

Drinfeld Modules, Hasse Invariants and Factoring Polynomials over Finite Fields

Anand Kumar Narayanan
Laboratoire d'informatique de Paris 6
Sorbonne Université

Seminar "Computations and Proofs" at SpecFun

INRIA Saclay

15 Oct 2018

Polynomial Factorization over Finite Fields

Decompose a given monic square-free $f(x) \in \mathbb{F}_q[x]$ of degree n into its monic irreducible factors.

$$f(x) = \prod_i p_i(x)$$

Gauss → Legendre → Berlekamp → Cantor/Zassenhaus → Camion → vonzur Gathen/Shoup → Kaltofen/Shoup → Kedlaya-Umans

Kaltofen-Shoup algorithm with Kedlaya-Umans fast modular composition takes expected time

$$n^{3/2+o(1)} (\log q)^{1+o(1)} + n^{1+o(1)} (\log q)^{2+o(1)}.$$

Drinfeld modules and Polynomial Factorization

- ▶ Panchishkin and Potemine (1989), van der Heiden (2005).

This Talk:

- ▶ Factor Degree Estimation using Euler-Poincaré Characteristic of Drinfeld modules.
- ▶ Rank-2 Drinfeld module analogue of Kaltofen-Lobo's blackbox Berlekamp algorithm.
- ▶ Drinfeld modules with complex multiplication, Hasse invariants/Deligne's congruence.

Polynomial Factorization over Finite Fields

Decompose a given monic square-free $f(x) \in \mathbb{F}_q[x]$ of degree n into its monic irreducible factors.

$$f(x) = \prod_i p_i(x)$$

Gauss \rightarrow Legendre \rightarrow Berlekamp \rightarrow Cantor/Zassenhaus \rightarrow Camion \rightarrow vonzur Gathen/Shoup \rightarrow Kaltofen/Shoup \rightarrow Kedlaya-Umans

Kaltofen-Shoup algorithm with Kedlaya-Umans fast modular composition takes expected time

$$n^{3/2+o(1)} (\log q)^{1+o(1)} + n^{1+o(1)} (\log q)^{2+o(1)}.$$

Drinfeld modules and Polynomial Factorization

- ▶ Panchishkin and Potemine (1989), van der Heiden (2005).

This Talk:

- ▶ Factor Degree Estimation using Euler-Poincare Characteristic of Drinfeld modules.
- ▶ Rank-2 Drinfeld module analogue of Kaltofen-Lobo's blackbox Berlekamp algorithm.
- ▶ Drinfeld modules with complex multiplication, Hasse invariants/Deligne's congruence.

Degree Estimation using Euler Characteristic of Drinfeld Modules

Decompose a given monic $f(x) \in \mathbb{F}_q[x]$ of degree n into its monic irreducible factors.

$$f(x) = \prod_i p_i(x)$$

Finding an irreducible factor degree with runtime exponent $< 3/2$



factorization with exponent $< 3/2$.

An algorithm to find the smallest irreducible factor degree using Euler-Poincare characteristics of random Drinfeld modules.

Rank-2 Drinfeld Modules

Let $\mathbb{F}_q[x]\langle\sigma\rangle$ denote the skew polynomial ring with the commutation rule

$$\sigma u(x) = u(x)^q \sigma, \forall u(x) \in \mathbb{F}_q[x].$$

A rank-2 Drinfeld module over $\mathbb{F}_q(x)$ is (the $\mathbb{F}_q[x]$ module structure on the additive group scheme over $\mathbb{F}_q(x)$ given by) a ring homomorphism

$$\phi : \mathbb{F}_q[x] \longrightarrow \mathbb{F}_q(x)\langle\sigma\rangle$$

$$x \longmapsto x + g_\phi(x)\sigma + d_\phi(x)\sigma^2$$

for some $g_\phi(x) \in \mathbb{F}_q[x]$ and non zero $d_\phi(x) \in \mathbb{F}_q[x]$.

Rank-2 Drinfeld Modules

Let $\mathbb{F}_q[x]\langle\sigma\rangle$ denote the skew polynomial ring with the commutation rule

$$\sigma u(x) = u(x)^q \sigma, \forall u(x) \in \mathbb{F}_q[x].$$

A rank-2 Drinfeld module over $\mathbb{F}_q(x)$ is (the $\mathbb{F}_q[x]$ module structure on the additive group scheme over $\mathbb{F}_q(x)$ given by) a ring homomorphism

$$\phi : \mathbb{F}_q[x] \longrightarrow \mathbb{F}_q(x)\langle\sigma\rangle$$

$$x \longmapsto x + \mathfrak{g}_\phi(x)\sigma + \mathfrak{d}_\phi(x)\sigma^2$$

for some $\mathfrak{g}_\phi(x) \in \mathbb{F}_q[x]$ and non zero $\mathfrak{d}_\phi(x) \in \mathbb{F}_q[x]$.

For $\mathfrak{b}(x) \in \mathbb{F}_q[x]$,

$$\mathfrak{b}(x) \longmapsto \underbrace{\mathfrak{b}(x) + \sum_{i=1}^{2 \deg(\mathfrak{b})} \phi_{\mathfrak{b},i}(x)\sigma^i}_{\text{Call } \phi_{\mathfrak{b}}}$$

Rank-2 Drinfeld Modules

Let $\mathbb{F}_q[x]\langle\sigma\rangle$ denote the skew polynomial ring with the commutation rule

$$\sigma u(x) = u(x)^q \sigma, \forall u(x) \in \mathbb{F}_q[x].$$

A rank-2 Drinfeld module over $\mathbb{F}_q(x)$ is (the $\mathbb{F}_q[x]$ module structure on the additive group scheme over $\mathbb{F}_q(x)$ given by) a ring homomorphism

$$\phi : \mathbb{F}_q[x] \longrightarrow \mathbb{F}_q(x)\langle\sigma\rangle$$

$$x \longmapsto x + \mathfrak{g}_\phi(x)\sigma + \mathfrak{d}_\phi(x)\sigma^2$$

for some $\mathfrak{g}_\phi(x) \in \mathbb{F}_q[x]$ and non zero $\mathfrak{d}_\phi(x) \in \mathbb{F}_q[x]$.

For $\mathfrak{b}(x) \in \mathbb{F}_q[x]$,

$$\mathfrak{b}(x) \longmapsto \underbrace{\mathfrak{b}(x) + \sum_{i=1}^{2 \deg(\mathfrak{b})} \phi_{\mathfrak{b},i}(x)\sigma^i}_{\text{Call } \phi_{\mathfrak{b}}}$$

Let M be an $\mathbb{F}_q[x]$ algebra, say $M = \mathbb{F}_q[x]/(\mathfrak{f}(x))$. Retain the addition in M but define a new $\mathbb{F}_q[x]$ action:

$$\mathfrak{b}(x) \star a(x) := \phi_{\mathfrak{b}}(a) = \mathfrak{b}(x)a(x) + \sum_{i=1}^{2 \deg(\mathfrak{b})} \phi_{\mathfrak{b},i}(x)a(x)^{q^i}$$

Let $\phi(M)$ denote the new $\mathbb{F}_q[x]$ module structure thus endowed to M .

Rank-2 Drinfeld Modules

Let $\mathbb{F}_q[x]\langle\sigma\rangle$ denote the skew polynomial ring with the commutation rule

$$\sigma u(x) = u(x)^q \sigma, \forall u(x) \in \mathbb{F}_q[x].$$

A rank-2 Drinfeld module over $\mathbb{F}_q(x)$ is (the $\mathbb{F}_q[x]$ module structure on the additive group scheme over $\mathbb{F}_q(x)$ given by) a ring homomorphism

$$\phi : \mathbb{F}_q[x] \longrightarrow \mathbb{F}_q(x)\langle\sigma\rangle$$

$$x \longmapsto x + \mathfrak{g}_\phi(x)\sigma + \mathfrak{d}_\phi(x)\sigma^2$$

for some $\mathfrak{g}_\phi(x) \in \mathbb{F}_q[x]$ and non zero $\mathfrak{d}_\phi(x) \in \mathbb{F}_q[x]$.

For $\mathfrak{b}(x) \in \mathbb{F}_q[x]$,

$$\mathfrak{b}(x) \longmapsto \underbrace{\mathfrak{b}(x) + \sum_{i=1}^{2 \deg(\mathfrak{b})} \phi_{\mathfrak{b},i}(x)\sigma^i}_{\text{Call } \phi_{\mathfrak{b}}}$$

Let M be an $\mathbb{F}_q[x]$ algebra, say $M = \mathbb{F}_q[x]/(f(x))$. Retain the addition in M but define a new $\mathbb{F}_q[x]$ action:

$$\mathfrak{b}(x) \star \mathfrak{a}(x) := \phi_{\mathfrak{b}}(\mathfrak{a}) = \mathfrak{b}(x)\mathfrak{a}(x) + \sum_{i=1}^{2 \deg(\mathfrak{b})} \phi_{\mathfrak{b},i}(x)\mathfrak{a}(x)^{q^i}$$

Let $\phi(M)$ denote the new $\mathbb{F}_q[x]$ module structure thus endowed to M .

Euler-Poincare Characteristic of Finite $\mathbb{F}_q[x]$ Modules: An $\mathbb{F}_q[x]$ measure of cardinality.

For a finite $\mathbb{F}_q[x]$ module A , $\chi(A) \in \mathbb{F}_q[x]$ is the monic polynomial s.t.

- ▶ If $A \cong \mathbb{F}_q[x]/(\mathfrak{p}(x))$ for a monic irreducible $\mathfrak{p}(x)$, then $\chi(A) = \mathfrak{p}(x)$.
- ▶ If $0 \rightarrow A_1 \rightarrow A \rightarrow A_2 \rightarrow 0$ is exact, then $\chi(A) = \chi(A_1)\chi(A_2)$.

For a finite \mathbb{Z} module G , $\#G \in \mathbb{Z}$ is the positive integer s.t.

- ▶ If $G \cong \mathbb{Z}/(p)$ for a positive prime p , then $\#G = p$.
- ▶ If $0 \rightarrow G_1 \rightarrow G \rightarrow G_2 \rightarrow 0$ is exact, then $\#G = \#G_1\#G_2$.

Drinfeld module analogue of Hasse bound (Gekeler)

For a monic irreducible $\mathfrak{p}(x) \in \mathbb{F}_q[x]$

$$\chi_{\phi, \mathfrak{p}}(x) := \chi(\phi(\mathbb{F}_q[x]/(\mathfrak{p}(x)))) = \mathfrak{p}(x) + \underbrace{t_{\phi, \mathfrak{p}}(x)}_{\leq \deg(\mathfrak{p})/2}$$

$$\#(E(\mathbb{Z}/p\mathbb{Z})) = p + 1 - \underbrace{t_{E, p}}_{-2\sqrt{p} \leq \leq 2\sqrt{p}}$$

$$\chi_{\phi, \mathfrak{p}}(x) = \mathfrak{p}(x) + \text{terms of degree at most } \deg(\mathfrak{p})/2.$$

Euler-Poincare Characteristic of Finite $\mathbb{F}_q[x]$ Modules: An $\mathbb{F}_q[x]$ measure of cardinality.

For a finite $\mathbb{F}_q[x]$ module A , $\chi(A) \in \mathbb{F}_q[x]$ is the monic polynomial s.t.

- ▶ If $A \cong \mathbb{F}_q[x]/(\mathfrak{p}(x))$ for a monic irreducible $\mathfrak{p}(x)$, then $\chi(A) = \mathfrak{p}(x)$.
- ▶ If $0 \rightarrow A_1 \rightarrow A \rightarrow A_2 \rightarrow 0$ is exact, then $\chi(A) = \chi(A_1)\chi(A_2)$.

For a finite \mathbb{Z} module G , $\#G \in \mathbb{Z}$ is the positive integer s.t.

- ▶ If $G \cong \mathbb{Z}/(p)$ for a positive prime p , then $\#G = p$.
- ▶ If $0 \rightarrow G_1 \rightarrow G \rightarrow G_2 \rightarrow 0$ is exact, then $\#G = \#G_1\#G_2$.

Drinfeld module analogue of Hasse bound (Gekeler)

For a monic irreducible $\mathfrak{p}(x) \in \mathbb{F}_q[x]$

$$\chi_{\phi, \mathfrak{p}}(x) := \chi(\phi(\mathbb{F}_q[x]/(\mathfrak{p}(x)))) = \mathfrak{p}(x) + \underbrace{t_{\phi, \mathfrak{p}}(x)}_{\leq \deg(\mathfrak{p})/2}$$

$$\#(E(\mathbb{Z}/p\mathbb{Z})) = p + 1 - \underbrace{t_{E, p}}_{-2\sqrt{p} \leq \leq 2\sqrt{p}}$$

$$\chi_{\phi, \mathfrak{p}}(x) = \mathfrak{p}(x) + \text{terms of degree at most } \deg(\mathfrak{p})/2.$$

Factor Degree Estimation

$$\begin{aligned}f(x) = \prod_i p_i(x) &\Rightarrow \phi(\mathbb{F}_q[x]/(f(x))) = \bigoplus_i \phi(\mathbb{F}_q[x]/(p_i(x))) \\ &\Rightarrow \chi_{\phi, f}(x) = \prod_i \chi_{\phi, p_i} = \prod_i (p_i(x) + t_{\phi, p_i}(x))\end{aligned}$$

Since $\forall i, \deg(t_{\phi, p_i}(x)) \leq \deg(p_i)/2$,

$$\chi_{\phi, f}(x) = f(x) + \text{terms of smaller degree.}$$

If s_f denotes the degree of the smallest degree factor of $f(x)$,

$$\begin{aligned}\chi_{\phi, f}(x) - f(x) &= \sum_{j: \deg(p_j)=s_f} (t_{\phi, p_j}(x) \prod_{i \neq j} p_i(x)) + \text{terms of degree} < (\deg(f) - \lceil s_f/2 \rceil) \\ &\Rightarrow \lceil s_f/2 \rceil \leq \deg(f) - \deg(\chi_{\phi, f} - f)\end{aligned}$$

Factor Degree Estimation

$$f(x) = \prod_i p_i(x) \Rightarrow \phi(\mathbb{F}_q[x]/(f(x))) = \bigoplus_i \phi(\mathbb{F}_q[x]/(p_i(x)))$$

$$\Rightarrow \chi_{\phi, f}(x) = \prod_i \chi_{\phi, p_i} = \prod_i (p_i(x) + t_{\phi, p_i}(x))$$

Since $\forall i, \deg(t_{\phi, p_i}(x)) \leq \deg(p_i)/2$,

$$\chi_{\phi, f}(x) = f(x) + \text{terms of smaller degree.}$$

If s_f denotes the degree of the smallest degree factor of $f(x)$,

$$\chi_{\phi, f}(x) - f(x) = \sum_{j: \deg(p_j)=s_f} (t_{\phi, p_j}(x) \prod_{i \neq j} p_i(x)) + \text{terms of degree} < (\deg(f) - \lceil s_f/2 \rceil)$$

$$\Rightarrow \lceil s_f/2 \rceil \leq \deg(f) - \deg(\chi_{\phi, f} - f)$$

Theorem : $\text{Prob}_{\phi} [\lceil s_f/2 \rceil = \deg(f) - \deg(\chi_{\phi, f} - f)] \geq 1/4$.

Factor Degree Estimation

$$\begin{aligned}f(x) = \prod_i p_i(x) &\Rightarrow \phi(\mathbb{F}_q[x]/(f(x))) = \bigoplus_i \phi(\mathbb{F}_q[x]/(p_i(x))) \\&\Rightarrow \chi_{\phi, f}(x) = \prod_i \chi_{\phi, p_i} = \prod_i (p_i(x) + t_{\phi, p_i}(x))\end{aligned}$$

Since $\forall i, \deg(t_{\phi, p_i}(x)) \leq \deg(p_i)/2$,

$$\chi_{\phi, f}(x) = f(x) + \text{terms of smaller degree.}$$

If s_f denotes the degree of the smallest degree factor of $f(x)$,

$$\begin{aligned}\chi_{\phi, f}(x) - f(x) &= \sum_{j: \deg(p_j)=s_f} (t_{\phi, p_j}(x) \prod_{i \neq j} p_i(x)) + \text{terms of degree} < (\deg(f) - \lceil s_f/2 \rceil) \\&\Rightarrow \lceil s_f/2 \rceil \leq \deg(f) - \deg(\chi_{\phi, f} - f)\end{aligned}$$

Theorem : $\text{Prob}_{\phi} [\lceil s_f/2 \rceil = \deg(f) - \deg(\chi_{\phi, f} - f)] \geq 1/4.$

Computing Euler-Poincare Characteristics

- ▶ Compute $\chi_{\phi, f}$ as the characteristic polynomial of the (\mathbb{F}_q -linear) ϕ_x action on $\mathbb{F}_q[x]/(f(x))$.
- ▶ Only need a Montecarlo algorithm for $\chi_{\phi, f}(x)$ that succeeds with constant probability !

For $a \in \phi(\mathbb{F}_q(x)/f(x))$, $Ord(a)$ is the smallest degree monic $g(x)$ such that $\phi_g(a) = 0$.

Theorem: It is likely that $\chi_{\phi, f}$ equals the order $Ord(a)$ of a random $a \in \phi(\mathbb{F}_q[x]/(f(x)))$.

$Ord(a)$ can be computed with run time exponent $3/2$ by (a Drinfeld version of) automorphism-projection followed by Berlekamp-Massey assuming the matrix multiplication exponent is 2.

Computing Euler-Poincare Characteristics

- ▶ Compute $\chi_{\phi, f}$ as the characteristic polynomial of the (\mathbb{F}_q -linear) ϕ_x action on $\mathbb{F}_q[x]/(f(x))$.
- ▶ Only need a Montecarlo algorithm for $\chi_{\phi, f}(x)$ that succeeds with constant probability !

For $a \in \phi(\mathbb{F}_q(x)/f(x))$, $Ord(a)$ is the smallest degree monic $g(x)$ such that $\phi_g(a) = 0$.

Theorem: It is likely that $\chi_{\phi, f}$ equals the order $Ord(a)$ of a random $a \in \phi(\mathbb{F}_q[x]/(f(x)))$.

$Ord(a)$ can be computed with run time exponent $3/2$ by (a Drinfeld version of) automorphism-projection followed by Berlekamp-Massey assuming the matrix multiplication exponent is 2.

Drinfeld Analog of Berlekamp/Lenstra's Algorithm

$$\text{Ord}(a) \text{ divides } \chi_{\phi, f}(x) = \prod_i \chi_{\phi, p_i}(x) = \prod_i \underbrace{(p_i(x) + t_{\phi, p_i}(x))}_{\in \mathcal{I}_{p_i}}$$

$$\mathcal{I}_{p_i} := \{p_i(x) + b(x), \deg(b) \leq \deg(p_i)/2\}$$

- ▶ Image of $\phi \mapsto p_i(x) + t_{\phi, p_i}(x) \in \mathcal{I}_{p_i}$ is random enough.
- ▶ Factorization patterns in the short intervals \mathcal{I}_{p_i} are random enough.

A random polynomial of degree $d > 1$ has a linear factor with probability roughly $1 - 1/e$.

$$g(x) := \text{Ord}(a) / \gcd(\text{Ord}(a), x^q - x)$$

Likely $\phi_g(a) = 0 \pmod{p_i(x)}$ for some but not all $p_i(x)$

$\Rightarrow \gcd(\phi_g(a), f)$ is a non trivial factor of $f(x)$.

Drinfeld Analog of Berlekamp/Lenstra's Algorithm

$$\text{Ord}(a) \text{ divides } \chi_{\phi, f}(x) = \prod_i \chi_{\phi, p_i}(x) = \prod_i \underbrace{(p_i(x) + t_{\phi, p_i}(x))}_{\in \mathcal{I}_{p_i}}$$

$$\mathcal{I}_{p_i} := \{p_i(x) + b(x), \deg(b) \leq \deg(p_i)/2\}$$

- ▶ Image of $\phi \mapsto p_i(x) + t_{\phi, p_i}(x) \in \mathcal{I}_{p_i}$ is random enough.
- ▶ Factorization patterns in the short intervals \mathcal{I}_{p_i} are random enough.

A random polynomial of degree $d > 1$ has a linear factor with probability roughly $1 - 1/e$.

$$g(x) := \text{Ord}(a) / \gcd(\text{Ord}(a), x^q - x)$$

Likely $\phi_g(a) = 0 \pmod{p_i(x)}$ for some but not all $p_i(x)$

$\Rightarrow \gcd(\phi_g(a), f)$ is a non trivial factor of $f(x)$.

Polynomial Factorization Patterns in Short Intervals

For every $f \in \mathbb{F}_q[x]$ of degree d bounded by $\log q \geq 3d \log d$, for every $m \geq 2$ and for every partition λ of d ,

$$\left(1 - \frac{1}{\sqrt{q}}\right) P(\lambda) \leq \frac{|\{g \in \mathcal{I}_{f,m} \mid \lambda_g = \lambda\}|}{|\mathcal{I}_{f,m}|} \leq \left(1 + \frac{1}{\sqrt{q}}\right) P(\lambda)$$

where $\mathcal{I}_{f,m} := f(x) + \mathbb{F}_q[x]_{\deg \leq m}$, λ_g denotes the partition of $\deg(g)$ induced by the degrees of the irreducible factors of g and $P(\lambda)$ is the fraction of permutations on d letters whose cycle decomposition corresponds to λ .

Density Theorem

Let F/E be a finite Galois extension of the rational function field $E := \mathbb{F}_q(x_1, \dots, x_m)$ in finitely many indeterminates. Let \mathcal{P}_F denote the set of \mathbb{F}_q rational places in E that are unramified in F . Fix an algebraic closure $\overline{\mathbb{F}_q}$ of \mathbb{F}_q and let $\alpha : \text{Gal}(F/E) \rightarrow \text{Gal}(\overline{\mathbb{F}_q} \cap F / \mathbb{F}_q)$ denote the restriction map. For a place $\mathfrak{p} \in \mathcal{P}_F$, let $\Theta_{\mathfrak{p}}$ denote the conjugacy class in $\ker(\alpha)$ of Artin symbols of places in F above \mathfrak{p} . For every conjugacy class $\Theta \subseteq \ker(\alpha)$,

$$\left| |\{\mathfrak{p} \in \mathcal{P}_F \mid \Theta_{\mathfrak{p}} = \Theta\}| - \frac{|\Theta|}{|\ker(\alpha)|} q^m \right| \leq \frac{|\Theta|}{|\ker(\alpha)|} [F : E]^{m+1} q^{m/2}.$$

Hasse Invariant: Joint work with Javad Doliskani and Éric Schost

Reduction of Drinfeld modules

For a prime ideal $(\mathfrak{p}(x)) \subset \mathbb{F}_q[x]$, if \mathfrak{d}_ϕ is non zero modulo \mathfrak{p} , then the reduction $\phi/\mathfrak{p} := \phi \otimes \mathbb{F}_q[x]/(\mathfrak{p}(x))$ of ϕ at \mathfrak{p} is defined through the ring homomorphism

$$\phi/\mathfrak{p} : \mathbb{F}_q[x] \longrightarrow \mathbb{F}_q[x]/(\mathfrak{p}(x))\langle\sigma\rangle$$

$$x \longmapsto x + (\mathfrak{g}_\phi(x) \pmod{\mathfrak{p}})\sigma + (\mathfrak{d}_\phi(x) \pmod{\mathfrak{p}})\sigma^2$$

and the image of $\mathfrak{b}(x) \in \mathbb{F}_q[x]$ under ϕ/\mathfrak{p} is denoted by $(\phi/\mathfrak{p})_{\mathfrak{b}}$.

Hasse Invariant

The Hasse invariant $\mathfrak{h}_{\phi, \mathfrak{p}}(x)$ of ϕ at \mathfrak{p} is the coefficient of $\sigma^{\deg(\mathfrak{p})}$ in the expansion

$$(\phi/\mathfrak{p})_{\mathfrak{b}} = \sum_{i=0}^{2 \deg(\mathfrak{p})} \mathfrak{h}_i((\phi/\mathfrak{p}))_x \sigma^i.$$

Hasse Invariant: Joint work with Javad Doliskani and Éric Schost

Reduction of Drinfeld modules

For a prime ideal $(\mathfrak{p}(x)) \subset \mathbb{F}_q[x]$, if \mathfrak{d}_ϕ is non zero modulo \mathfrak{p} , then the reduction $\phi/\mathfrak{p} := \phi \otimes \mathbb{F}_q[x]/(\mathfrak{p}(x))$ of ϕ at \mathfrak{p} is defined through the ring homomorphism

$$\begin{aligned}\phi/\mathfrak{p} : \mathbb{F}_q[x] &\longrightarrow \mathbb{F}_q[x]/(\mathfrak{p}(x))\langle\sigma\rangle \\ x &\longmapsto x + (\mathfrak{g}_\phi(x) \pmod{\mathfrak{p}})\sigma + (\mathfrak{d}_\phi(x) \pmod{\mathfrak{p}})\sigma^2\end{aligned}$$

and the image of $\mathfrak{b}(x) \in \mathbb{F}_q[x]$ under ϕ/\mathfrak{p} is denoted by $(\phi/\mathfrak{p})_{\mathfrak{b}}$.

Hasse Invariant

The Hasse invariant $\mathfrak{h}_{\phi,\mathfrak{p}}(x)$ of ϕ at \mathfrak{p} is the coefficient of $\sigma^{\deg(\mathfrak{p})}$ in the expansion

$$(\phi/\mathfrak{p})_{\mathfrak{p}} = \sum_{i=0}^{2 \deg(\mathfrak{p})} \mathfrak{h}_i((\phi/\mathfrak{p}))(x)\sigma^i.$$

ϕ is supersingular at \mathfrak{p} if and only if $\mathfrak{h}_{\phi,\mathfrak{p}}(x) = 0 \pmod{\mathfrak{p}(x)}$

Hasse Invariant: Joint work with Javad Doliskani and Éric Schost

Reduction of Drinfeld modules

For a prime ideal $(\mathfrak{p}(x)) \subset \mathbb{F}_q[x]$, if \mathfrak{d}_ϕ is non zero modulo \mathfrak{p} , then the reduction $\phi/\mathfrak{p} := \phi \otimes \mathbb{F}_q[x]/(\mathfrak{p}(x))$ of ϕ at \mathfrak{p} is defined through the ring homomorphism

$$\phi/\mathfrak{p} : \mathbb{F}_q[x] \longrightarrow \mathbb{F}_q[x]/(\mathfrak{p}(x))\langle\sigma\rangle$$

$$x \longmapsto x + (\mathfrak{g}_\phi(x) \pmod{\mathfrak{p}})\sigma + (\mathfrak{d}_\phi(x) \pmod{\mathfrak{p}})\sigma^2$$

and the image of $\mathfrak{b}(x) \in \mathbb{F}_q[x]$ under ϕ/\mathfrak{p} is denoted by $(\phi/\mathfrak{p})_{\mathfrak{b}}$.

Hasse Invariant

The Hasse invariant $\mathfrak{h}_{\phi,\mathfrak{p}}(x)$ of ϕ at \mathfrak{p} is the coefficient of $\sigma^{\deg(\mathfrak{p})}$ in the expansion

$$(\phi/\mathfrak{p})_{\mathfrak{p}} = \sum_{i=0}^{2 \deg(\mathfrak{p})} \mathfrak{h}_i((\phi/\mathfrak{p}))(x)\sigma^i.$$

ϕ is supersingular at \mathfrak{p} if and only if $\mathfrak{h}_{\phi,\mathfrak{p}}(x) = 0 \pmod{\mathfrak{p}(x)}$

Deligne's Congruence

Recursively define a sequence $(\tau_{\phi,k}(x) \in \mathbb{F}_q[x], k \in \mathbb{N})$ as

$$\tau_{\phi,0}(x) := 1, \tau_{\phi,1}(x) := g_{\phi}(x) \text{ and for } m > 1,$$

$$\tau_{\phi,m}(x) := (g_{\phi}(x))^{q^{m-1}} \tau_{\phi,m-1}(x) - (x^{q^{m-1}} - x) (d_{\phi}(x))^{q^{m-2}} \tau_{\phi,m-2}(x)$$

Gekeler showed that $\tau_{\phi,m}(x)$ is the value of the normalized Eisenstein series of weight $q^m - 1$ on ϕ and established Deligne's congruence for Drinfeld modules, which ascertains for any \mathfrak{p} of degree $k \geq 1$ with $d_{\phi}(x) \not\equiv 0 \pmod{\mathfrak{p}}$ that

$$h_{\phi,\mathfrak{p}}(x) = \tau_{\phi,k}(x) \pmod{\mathfrak{p}}.$$

Deligne's Congruence

Recursively define a sequence $(\tau_{\phi,k}(x) \in \mathbb{F}_q[x], k \in \mathbb{N})$ as

$$\tau_{\phi,0}(x) := 1, \tau_{\phi,1}(x) := g_{\phi}(x) \text{ and for } m > 1,$$

$$\tau_{\phi,m}(x) := (g_{\phi}(x))^{q^{m-1}} \tau_{\phi,m-1}(x) - (x^{q^{m-1}} - x) (d_{\phi}(x))^{q^{m-2}} \tau_{\phi,m-2}(x)$$

Gekeler showed that $\tau_{\phi,m}(x)$ is the value of the normalized Eisenstein series of weight $q^m - 1$ on ϕ and established Deligne's congruence for Drinfeld modules, which ascertains for any \mathfrak{p} of degree $k \geq 1$ with $d_{\phi}(x) \not\equiv 0 \pmod{\mathfrak{p}}$ that

$$h_{\phi,\mathfrak{p}}(x) = \tau_{\phi,k}(x) \pmod{\mathfrak{p}}.$$

Hence $\tau_{\phi,k}(x)$ is a lift to $\mathbb{F}_q[x]$ of all the Hasse invariants of ϕ at primes of degree k .

Deligne's Congruence

Recursively define a sequence $(\tau_{\phi,k}(x) \in \mathbb{F}_q[x], k \in \mathbb{N})$ as

$$\tau_{\phi,0}(x) := 1, \tau_{\phi,1}(x) := g_{\phi}(x) \text{ and for } m > 1,$$

$$\tau_{\phi,m}(x) := (g_{\phi}(x))^{q^{m-1}} \tau_{\phi,m-1}(x) - (x^{q^{m-1}} - x) (d_{\phi}(x))^{q^{m-2}} \tau_{\phi,m-2}(x)$$

Gekeler showed that $\tau_{\phi,m}(x)$ is the value of the normalized Eisenstein series of weight $q^m - 1$ on ϕ and established Deligne's congruence for Drinfeld modules, which ascertains for any \mathfrak{p} of degree $k \geq 1$ with $d_{\phi}(x) \not\equiv 0 \pmod{\mathfrak{p}}$ that

$$h_{\phi,\mathfrak{p}}(x) = \tau_{\phi,k}(x) \pmod{\mathfrak{p}}.$$

Hence $\tau_{\phi,k}(x)$ is a lift to $\mathbb{F}_q[x]$ of all the Hasse invariants of ϕ at primes of degree k .

Further, $\tau_{\phi,k}(x), \tau_{\phi,k+1}(x)$ are both zero precisely modulo the supersingular \mathfrak{p} of degree $\leq k$.

Deligne's Congruence

Recursively define a sequence $(\tau_{\phi,k}(x) \in \mathbb{F}_q[x], k \in \mathbb{N})$ as

$$\tau_{\phi,0}(x) := 1, \tau_{\phi,1}(x) := g_{\phi}(x) \text{ and for } m > 1,$$

$$\tau_{\phi,m}(x) := (g_{\phi}(x))^{q^{m-1}} \tau_{\phi,m-1}(x) - (x^{q^{m-1}} - x) (d_{\phi}(x))^{q^{m-2}} \tau_{\phi,m-2}(x)$$

Gekeler showed that $\tau_{\phi,m}(x)$ is the value of the normalized Eisenstein series of weight $q^m - 1$ on ϕ and established Deligne's congruence for Drinfeld modules, which ascertains for any \mathfrak{p} of degree $k \geq 1$ with $d_{\phi}(x) \not\equiv 0 \pmod{\mathfrak{p}}$ that

$$h_{\phi,\mathfrak{p}}(x) = \tau_{\phi,k}(x) \pmod{\mathfrak{p}}.$$

Hence $\tau_{\phi,k}(x)$ is a lift to $\mathbb{F}_q[x]$ of all the Hasse invariants of ϕ at primes of degree k .

Further, $\tau_{\phi,k}(x), \tau_{\phi,k+1}(x)$ are both zero precisely modulo the supersingular \mathfrak{p} of degree $\leq k$.

To factor $f(x)$, choose a Drinfeld module ϕ , compute $\gcd(\tau_{\phi,k}(x), \tau_{\phi,k+1}(x)) \pmod{f(x)}$ and output its gcd with $f(x)$ to separate the degree at most k irreducible factors of $f(x)$ where ϕ is supersingular.

Deligne's Congruence

Recursively define a sequence $(\tau_{\phi,k}(x) \in \mathbb{F}_q[x], k \in \mathbb{N})$ as

$$\tau_{\phi,0}(x) := 1, \tau_{\phi,1}(x) := g_{\phi}(x) \text{ and for } m > 1,$$

$$\tau_{\phi,m}(x) := (g_{\phi}(x))^{q^{m-1}} \tau_{\phi,m-1}(x) - (x^{q^{m-1}} - x) (d_{\phi}(x))^{q^{m-2}} \tau_{\phi,m-2}(x)$$

Gekeler showed that $\tau_{\phi,m}(x)$ is the value of the normalized Eisenstein series of weight $q^m - 1$ on ϕ and established Deligne's congruence for Drinfeld modules, which ascertains for any \mathfrak{p} of degree $k \geq 1$ with $d_{\phi}(x) \not\equiv 0 \pmod{\mathfrak{p}}$ that

$$h_{\phi,\mathfrak{p}}(x) = \tau_{\phi,k}(x) \pmod{\mathfrak{p}}.$$

Hence $\tau_{\phi,k}(x)$ is a lift to $\mathbb{F}_q[x]$ of all the Hasse invariants of ϕ at primes of degree k .

Further, $\tau_{\phi,k}(x), \tau_{\phi,k+1}(x)$ are both zero precisely modulo the supersingular \mathfrak{p} of degree $\leq k$.

To factor $f(x)$, choose a Drinfeld module ϕ , compute $\gcd(\tau_{\phi,k}(x), \tau_{\phi,k+1}(x)) \pmod{f(x)}$ and output its gcd with $f(x)$ to separate the degree at most k irreducible factors of $f(x)$ where ϕ is supersingular.

Drinfeld Modules with Complex Multiplication

A Drinfeld module ϕ has complex multiplication by an imaginary quadratic extension $L/\mathbb{F}_q(x)$ if

$$\text{End}_{\mathbb{F}_q(x)}(\phi) \otimes_{\mathbb{F}_q[x]} \mathbb{F}_q(x) \cong L.$$

$$\begin{array}{c} L \\ | \\ \mathbb{F}_q(x) \end{array}$$

$$\begin{array}{c} \infty \\ | \\ (1/x) \end{array} \text{ notsplit}$$

$$\begin{array}{c} \mathfrak{P} \\ | \\ (\mathfrak{p}(x)) \end{array} \text{ supersingular}$$

$$\begin{array}{ccc} \mathfrak{P}_1 & & \mathfrak{P}_2 \\ & \searrow \text{ordinary} \swarrow & \\ & (\mathfrak{p}(x)) & \end{array}$$

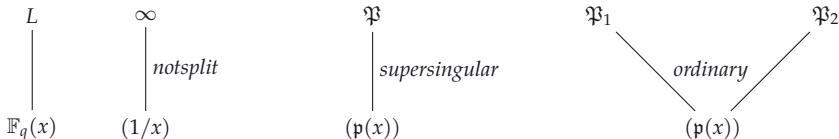
To get a Drinfeld module with complex multiplication by $L := \mathbb{F}_q(x)(\sqrt{b(x)})$, pick

$$\mathfrak{g}_{\phi'}(x) := \sqrt{b(x)} + \left(\sqrt{b(x)}\right)^q, \mathfrak{d}_{\phi'}(x) := 1$$

Drinfeld Modules with Complex Multiplication

A Drinfeld module ϕ has complex multiplication by an imaginary quadratic extension $L/\mathbb{F}_q(x)$ if

$$\text{End}_{\mathbb{F}_q(x)}(\phi) \otimes_{\mathbb{F}_q[x]} \mathbb{F}_q(x) \cong L.$$



To get a Drinfeld module with complex multiplication by $L := \mathbb{F}_q(x)(\sqrt{\mathfrak{b}(x)})$, pick

$$\mathfrak{g}_{\phi'}(x) := \sqrt{\mathfrak{b}(x)} + \left(\sqrt{\mathfrak{b}(x)}\right)^q, \mathfrak{d}_{\phi'}(x) := 1$$

which is isomorphic to

$$\mathfrak{g}_{\phi}(x) := J_{\phi'}(x), \mathfrak{d}_{\phi}(x) := (J_{\phi'}(x))^q, \text{ where}$$

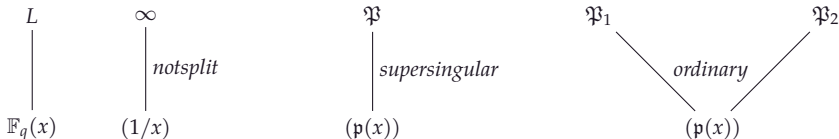
$$J_{\phi'}(x) := \frac{\mathfrak{g}_{\phi'}(x)^{q+1}}{\mathfrak{d}_{\phi'}(x)} = \mathfrak{b}(x)^{(q+1)/2} \left(1 + \mathfrak{b}(x)^{(q-1)/2}\right)^{q+1}$$

Algorithm: Choose $\mathfrak{b}(x) = x - c$ at random, compute $\tau_{\phi,k}$ for large enough k and split.

Drinfeld Modules with Complex Multiplication

A Drinfeld module ϕ has complex multiplication by an imaginary quadratic extension $L/\mathbb{F}_q(x)$ if

$$\text{End}_{\mathbb{F}_q(x)}(\phi) \otimes_{\mathbb{F}_q[x]} \mathbb{F}_q(x) \cong L.$$



To get a Drinfeld module with complex multiplication by $L := \mathbb{F}_q(x)(\sqrt{\mathfrak{b}(x)})$, pick

$$\mathfrak{g}_{\phi'}(x) := \sqrt{\mathfrak{b}(x)} + \left(\sqrt{\mathfrak{b}(x)}\right)^q, \mathfrak{d}_{\phi'}(x) := 1$$

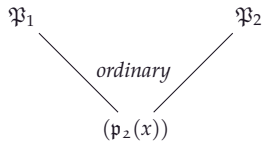
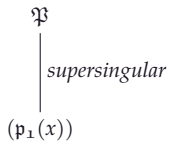
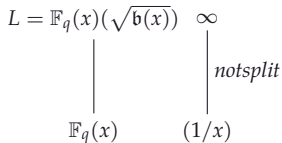
which is isomorphic to

$$\mathfrak{g}_{\phi}(x) := J_{\phi'}(x), \mathfrak{d}_{\phi}(x) := (J_{\phi'}(x))^q, \text{ where}$$

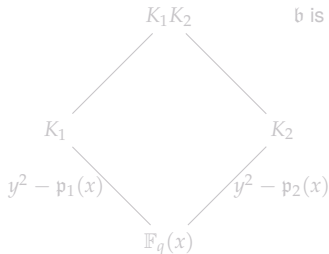
$$J_{\phi'}(x) := \frac{\mathfrak{g}_{\phi'}(x)^{q+1}}{\mathfrak{d}_{\phi'}(x)} = \mathfrak{b}(x)^{(q+1)/2} \left(1 + \mathfrak{b}(x)^{(q-1)/2}\right)^{q+1}$$

Algorithm: Choose $\mathfrak{b}(x) = x - c$ at random, compute $\tau_{\phi,k}$ for large enough k and split.

Splitting Probabilities



Consider $\mathfrak{p}_1(x), \mathfrak{p}_2(x)$ of degree at most k , what is the probability that b separates them ?

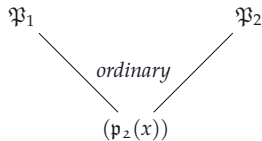
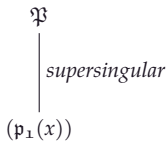
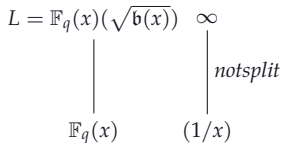


b is neither split nor inert in $K_1 K_2$ with prob $1/2$ if

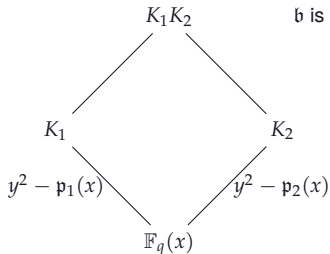
$$g(K_1 K_2) \approx k \leq \sqrt{q}$$



Splitting Probabilities



Consider $p_1(x), p_2(x)$ of degree at most k , what is the probability that b separates them ?



b is neither split nor inert in $K_1 K_2$ with prob $1/2$ if

$$g(K_1 K_2) \approx k \leq \sqrt{q}$$



Fast Computation of the Hasse-Invariant

The recursion for computing $\tau_{\phi,n}(x)$ can be written as

$$\begin{bmatrix} \tau_{\phi,k-1} \\ \tau_{\phi,k} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -[k-1]\partial_{\phi}^{q^{k-2}} & \mathfrak{g}_{\phi}^{q^{k-1}} \end{bmatrix} \begin{bmatrix} \tau_{\phi,k-2} \\ \tau_{\phi,k-1} \end{bmatrix}.$$

where $[k-1] := x^{q^{k-1}} - x \pmod{f(x)}$. Define the following sequence of matrices

$$A_k := \begin{bmatrix} 0 & 1 \\ -[k-1]\partial_{\phi}^{q^{k-2}} & \mathfrak{g}_{\phi}^{q^{k-1}} \end{bmatrix}.$$

Then we have

$$\begin{bmatrix} \tau_{\phi,k-1} \\ \tau_{\phi,k} \end{bmatrix} = A_k A_{k-1} \cdots A_2 \begin{bmatrix} \tau_{\phi,0} \\ \tau_{\phi,1} \end{bmatrix}.$$

Our goal is to compute the product

$$B_n := A_n A_{n-1} \cdots A_2 \in M(\mathbb{F}_q(x)/(f))$$

for then we can read off $\tau_{\phi,n}$ from $B_n \begin{bmatrix} \tau_{\phi,0} \\ \tau_{\phi,1} \end{bmatrix}$.

Baby-Step-Giant-Step

Extend the \mathbb{F}_q -linear q^{th} -power Frobenius map $\tau : \mathbb{F}_q[x]/(f) \rightarrow \mathbb{F}_q[x]/(f)$ to the polynomial ring $M_2(\mathbb{F}_q[x]/(f))[Y]$ by leaving Y fixed and acting on the coefficient matrices entry-wise.

Let

$$\mathcal{A} := \begin{bmatrix} 0 & 1 \\ -\tau(x)\mathfrak{d}_\phi(x) & \tau(\mathfrak{g}_\phi(x)) \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ \mathfrak{d}_\phi(x) & 0 \end{bmatrix} Y \in M_2(\mathbb{F}_q[x]/(f))[Y].$$

Then, for any $k \geq 1$, we have

$$A_k = \tau^{k-2}(\mathcal{A})(x).$$

Let $\ell := \lceil \sqrt{n} \rceil$, $m := \lfloor n/\ell \rfloor \sim \sqrt{n}$ and define

$$\mathcal{B} := \tau^{\ell-1}(\mathcal{A}) \cdots \tau(\mathcal{A})\mathcal{A}.$$

It follows from the above that

$$\mathcal{B}(x) = A_{\ell+1}A_{\ell-2} \cdots A_2.$$

More generally, using the fact that for all i, j

$$A_{i+j+2} = \tau^{i+j}(\mathcal{A})(x) = \tau^j\left(\tau^i(\mathcal{A})(\tau^{-j}(x))\right),$$

we deduce for all $i \geq 1$ that

$$\tau^i\left(\mathcal{B}(\tau^{-i}(x))\right) = A_{i+\ell+1} \cdots A_{i+3}A_{i+2}.$$

In particular, B_n can be computed as the product of the following matrices,

$$\mathcal{B}(x), \tau^\ell\left(\mathcal{B}(\tau^{-\ell}(x))\right), \dots, \tau^{m\ell}\left(\mathcal{B}(\tau^{-m\ell}(x))\right).$$