Computing modular polynomials of rank 2 Drinfeld modules

Renate Scheidler

UNIVERSITY OF CALGARY

Joint work with **Perlas Caranay** and **Matthew Greenberg**

(*75 Years Mathematics of Computation*, Contemp. Math., vol. 754, AMS 2020)

Géométrie algébrique, Théorie des nombres et Applications
Université de la Polynésie Française
August 16, 2021

Alexey Zykin (1984-2017)

Dinner with GAATI Number Theorists, January 27, 2015

Drinfeld Modules — Motivation

- Introduced in 1974 by Vladimir Drinfeld as **elliptic modules** in the course of proving the Langlands conjectures for GL_2 over global function fields
- Provide a function field analogue of the theory of complex multiplication
- Parallels:

$$\begin{array}{lcl} \text{Rank 1 Drinfeld modules} & \longleftrightarrow & \text{cyclotomic fields} \\ \text{Rank 2 Drinfeld modules} & \longleftrightarrow & \text{elliptic curves} \end{array}$$

Rank 2 DMs vs ECs — Similarities

There are many similarities between rank 2 Drinfeld modules and elliptic curves over finite fields:

- Classification of ordinary and supersingular
- j-invariants (with outlier $j = 0$)
- Similar automorphisms, mostly trivial automorphism group
- Torsion "points"
- Isogenies with duals
- n-th Drinfeld modular polynomial parameterizes pairs of n-isogenous Drinfeld Modules
- ℓ-isogeny graph has analogous structure (ℓ prime)
- Endomorphism ring has analogous form

Rank 2 DMs vs ECs — Differences

There are also some very notable differences:

- No geometry like for points on elliptic curves
- No Vélu formulas
- Infintite valuations are non-archimedian
- Drinfeld modular forms and their Puiseux expansions (Fourier expansion equivalent) depend heavily on the base field $\mathbb{F}_q$
- j-Function looks and behaves very differently
- Modular polynomials look and behave differently
- Totally unsuitable for crytography (classical and post-quantum)

Computational Work To Date

- Sporadic examples
- Some work on parameterized families
- Algorithms:
  - Trace of Frobenius (Musleh 2018, Musleh-Schost 2019)
  - *j*-function expansions, modular polynomials, isogeny volcanos, endomorpism rings, isogenies, dual isogenies (CGS 2020, this work)
  - Improved algorithms (joint with Edgar Pacheco Castan, ongoing)

Notation

Notation:

- q a prime power
- $\mathbb{F}_q$ a finite field of order q
- $\mathbb{L} \supsetneq \mathbb{F}_q$ a proper extension of $\mathbb{F}_q$
- τ the q-power Frobenius on $\mathbb{L}$, defined via $\tau(\alpha) = \alpha^q$ for $\alpha \in \mathbb{L}$

Two scenarios for $\mathbb{L}$ later on:

- $\mathbb{L} = \mathbb{F}_P := \mathbb{F}_q[T]/(P) \cong \mathbb{F}_{q^d}$
  $P(T) \in \mathbb{F}_q[T]$ monic, irreducible, of degree d
- $\mathbb{L} = \mathbb{C}_\infty := (\overline{\mathbb{F}_q(T)_\infty})_\infty$ (function field analogue of $\mathbb{C}$)

Twisted Polynomials

Definition

$\mathbb{L}\{\tau\} \subset \mathrm{End}(\mathbb{L})$ is the ring of **twisted polynomials** in τ with

- standard polynomial addition
- twisted multiplication $\tau\alpha = \alpha^q\tau$ for $\alpha \in \mathbb{L}$ (non-commutative)

Motivation:

For $\alpha \in \mathbb{L}$, multiplication by α is an endomorphism on $\mathbb{L}$ and we have

$$(\tau\alpha)(x) = \tau(\alpha x) = \alpha^q x^q = (\alpha^q\tau)(x)$$

Structure Maps

There are natural maps $\mathbb{F}_q[T] \to \mathbb{L}$:

- $\mathbb{L} = \mathbb{F}_P$: reduction mod P
- $\mathbb{L} = \mathbb{C}_\infty$: inclusion

Sample computation in $\mathbb{F}_q[T] \to \mathbb{L} \hookrightarrow \mathbb{L}\{\tau\}$:

$$\begin{aligned}
(T + \tau^2)(2T^2 + \tau) &= 2T^3 + T\tau + 2\tau^2 T^2 + \tau^3 \\
&= 2T^3 + T\tau + 2\tau(\tau T^2) + \tau^3 \\
&= 2T^3 + T\tau + 2\tau(T^{2q}\tau) + \tau^3 \\
&= 2T^3 + T\tau + 2(\tau T^{2q})\tau + \tau^3 \\
&= 2T^3 + T\tau + 2T^{2q^2}\tau^2 + \tau^3
\end{aligned}$$

Drinfeld Modules

Definition

A **Drinfeld module** over $\mathbb{L}$ is an $\mathbb{F}_q$-algebra homomorphism

$$\varphi : \mathbb{F}_q[T] \to \mathbb{L}\{\tau\}, \quad a \mapsto \varphi_a$$

with the following properties:

1. The constant term of φ_a is a (image of a under map $\mathbb{F}_q[T] \to \mathbb{L}$)
2. $\varphi(\mathbb{F}_q[T]) \not\subset \mathbb{L}$

Why a module?

$\mathbb{L}$ is an $\mathbb{F}_q[T]$-module in two different ways ($a \in \mathbb{F}_q[T], \alpha \in \mathbb{L}$):

$$a * \alpha = a\alpha$$
$$a * \alpha = \varphi_a(\alpha) = a\alpha + \text{higher terms in } \tau(\alpha)$$

By property 2, these are two different actions.

Properties of Drinfeld Modules

- Injective when $\mathbb{L} = \mathbb{C}_\infty$ by property 1

- Uniquely determined by the image of T:

$$\varphi_T = T + c_1\tau + c_2\tau^2 + \ldots + c_r\tau^r \quad (c_i \in \mathbb{L})$$

with $c_r \neq 0$. The degree $r = \deg_\tau(\varphi_T)$ is the **rank** of φ.

- For $m \in \mathbb{F}_q[T]$, the m-**torsion** of φ is

$$\varphi[m] = \ker(\varphi_m) = \{\alpha \in \overline{\mathbb{L}} \mid \varphi_m(\alpha) = 0\}$$

If $P \nmid m$ (when $\mathbb{L} = \mathbb{F}_P$), then

$$\varphi[m] \quad \cong \quad \underbrace{\mathbb{F}_q[T]/(m) \times \mathbb{F}_q[T]/(m) \times \cdots \times \mathbb{F}_q[T]/(m)}_{r \text{ times}}$$

Rank 1 and 2 Drinfeld Modules

Rank 1: $\rho_T = T + \tau$ **Carlitz module** (1935)

$\mathrm{Gal}(\mathbb{L}(\rho[m])/\mathbb{L}) \cong (\mathbb{F}_q[T]/(m))^*$ — function field analogue of $\mathbb{Q}(\zeta_m)$.

Rank 2: $\varphi = (g, \Delta)$ via $\varphi_T = T + g\tau + \Delta\tau^2$ $(g \in \mathbb{L},\ \Delta \in \mathbb{L}^*)$

j-**invariant** of φ: $j = \dfrac{g^{q+1}}{\Delta} \in \mathbb{L}$

$$\varphi : \mathbb{F}_q[T] \longrightarrow \mathbb{F}_P\{\tau\} \text{ is } \begin{cases} \textbf{ordinary} & \text{if } \varphi[P] \cong \mathbb{F}_q[T]/(P) \\ \textbf{supersingular} & \text{if } \varphi[P] = \{0\} \end{cases}$$

Function field analogue of an elliptic curve.

Maps of Drinfeld Modules

Let φ, ψ be Drinfeld modules (of any rank) over $\mathbb{L}$.

Definition

A **morphism** $u : \varphi \longrightarrow \psi$ over $\mathbb{L}$ is a polynomial $u(\tau) \in \mathbb{L}\{\tau\}$ such that

$$u\varphi_a = \psi_a u \qquad \text{for all } a \in \mathbb{F}_q[T] \,.$$

Endomorpism: $\varphi = \psi$

Isomorphism: u is invertible (i.e. $u \in \mathbb{L}^*$)

Isogeny: non-zero morphism (preserves rank)

Dual isogeny: $\hat{u} \in \mathbb{L}\{\tau\}$ with $\hat{u}u = \varphi_n$ and $u\hat{u} = \psi_n$ for some $n \in \mathbb{F}_q[T]$

Degree of the isogeny: n (then u is called an n-**isogeny**)

Isogeny & Degree Linear and Monic

Let $q = 3$, $P(T) = T^5 + 2T + 1$.

- $u = \tau + 2T^3 + T + 1 : (T^2, T^3) \longrightarrow (2T^4 + T^2, 2T^4 + T + 2)$ is a T-isogeny with dual $\hat{u} = T^3\tau + T^4 + T^2 + T$
- $u = \tau + 2T^2 + 1 : (T^2, T^2 + 2T) \longrightarrow (2T^4 + 2T + 2, 2T^3 + T^2 + 2T)$ is a $(T+1)$-isogeny with dual $\hat{u} = (T^2 + 2T)\tau + T^4 + T^3 + T^2 + T$
- $u = \tau + 2T^3 + 2T : (T^3, T^4 + 1) \longrightarrow (2T^4 + 1, T^4 + T^3 + T^2 + 1)$ is a $(T+2)$-isogeny with dual $\hat{u} = (T^4 + 1)\tau + T^3 + 2T^2 + 2T + 1$

Proposition (Linear monic isogenies of linear monic degree)

Let $n \in \mathbb{F}_q[T]$ be linear and monic, and let $g \in \mathbb{L}$ and $\Delta, \alpha \in \mathbb{L}^*$. Then $u = \tau - \alpha \in \mathbb{L}\{\tau\}$ is an n-isogeny on the rank 2 Drinfeld module $\varphi = (g, \Delta)$ over $\mathbb{L}$ if and only if $\Delta\alpha^{q+1} + g\alpha + n = 0$. In this case, u maps φ to the Drinfeld module $\psi = (g^q - \alpha\Delta + \alpha^{q^2}\Delta^q, \Delta^q)$. Moreover, the dual isogeny of u is $\hat{u} = \Delta\tau + g + \Delta\alpha^q$.

Analytic Theory Drinfeld Modules

- Drinfeld modules of rank r over $\mathbb{C}_\infty$ are in one-to-one correspondence with rank r lattices over $\mathbb{F}_q[T]$ in $\mathbb{C}_\infty$.

- This correspondence extends to a group isomorphism and an $\mathbb{F}_q$-vector space isomorphism mapping morphisms between rank r Drinfeld modules over $\mathbb{C}_\infty$ onto morphisms between $\mathbb{F}_q[T]$-lattices of rank r in $\mathbb{C}_\infty$.

- The coefficients of a Drinfeld module over $\mathbb{C}_\infty$ are Drinfeld modular forms that can be written in terms of Eisenstein series. As such, they have Puiseux expansions with respect to a suitable uniformizer.

- There is reduction and lifting à la Deuring between pairs consisting of a Drinfeld module φ and an endomorphism on φ over $\mathbb{C}_\infty$ and pairs consisting of a Drinfeld module $\overline{\varphi}$ and an endomorphism on $\overline{\varphi}$ over $\mathbb{F}_P$.

Gekeler 1983, 1986, 1988, 1999; Goss 1978, 1980, 1998

Coefficients in Rank 2

Let $\varphi = (g, \Delta)$ be a rank 2 Drinfeld module over $\mathbb{C}_\infty$ with associated $\mathbb{F}_q[T]$-lattice Λ. Then

$$g = g(\Lambda) = [1]\, E_{q-1}(\Lambda)$$

$$\Delta = \Delta(\Lambda) = [1]^q\, E_{q-1}^{q+1}(\Lambda) + [2]\, E_{q^2-1}(\Lambda)$$

$$[i] = T^{q^i} - T \in \mathbb{F}_q[T]$$

$$E_k(\Lambda) = \sum_{0 \neq \lambda \in \Lambda} \frac{1}{\lambda^k} \quad \text{Eisenstein series of weight } k \text{ for } \Lambda$$

Coefficients in Rank 2 Explicitly

The first few coefficients of g and Δ are given as follows:

$$\overline{\pi}^{1-q} g(\Lambda) = 1 - [1]s - [1]s^{q^2-q+1} + [1]s^{q^2} - [1]([1]+\epsilon)s^{q^2+1} + \ldots$$

$$\overline{\pi}^{1-q^2} \Delta(\Lambda) = -s + s^2 - [1]s^{q+1} - s^{q^2-q+1} + s^{q^2} - ([1]-[1]^q+\epsilon)s^{q^2+1} + \ldots$$

$$\overline{\pi}^{q-1} = [1]\, E_{q-1}(\mathbb{F}_q[T]) \quad \text{(normalization factor, analogue of } 2\pi i \in \mathbb{C})$$

$\epsilon = 1$ if $q = 2$ and $\epsilon = 0$ otherwise

$$s = t^{q-1} \text{ with } t^{-1} = e_{\overline{\pi}\mathbb{F}_q[T]}(\overline{\pi} z) \quad \text{(analogue of } e^{2\pi i z})$$

$$e_\Lambda(z) = z \prod_{0 \neq \lambda \in \Lambda} \left(1 - \frac{z}{\lambda}\right) \text{ exponential function associated to } \Lambda$$

j-Function in Rank 2

$$j = j(\Lambda) = \frac{g^{q+1}}{\Delta} = s^{-1} + a_0 s^0 + a_1 s + a_2 s^2 + a_3 s^3 + \dots \qquad (a_i \in \mathbb{F}_q[T])$$

Examples:

q	j-**function**
2	$s^{-1} + (T^2 + T + 1)s^0 + (T^4 + T^2)s + (T^6 + T^5 + T^4 + T^3 + T^2 + T)s^2$ $+(T^8 + T^6 + T^5 + T^3 + 1)s^4 + (T^4 + T^2)s^5 + (T^6 + T^5 + T^3 + T^2)s^6$ $+(T^4 + T^2)s^7 + (T^4 + T^2)s^8 + (T^8 + T^2)s^9 + \dots$
3	$2s^{-1} + (T^3 + 2T)s^0 + 2s + (T^9 + T^3 + T)s^2 + (2T^{12} + T^{10} + T^4 + 2T^2 + 2)s^3$ $+(T^9 + 2T^3)s^4 + (T^{12} + 2T^{10} + 2T^6 + T^4)s^5 + (T^{15} + T^{13} + T^{11} + T^9$ $+2T^7 + 2T^5 + 2T^3 + 2T)s^6 + (2T^{18} + T^{12} + T^{10} + 2T^4)s^9 + \dots$
5	$4s^{-1} + (T^5 + 4T)s^0 + 4s^3 + (T^{25} + T^5 + 3T)s^4 + (4T^{30} + T^{26} + T^6 + 4T^2)s^5$ $+4s^7 + (T^{25} + 2T^5 + 2T)s^8 + (3T^{30} + 2T^{26} + 4T^{10} + 4T^6 + 2T^2)s^9 + \cdots$
7	$6s^{-1} + (T^7 + 6T)s^0 + 6s^5 + (T^{49} + T^7 + 5T)s^6 + (6T^{56} + T^{50} + T^8 + 6T^2)s^7$ $+6s^{11} + (T^{49} + 2T^7 + 4T)s^{12} + (5T^{56} + 2T^{50} + 6T^{14} + 4T^8 + 4T^2)s^{13} + \cdots$

Can compute $j(z)$ to arbitrary precision N in time $\widetilde{O}(N^2(\sqrt{N} + q))$ and space $\widetilde{O}(qN^2)$ (implemented in SAGE).

Rank 2 Drinfeld Modular Polynomials

UNIVERSITY OF CALGARY

Definition

For $n \in \mathbb{F}_q[T]$, the *n-th Drinfeld modular polynomial* $\Phi_n(X, j(z))$ is the minimal polynomial of $j(nz)$ over $\mathbb{C}_\infty(j(z))$.

Properties (Bae 1992):

- The coefficients of $\Phi_n(X, j(z))$ are power series in s over $\mathbb{F}_q[T]$.
- $\Phi_n(j', j) = 0 \iff j, j'$ are n-isogenous.
- As a polynomial in two variables, $\Phi_n(X, Y)$ has coefficients in $\mathbb{F}_q[T]$ and is symmetric in X and Y. Leading terms are $X^{N(n)}$ and $Y^{N(n)}$ with
$$N(n) = |n| \prod_{p|n} \left(1 + \frac{1}{|p|}\right)$$
where $|a| = q^{\deg_T(a)}$ for $a \in \mathbb{F}_q[T]$.
For $n = \ell$ irreducible, we have $N(\ell) = |\ell| + 1 = q^{\deg_T(\ell)} + 1$.

A Small Parameterization Example

Let $q = 3$, $P(T) = T^5 + 2T + 1$, and recall the T-isogeny

$$u = \tau + 2T^3 + T + 1 : \varphi = (T^2, T^3) \to \psi = (T^4 + T^2, 2T^4 + T + 2)$$

$$j(\varphi) = T + 2\ , \qquad j(\psi) = 2T^4 + T^3 + 2T^2 + T + 2$$

$$\begin{aligned}\Phi_T(X, j(\varphi)) \equiv X^4 + (2T^3+1)X^3 + (T^3+2T^2+1)X^2 \\ + (T^3+2T^2+T+1)X + 2T^3+T^2+2T+1 \\ \pmod{P}\end{aligned}$$

The four roots of $\Phi_T(X, j(\varphi))$ in $\mathbb{L}$ are

$$\begin{array}{ll} T^4 + T^2 + T + 2 & T^4 + T^3 + 2T^2 \\ 2T^4 + 2T^3 + T^2 + T + 1 & 2T^4 + T^3 + 2T^2 + T + 2 = j(\psi) \end{array}$$

Hence, $\Phi_T(j(\psi), j(\varphi)) = 0$, which confirms that ψ is T-isogenous to φ.

Example: T-th Modular Polynomial

Schweizer 1995, Bassa-Beelen 2012:

$$\Phi_T(X,Y) = \left(X + Y + T(T^{q-1}-1)^{q+1}\right)^{q+1} - X^q Y^{-} XY^q$$
$$+ (XY)^q(T^{1-q}-1) + XY(T^{q-1}-1)^{q^2} - T^{1-q}XY\,S(X,Y)$$

$$S(X,Y) = \sum_{n=0}^{\lfloor (q-1)/2 \rfloor} C_n\,(XYT^{q^2+1})^n \left(XY - T^q(X + Y + T(T^{q-1}-1)^{q+1}\right)^{q-1-2n}$$

$$C_n = \frac{1}{n+1}\binom{2n}{n} \quad n\text{-th Catalan number}$$

Polynomial in $\mathbb{F}_q[T][X,Y]$ of degree $q+1$.

Computing $\Phi_\ell(X, Y)$

Consider the case $n = \ell \in \mathbb{F}_q[T]$ with $\ell \neq P$ monic and irreducible.

The analytic method for computing $\Phi_\ell(X, Y)$ computes $j(z)$ and $j(\ell z)$ to sufficient precision and recovers the coefficients of $\Phi_\ell(X, Y)$ from

$$\Phi_\ell(j(\ell z), j(z)) = 0 \qquad (*)$$

1. Compute $j(z)$ to precision $|\ell|^2 + |\ell| - 1$ and $j(\ell z)$ to precision $|\ell|^2$.
2. Compute the powers $j(z)^i$ and $j(\ell z)^i$, $2 \leq i \leq |\ell| + 1$ using this precision.
3. Substitute the approximations into $(*)$ and find the coefficients of $\Phi_\ell(X, Y)$ via linear algebra (Bae-Li 1997).

Example: $\Phi_{T^2+1}(X, Y)$ over $\mathbb{F}_3$

Term	Coefficient
X^{10}, Y^{10}	1
X^9Y^9	2
X^9Y^8, X^8Y^9	0
X^9Y^7, X^7Y^9	0
X^9Y^6, X^6Y^9	$2T^3+2T$
X^9Y^5, X^5Y^9	T^2+1
X^9Y^4, X^4Y^9	T^5+2T
X^9Y^3, X^3Y^9	$2T^{12}+2T^{10}+T^8+2T^6+T^4+T^2+1$
X^9Y^2, X^2Y^9	T^5+T^3
X^9Y, XY^9	$T^{14}+2T^{10}+T^8+2T^6+T^4+2T^2+2$
X^9, Y^9	$T^{27}+2T^{21}+2T^{19}+2T^{17}+T^{15}+2T^{13}+2T^9+2T^7+T^5$
X^8Y^8	$T^{14}+T^{12}+T^2+1$
X^8Y^7, X^7Y^8	$T^{23}+2T^{19}+2T^{17}+T^{15}+2T^{13}+T^{11}+2T^7+2T^5+2T^3$
X^8Y^6, X^6Y^8	$2T^{30}+2T^{28}+2T^4+1$
X^8Y^5, X^5Y^8	$T^{29}+T^{27}+T^{23}+T^{21}+T^{17}+2T^{15}+T^{13}+T^3+T$
X^8Y^4, X^4Y^8	$2T^{32}+T^{28}+T^{26}+T^{24}+2T^{22}+T^{20}+2T^{16}+2T^{14}$ $+T^{10}+2T^8+T^6+T^2+2$
X^8Y^3, X^3Y^8	$T^{39}+T^{37}+2T^{35}+T^{29}+2T^{27}+2T^{25}+2T^{23}+T^{21}$ $+T^{19}+T^{13}+T^{11}+2T^9+2T^7+T^5+2T^3+T$
X^8Y^2, X^2Y^8	$2T^{32}+T^{30}+T^{28}+2T^{26}+2T^{22}+T^{20}+T^{16}+2T^{12}$ $+T^{10}+2T^8+T^6+2T^2$
X^8Y, XY^8	$T^{35}+T^{33}+2T^{27}+T^{25}+T^{21}+2T^{19}+2T^{17}+2T^{15}$ $+2T^{13}+T^{11}+T^7+2T^5$
X^8, Y^8	$2T^{26}+T^{24}+T^{22}+T^{20}+T^{18}+T^{16}+T^{14}+T^{12}$ $+T^{10}+2T^8$
X^7Y^7	$T^{32}+T^{24}+2T^{22}+T^{20}+T^{16}+T^{14}+2T^{12}+T^4$ * $+2T^2+1$
X^7Y^6, X^6Y^7	$T^{41}+2T^{39}+2T^{35}+2T^{31}+T^{29}+2T^{25}+T^{23}+2T^{21}$ $+T^{19}+2T^{17}+T^{15}+T^{13}+T^{11}+2T^9+T^7+2T^3+2T$
X^7Y^5, X^5Y^7	$2T^{50}+2T^{46}+T^{38}+2T^{36}+2T^{34}+T^{32}+T^{24}+T^{22}$ $+T^{20}+2T^{18}+T^{14}+2T^{12}+2T^{10}+2T^8+2T^6$
X^7Y^4, X^4Y^7	$T^{59}+2T^{55}+T^{53}+T^{51}+2T^{49}+T^{47}+2T^{43}+2T^{37}$ $+T^{35}+T^{33}+T^{29}+T^{27}+T^{25}+T^{23}+T^{15}+T^{13}$ $+T^{11}$

Term	Coefficient
X^7Y^3, X^3Y^7	$2T^{66}+2T^{64}+T^{62}+T^{60}+2T^{58}+T^{54}+2T^{52}+T^{50}$ $+2T^{48}+T^{46}+T^{42}+2T^{40}+T^{34}+T^{32}+2T^{28}+T^{26}$ $+T^{22}+2T^{20}+T^{16}+2T^{12}+2T^{10}+2T^8+2T^6+2T^4$ $+2T^2$
X^7Y^2, X^2Y^7	$T^{59}+2T^{57}+2T^{55}+2T^{53}+2T^{49}+T^{47}+T^{43}+T^{39}$ $+2T^{37}+T^{35}+T^{29}+2T^{27}+T^{25}+2T^{21}+2T^{15}+T^7$
X^7Y, XY^7	$2T^{62}+2T^{60}+T^{56}+T^{52}+T^{50}+2T^{48}+2T^{46}+T^{44}$ $+2T^{40}+T^{38}+2T^{36}+2T^{34}+T^{32}+2T^{30}+2T^{24}+2T^{22}$ $+2T^{20}+2T^{18}+T^{16}+2T^{14}+2T^{10}+T^8$
X^7, Y^7	$T^{81}+2T^{63}+2T^{57}+2T^{51}+T^{45}+2T^{39}+2T^{27}+2T^{21}$ $+T^{15}$
X^6Y^6	$T^{46}+T^{40}+T^{38}+T^{34}+T^{32}+2T^{28}+2T^{26}+2T^{18}$ $+T^{16}+T^{14}+2T^{10}+2T^8+2T^6+T^2$
X^6Y^5, X^5Y^6	$T^{57}+2T^{55}+T^{53}+2T^{51}+2T^{49}+T^{47}+2T^{45}+2T^{43}$ $+2T^{41}+2T^{37}+2T^{35}+2T^{33}+2T^{31}+T^{29}+T^{27}+2T^{25}$ $+T^{23}+T^{21}+2T^{19}+T^{17}+T^{15}+T^{11}+T^9+2T^7+2T^5$ $+2T$
X^6Y^4, X^4Y^6	$2T^{68}+2T^{66}+2T^{60}+2T^{56}+2T^{54}+T^{52}+2T^{48}+T^{46}$ $+2T^{44}+2T^{42}+2T^{40}+T^{36}+2T^{30}+2T^{22}+T^{20}+2T^{18}$ $+T^{10}+T^8+2T^6+2T^4+2T^2$
X^6Y^3, X^3Y^6	$T^{81}+T^{69}+2T^{65}+2T^{61}+T^{53}+2T^{51}+T^{47}+2T^{45}$ $+T^{43}+2T^{39}+2T^{37}+2T^{35}+T^{33}+2T^{27}+T^{25}+T^{23}$ $+2T^{21}+2T^{19}+2T^{17}+T^{15}+T^{13}+T^{11}+T^9+2T^5$
X^6Y^2, X^2Y^6	$2T^{84}+T^{82}+2T^{68}+T^{66}+2T^{64}+2T^{60}+T^{56}+2T^{52}$ $+T^{50}+2T^{48}+2T^{46}+2T^{44}+2T^{40}+2T^{38}+T^{36}+T^{34}$ $+2T^{32}+2T^{28}+T^{26}+T^{24}+T^{22}+2T^{18}+T^{14}+T^{12}$ $+2T^{10}$
X^6Y, XY^6	$T^{95}+2T^{91}+2T^{89}+T^{85}+2T^{77}+T^{75}+2T^{73}+2T^{71}$ $+T^{69}+T^{67}+T^{65}+T^{57}+2T^{55}+2T^{53}+2T^{51}+2T^{49}$ $+T^{47}+T^{43}+2T^{39}+2T^{37}+2T^{35}+T^{33}+T^{31}+T^{29}$ $+2T^{25}+2T^{21}+T^{19}+T^{17}+2T^{15}+T^{13}$
X^6, Y^6	$T^{108}+2T^{102}+2T^{100}+2T^{98}+T^{96}+2T^{94}+T^{90}+2T^{88}$ $+T^{86}+T^{82}+T^{80}+2T^{78}+2T^{76}+T^{74}+2T^{72}+T^{66}$ $+T^{64}+T^{62}+T^{58}+T^{50}+T^{48}+2T^{46}+T^{42}+2T^{40}$ $+T^{38}+2T^{36}+T^{34}+T^{32}+2T^{30}+2T^{26}+2T^{24}+2T^{22}$ $+T^{20}$

Term	Coefficient
X^5Y^5	$2T^{64}+2T^{62}+T^{58}+T^{52}+T^{46}+T^{44}+T^{38}+T^{36}$ $+T^{34}+T^{32}+2T^{30}+2T^{28}+T^{26}+T^{20}+T^{18}+2T^{14}$ $+T^{10}+T^8+2T^4+2T^2$
X^5Y^4, X^4Y^5	$T^{77}+2T^{73}+2T^{71}+T^{69}+2T^{63}+T^{61}+2T^{57}+2T^{55}$ $+2T^{53}+2T^{51}+2T^{49}+T^{47}+T^{45}+2T^{43}+2T^{41}+2T^{39}$ $+T^{37}+2T^{35}+2T^{31}+2T^{23}+2T^{19}+2T^{15}+2T^{13}+2T^{11}$ $+2T^7+T^5$
X^5Y^3, X^3Y^5	$2T^{82}+T^{76}+T^{74}+T^{72}+2T^{70}+2T^{68}+T^{66}+2T^{64}$ $+2T^{62}+2T^{54}+T^{52}+2T^{44}+T^{42}+2T^{40}+2T^{38}+T^{36}$ $+2T^{34}+T^{28}+2T^{26}+2T^{24}+2T^{18}+T^{16}+T^{14}+2T^{12}$ $+T^{10}$
X^5Y^2, X^2Y^5	$2T^{95}+2T^{93}+T^{91}+T^{89}+T^{85}+2T^{83}+T^{79}+2T^{77}$ $+2T^{73}+T^{71}+2T^{69}+2T^{67}+2T^{65}+2T^{63}+2T^{59}+2T^{57}$ $+T^{55}+2T^{53}+2T^{47}+T^{43}+T^{35}+2T^{33}+T^{31}+T^{27}$ $+T^{25}+2T^{21}+2T^{19}+T^{17}+2T^{15}+2T^{13}$
X^5Y, XY^5	$T^{104}+2T^{100}+2T^{98}+T^{92}+T^{90}+2T^{88}+T^{86}+T^{78}$ $+2T^{76}+T^{74}+T^{70}+T^{68}+2T^{66}+2T^{64}+T^{62}+T^{60}$ $+T^{56}+2T^{54}+T^{52}+2T^{48}+2T^{44}+T^{42}+T^{36}+2T^{34}$ $+2T^{30}+2T^{28}+T^{26}+T^{22}+2T^{18}$
X^5, Y^5	$2T^{107}+T^{105}+T^{103}+T^{101}+T^{99}+T^{97}+T^{95}+T^{93}$ $+T^{91}+2T^{87}+2T^{85}+T^{81}+T^{79}+2T^{77}+T^{71}+2T^{69}$ $+2T^{67}+2T^{65}+2T^{63}+2T^{61}+T^{59}+2T^{53}+T^{51}+T^{49}$ $+T^{47}+T^{45}+T^{43}+2T^{39}+2T^{37}+T^{35}+2T^{29}+T^{27}$ $+T^{25}+2T^{23}$
X^4Y^4	$T^{86}+T^{82}+T^{80}+T^{78}+2T^{70}+2T^{66}+T^{64}+2T^{60}$ $+2T^{58}+T^{56}+2T^{52}+T^{48}+2T^{46}+T^{44}+2T^{42}+2T^{40}$ $+T^{36}+T^{34}+2T^{32}+T^{30}+2T^{28}+T^{22}+T^{20}+T^{18}$ $+2T^{14}+T^{12}+2T^{10}$
X^4Y^3, X^3Y^4	$2T^{93}+T^{83}+T^{81}+2T^{79}+2T^{75}+2T^{71}+2T^{69}+T^{65}$ $+T^{61}+2T^{59}+2T^{57}+T^{53}+T^{47}+T^{45}+2T^{43}+2T^{41}$ $+T^{39}+2T^{37}+T^{35}+T^{33}+T^{27}+T^{25}+2T^{23}+2T^{21}$ $+T^{19}+2T^{17}$
X^4Y^2, X^2Y^4	$2T^{104}+2T^{98}+2T^{96}+T^{94}+T^{90}+T^{88}+2T^{86}+2T^{84}$ $+2T^{80}+T^{78}+T^{76}+T^{74}+T^{68}+T^{64}+2T^{62}+2T^{58}$ $+T^{56}+T^{54}+T^{50}+T^{48}+T^{46}+2T^{44}+2T^{42}+T^{40}$ $+T^{36}+2T^{34}+T^{28}+T^{26}+T^{24}+T^{22}+T^{20}$

Term	Coefficient
X^4Y, XY^4	$T^{107}+T^{103}+2T^{101}+T^{99}+T^{97}+2T^{95}+T^{93}+2T^{85}$ $+2T^{81}+T^{79}+T^{77}+2T^{75}+2T^{73}+T^{71}+2T^{69}+T^{67}$ $+2T^{65}+T^{63}+T^{61}+T^{59}+T^{57}+2T^{55}+2T^{51}+2T^{41}$ $+2T^{37}+T^{35}+2T^{33}+2T^{31}+2T^{29}+2T^{27}+2T^{21}$
X^4, Y^4	$2T^{78}+T^{72}+T^{66}+T^{60}+T^{54}+T^{48}+T^{42}+T^{36}$ $+T^{30}+2T^{24}$
X^3Y^3	$T^{108}+2T^{102}+T^{100}+2T^{98}+2T^{92}+T^{90}+T^{88}+T^{84}$ $+T^{82}+2T^{80}+T^{78}+2T^{76}+T^{70}+2T^{68}+T^{66}+2T^{64}$ $+2T^{62}+2T^{60}+T^{58}+T^{56}+T^{54}+T^{52}+2T^{50}+2T^{48}$ $+T^{46}+2T^{42}+T^{40}+2T^{38}+T^{36}+2T^{32}+T^{28}+T^{24}$ $+2T^{22}+T^{20}+2T^{18}$
X^3Y^2, X^2Y^3	$2T^{103}+2T^{101}+2T^{97}+T^{93}+2T^{91}+T^{89}+2T^{83}+2T^{81}$ $+2T^{79}+2T^{77}+T^{71}+T^{69}+T^{65}+2T^{63}+T^{61}+2T^{59}$ $+T^{57}+T^{53}+T^{51}+T^{49}+2T^{47}+2T^{45}+2T^{43}+2T^{41}$ $+T^{37}+T^{33}+2T^{29}+2T^{25}+T^{21}$
X^3Y, XY^3	$2T^{106}+T^{86}+T^{82}+2T^{76}+T^{74}+T^{72}+2T^{70}+T^{68}$ $+T^{66}+2T^{64}+T^{62}+T^{60}+2T^{58}+T^{56}+T^{54}+T^{50}$ $+T^{48}+2T^{46}+T^{44}+T^{42}+2T^{40}+T^{38}+T^{36}+2T^{34}$ $+T^{30}+T^{28}+T^{26}+T^{24}$
X^3, Y^3	$2T^{105}+2T^{99}+T^{97}+T^{95}+2T^{93}+2T^{89}+2T^{87}+2T^{85}$ $+T^{83}+T^{51}+T^{45}+2T^{43}+2T^{41}+T^{39}+T^{35}+T^{33}$ $+T^{31}+2T^{29}$
X^2Y^2	$2T^{106}+2T^{104}+2T^{98}+T^{94}+2T^{92}+2T^{90}+2T^{88}+2T^{86}$ $+2T^{84}+T^{82}+2T^{80}+T^{78}+T^{76}+T^{72}+T^{70}+T^{66}$ $+T^{64}+T^{60}+T^{58}+T^{54}+2T^{52}+T^{50}+T^{48}+T^{46}$ $+T^{44}+T^{42}+T^{38}+2T^{36}+2T^{34}+T^{32}+2T^{30}+T^{26}$
X^2Y, XY^2	$T^{105}+2T^{103}+2T^{99}+2T^{95}+2T^{93}+2T^{91}+T^{89}+2T^{87}$ $+2T^{85}+2T^{83}+2T^{51}+T^{49}+T^{45}+T^{41}+T^{39}+T^{37}$ $+2T^{35}+T^{33}+T^{31}+T^{29}$
X^2, Y^2	$T^{104}+2T^{102}+2T^{100}+T^{98}+2T^{92}+T^{90}+T^{88}+2T^{86}$ $+2T^{50}+T^{48}+T^{46}+2T^{44}+T^{38}+2T^{36}+2T^{34}+T^{32}$
XY	$T^{104}+T^{100}+T^{98}+T^{96}+2T^{94}+2T^{92}+2T^{90}+2T^{86}$ $+2T^{50}+2T^{46}+2T^{44}+2T^{42}+T^{40}+T^{38}+T^{36}+T^{32}$
X, Y	0
1	0

ECs vs DMs — Complexity Comparison

Asymptotic complexity ($\widetilde{O}$)	Elliptic curves	Rank 2 Drinfeld modules
Time	$\ell^{4.5*}$	$q\lvert\ell\rvert^8$
Space	ℓ^3	$q\lvert\ell\rvert^6$

* Elkies 1998, Charles-Lauter 2005

Reasons for the discrepancy: different growth rates for

- the coefficients of the powers of j
- the coefficients of $\Phi_\ell(X,Y)$

Growth rate	Elliptic curves	Rank 2 Drinfeld modules
k-th coefficient of j^i	$\sqrt{ki}\,^*$	$qi\,^{**}$
Log height of $\Phi_\ell(X,Y)$	$6\ell\log(\ell)^{***}$	between** $\frac{\lvert\ell\rvert}{q}$ and $\frac{q\lvert\ell\rvert(\lvert\ell\rvert+1)^2}{2}$

* Charles-Lauter 2005 ** Bae-Li 1997 *** Cohen 1984

Complexity Comparison (cont'd)

Thanks to Drew Sutherland for the following viewpoint:

Let B be a provable upper bound on the coefficients of Φ_ℓ.

- $B = \widetilde{O}(\ell)$ for elliptic curves
- $B = \widetilde{O}(\ell^3)$ for rank 2 Drinfeld modules (assuming q fixed, $\deg(\ell) \to \infty$)

Asymptotic complexity ($\widetilde{O}$)	Elliptic curves	Rank 2 Drinfeld modules
Time	$B^{1.5}$	$B^{1.6}$
Space	B^3	B^2

For ℓ linear, our computations suggest that the coefficients of Φ_ℓ grow as

$$q^2(q+1) = q|\ell|(|\ell|+1) \ .$$

Other Algorithms

Current (SAGE code at `https://github.com/pcaranay/DModules`):

- Modular polynomials via the classical analytic method
- Ordinary ℓ-isogeny graph (from $\Phi_\ell(X, Y)$)
- Ordinary endomorphism ring (after Kohel 1996, Fouquet 2001, Fouquet-Morain 2002)
- ℓ-isogeny (detection and computation)
- Dual isogeny

Future and in progress:

- Modular polynomials via Chinese Remaindering (after Bröker-Lauter-Sutherland 2011) — joint work with E. Pacheco Castan
- Modular polynomials via evaluation/interpolation (after Enge 2009)
- Endomorphism ring (after Bisson-Sutherland 2011)
- Supersingular case

Modular Polynomials via CRT

Bröker-Lauter-Sutherland's algorithm (2011) for finding classical modular polynomials uses the following ingredients:

1. Hilbert class polynomial
   - Roots are all the j-invariants with CM by the same order $\mathcal{O}$
   - Integer coefficients
   - Time $\widetilde{O}(|\mathrm{disc}(\mathcal{O})|)$, space $\widetilde{O}(|\mathrm{disc}(\mathcal{O})|^{1/2})$ (Sutherland 2011)
2. ℓ-isogeny graph
   - Vertices: j-invariants, edges: ℓ-isogenies
   - All valencies are $\ell + 1$ or 1
   - Ordinary components are **volcanos**
3. Chinese Remainder Theorem
   - Compute $\Phi_\ell(X, Y) \pmod{p}$ for suitable primes p and apply CRT

Time and space complexity $\widetilde{O}(\ell^3)$.

Currently adapting this method to rank 2 Drinfeld modules (joint work with Edgar Pacheco-Castan)

Final Motivation

One more reason to study Drinfeld modules: counter-terrorism!

From *Twenty Four*, Season 4, Episode 11:

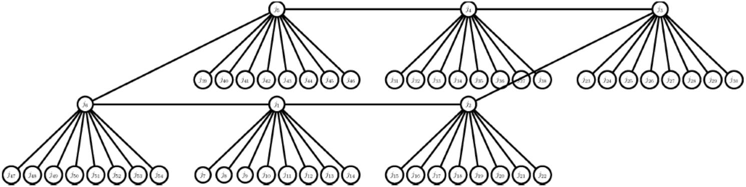
Ali: *"I'm sorry I had to call you here, Marwan, but I had no choice. CTU is trying to disable the override using a* ***Drinfeld module****. They've already shut down over 90 reactors."*

Marwan: *"I always knew they'd stop some of them. The important thing is that one of the reactors has melted down. As long as the override has control of the other five, I can do the rest from here."*

`https://www.youtube.com/watch?v=YKHNYBDazAU`

That's All, Folks!

$\ast\ \ast\ \ast$ Thank You! Questions? $\ast\ \ast\ \ast$



j_5
j_4
j_3
j_{39} j_{40} j_{41} j_{42} j_{43} j_{44} j_{45} j_{46}
j_{31} j_{32} j_{33} j_{34} j_{35} j_{36} j_{37} j_{38}
j_{23} j_{24} j_{25} j_{26} j_{27} j_{28} j_{29} j_{30}
j_6
j_1
j_2
j_{47} j_{48} j_{49} j_{50} j_{51} j_{52} j_{53} j_{54}
j_7 j_8 j_9 j_{10} j_{11} j_{12} j_{13} j_{14}
j_{15} j_{16} j_{17} j_{18} j_{19} j_{20} j_{21} j_{22}

$(T^2 + T + 2)$-isogeny volcano containing

$$j = T^9 + 2T^8 + T^7 + T^6 + 2T^5 + T^4 + 2T^3$$

over $\mathbb{L} = \mathbb{F}_3[T]/(T^{10} + 2T^6 + 2T^5 + 2T^4 + T + 2)$