Intertwinned towers of Shimura curves and bilinear multiplication

Matthieu Rambaud

Telecom ParisTech

AGC^{2}T, Jun. 20, 2017

Bilinear multiplication

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

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* $\left\{ f \cdot g(P_i) = f(P_i) \bullet g(P_i) \right\}_i$: $2m+1$ multiplications.
4. *Lagrange's interpolation:* recover $f \cdot g$.

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

the Graal

Conjecture

Let p be a prime and $2t \geqslant 4$. Does there exist a family $(X_s)_{s\geqslant 1}$ of curves, with genera $g_s \longrightarrow \infty$ such that:

1. X_s is *defined over* $\mathbf{F}_p$;
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* $\mathbf{F}_{p^{2t}}$) ?

the Graal

Conjecture

Let p be a prime and $2t \geqslant 4$. Does there exist a family $(X_s)_{s \geqslant 1}$ of curves, with genera $g_s \longrightarrow \infty$ such that:

1. X_s is *defined over* $\mathbf{F}_p$;
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* $\mathbf{F}_{p^{2t}}$) ?

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

a Solution 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 $\mathbf{F}_3$.

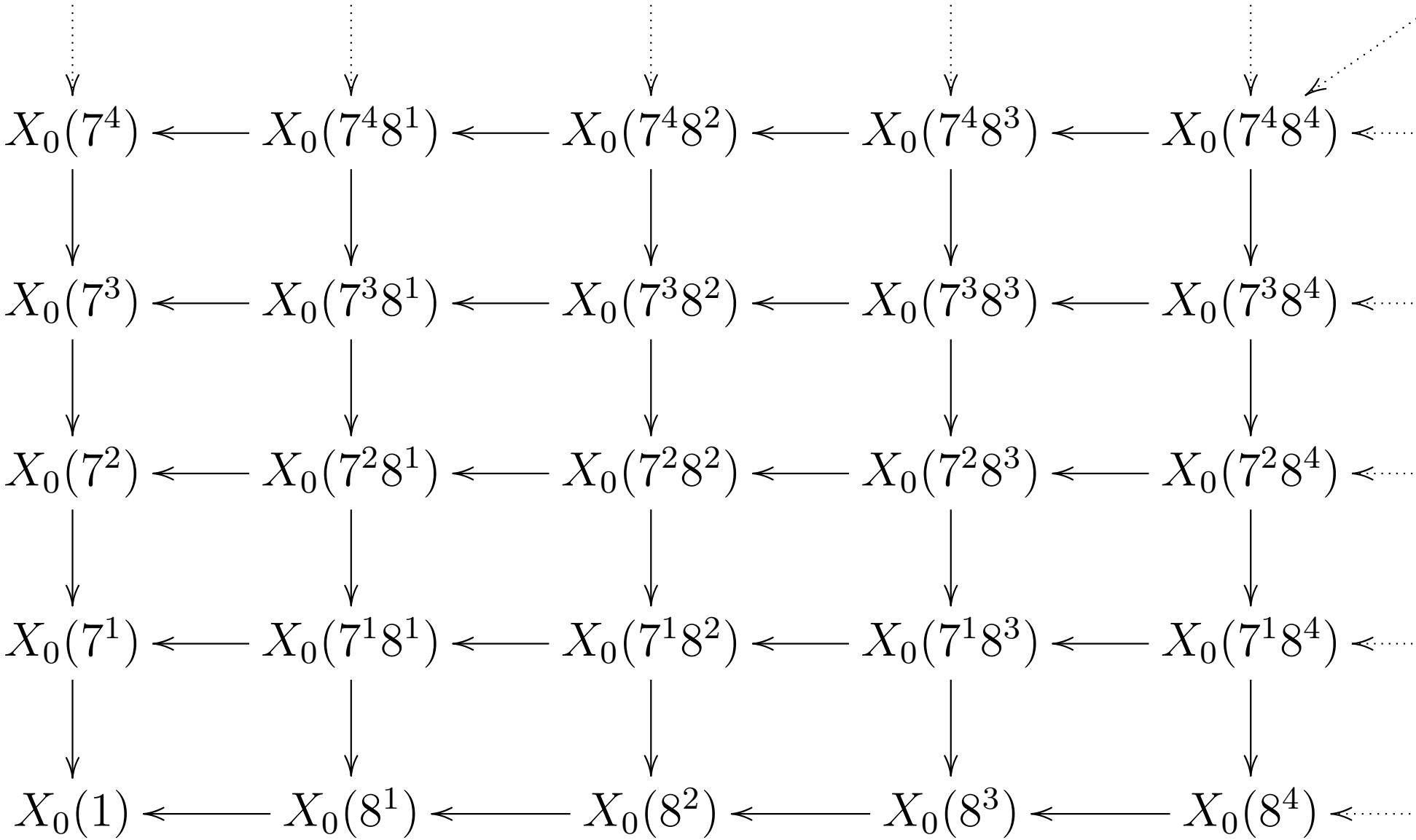
a Solution for p=3 and 2t=6

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



The genus one Belyi map

$$X_0(7^2) \xrightarrow{f_2} X_0(7)$$

Goal: j-invariant of $X_0(7^2)_{\mathbf{C}}$? Input: $\Gamma_0(7^2) \subset \mathrm{PSL}_2(\mathbf{R})$

Algorithm [Klug–Musty–Schiavone–Voight]

- Fundamental domain for $\Gamma_0(7^2)$.
- The differential form g on $X_0(7^2)_{\mathbf{C}}$:

$$g(w) = 1 - 2/3 \cdot w + 2^3/3^3 \cdot w^3 + 2^7/(3^7 \cdot 7)w^7 + 2^7/(3^7 \cdot 7)w^8 + 2^9/(3^{10} \cdot 7^1)w^{10} - 2^{13} \cdot 5/(3^{13} \cdot 7^2 \cdot 13)w^{14} - 2^{15} \cdot 5/(3^{15} \cdot 7^2 \cdot 13) \cdot w^{15} + 2^{15}/(3^{16} \cdot 7^2 \cdot 13)w^{17} - 2^{19} \cdot 31/(3^{16} \cdot 7^2 \cdot 13)w^{21} + \dots$$

- Periods of $g \to$ Periods lattice of $X_0(7^2)_{\mathbf{C}} \to j = -3375$.

The genus one Belyi map

$X_0(7^2) \xrightarrow{f_2} X_0(7)$

Goal: canonical model of $X_0(7^2)$? Inputs:

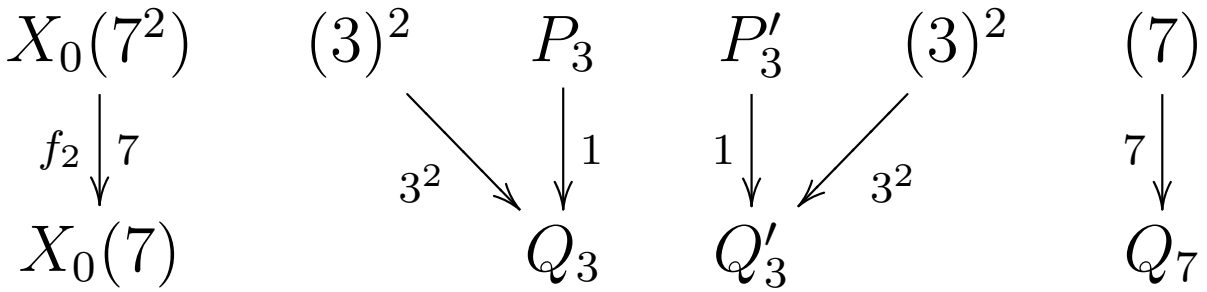
- j-invariant: -3375;
- *Descends to an elliptic curve over* $\mathbf{Q}$ (specific Theorem);
- Conductor equals $7^{1 \text{ or } 2}$ (the Theory);
- Traces of Frobenius equals traces of quaternionic Hecke operators (the Theory).

Output: $X_0(7^2)_{\mathbf{Q}}$ is either 49.a2 or 49.a4 (LMFBD)

The genus one Belyi map

$X_0(7^2) \xrightarrow{f_2} X_0(7)$

Goal: equation for f_2 ? Input: $\{49.a2 \text{ or } 49.a4\}$, ramification:



And monodromy: $[(1,6,4,2,7,5,3),(1,6,2)(4,5,7),(1,3,4)(2,7,6)]$
Method: [Sijsling & Voight][2] for computation and descent.
Output : $X_0(7^2)_{\mathbf{Q}} = 49.a4$ and

$$f_2(x,y) = 2x + 5x^2 - 3x^3 + (-3 + 3x + x^2)y$$

Thanks to J. Voight, J. Sijsling, N. Elkies, H. Randriam, V. Ducet,

D. Madore, S. Ballet . . .

Not meant to be shown

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

$$\omega_1 \circ f_2 \circ \omega_2 : X_0(8^2) \to X_0(8^1) \quad f_2 : X_0(8^2) \to X_0(8^1)$$

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

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

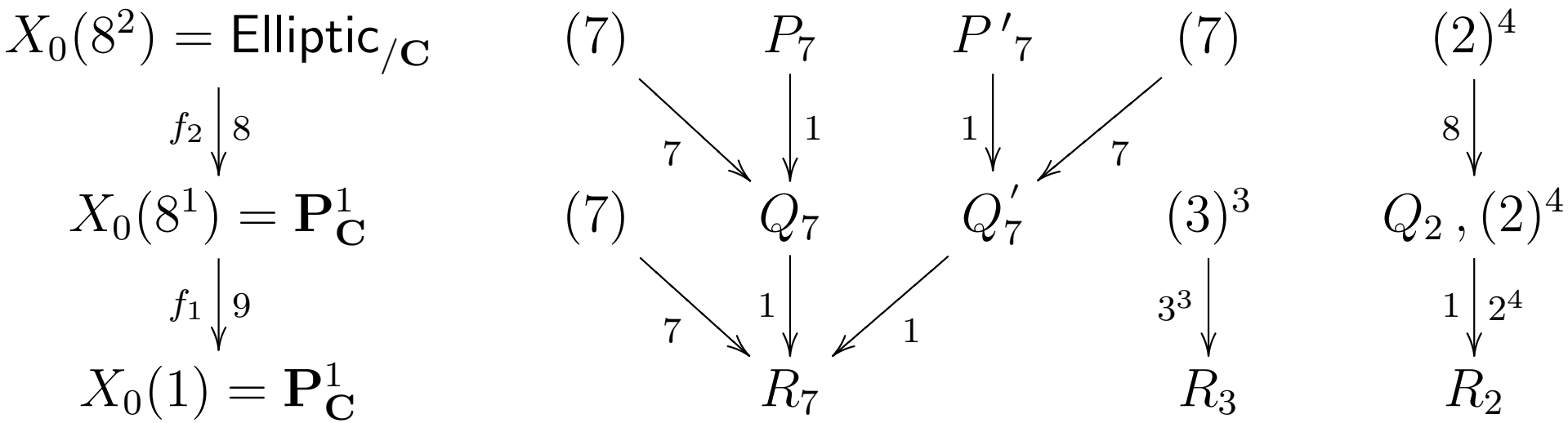
$$f_2 : (x, y) \longmapsto \frac{1+x^2+x^3+x^4+(x+2x^2)y}{2+x^2+x^3+x^4+x^2y}$$

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

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

of genus 7 and having 1760 points over $\mathbf{F}_{36}$, as predicted from traces of Hecke operators.

Not meant to be shown



Bilinear multiplication

Symmetric bilinear complexity in $\mathbf{F}_{p^m}/\mathbf{F}_p$

$$\mathbf{F}_{q^m} \times \mathbf{F}_{q^m} \longrightarrow \mathbf{F}_{q^m} \tag{1}$$

$$m : (x_1, x_2) \longrightarrow \sum_{i=1}^{\mu_p(m)} \phi_i(x_1) \bullet \phi_i(x_2) \cdot w_i \ (\phi_i \in \mathbf{F}_{p^m}^*, w_i \in \mathbf{F}_{p^m}) \tag{2}$$

Bilinear multiplication

Symmetric bilinear complexity in $\mathbf{F}_{p^m}/\mathbf{F}_p$

$$\mathbf{F}_{q^m} \times \mathbf{F}_{q^m} \longrightarrow \mathbf{F}_{q^m} \tag{1}$$

$$m : (x_1, x_2) \longrightarrow \sum_{i=1}^{\mu_p(m)} \phi_i(x_1) \bullet \phi_i(x_2) \cdot w_i \ (\phi_i \in \mathbf{F}_{p^m}^*, w_i \in \mathbf{F}_{p^m}) \tag{2}$$

Table: $\limsup_{m\to\infty} \frac{1}{m}\mu_3(m)$

before	after
$7, 7$	$\mathbf{5}, \mathbf{4}$