Intertwinned towers of Shimura curves and Bilinear multiplication

Matthieu Rambaud

Telecom ParisTech

JC2, la Bresse Apr. 28, 2017

Bilinear multiplication

f *and* g *in* $\mathbf{F}_p[X]$ *of degree* m*, compute* $f.g$

1. *Choose* $P_1, \ldots, P_{2m+1}$ in $\mathbf{F}_p$
2. *Evaluate* $f(P_i)_{i=1..2m+1}$ and $g(P_i)_{i=1..2m+1}$
3. *Compute* $\left\{ f.g(P_i) = f(P_i) \bullet g(P_i) \right\}_i$: $2m+1$ multiplications
4. *Lagrange's interpolation:* recover $f.g$.

Chudnovsky^2's improvement

	Before	After
set:	$\mathbf{F}_p$	curve $X_{/\mathbf{F}_p}$
f and g in $\mathbf{F}_p[X]$:	polynomials	rational functions f and g in $\mathcal{L}(D)$
evaluation on:	points $P_1, \ldots P_{2m+1}$ in $\mathbf{F}_p$	points $P_1, \ldots P_{2m+\mathbf{g}+1}$ in $X(\mathbf{F}_p)$

Small genera, small fields, many thick points

Conjecture

Let p prime and $2t \geqslant 4$. Does there exist a family $\left(X_s/\mathbf{F}_p\right)_{s\geqslant 1}$ of curves *defined over* $\mathbf{F}_p$, with genera g_s such that:

1. $g_s \longrightarrow \infty$
2. $g_{s+1}/g_s \longrightarrow 1$ (*density* of $(X_s)_s$)
3. $\left|X_s(\mathbf{F}_{p^{2t}})\right|/g_s \xrightarrow[s\to\infty]{} p^t - 1$ (*Optimality over* $\mathbf{F}_{p^{2t}}$) ?

the Graal

Conjecture

Let p prime and $2t \geqslant 4$. Does there exist a family $(X_s/\mathbf{F}_p)_{s\geqslant 1}$ of curves *defined over* $\mathbf{F}_p$, with genera g_s such that:

1. $g_s \longrightarrow \infty$
2. $g_{s+1}/g_s \longrightarrow 1$ (*density* of $(X_s)_s$)
3. $|X_s(\mathbf{F}_{p^{2t}})|/g_s \xrightarrow[s\to\infty]{} p^t - 1$ (*Optimality over* $\mathbf{F}_{p^{2t}}$) ?

1. Classical modular curves $X_0(N)$? ⚠ $2t = 2$
2. Shimura curves $X_0(\mathcal{N})$? ⚠ $2t \geqslant 4 \Rightarrow$ defined over $\mathbf{F}_{p^t}$
3. Garcia–Stichtenoth's towers F_s ? ⚠ $g_{s+1}/g_s \sim p^{2t}$

Solution proposed for p=3 and 2t=6

1. Hard work: *compute two towers* of Shimura curves over $\mathbf{F}_{3^6}$!

$$\ldots \xrightarrow{f_4} X_0(7^3) \xrightarrow{f_3} X_0(7^2) \xrightarrow{f_2} X_0(7^1) \xrightarrow{f_1} X_0(1)$$
$$\ldots \xrightarrow{g_4} X_0(8^3) \xrightarrow{g_3} X_0(8^2) \xrightarrow{g_2} X_0(8^1) \xrightarrow{g_1} X_0(1)$$

2. *Descend* everything over $\mathbf{F}_3$.

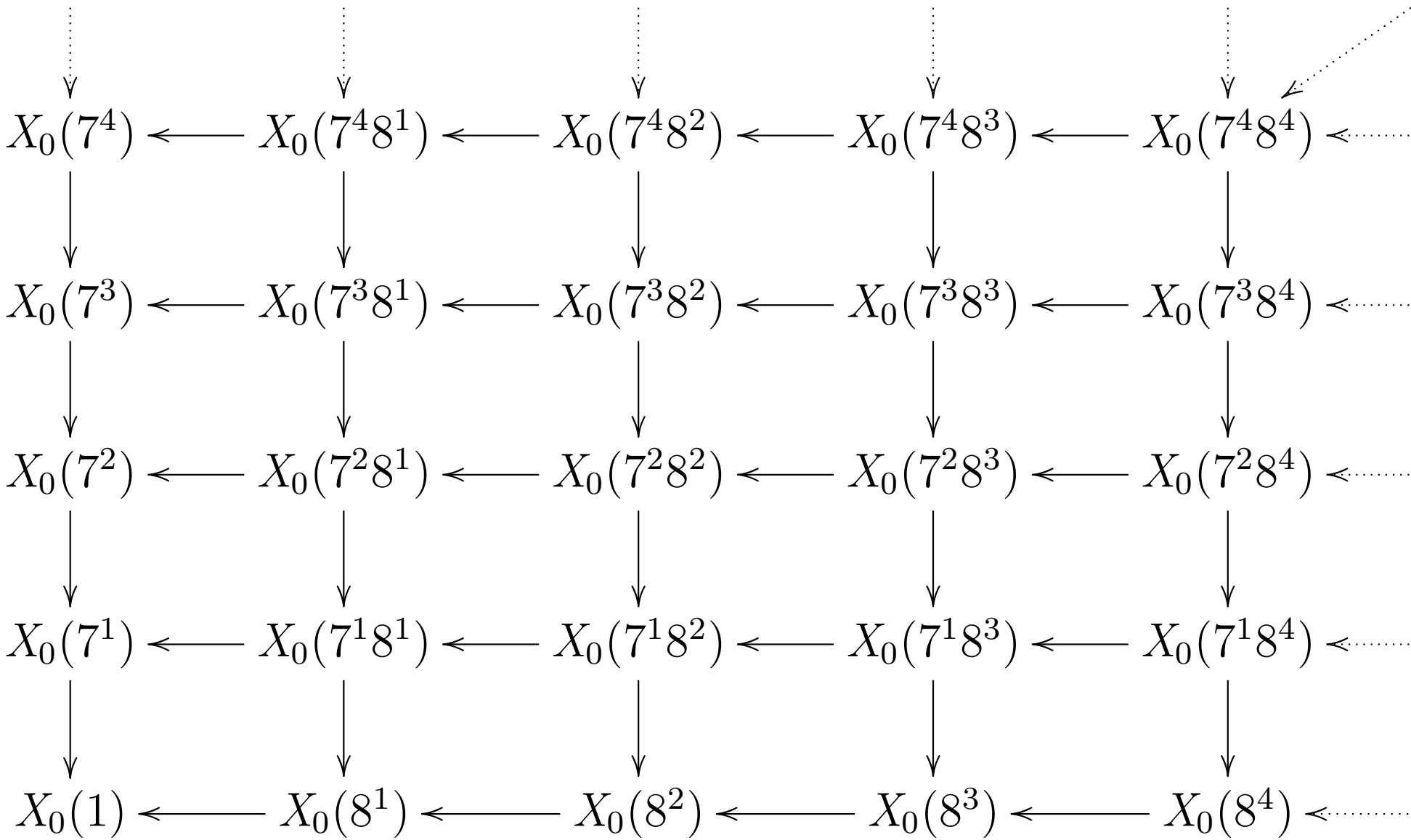
Solution proposed for p=3 and 2t=6

1. Hard work: *compute two towers* of Shimura curves over $\mathbf{F}_{3^6}$!

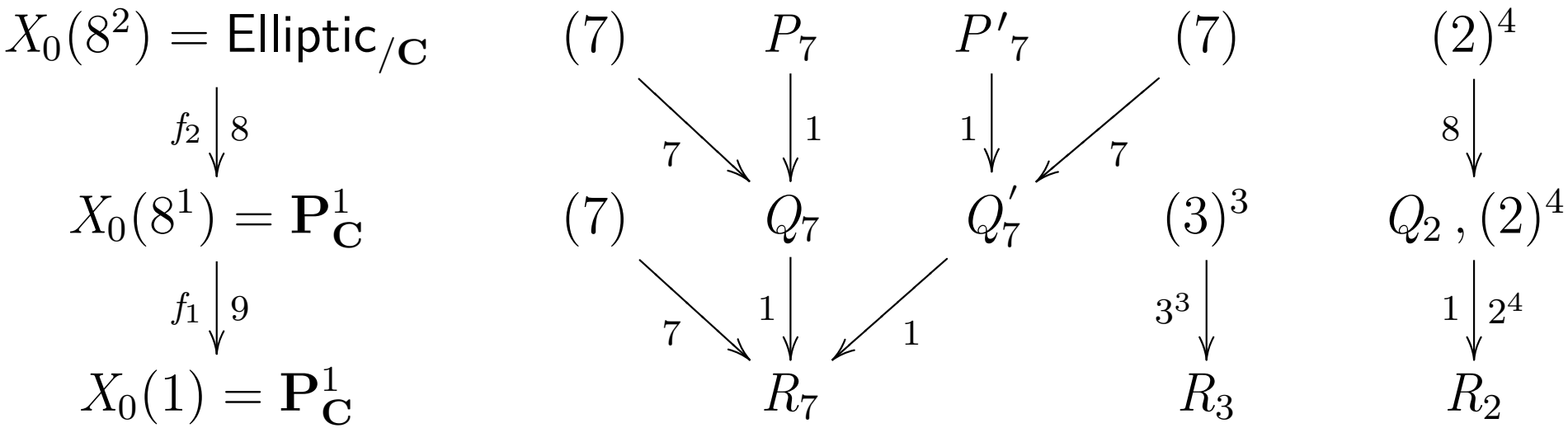
$$\ldots \xrightarrow{f_4} X_0(7^3) \xrightarrow{f_3} X_0(7^2) \xrightarrow{f_2} X_0(7^1) \xrightarrow{f_1} X_0(1)$$
$$\ldots \xrightarrow{g_4} X_0(8^3) \xrightarrow{g_3} X_0(8^2) \xrightarrow{g_2} X_0(8^1) \xrightarrow{g_1} X_0(1)$$

2. *Descend* everything over $\mathbf{F}_3$.
3. Then for the density...

Elkies' Trick



Example: starting a tower



Example: ...and a recursion

$$X_0(8^3) = \quad X_0(8^2) \quad \times \quad X_0(8^2)$$

$$\omega_1 \circ f_2 \circ \omega_2 \searrow \quad X_0(8^1) \quad \swarrow f_2$$

$$X_0(8^2)_{\mathbf{F}_3} : y^2 = x^3 + x^2 + 2$$

$$X_0(8^1)_{\mathbf{F}_3} = \mathbf{P}^1_{\mathbf{F}_3}$$

$$f_2(x, y) = \frac{1 + x^2 + x^3 + x^4 + (x + 2x^2)y}{2 + x^2 + x^3 + x^4 + x^2 y}$$

$$\omega_2 : X_0(8^2)_{\mathbf{F}_3} \ni P \longrightarrow (1, 2, 1) - P$$

$$\omega_1 : t \in \mathbf{P}^1_{\mathbf{F}_3} \ni t \longrightarrow -t$$