}^{n} t_{ijh} e_h,$$

where $t_{ijh} \in \mathbb{F}_q$ are some constants in $\mathbb{F}_q$.

- n^2 bilinear multiplications $(x_i, y_j) \mapsto x_i y_j$ where $x_i, y_j \in \mathbb{F}_q$ depend on the elements x and y of $\mathbb{F}_{q^n}$ being multiplied,
- n^3 scalar multiplications : $x_i \mapsto \alpha \cdot x_i$ where $\alpha, x_i \in \mathbb{F}_q$, and α is constant,
- $n^3 - n$ additions,

Bilinear Complexity

Definition

The number of bilinear multiplications in $\mathbb{F}_q$ used by an algorithm $\mathcal{U}$ for the multiplication in $\mathbb{F}_{q^n}$ is called its **bilinear complexity**, *denoted by*

$$\mu(\mathcal{U}).$$

Definition

The **bilinear complexity of the multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$**, *denoted by $\mu_q(n)$, is the quantity:*

$$\mu_q(n) = \min_{\mathcal{U}} \mu(\mathcal{U}),$$

where $\mathcal{U}$ is running through all algorithms for the multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Polynomial interpolation

Let $\mathbb{F}_{q^n} = \frac{\mathbb{F}_q[x]}{Q(x)}$, for Q a monic irreducible polynomial of degree n over $\mathbb{F}_q$, and let α be a root of Q. Then, $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Let $a, b \in \mathbb{F}_{q^n}$. We write $a = \sum_{i=0}^{n-1} a_i \alpha^i$ and $b = \sum_{i=0}^{n-1} b_i \alpha^i$,

that can be identified to $A(x) = \sum_{i=0}^{n-1} a_i x^i$ and $B(x) = \sum_{i=0}^{n-1} b_i x^i$.

Suppose that $|\mathbb{F}_q| \geqslant 2n-1$. We can compute $A(x)B(x)$ as follows:

1. evaluate $A(x)$ and $B(x)$ at $2n-1$ distinct elements $x_1, x_2, \ldots, x_{2n-1} \in \mathbb{F}_q$,
2. compute the products of these evaluations $C(x_i) = A(x_i)B(x_i)$, for $i = 1, \ldots 2n-1$,
3. reconstruct $C(x) = A(x)B(x)$ from these evaluations.

The result in $\mathbb{F}_{q^n}$ is obtained by the reduction $C(x) \equiv \sum_{i=0}^{n-1} c'_i x^i \pmod{Q(x)}$, and finally $ab = \sum_{i=0}^{n-1} c'_i \alpha^i$.

Lower bound for the bilinear complexity

The method provided in the previous slide gives an algorithm of bilinear complexity equal to $2n-1$, as long as $n < \frac{1}{2}q+1$. This is optimal:

Theorem (Winograd and de Groote, 1979)

The bilinear complexity of the multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ verifies

$$\mu_q(n) \geqslant 2n-1,$$

equality being ensured if and only if $n \leqslant \frac{1}{2}q+1$.

Question: What can we do if $n \geqslant \frac{1}{2}q+1$?

Idea: Use points of a curve defined over $\mathbb{F}_q$,
(i.e. rational places of a function field).

From polynomials to algebraic curves

Polynomial Interpolation	**CCMA[1] (with algebraic curves)**
$n \leqslant \frac{1}{2}q + 1$	n arbitrary
$F_q[x]$	$F/\mathbb{F}_q$ of genus g
$Q(x)$ irred. polynomial of degree n	Q a place of degree n; $\mathcal{D}$ a divisor
$\alpha_1, \ldots, \alpha_{2n-1} \in \mathbb{F}_q$	$P_1, \ldots, P_{2n+g-1}$ rational places
$a, b \in \mathbb{F}_{q^n} = F_q[x]/Q(x)$	$a, b \in \mathbb{F}_{q^n} = F_Q$
$A(x), B(x)$ of degrees at most $n-1$	$f, g \in \mathcal{L}(\mathcal{D})$
$A(\alpha_1)B(\alpha_1), \ldots, A(\alpha_{2n-1})B(\alpha_{2n-1})$	$f(P_1)g(P_1), \ldots, f(P_{2n+g-1})g(P_{2n+g-1})$
($2n-1$ bilinear multiplications)	($2n+g-1$ bilinear multiplications)
$C(x) = A(x)B(x)$ of degree $2n-2$	$fg \in \mathcal{L}(2\mathcal{D})$
$ab \in \mathbb{F}_{q^n}$	$Ev_Q(fg) = ab \in \mathbb{F}_{q^n}$

[1] Chudnovsky & Chudnovsky, *Algebraic Complexities and Algebraic curves over Finite Fieds*, 1988.

Construction stragy when $n \longrightarrow +\infty$

By the Hasse-Weil bound, the number of rational places is bounded according to the genus.

- **Use a family of function fields of increasing genus**
  - Bilinear complexity is **linear** according to the extension degree:

$$\mu_q(n) \leqslant C_q n.$$

  - There is no method to construct the degree n place: no information on the complexity of construction.

Reference: survey[2].

[2] Ballet, Chaumine, Pieltant, Rambaud, Randriambololona and Rolland, *On the tensor rank of multiplication in finite extensions of finite fields and related issues in algebraic geometry, 2021.*

Generalizations

- **Evaluation at places of arbitrary degrees (Ballet-Rolland, Cenk-Özbudak[3]):**

The evaluation at a place P of degree d lies in the residue class field $F_P \simeq \mathbb{F}_{q^d}$.
The product of two such evaluations can be computed as a product in $\mathbb{F}_{q^d}$.

- **Derivative evaluations (Arnaud, Cenk-Özbudak):**

The local expansion of f at a place P is given by

$$f = f(P) + f'(P)t_P + f''(P)t_P^2 + \cdots + f^{(k)}(P)t_P^k + \cdots$$

where t_P is a local parameter for P.
The u first elements of this expansion can be used as a derivative evaluation at order u.

- **Asymetric construction (Randriambololona[4]):**

Use different divisors and $\mathcal{L}(\mathcal{D}_1) \times \mathcal{L}(\mathcal{D}_2) \longmapsto \mathcal{L}(\mathcal{D}_1 + \mathcal{D}_2)$.

---

[3] Cenk and Özbudak, *On multiplication in finite field*, 2010.

[4] Randriambololona, *Bilinear complexity of algebras and the Chudnovshy-Chudnovsky interpolation method*, 2013.

Focus on the evaluation at places of arbitrary degrees

Polynomial Interpolation	**A generalization of CCMA**
$F_q[x]$	$F/\mathbb{F}_q$ of genus g
$Q(x)$ irred. polynomial of degree n	Q a place of degree n - $\mathcal{D}$ a divisor
$\alpha_1, \ldots, \alpha_{2n-1} \in \mathbb{F}_q$	$P_1, \ldots, P_N$ places of arbitrary degrees
$a, b \in \mathbb{F}_{q^n} = F_q[x]/Q(x)$	$a, b \in \mathbb{F}_{q^n} = F_Q$
$A(x), B(x)$ of degrees at most $n-1$	$f, g \in \mathcal{L}(\mathcal{D})$
$A(\alpha_1)B(\alpha_1), \ldots, A(\alpha_{2n-1})B(\alpha_{2n-1})$	$f(P_1)g(P_1), \ldots, f(P_N)g(P_N)$
$(2n-1$ bilinear multiplications$)$	$(\sum_{i=1}^{N} \mu_q(\deg(P_i))$ bilinear multiplications$)$
$C(x) = A(x)B(x)$ of degree $2n-2$	$fg \in \mathcal{L}(2\mathcal{D})$

Recursive constructions

This generalization lead to a new strategy of construction, fixing the genus of the function field (e.g. using only elliptic curves[5])

- **Use places of increasing degrees**
  - Bilinear complexity is **quasi-linear** according to the extension degree:

$$\mu_q(n) \in \mathcal{O}\left((2q)^{\log^*(n)} n\right).$$

  - The algorithms are constructible in polynomial time.

[5] Ballet, Bonnecaze & Tukumuli, *On the construction of elliptic Chudnovsky-type algorithms for multiplication in large extensions of finite fields*, 2013

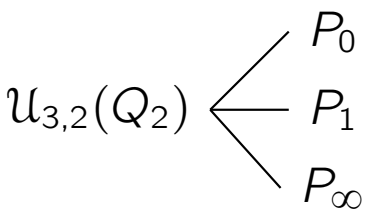
Recursive construction over the projective line

For q a prime power and $n \geqslant 2$ a positive integer, let Q be a place of degree n of $\mathbb{F}_q(x)$. Then, $\mathcal{U}_{q,n}^{\mathcal{P}_n}(Q)$ is an algorithm for the multiplication in $\mathbb{F}_{q^n}$, with the following settings:

- $\mathcal{D} = (n-1)P_\infty$,
- $\mathcal{P}_n = \{P_1, \ldots, P_N\}$ is a set of places such that $\sum_{i=1}^{N} \deg P_i = 2n-1$,
- the basis of $\mathcal{L}(\mathcal{D})$ is $\{1, x, \ldots, x^{n-1}\}$,
- the basis of $\mathcal{L}(2\mathcal{D})$ is $\{1, x, \ldots, x^{2n-1}\}$, and
- apply recursively RPGC to every non-rational places in $\mathcal{P}_n$.

$\mathbb{F}_{3^2}$ and $\mathbb{F}_{3^3}$

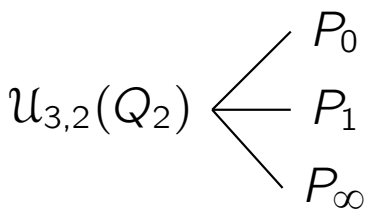
$q = 3$, $n = 2$. Q_2 a degree 2 place of $\mathbb{F}_3(x)$.
P_0, P_1 and P_∞ as previously.



Bilinear complexity: $\mu(\mathcal{U}_{3,2}) = 3$

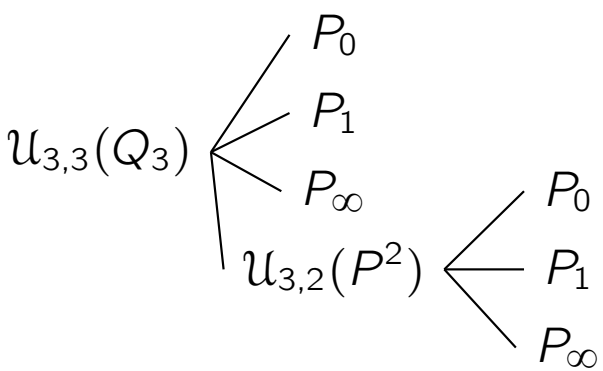
$\mathbb{F}_{3^2}$ and $\mathbb{F}_{3^3}$

$q = 3$, $n = 2$. Q_2 a degree 2 place of $\mathbb{F}_3(x)$.
P_0, P_1 and P_∞ as previously.



Bilinear complexity: $\mu(\mathcal{U}_{3,2}) = 3$

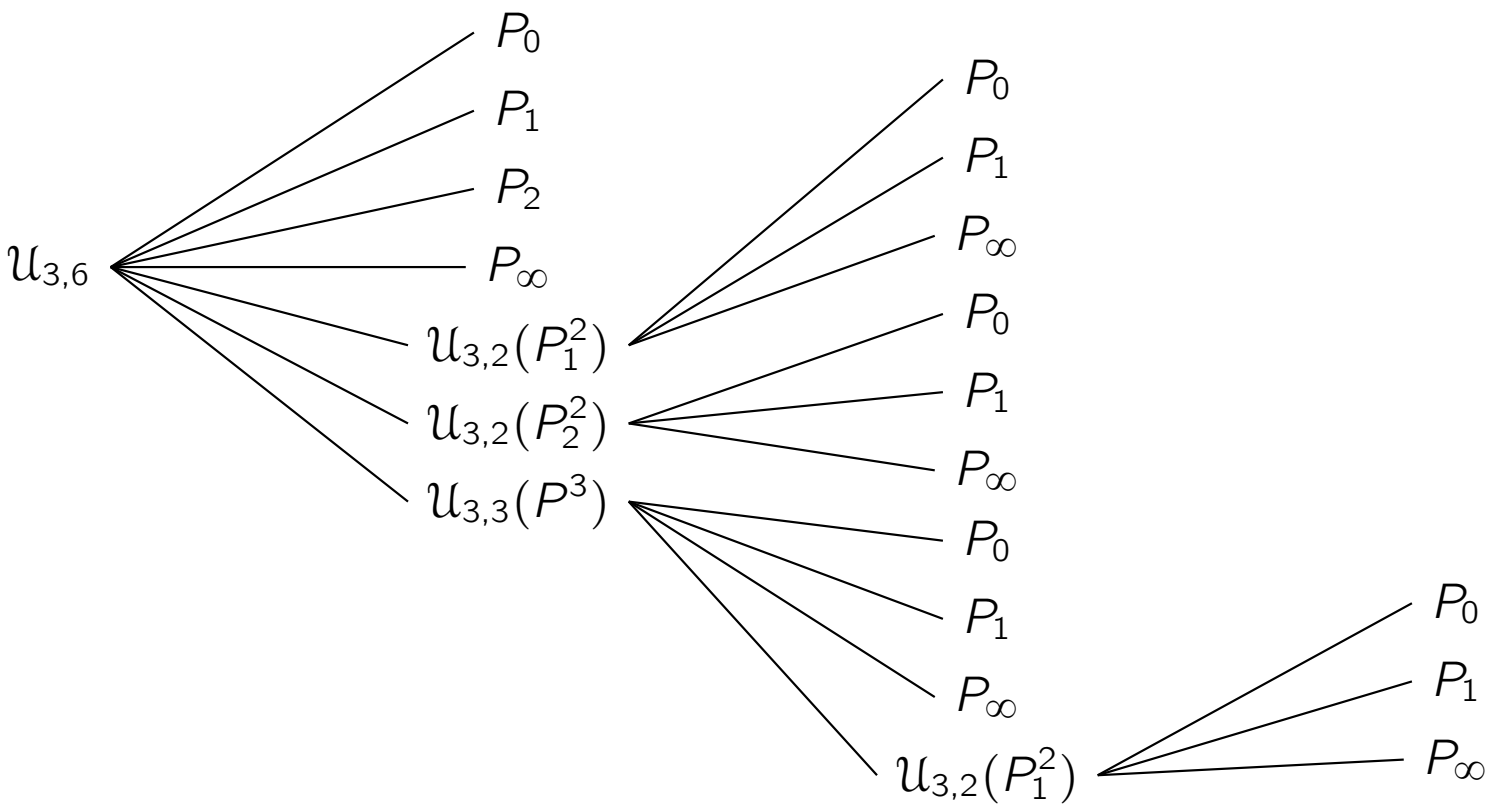
$q = 3$, $n = 3$. Q_3 a degree 3 place of $\mathbb{F}_3(x)$.
P_0, P_1 and P_∞ as previously. P^2 a place of degree 2.



Bilinear complexity: $\mu(\mathcal{U}_{3,3}) = 6$

$\mathbb{F}_{3^6}$

$q = 3$, $n = 6$. Q_6 a degree 6 place of $\mathbb{F}_3(x)$.
P_0, P_1 and P_∞ as previously, P_2 the last rational place.
P_1^2, P_2^2 and P_3^2 the 3 degree 2 places. P^3 a place of degree 3.



Bilinear complexity: $\mu(\mathcal{U}_{3,6}) = 16$

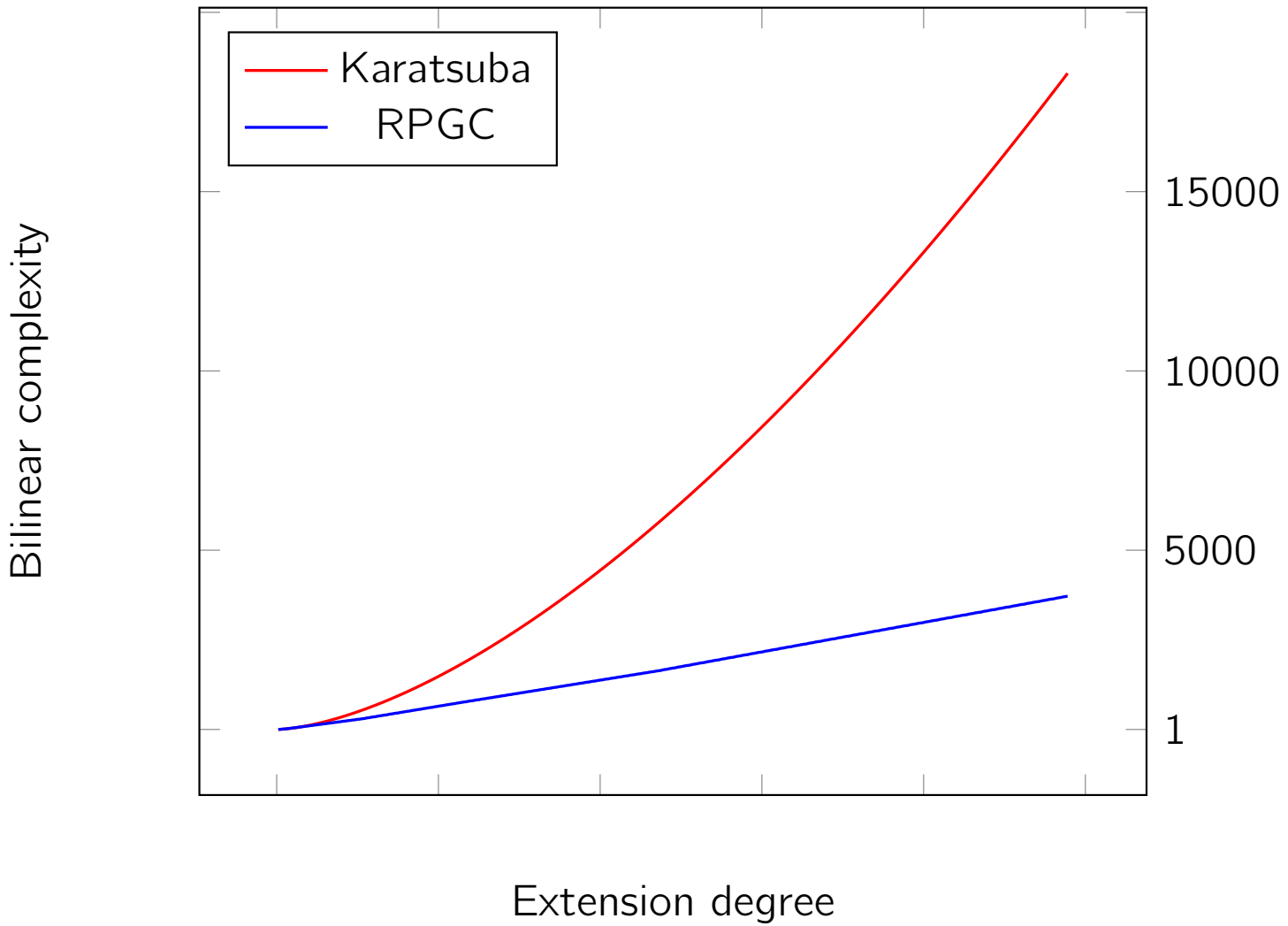
Some bilinear complexities obtained

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mu(\mathcal{U}_{2,n})$	3	6	11	15	18	26	29	37	40	48	51	60	65	70	78	81	90
$\mu(\mathcal{U}_{3,n})$	3	6	9	12	16	19	24	28	31	36	40	43	48	52	55	60	64
$\mu(\mathcal{U}_{4,n})$	3	5	8	11	14	17	20	23	27	30	33	37	40	43	47	50	53

Table: Bilinear complexity of $\mathcal{U}_{q,n}$ in small extensions of $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_4$.

In blue is the best known result.
In orange is an improvement.
Results compared to Table 2 (survey).

Comparison with Karatsuba Algorithm ($q = 2$, $n \leqslant 489$, $d \leqslant 10$)



Asymptotical results

Theorem

Let q be a prime power and let n be a positive integer. Then, our construction provides a Chudnvsky-type algorithm $\mathcal{U}_{q,n}$ for the multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and its bilinear complexity verifies

$$\mu(\mathcal{U}_{q,n}) \leqslant Cn\left(\frac{4q^2}{(q-1)}\right)^{\log^*_{\sqrt{q}}(2n)},$$

where $C = 1$ if $q \geqslant 3$ and $C = 3$ if $q = 2$.

Theorem

The algorithm $\mathcal{U}_{q,n}$ is constructible deterministically and in time $\mathcal{O}(n^4)$, or in expected time $\mathcal{O}(n^{\log_2 7})$ using a Las Vegas algorithm[a].

[a] Couveignes and Lervier, *Fast construction of irreducible polynomials over finite fields*, 2013.

Using a second generalization

- **Evaluation at places of arbitrary degrees (Ballet-Rolland, Cenk-Özbudak[6]):**

The evaluation at a place P of degree d lies in the residue class field $F_P \simeq \mathbb{F}_{q^d}$.
The product of two such evaluations can be computed as a product in $\mathbb{F}_{q^d}$.

- **Derivative evaluations (Arnaud, Cenk-Özbudak):**

The local expansion of f at a place P is given by

$$f = f(P) + f'(P)t_P + f''(P)t_P^2 + \cdots + f^{(k)}(P)t_P^k + \cdots$$

where t_P is a local parameter for P.
The u first elements of this expansion can be used as a derivative evaluation at order u.

- **Asymetric construction (Randriambololona[7]):**

Use different divisors and $\mathcal{L}(\mathcal{D}_1) \times \mathcal{L}(\mathcal{D}_2) \longmapsto \mathcal{L}(\mathcal{D}_1 + \mathcal{D}_2)$.

---

[6] Cenk and Özbudak, *On multiplication in finite field*, 2010.

[7] Randriambololona, *Bilinear complexity of algebras and the Chudnovshy-Chudnovsky interpolation method*, 2013.

Generalized evaluation maps

Definition

For any divisor $\mathcal{D}$, P a place of degree d and the multiplicity $u \geqslant 1$ an integer, we define the generalized evaluation map

$$\varphi_{\mathcal{D},P,u} : \left| \begin{array}{ccc} \mathscr{L}(\mathcal{D}) & \longrightarrow & (\mathbb{F}_{q^d})^u \\ f & \mapsto & (f(P), f'(P), \ldots, f^{(u-1)}(P)) \end{array} \right. \tag{2}$$

where the $f^{(k)}(P)$ are the coefficients of the local expansion

$$f = f(P) + f'(P)t_P + f''(P)t_P^2 + \cdots + f^{(k)}(P)t_P^k + \cdots \tag{3}$$

of f at P with respect to the local parameter t_P, i.e. in $\mathbb{F}_{q^d}[[t_P]]$.

The bilinear complexity of the multiplication in the truncated local expansion of order u at a place P of degree d, i.e. in $\mathbb{F}_{q^d}[[t_P]]/(t_P^u)$, is denoted by $\mu_q(d, u)$.

Using places of arbitrary degrees and generalized evaluation maps

Another generalization of CCMA

$F/\mathbb{F}_q$ of genus g
Q a place of degree n - $\mathcal{D}$ a divisor

$P_1, \ldots, P_N$ places of arbitrary degrees
$u_1, \ldots, u_N$ positive integers

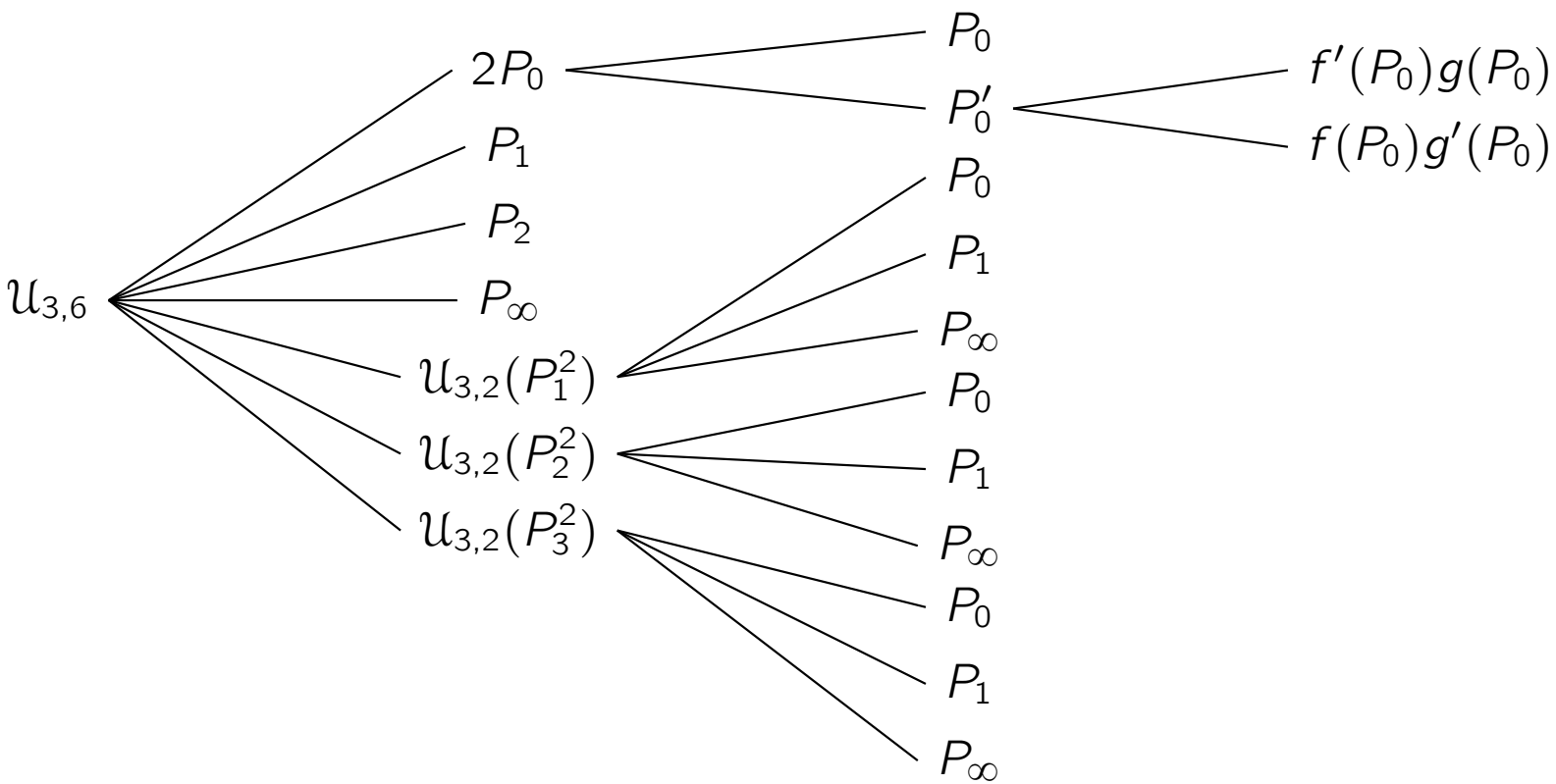
$a, b \in \mathbb{F}_{q^n} = F_Q$
$f, g \in \mathcal{L}(\mathcal{D})$

$\varphi_{\mathcal{D},P_1,u_1}(f)\varphi_{\mathcal{D},P_1,u_1}(g) \ldots, \varphi_{\mathcal{D},P_N,u_N}(f)\varphi_{\mathcal{D},P_N,u_N}(g)$
($\sum_{i=1}^{N} \mu_q(\deg(P_i), u_i)$ bilinear multiplications)

$fg \in \mathcal{L}(2\mathcal{D})$

$\mathbb{F}_{3^6}$ using a derivative evaluation

$q = 3$, $n = 6$. Q_6 a degree 6 place of$\mathbb{F}_q(x)$.
P_0, P_1, P_2 and P_∞ the 4 rational places.
P_1^2, P_2^2 and P_3^2 the 3 degree 2 places.



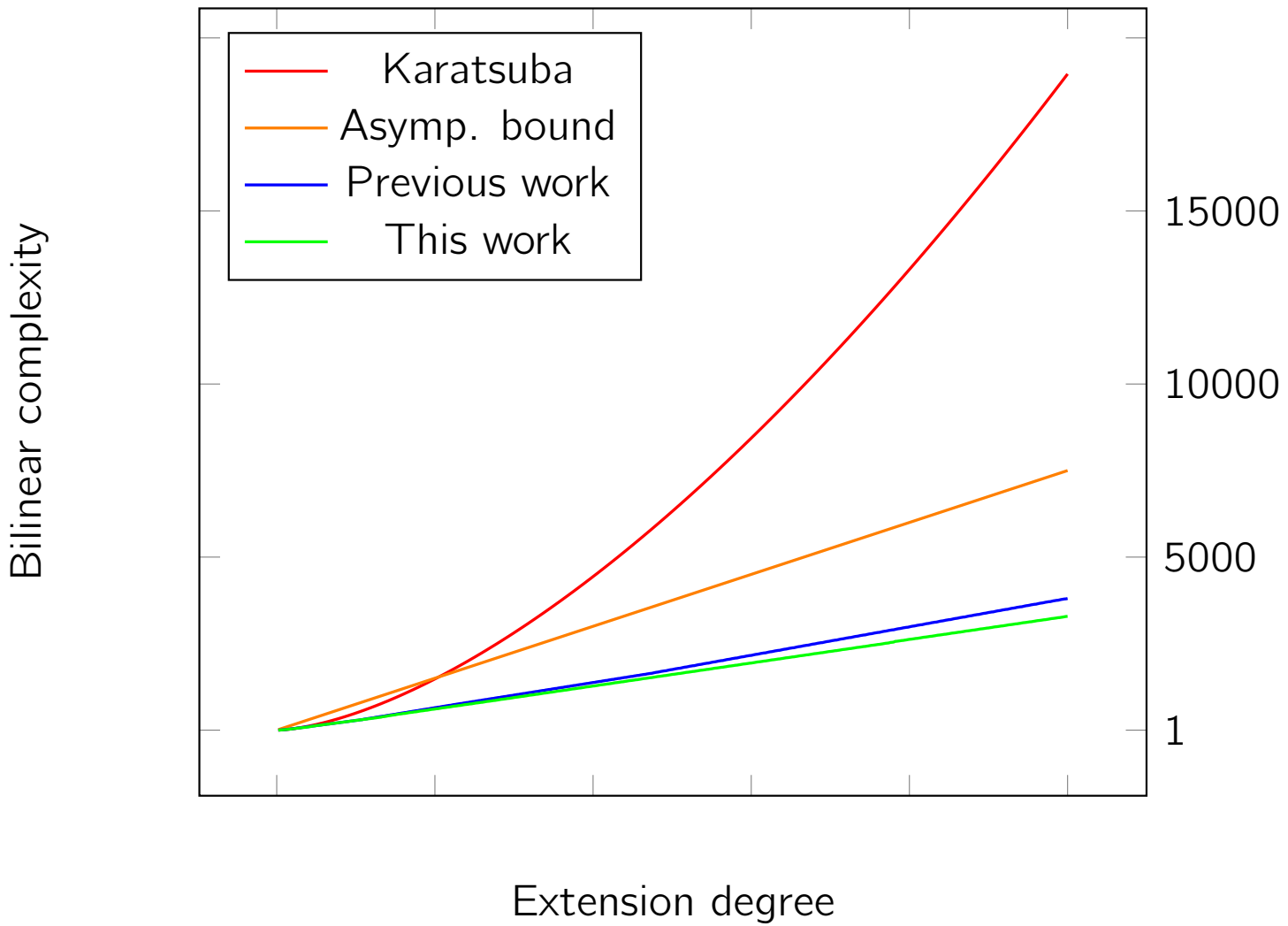
Bilinear complexity: $\mu(\mathcal{U}_{3,6}) = 15$

New strategy

Definition

Let $\mathcal{U}_{q,d,u}$ be an algorithm for the multiplication in the power series ring of truncated local expansions of order u at place P of degree d. Its relative bilinear complexity is given by

$$\frac{\mu(\mathcal{U}_{q,d,u})}{du}.$$


Karatsuba
Asymp. bound
Previous work
This work
Bilinear complexity
15000
10000
5000
1
Extension degree

Thanks for your attention!