Conference On alGebraic varieties over fiNite fields and Algebraic geometry Codes
02/13/2023, CIRM, Marseille.

Polynomial constructions of Chudnovsky-type algorithms for multiplication in finite fields with linear bilinear complexity

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).

D.V. and G.V. Chudnovsky's Algorithm (1987)

Theorem (D. V. and G. V. Chudnovsky (1987))

Let

- $\mathsf{F}/\mathbb{F}_q$ *be an algebraic function field defined over* $\mathbb{F}_q$,
- Q *be a place of degree* n,
- $\mathcal{P} = \{P_1, \ldots, P_N\}$ *be a set of rational places of* $F/\mathbb{F}_q$,
- $\mathcal{D}$ *be a divisor such that* $\mathbf{supp}\,\mathcal{D} \cap \{Q, P_1, \ldots, P_N\} = \varnothing$.

If

(i) *the map* $\mathsf{Ev}_Q : \begin{array}{ccc} \mathscr{L}(\mathcal{D}) & \longrightarrow & \mathsf{F}_Q \simeq \mathbb{F}_{q^n} \\ f & \longmapsto & f(Q) \end{array}$ *is* **surjective**,

(ii) *the following map is* **injective**:

$$\mathsf{Ev}_{\mathscr{P}} : \begin{array}{ccc} \mathscr{L}(2\mathcal{D}) & \longrightarrow & \mathbb{F}_q^N \\ f & \longmapsto & \big(f(P_1), \ldots, f(P_N)\big) \end{array}$$

Then,

(1) for all x, y in $\mathbb{F}_{q^n}$, the multiplication algorihm $\mathcal{U}_{q,n}^{F,\mathcal{P}}(\mathcal{D},Q)$ is defined by:

$$xy = E_Q \circ Ev_{\mathcal{P}}|_{ImEv_{\mathcal{P}}}{}^{-1}\left(E_{\mathcal{P}} \circ Ev_Q^{-1}(x) \odot E_{\mathcal{P}} \circ Ev_Q^{-1}(y)\right), \qquad (2)$$

where

- E_Q: the canonical projection from the valuation ring $\mathcal{O}_Q$ at the place Q in its residue class field F_Q,
- $E_{\mathcal{P}}$: the extension of $Ev_{\mathcal{P}}$ to the valuation ring $\mathcal{O}_Q$ at the place Q,
- $Ev_{\mathcal{P}}|_{ImEv_{\mathcal{P}}}{}^{-1}$: the reverse map of $Ev_{\mathcal{P}}$ restricted to its image,
- $\circ$: the standard composition and $\odot$: the Hadamard product.

(2) the bilinear complexity of the algorithm $\mathcal{U}_{q,n}^{F,\mathcal{P}}(\mathcal{D},Q)$ verifies:

$$\mu_q(\mathcal{U}_{q,n}^{F,\mathcal{P}}(\mathcal{D},Q)) = N.$$

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[1].

[1] 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.*

Example

For any $q > 3$, Ballet[2] proved the existence of a family of CCMA $(\mathcal{U}^{\mathcal{F}}_{q^2,n})_{n\geqslant 2}$ such that:

- F_k is the step with the smallest possible genus in the tower of function fields $\mathcal{F} = (F_1, \ldots, F_k, \ldots)$ over $\mathbb{F}_{q^2}$ introduced by Garcia and Stichtenoth, that is recursively defined by the equation $Y^q + Y = \frac{X^q}{X^{q-1}+1}$, such that
  1. $F_k/\mathbb{F}_q$ contains a place of degree n,
  2. $N_1(F_k/\mathbb{F}_q) > 2n + 2g(F_k) - 1$
- $\mathcal{P}$ is a set of $2n + g(F_k) - 1$ rational places,
- $\mathcal{D}$ is a divisor of degree $n + g(F_k) - 1$
- and Q is a place of degree n.

These algorithm verify

$$\mu(\mathcal{U}^{\mathcal{F}}_{q^2,n}) \leqslant 2\left(1 + \frac{q}{q-3}\right) n.$$

[2] Ballet, *Curves with Many Points and Multiplication Complexity in Any Extension of* $\mathbb{F}_q$, 1999.

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 ℓ first elements of this expansion can be used as a derivative evaluation at order ℓ.

- **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.

Generalization to the use of places of arbitrary degrees

Theorem (D. V. and G. V. Chudnovsky (1987))

Let

- $\mathsf{F}/\mathbb{F}_q$ *be an algebraic function field defined over* $\mathbb{F}_q$,
- Q *be a place of degree* n,
- $\mathcal{P} = \{P_1, \ldots, P_N\}$ *be a set of* **places of arbitrary degrees** *of* $F/\mathbb{F}_q$,
- $\mathcal{D}$ *be a divisor such that* $\operatorname{supp}\mathcal{D} \cap \{Q, P_1, \ldots, P_N\} = \varnothing$.

If

(i) *the map* $\begin{array}{rccc} \mathrm{Ev}_Q : & \mathscr{L}(\mathcal{D}) & \longrightarrow & \mathsf{F}_Q \simeq \mathbb{F}_{q^n} \\ & f & \longmapsto & f(Q) \end{array}$ *is* **surjective**,

(ii) *the following map is* **injective**:

$$\begin{array}{rccc} \mathrm{Ev}_{\mathscr{P}} : & \mathscr{L}(2\mathcal{D}) & \longrightarrow & \mathbb{F}_q^N \\ & f & \longmapsto & \big(f(P_1), \ldots, f(P_N)\big) \end{array}$$

Then,

(1) for all x, y in $\mathbb{F}_{q^n}$, the multiplication algorihm $\mathcal{U}_{q,n}^{F,\mathcal{P}}(\mathcal{D},Q)$ is defined by:

$$xy = E_Q \circ Ev_{\mathcal{P}}|_{ImEv_{\mathcal{P}}}{}^{-1} \left(E_{\mathcal{P}} \circ Ev_Q^{-1}(x) \odot E_{\mathcal{P}} \circ Ev_Q^{-1}(y) \right), \qquad (3)$$

where

- E_Q: the canonical projection from the valuation ring $\mathcal{O}_Q$ at the place Q in its residue class field F_Q,
- $E_{\mathcal{P}}$: the extension of $Ev_{\mathcal{P}}$ to the valuation ring $\mathcal{O}_Q$ at the place Q,
- $Ev_{\mathcal{P}}|_{ImEv_{\mathcal{P}}}{}^{-1}$: the reverse map of $Ev_{\mathcal{P}}$ restricted to its image,
- $\circ$: the standard composition and $\odot$: the Hadamard product.

(2) the bilinear complexity of the algorithm $\mathcal{U}_{q,n}^{F,\mathcal{P}}(\mathcal{D},Q)$ verifies:

$$\mu_q(\mathcal{U}_{q,n}^{F,\mathcal{P}}(\mathcal{D},Q)) = \sum_{i=1}^{N} \mu_q(\deg(P_i))$$

.

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.

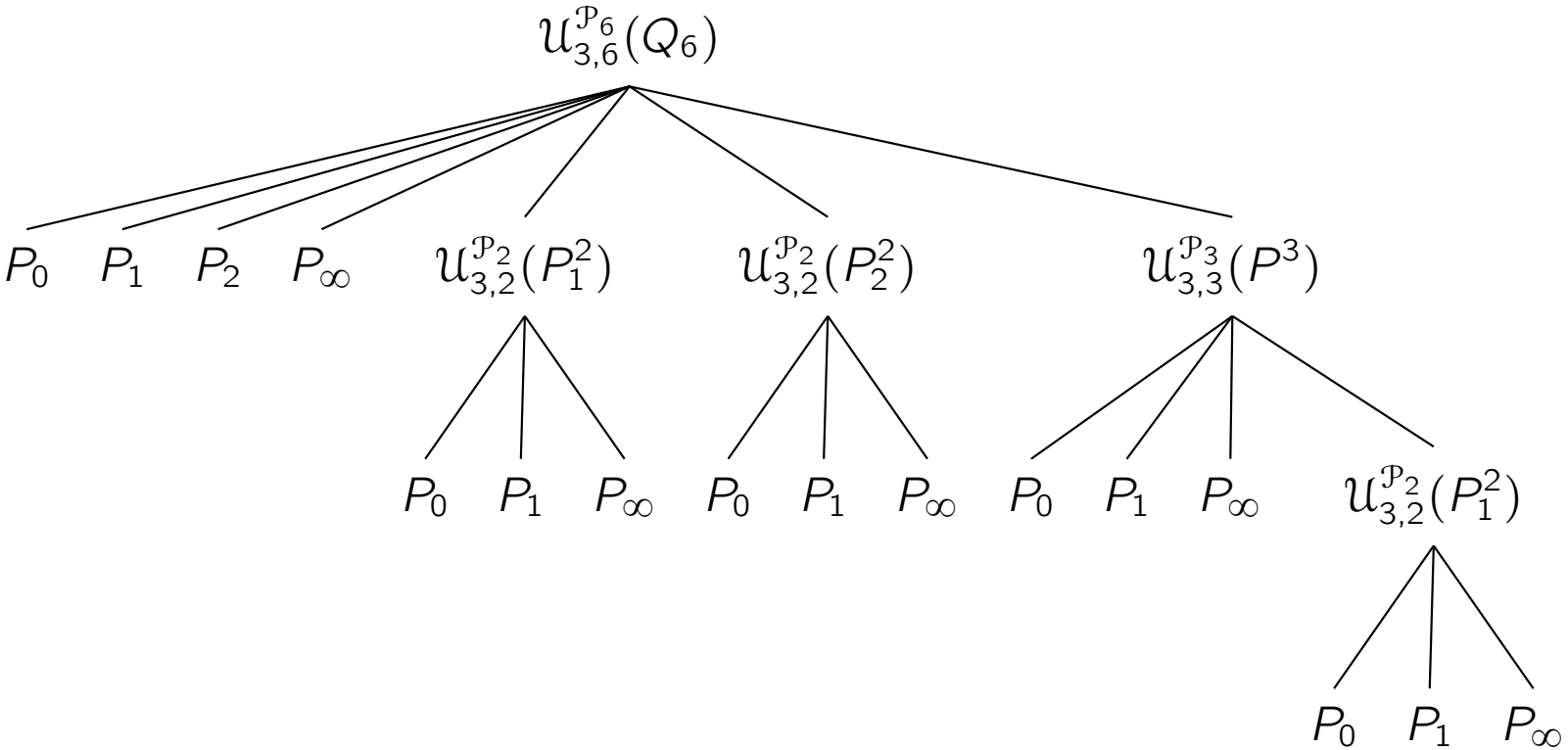
[5] Ballet, Bonnecaze & Tukumuli, *On the construction of elliptic Chudnovsky-type algorithms for multiplication in large extensions of finite fields*, 2013

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 $\mathcal{P}_n$.

Concrete example : multiplication in $\mathbb{F}_{3^6}$



In a nutshell

- **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.

- **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.

Thanks to the notion of tester, Bshouty[6] obtained a construction in polynomial time of multiplication algorithms with a linear bilinear complexity.

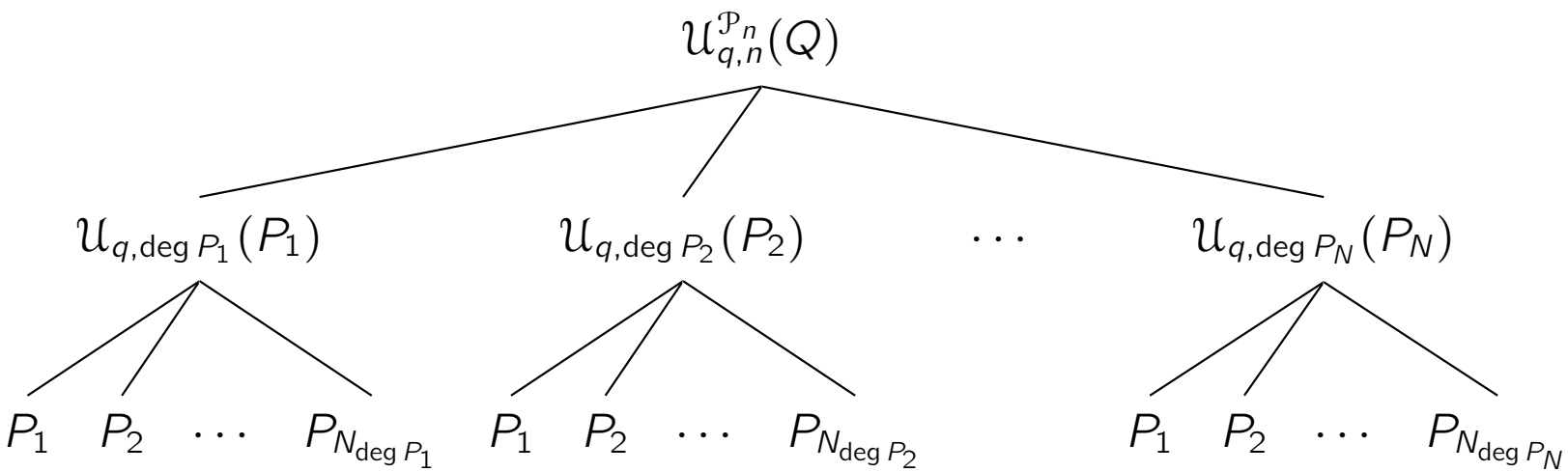
[6] Bshouty, *Testers and their applications*, 2012.

Hybrid Chudnovsky-type algorithms

Definition

Let q be a prime power and n be a positive integer. A Hybrid Chudnovsky-type Algorithm $\mathcal{U}_{q,n}^{\mathcal{H}}$ for the multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is such that

- *first, we use a Chudnovsky-type algorithm over the projective line, $\mathcal{U}_{q,n}^{\mathcal{P}_n}(Q)$,*
- *then, the evaluations are multiplied using a family $\mathcal{U}_q$ of Chudnovsky-type algorithms constructed using the increasing genus strategy.*



First, Chudnovsky-type algorithm over the projective line

The algorithm $\mathcal{U}_{q,n}^{\mathcal{P}_n}(Q)$

- is constructible deterministically and in polynomial time $\mathcal{O}(n^4)$,
- and its bilinear complexity is given by

$$\mu\left(\mathcal{U}_{q,n}^{\mathcal{P}_n}(Q)\right) = \sum_{i=1}^{N} \mu\left(\mathcal{U}_{q,\deg P_i}(P_i)\right).$$

- There exists $d \leqslant \log_q(2n)$ such that for all i, $\deg P_i \leqslant d$.

Then, specific construction over the Garcia-Stichtenoth tower

Let $q > 5$ be a prime power. As earlier, we use the recursive tower $\mathcal{F}$, and define the algorithms $\mathcal{U}_{q^2,n}$ with

- $F = F_k$ is the step of $\mathcal{F}$ with the smallest possible genus such that
  1. $2g_k + 1 \leqslant q^{n-1}(q-1)$, where $g_k = g(F_k)$,
  2. $N_1(F_k) \geqslant 2n + 4g_k$.
- $\mathcal{D} = (n + 2g - 1)P$, where P is a rational place of F_k.
- $\mathcal{P}$ is a set of $2n + 4g_k - 1$ rational places of F_k, distinct from P.
- Q is a degree n place of F_k.

Bilinear complexity

The latest algorithms over the tower $\mathcal{F}$ verify

$$\mu\left(\mathcal{U}_{q^2,n}\right) \leqslant 2\left(1+\frac{3q}{q-5}\right)n.$$

Thus, the bilinear complexity of $\mathcal{U}^{\mathcal{H}}_{q^2,n}$ verifies

$$\begin{aligned}\mu\left(\mathcal{U}^{\mathcal{H}}_{q^2,n}\right) &= \textstyle\sum_i \mu\left(\mathcal{U}_{q,\deg P_i}(P_i)\right)\\ &\leqslant \textstyle\sum_i 2\left(1+\frac{3q}{q-5}\right)\deg P_i\\ &= 2\left(1+\frac{3q}{q-5}\right)(2n-1),\end{aligned}$$

since $\sum_i \deg P_i = 2n-1$.

Complexity of construction

- The tower $\mathcal{F}$ is a family of Drinfeld modular curves by Elkies[7].
- The form of $\mathcal{D}$ is specified.
- By Shparlinski, Tsfasman and Vladuts[8], one can work polynomially with such curves, i.e. compute bases of the Riemann-Roch spaces, and the evaluation maps.
- Thus, the specific algorithms $\mathcal{U}_{q^2,\deg P_i}$ over $\mathcal{F}$ are constructible in polynomial time (in $\deg P_i$) if a place of degree $\deg P_i$ is given.
- Such a place can be constructed in exponential time $\mathcal{O}\left((q^2)^{2\deg P_i} M(\deg P_i) \log \deg P_i\right)$.
- But $\deg P_i \leqslant \log_q(2n)$.
- Finally the hybrid Chudnovsky-type algorithms are constructible in polynomial time in n.

[7] Elkies, *Explicit towers of Drinfeld modular curves*, 2001.

[8] Shparlinski, Tsfasman and Vladuts, *Curves with many points and multiplication in finite fields*, 1992.

Conclusion

Theorem

For all prime power q and all integer n, there exists a Hybrid Chudnovsky-type algorithm $\mathcal{U}_{q,n}^{\mathcal{H}}$ such that

- *the bilinear complexity of $\mathcal{U}_{q,n}^{\mathcal{H}}$ verifies $\mu(\mathcal{U}_{q,n}^{\mathcal{H}}) \leqslant C_q n$, where*

$$C_q = \begin{cases} 4\left(1+\frac{3\sqrt{q}}{\sqrt{q}-5}\right) & \text{if } q > 25 \text{ is a square,} \\ 12\left(1+\frac{3q}{q-5}\right) & \text{if } q > 5, \\ 152 & \text{if } q = 5, \\ 172 & \text{if } q = 4, \\ 279 & \text{if } q = 3, \\ 648 & \text{if } q = 2. \end{cases}$$

- *the algorithm $\mathcal{U}_{q,n}^{\mathcal{H}}$ is constructible deterministically, and in polynomial time in $\mathcal{O}(n^4)$.*

Thanks for your attention!