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

$$\mathfrak{f}(x) = \prod_i \mathfrak{p}_i(x)$$

Gauss->Legendre->Berlekamp->Cantor/Zassenhaus->Camion->vonzur Gathern/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-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.

Polynomial Factorization over Finite Fields

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

$$\mathfrak{f}(x) = \prod_i \mathfrak{p}_i(x)$$

Gauss->Legendre->Berlekamp->Cantor/Zassenhaus->Camion->vonzur Gathern/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-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 $\mathfrak{f}(x) \in \mathbb{F}_q[x]$ of degree n into its monic irreducible factors.

$$\mathfrak{f}(x) = \prod_i \mathfrak{p}_i(x)$$

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

$\Downarrow$

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

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

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 $\mathfrak{d}_\phi(x) \in \mathbb{F}_q[x]$.

Rank-2 Drinfeld Modules

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

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

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 $\mathfrak{b}(x) \in \mathbb{F}_q[x]$, $$\mathfrak{b}(x) \longmapsto \underbrace{\mathfrak{b}(x) + \sum_{i=1}^{2\deg(\mathfrak{b})} \phi_{\mathfrak{b},i}(x)\sigma^i}_{\textit{Call } \phi_{\mathfrak{b}}}.$$

Rank-2 Drinfeld Modules

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

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

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 $\mathfrak{b}(x) \in \mathbb{F}_q[x]$, $$\mathfrak{b}(x) \longmapsto \underbrace{\mathfrak{b}(x) + \sum_{i=1}^{2\deg(\mathfrak{b})} \phi_{\mathfrak{b},i}(x)\sigma^i}_{\textit{Call } \phi_{\mathfrak{b}}}.$$

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:

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

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

Rank-2 Drinfeld Modules

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

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

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

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

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:

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

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 $0 \to A_1 \to A \to A_2 \to 0$ 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 $0 \to G_1 \to G \to G_2 \to 0$ is exact, then $\#G = \#G_1 \#G_2$.

Drinfeld module analogue of Hasse bound (Gekeler)

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

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

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

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

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 $0 \to A_1 \to A \to A_2 \to 0$ 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 $0 \to G_1 \to G \to G_2 \to 0$ is exact, then $\#G = \#G_1 \#G_2$.

Drinfeld module analogue of Hasse bound (Gekeler)

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

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

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

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

Factor Degree Estimation

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

$$\Rightarrow \chi_{\phi,\mathfrak{f}}(x) = \prod_i \chi_{\phi,\mathfrak{p}_i} = \prod_i (\mathfrak{p}_i(x) + \mathfrak{t}_{\phi,\mathfrak{p}_i}(x))$$

Since $\forall i, \deg(\mathfrak{t}_{\phi,\mathfrak{p}_i}(x)) \leq \deg(\mathfrak{p}_i)/2$,

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

If $s_{\mathfrak{f}}$ denotes the degree of the smallest degree factor of $\mathfrak{f}(x)$,

$$\chi_{\phi,\mathfrak{f}}(x) - \mathfrak{f}(x) = \sum_{j:\deg(\mathfrak{p}_j)=s_{\mathfrak{f}}} (\mathfrak{t}_{\phi,\mathfrak{p}_j}(x) \prod_{i \neq j} \mathfrak{p}_i(x)) + \textit{terms of degree} < (\deg(\mathfrak{f}) - \lceil s_{\mathfrak{f}}/2 \rceil)$$

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

Factor Degree Estimation

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

$$\Rightarrow \chi_{\phi,\mathfrak{f}}(x) = \prod_i \chi_{\phi,\mathfrak{p}_i} = \prod_i (\mathfrak{p}_i(x) + \mathfrak{t}_{\phi,\mathfrak{p}_i}(x))$$

Since $\forall i, \deg(\mathfrak{t}_{\phi,\mathfrak{p}_i}(x)) \leq \deg(\mathfrak{p}_i)/2$,

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

If $s_\mathfrak{f}$ denotes the degree of the smallest degree factor of $\mathfrak{f}(x)$,

$$\chi_{\phi,\mathfrak{f}}(x) - \mathfrak{f}(x) = \sum_{j:\deg(\mathfrak{p}_j)=s_\mathfrak{f}} (\mathfrak{t}_{\phi,\mathfrak{p}_j}(x) \prod_{i \neq j} \mathfrak{p}_i(x)) + \textit{terms of degree} < (\deg(\mathfrak{f}) - \lceil s_\mathfrak{f}/2 \rceil)$$

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

$$\textit{Theorem} : \textit{Prob}_\phi \left[\lceil s_{\mathfrak{f}/2} \rceil = \deg(\mathfrak{f}) - \deg(\chi_{\phi,\mathfrak{f}} - \mathfrak{f}) \right] \geq 1/4.$$

Factor Degree Estimation

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

$$\Rightarrow \chi_{\phi,\mathfrak{f}}(x) = \prod_i \chi_{\phi,\mathfrak{p}_i} = \prod_i (\mathfrak{p}_i(x) + \mathfrak{t}_{\phi,\mathfrak{p}_i}(x))$$

Since $\forall i, \deg(\mathfrak{t}_{\phi,\mathfrak{p}_i}(x)) \leq \deg(\mathfrak{p}_i)/2$,

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

If $s_\mathfrak{f}$ denotes the degree of the smallest degree factor of $\mathfrak{f}(x)$,

$$\chi_{\phi,\mathfrak{f}}(x) - \mathfrak{f}(x) = \sum_{j:\deg(\mathfrak{p}_j)=s_\mathfrak{f}} (\mathfrak{t}_{\phi,\mathfrak{p}_j}(x) \prod_{i \neq j} \mathfrak{p}_i(x)) + \textit{terms of degree} < (\deg(\mathfrak{f}) - \lceil s_\mathfrak{f}/2 \rceil)$$

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

$$\textit{Theorem} : \textit{Prob}_\phi \left[\lceil s_{\mathfrak{f}/2} \rceil = \deg(\mathfrak{f}) - \deg(\chi_{\phi,\mathfrak{f}} - \mathfrak{f}) \right] \geq 1/4.$$

Computing Euler-Poincare Characteristics

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

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

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

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

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

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

$Ord(a)$ 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

$$\mathit{Ord}(a) \text{ divides } \chi_{\phi,\mathfrak{f}}(x) = \prod_i \chi_{\phi,\mathfrak{p}_i}(x) = \prod_i \underbrace{(\mathfrak{p}_i(x) + \mathfrak{t}_{\phi,\mathfrak{p}_i}(x))}_{\in \mathcal{I}_{\mathfrak{p}_i}}$$

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

- Image of $\phi \longmapsto \mathfrak{p}_i(x) + \mathfrak{t}_{\phi,\mathfrak{p}_i}(x) \in I_{\mathfrak{p}_i}$ is random enough.
- Factorization patterns in the short intervals $\mathcal{I}_{\mathfrak{p}_i}$ are random enough.

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

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

$$\textit{Likely } \phi_{\mathfrak{g}}(a) = 0 \mod \mathfrak{p}_i(x) \textit{ for some but not all } \mathfrak{p}_i(x)$$

$$\Rightarrow \gcd(\phi_{\mathfrak{g}}(a), \mathfrak{f}) \textit{ is a non trivial factor of } f(x).$$

Drinfeld Analog of Berlekamp/Lenstra's Algorithm

$$Ord(a) \text{ divides } \chi_{\phi,\mathfrak{f}}(x) = \prod_i \chi_{\phi,\mathfrak{p}_i}(x) = \prod_i \underbrace{(\mathfrak{p}_i(x) + \mathfrak{t}_{\phi,\mathfrak{p}_i}(x))}_{\in \mathcal{I}_{\mathfrak{p}_i}}$$

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

- Image of $\phi \longmapsto \mathfrak{p}_i(x) + \mathfrak{t}_{\phi,\mathfrak{p}_i}(x) \in I_{\mathfrak{p}_i}$ is random enough.
- Factorization patterns in the short intervals $\mathcal{I}_{\mathfrak{p}_i}$ are random enough.

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

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

$$\textit{Likely } \phi_{\mathfrak{g}}(a) = 0 \mod \mathfrak{p}_i(x) \textit{ for some but not all } \mathfrak{p}_i(x)$$

$$\Rightarrow \gcd(\phi_{\mathfrak{g}}(a), \mathfrak{f}) \textit{ is a non trivial factor of } f(x).$$

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,

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

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 $E := \mathbb{F}_q(x_1, \ldots, x_m)$ 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 $\alpha : Gal(F/E) \longrightarrow Gal((\overline{\mathbb{F}}_q \cap F)/\mathbb{F}_q)$ 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 $\Theta \subseteq ker(\alpha)$,

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

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 $\mathfrak{d}_\phi$ 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

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

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

and the image of $\mathfrak{b}(x) \in \mathbb{F}_q[x]$ under $\phi/\mathfrak{p}$ 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 $\sigma^{\deg(p)}$ in the expansion

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

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 $\mathfrak{d}_\phi$ 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

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

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

and the image of $\mathfrak{b}(x) \in \mathbb{F}_q[x]$ under $\phi/\mathfrak{p}$ 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 $\sigma^{\deg(p)}$ in the expansion

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

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

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 $\mathfrak{d}_\phi$ 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

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

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

and the image of $\mathfrak{b}(x) \in \mathbb{F}_q[x]$ under $\phi/\mathfrak{p}$ 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 $\sigma^{\deg(p)}$ in the expansion

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

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

Deligne's Congruence

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

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

$$\mathfrak{r}_{\phi,m}(x) := \left(\mathfrak{g}_\phi(x)\right)^{q^{m-1}} \mathfrak{r}_{\phi,m-1}(x) - (x^{q^{m-1}} - x) \left(\mathfrak{d}_\phi(x)\right)^{q^{m-2}} \mathfrak{r}_{\phi,m-2}(x)$$

Gekeler showed that $\mathfrak{r}_{\phi,m}(x)$ 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 $\mathfrak{d}_\phi(x) \neq 0 \mod \mathfrak{p}$ that

$$\mathfrak{h}_{\phi,\mathfrak{p}}(x) = \mathfrak{r}_{\phi,k}(x) \mod \mathfrak{p}.$$

Deligne's Congruence

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

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

$$\mathfrak{r}_{\phi,m}(x) := \left(\mathfrak{g}_\phi(x)\right)^{q^{m-1}} \mathfrak{r}_{\phi,m-1}(x) - (x^{q^{m-1}} - x) \left(\mathfrak{d}_\phi(x)\right)^{q^{m-2}} \mathfrak{r}_{\phi,m-2}(x)$$

Gekeler showed that $\mathfrak{r}_{\phi,m}(x)$ 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 $\mathfrak{d}_\phi(x) \neq 0 \mod \mathfrak{p}$ that

$$\mathfrak{h}_{\phi,\mathfrak{p}}(x) = \mathfrak{r}_{\phi,k}(x) \mod \mathfrak{p}.$$

Hence $\mathfrak{r}_{\phi,k}(x)$ 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 $(\mathfrak{r}_{\phi,k}(x) \in \mathbb{F}_q[x], k \in \mathbb{N})$ as

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

$$\mathfrak{r}_{\phi,m}(x) := \left(\mathfrak{g}_\phi(x)\right)^{q^{m-1}} \mathfrak{r}_{\phi,m-1}(x) - (x^{q^{m-1}} - x)\left(\mathfrak{d}_\phi(x)\right)^{q^{m-2}} \mathfrak{r}_{\phi,m-2}(x)$$

Gekeler showed that $\mathfrak{r}_{\phi,m}(x)$ 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 $\mathfrak{d}_\phi(x) \neq 0 \mod \mathfrak{p}$ that

$$\mathfrak{h}_{\phi,\mathfrak{p}}(x) = \mathfrak{r}_{\phi,k}(x) \mod \mathfrak{p}.$$

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

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

Deligne's Congruence

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

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

$$\mathfrak{r}_{\phi,m}(x) := \left(\mathfrak{g}_\phi(x)\right)^{q^{m-1}} \mathfrak{r}_{\phi,m-1}(x) - (x^{q^{m-1}} - x) \left(\mathfrak{d}_\phi(x)\right)^{q^{m-2}} \mathfrak{r}_{\phi,m-2}(x)$$

Gekeler showed that $\mathfrak{r}_{\phi,m}(x)$ 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 $\mathfrak{d}_\phi(x) \neq 0 \mod \mathfrak{p}$ that

$$\mathfrak{h}_{\phi,\mathfrak{p}}(x) = \mathfrak{r}_{\phi,k}(x) \mod \mathfrak{p}.$$

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

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

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

Deligne's Congruence

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

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

$$\mathfrak{r}_{\phi,m}(x) := \left(\mathfrak{g}_\phi(x)\right)^{q^{m-1}} \mathfrak{r}_{\phi,m-1}(x) - (x^{q^{m-1}} - x)\left(\mathfrak{d}_\phi(x)\right)^{q^{m-2}} \mathfrak{r}_{\phi,m-2}(x)$$

Gekeler showed that $\mathfrak{r}_{\phi,m}(x)$ 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 $\mathfrak{d}_\phi(x) \neq 0 \mod \mathfrak{p}$ that

$$\mathfrak{h}_{\phi,\mathfrak{p}}(x) = \mathfrak{r}_{\phi,k}(x) \mod \mathfrak{p}.$$

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

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

To factor $\mathfrak{f}(x)$, choose a Drinfeld module ϕ, compute $\gcd(\mathfrak{r}_{\phi,k}(x), \mathfrak{r}_{\phi,k+1}(x)) \mod f(x)$ and output its gcd with $\mathfrak{f}(x)$ to separate the degree at most k irreducible factors of $\mathfrak{f}(x)$ 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

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

$$\begin{tikzcd} L \arrow[d, dash] \\ \mathbb{F}_q(x) \end{tikzcd} \qquad \begin{tikzcd} \infty \arrow[d, dash, "notsplit"] \\ (1/x) \end{tikzcd} \qquad \begin{tikzcd} \mathfrak{P} \arrow[d, dash, "supersingular"] \\ (\mathfrak{p}(x)) \end{tikzcd} \qquad \begin{tikzcd} \mathfrak{P}_1 \arrow[dr, dash] & & \mathfrak{P}_2 \arrow[dl, dash] \\ & (\mathfrak{p}(x)) \arrow[u, phantom, "ordinary"] & \end{tikzcd}$$

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

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

Drinfeld Modules with Complex Multiplication

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

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

$$\begin{tikzcd}[arrows=dash] L \arrow[d] & \infty \arrow[d, "notsplit"] & \mathfrak{P} \arrow[d, "supersingular"] & \mathfrak{P}_1 \arrow[dr] & & \mathfrak{P}_2 \arrow[dl] \\ \mathbb{F}_q(x) & (1/x) & (\mathfrak{p}(x)) & & (\mathfrak{p}(x)) \arrow[u, phantom, "ordinary"] & \end{tikzcd}$$

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

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

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

Algorithm: Choose $\mathfrak{b}(x) = x - c$ at random, compute $\mathfrak{r}_{\phi,k}$ 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

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

$$
\begin{tikzcd}[arrows=dash]
L \arrow[d] & \infty \arrow[d, "notsplit"] & \mathfrak{P} \arrow[d, "supersingular"] & \mathfrak{P}_1 \arrow[dr, "ordinary"] & & \mathfrak{P}_2 \arrow[dl] \\
\mathbb{F}_q(x) & (1/x) & (\mathfrak{p}(x)) & & (\mathfrak{p}(x)) &
\end{tikzcd}
$$

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

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

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

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

Splitting Probabilities

$$\begin{tikzcd}
L = \mathbb{F}_q(x)(\sqrt{\mathfrak{b}(x)}) \arrow[d, dash] & \infty \arrow[d, dash, "notsplit"] \\
\mathbb{F}_q(x) & (1/x)
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathfrak{P} \arrow[d, dash, "supersingular"] \\
(\mathfrak{p}_1(x))
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathfrak{P}_1 \arrow[dr, dash] & & \mathfrak{P}_2 \arrow[dl, dash] \\
& (\mathfrak{p}_2(x)) \arrow[u, phantom, "ordinary"] &
\end{tikzcd}$$

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

$$\begin{tikzcd}
& K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\
K_1 \arrow[dr, dash, "y^2 - \mathfrak{p}_1(x)"'] & & K_2 \arrow[dl, dash, "y^2 - \mathfrak{p}_2(x)"] \\
& \mathbb{F}_q(x) &
\end{tikzcd}$$

$\mathfrak{b}$ is neither split nor inert in K_1K_2 with prob $1/2$ if

$$g(K_1K_2) \approx k \leq \sqrt{q}$$

$$\begin{tikzcd}
? \arrow[dr, dash] & & ? \arrow[dl, dash] \\
& (\mathfrak{b}(x)) &
\end{tikzcd}$$

Splitting Probabilities

$$
\begin{tikzcd}
L = \mathbb{F}_q(x)(\sqrt{\mathfrak{b}(x)}) \arrow[d, dash] & \infty \arrow[d, dash, "notsplit"] \\
\mathbb{F}_q(x) & (1/x)
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathfrak{P} \arrow[d, dash, "supersingular"] \\
(\mathfrak{p}_1(x))
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathfrak{P}_1 \arrow[dr, dash] & & \mathfrak{P}_2 \arrow[dl, dash] \\
& (\mathfrak{p}_2(x)) \arrow[u, phantom, "ordinary"] &
\end{tikzcd}
$$

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

$$
\begin{tikzcd}
& K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\
K_1 \arrow[dr, dash, "y^2 - \mathfrak{p}_1(x)"'] & & K_2 \arrow[dl, dash, "y^2 - \mathfrak{p}_2(x)"] \\
& \mathbb{F}_q(x) &
\end{tikzcd}
$$

$\mathfrak{b}$ is neither split nor inert in K_1K_2 with prob $1/2$ if

$$g(K_1K_2) \approx k \leq \sqrt{q}$$

$$
\begin{tikzcd}
? \arrow[dr, dash] & & ? \arrow[dl, dash] \\
& (\mathfrak{b}(x)) &
\end{tikzcd}
$$

Fast Computation of the Hasse-Invariant

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

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

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

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

Then we have

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

Our goal is to compute the product

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

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

Baby-Step-Giant-Step

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

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

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

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

we deduce for all $i \geq 1$ that

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

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

$$\mathcal{B}(x), \tau^\ell\Big(\mathcal{B}\big(\tau^{-\ell}(x)\big)\Big), \ldots, \tau^{m\ell}\Big(\mathcal{B}\big(\tau^{-m\ell}(x)\big)\Big).$$