Finding optimal Chudnovsky-Chudnovsky multiplication algorithms

Matthieu Rambaud

Telecom ParisTech, Paris, France

WAIFI 2014, Gebze
September 27, 2014

A trick

Compute $(ax+b)(cx+d)$
$$= a{\color{red}\bullet}cx^2 + (a{\color{red}\bullet}d + b{\color{red}\bullet}c)x + b{\color{red}\bullet}d$$

Total : **4** multiplications

A trick

Can one do better ?

Compute $(ax+b)(cx+d)$

$$= a \bullet c x^2 + (a \bullet d + b \bullet c)x + b \bullet d$$

Total : **4** multiplications

A trick

$$\text{Evaluate } \begin{aligned} m_0 &= b \bullet d \\ m_1 &= (a+b) \bullet (c+d) \\ m_\infty &= a \bullet c \end{aligned}$$

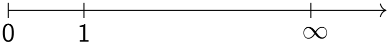
Then, $(ax+b)(cx+d) = m_\infty x^2 + (m_1 - m_0 - m_\infty)x + m_0$

Total : **3** multiplications

What happened ?

Lagrange's interpolation (over $\mathbb{R} \cup \infty$)

The degree 2 polynomial P(x)=(ax+b)(cx+d) is fully determined by the 3 evaluations $m_0 = P(0)$, $m_1 = P(1)$, $m_\infty = P(\infty)$.



What happened ?

Lagrange's interpolation (over $\mathbb{R} \cup \infty$)

The degree 2 polynomial P(x)=(ax+b)(cx+d) is fully determined by the 3 evaluations $m_0 = P(0)$, $m_1 = P(1)$, $m_\infty = P(\infty)$.

Problem : only $q+1$ points on $\mathbb{F}_q \cup \infty$

Ch&Ch's interpretation

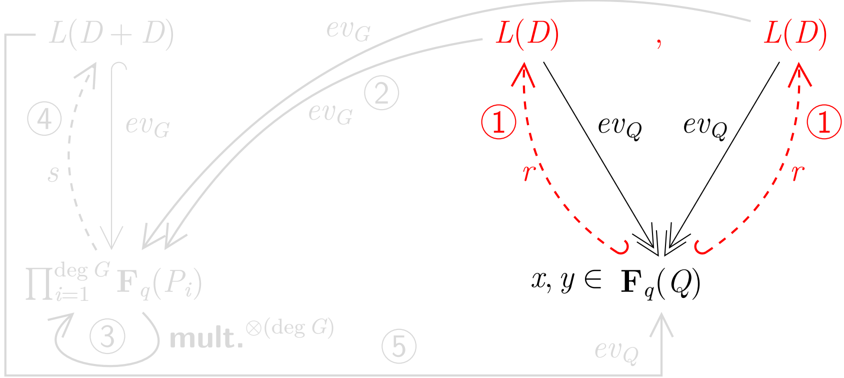
	Before	After
set:	$\mathbf{F}_q \cup \infty$	curve $X = P^1_{\mathbf{F}_q}$
$(ax+b)$ and $(cx+d)$:	polynomials	sections of $D = \mathcal{O}_X(\infty)$
evaluation on:	points $0,1,\infty$	divisor $G = [0]+[1]+[\infty]$

Multiply x, y *in* F_{q^m} *(Ch&Ch)*

$$\begin{tikzcd}
L(D+D) \arrow[d, hook, "ev_G"] \arrow[drrr, bend right=60, "ev_Q", "5"'] & & L(D) \arrow[dll, "ev_G", "2"'] \arrow[dr, "ev_Q"] & , & L(D) \arrow[dl, "ev_Q"'] \arrow[dllll, bend right, "ev_G"'] \\
\prod_{i=1}^{\deg G} \mathbf{F}_q(P_i) \arrow[u, dashed, bend left, "s", "4"'] \arrow[loop below, "\mathbf{mult.}^{\otimes(\deg G)}", "3"'] & & & x, y \in \mathbf{F}_q(Q) \arrow[ul, dashed, bend left, "r", "1"'] \arrow[ur, dashed, bend right, "r"', "1"] &
\end{tikzcd}$$

0 *choose* Q on X of degree m, fix isomorphism $x, y \in \mathbf{F}_{q^m} \cong \mathbf{F}_q(Q)$

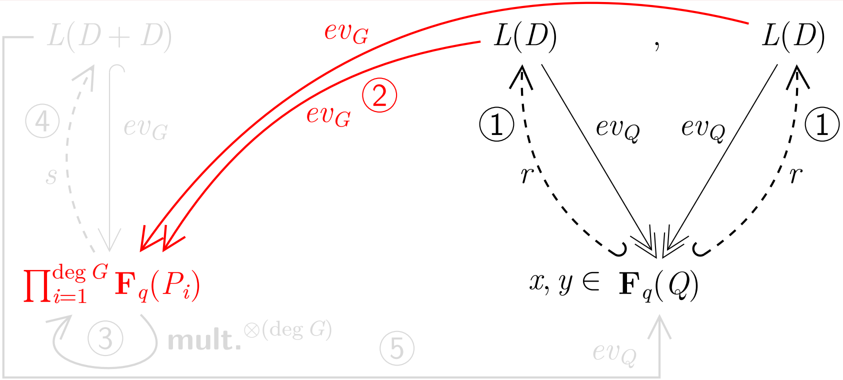
Multiply x, y in $\mathbf{F}_{q^m}$ (Ch&Ch)



0 *choose* Q on X of degree m, fix isomorphism $x, y \in \mathbf{F}_{q^m} \cong \mathbf{F}_q(Q)$

1 find divisor D; *lift* x, y to f_x, f_y in $L(D)$.

Multiply x, y in $\mathbf{F}_{q^m}$ (Ch&Ch)

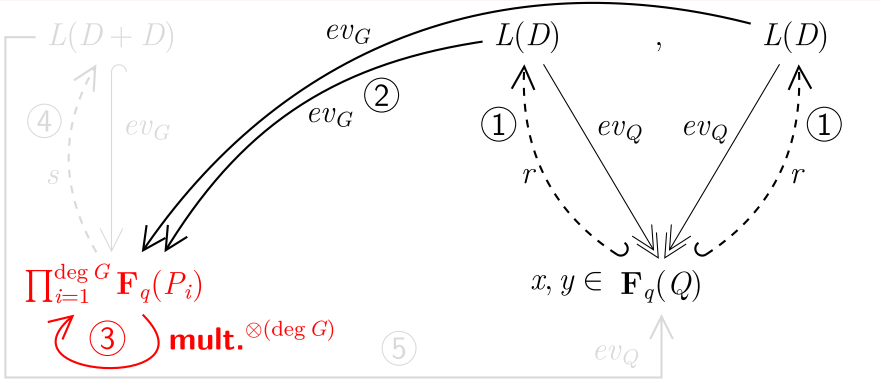


0 *choose* Q on X of degree m, fix isomorphism $x, y \in \mathbf{F}_{q^m} \cong \mathbf{F}_q(Q)$

1 find divisor D; *lift* x, y to f_x, f_y in $L(D)$.

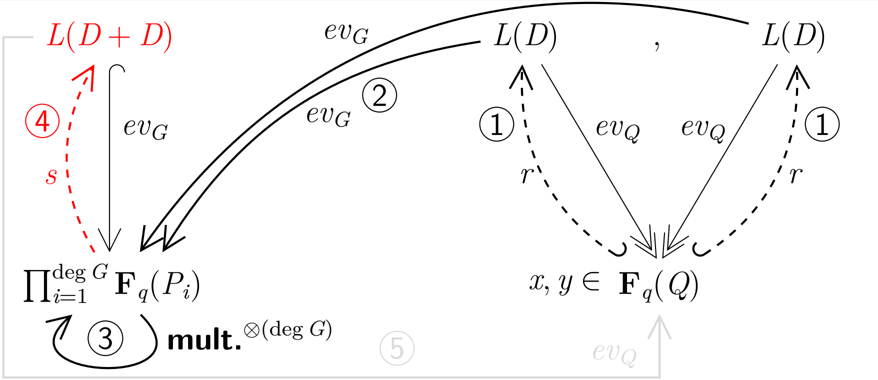
2 find divisor $G = P_1 + \ldots + P_{\deg G}$; *evaluate* the $f_x(P_i)$ and $f_y(P_i)$.

Multiply x, y in $\mathbb{F}_{q^m}$ *(Ch&Ch)*



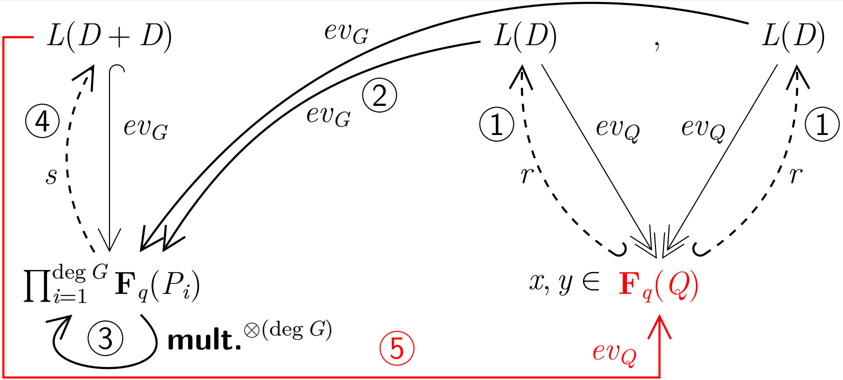
0. *choose* Q on X of degree m, fix isomorphism $x, y \in \mathbf{F}_{q^m} \cong \mathbf{F}_q(Q)$
1. find divisor D; *lift* x, y to f_x, f_y in $L(D)$.
2. find divisor $G = P_1 + \ldots + P_{\deg G}$; *evaluate* the $f_x(P_i)$ and $f_y(P_i)$.
3. *compute* the $m_i = f_x(P_i) \bullet f_y(P_i)$: **deg *G*** multiplications.

Multiply x, y *in* $\mathbf{F}_{q^m}$ *(Ch&Ch)*



- **0** *choose* Q on X of degree m, fix isomorphism $x, y \in \mathbf{F}_{q^m} \cong \mathbf{F}_q(Q)$
- **1** find divisor D; *lift* x, y to f_x, f_y in $L(D)$.
- **2** find divisor $G = P_1 + \ldots + P_{\deg G}$; *evaluate* the $f_x(P_i)$ and $f_y(P_i)$.
- **3** *compute* the $m_i = f_x(P_i) \bullet f_y(P_i)$: **deg *G*** multiplications.
- **4** *interpolate* $[m_1, \cdots, m_n]$ to unique $g \in L(D+D)$

Multiply x, y in $\mathbf{F}_{q^m}$ (Ch&Ch)



0. *choose* Q on X of degree m, fix isomorphism $x, y \in \mathbf{F}_{q^m} \cong \mathbf{F}_q(Q)$
1. find divisor D; *lift* x, y to f_x, f_y in $L(D)$.
2. find divisor $G = P_1 + \ldots + P_{\deg G}$; *evaluate* the $f_x(P_i)$ and $f_y(P_i)$.
3. *compute* the $m_i = f_x(P_i) \bullet f_y(P_i)$: **deg** ***G*** multiplications.
4. *interpolate* $[m_1, \cdots, m_n]$ to unique $g \in L(D+D)$
5. *evaluate* g at Q to find the product of x and y.

Need more interpolation data ?

	Before	After	Evaluation in:
degree(P_i) :	1	$d \geqslant 1$	$\mathbf{F}_{q^d}$
"$f_x(P_i)$" :	value $f_x(P_i)$	derivatives of f_x at P_i up to $l \geqslant 0$	$\frac{\mathbf{F}_q[y]}{y^l}$
...Both :			$\frac{\mathbf{F}_{q^d}[y]}{y^l}$

Putting things together

Note $\mu_q^{\text{sym}}(d, l)$ the bilinear complexity of the multiplication in $\frac{\mathbf{F}_{q^d}[y]}{y^l}$.

Complexity of the algorithm [Randriam 2012, see Th. 2]

X a curve of genus g over $\mathbf{F}_q$, Q a point of degree m, D a divisor, $G := l_1 P_1 + \cdots l_n P_n$ [with $\deg P_i = d_i$], and suppose (G, D, Q) "suitable for interpolation". Then :

$$\mu_q^{\text{sym}}(m) \leqslant \underbrace{\boxed{\sum_{i=1}^{\deg G} \mu_q^{\text{sym}}(d_i, l_i)}}_{\text{weighted degree of } G}$$

Find suitable (G, D, Q), G of smallest weighted degree

Lowering the weights

Table: New lower–upper bounds on the $\mu_2^{\mathrm{sym}}(d,l)$ [see R., §2]

$l \backslash d$	1	2	3	4	5	6	7	8	9	10
1	1	3	6	9	13	15	16–22	–24	–30	–33
2	3	9	**16**	–24	.	.	.	.	.	.
3	5	15	–30	.	.	.	.	.	.	.
4	8	–**21**	.	.	.	.	.	.	.	.
5	11	.	.	.	.	.	.	.	.	.
6	14	.	.	.	.	.	.	.	.	.
7	16–18	.	.	.	.	.	.	.	.	.
8	–22	.	.	.	.	.	.	.	.	.
9	–27	.	.	.	.	.	.	.	.	.
10	–**30**	.	.	.	.	.	.	.	.	.

(G, D, Q), G of smallest degree?

Best expectable (G, D, Q) [see R., Prop. 8 & 10]

X a curve of genus g. Assume $\boldsymbol{m > g}$. Then : criterion for (G, D, Q) being "suitable for interpolation on $\mathbf{F}_{q^m}$" depends only on the classes of G, D, Q in $\mathrm{Cl}(X)$. When the case :

1. $\deg G \geqslant 2m + g - 1$
2. ...and if this lower bound attained, then $\deg D = m + g - 1$.

Example [see 4.2]

Multiplication in $\mathbf{F}_{2^m}$, $m = 163$:
Step 0 : find a curve X having a divisor G of smallest weighted degree, under the constraint $\deg G \geqslant 2m + g - 1 = 331$ (condition 1.).
$\rightarrow$ Exhaustive search on the $X_0(N)$ ...Winner : $X_0(71)$, with a G of weighted degree 900.

! G is not necessarily part of a suitable (G, D, Q)

Example [see 4.2]

class group : $\mathrm{Cl}(X_0(71)) \sim \mathbf{Z}/315\mathbf{Z} \times \mathbf{Z}$, generators : (D_1, D_2).
Step 1 : Choose a G on X of weighted degree 900.

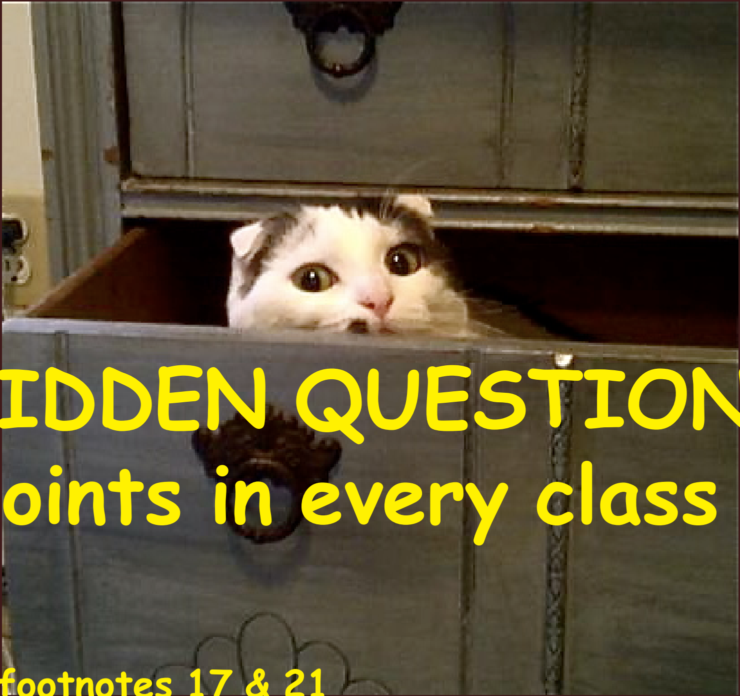
- Step 2 $\deg D$ must be $m + g - 1 = 168 \rightarrow$ Loop over the classes : $D := i * D_1 + 168 * D_2$, until $l(2D - G) = 0$ [Theorem 2, condition (i')]. $\rightarrow$ Success for $i = 2$.
  - Step 3 : Loop over the classes of random Q of degree m, until $l(D - Q) = 0$ [Theorem 2, condition (ii') & Footnote 16] $\rightarrow$ Success at first attempt.

$\rightarrow$ 900 is a new upper bound for the multiplication in $\mathbf{F}_{2^{163}}$.

Search on the curves $X_0(N)$*,* $N = 0 \ldots 1000 \longrightarrow$ *new bounds:*

Table: New upper bounds on $\mu_2^{\mathrm{sym}}(m)$, sorted by the genus of curves used

$m \backslash g$	1 (ECs)	2	3	4	5	6
163	905	903	901	.	.	**900**
233	1339	1336	.	**1335**	.	.
283	1661	1660	.	**1654**	.	.
409	2492	2491	.	**2486**	.	.
571	3562	3561	3560	**3555**	.	.



HIDDEN QUESTION : points in every class ?

...see footnotes 17 & 21