COMPUTING ISOGENIES BETWEEN FINITE DRINFELD MODULES

BENJAMIN WESOLOWSKI

Univ. Bordeaux, CNRS, Bordeaux INP, IMB, UMR 5251, F-33400, Talence, France
INRIA, IMB, UMR 5251, F-33400, Talence, France

Abstract. We prove that isogenies between Drinfeld modules over a finite field can be computed in polynomial time. This breaks Drinfeld analogs of isogeny-based cryptosystems.

1. Introduction

In this short note we prove the following theorem.

Theorem 1.1. *Given an integer n and two Drinfeld $\mathbf{F}_q[x]$-modules ϕ and ψ over a finite field L, one can compute an isogeny $\iota : \phi \to \psi$ of τ-degree n, or decide that none exists, in polynomial time in n and in the length of the input. More precisely, the set of morphisms from ϕ to ψ of degree at most n is an $\mathbf{F}_q$-linear space, of which the algorithm finds a basis.*

This algorithm breaks Drinfeld analogs of isogeny-based cryptosystems in polynomial time. A first algorithm to compute such isogenies was described in [JN19], also with the aim to break such cryptosystems. However, it was observed in [LS22] that the algorithm of [JN19] has an exponential complexity in n, heuristically. A similar algorithm to [JN19] was independently proposed in [CGS20], together with an analysis that indeed features an exponential dependence in n. That exponential complexity raised new hope that Drinfeld-based cryptosystems could be secure.

The strategy we propose in this note starts similarly, reducing the problem to a system of polynomial equations. In [JN19] and [CGS20], this system is solved by a recursive strategy, resulting in a tree of potential solutions. One can then explore the tree to find actual solutions, but the tree has exponential size, and solutions may be sparse. Instead, we linearise the system of equations, and find the space of all solutions with efficient linear algebra.

2. Drinfeld modules

Consider a field extension $L/\mathbf{F}_q$, and the Frobenius endomorphism $\tau : \alpha \mapsto \alpha^q$ of $\overline{L}$. The ring of Ore polynomials is the subring $L\{\tau\}$ of $\mathbf{F}_q$-linear endomorphisms of $\overline{L}$ consisting of elements of the form

$$\sum_{i=0}^{n} \alpha_i \tau^i,$$

for arbitrary $n \in \mathbf{Z}_{\geq 0}$ and $\alpha_i \in L$. If $\alpha_n \neq 0$, the integer n is called the τ-degree of the polynomial, written $\deg_\tau$. As soon as $L \neq \mathbf{F}_q$, the ring is not commutative, as $\tau\alpha = \alpha^q\tau$ for any $\alpha \in L$.

Let $\mathbf{k}$ be an extension of $\mathbf{F}_q$ of transcendance degree 1, with a place ∞, and $\mathbf{A}$ its subring of regular functions outside ∞. Given any non-zero ideal $\mathfrak{a}$ in $\mathbf{A}$, we write $\deg(\mathfrak{a}) = \log_q(\mathbf{A}/\mathfrak{a})$. Given any non-zero element $a \in \mathbf{A}$, we write $\deg(a) = \deg(a\,\mathbf{A})$. Let L be a field equipped with a non-zero ring homomorphism $\gamma : \mathbf{A} \to L$.

Definition 2.1. A Drinfeld $\mathbf{A}$-module over L is a ring homomorphism $\phi : \mathbf{A} \to L\{\tau\}$ such that $\phi(\mathbf{A}) \not\subseteq L$ and the τ^0 coefficient of $\phi(a)$ is $\gamma(a)$ for any $a \in \mathbf{A}$. For any $a \in \mathbf{A}$, we write $\phi_a = \phi(a)$. The rank of ϕ is the integer r such that $\deg_\tau(\phi_a) = r\deg(a)$ for any $a \in \mathbf{A}$. We write $\mathrm{Dr}_r(\mathbf{A}, L)$ the set of Drinfeld $\mathbf{A}$-modules over L of rank r.

For simplicity, we focus the rest of this note on the archetypical case $\mathbf{A} = \mathbf{F}_q[x]$. Then, a Drinfeld module is fully determined by ϕ_x, the image of $x \in \mathbf{F}_q[x]$.

Definition 2.2. A *morphism* of Drinfeld $\mathbf{A}$-modules $\iota : \phi \to \psi$ over L is an Ore polynomial $\iota \in L\{\tau\}$ such that $\iota\phi_a = \psi_a\iota$ for any $a \in \mathbf{A}$. An *isogeny* is a non-zero morphism.

For $\iota : \phi \to \psi$ to be an isogeny of Drinfeld $\mathbf{F}_q[x]$-modules, it is sufficient to verify $\iota\phi_x = \psi_x\iota$.

3. Proof of the main theorem

We fix an integer n and two Drinfeld $\mathbf{F}_q[x]$-modules ϕ and ψ over a finite field L. We prove in this section that one can compute an isogeny $\iota : \phi \to \psi$ of τ-degree n, or decide that none exists, in polynomial time in n and in the length of the input.

Proof of Theorem 1.1. Write $\phi_x = \sum_{j=0}^{r} \alpha_j\tau^j$ and $\psi_x = \sum_{j=0}^{r} \beta_j\tau^j$, with $\omega = \alpha_0 = \beta_0 = \gamma(x)$. The strategy starts similarly to previous work. It is sufficient to find the coefficients of an Ore polynomial $\iota = \sum_{i=0}^{n} \iota_i\tau^i \in L\{\tau\}$ such that $\iota\phi_x = \psi_x\iota$. We wish to solve

$$\left(\sum_{i=0}^{n} \iota_i\tau^i\right)\left(\sum_{j=0}^{r} \alpha_j\tau^j\right) = \left(\sum_{j=0}^{r} \beta_j\tau^j\right)\left(\sum_{i=0}^{n} \iota_i\tau^i\right).$$

Writing $\alpha_i = \beta_i = 0$ for any $i > r$, the left hand side can be written

$$\sum_{i=0}^{n}\sum_{j=0}^{r} \iota_i\tau^i\alpha_j\tau^j = \sum_{i=0}^{n}\sum_{j=0}^{r} \iota_i\alpha_j^{q^i}\tau^{i+j} = \sum_{k=0}^{n+r}\left(\sum_{i=0}^{\min(k,n)} \iota_i\alpha_{k-i}^{q^i}\right)\tau^k.$$

Similarly, the right hand side can be written as

$$\sum_{j=0}^{r}\sum_{i=0}^{n} \beta_j\tau^j\iota_i\tau^i = \sum_{j=0}^{r}\sum_{i=0}^{n} \beta_j\iota_i^{q^j}\tau^{i+j} = \sum_{k=0}^{n+r}\left(\sum_{i=0}^{\min(k,n)} \beta_{k-i}\iota_i^{q^{k-i}}\right)\tau^k.$$

Comparing the coefficients, we obtain the system

$$\sum_{i=0}^{\min(k,n)} \iota_i\alpha_{k-i}^{q^i} = \sum_{i=0}^{\min(k,n)} \beta_{k-i}\iota_i^{q^{k-i}}, \text{ for all } k \in [1, k+r].$$

The field L is an $\mathbf{F}_q$-vector space of finite dimension $d = [L : \mathbf{F}_q]$, and each $\alpha \mapsto \alpha^{q^i}$ is a linear map. Hence, the above system is an $\mathbf{F}_q$-linear system of $(n+r)d$ equations in $(n+1)d$ variables. One can thus solve this system and find a solution ι such that $\iota_n \neq 0$ (i.e., an isogeny of τ-degree n), or decide that none exists, in polynomial time. □

4. Comparison with previous work

Previous work on computing isogenies focused on the case of rank 2, where the two Drinfeld modules $\phi, \psi \in \mathrm{Dr}_2(\mathbf{F}_q[x], L)$ are fully determined by Ore polynomials $\phi_x = \Delta_\phi\tau^2 + g_\phi\tau + \gamma(x)$ and $\psi_x = \Delta_\psi\tau^2 + g_\psi\tau + \gamma(x)$ in $L\{\tau\}$, with $\Delta_\phi \neq 0$ and $\Delta_\psi \neq 0$. To find an isogeny, one has to find $\iota = \sum_{i=0}^{n} \iota_i\tau^i \in L\{\tau\}$ such that $\iota\phi_x = \psi_x\iota$. In [JN19] and [CGS20], one starts with the same strategy followed above, expanding both sides of the equality

$$\left(\sum_{i=0}^{n} \iota_i\tau^i\right)\left(\Delta_\phi\tau^2 + g_\phi\tau + \omega\right) = \left(\Delta_\psi\tau^2 + g_\psi\tau + \omega\right)\left(\sum_{i=0}^{n} \iota_i\tau^i\right),$$

and identifying the coefficients in τ^i, which yields the system

$$\begin{aligned}
\tau^{n+2} &: \Delta_\phi^{q^n}\iota_n = \Delta_\psi\iota_n^{q^2},\\
\tau^{n+1} &: \Delta_\phi^{q^{n-1}}\iota_{n-1} + g_\phi^{q^n}\iota_n = \Delta_\psi\iota_{n-1}^{q^2} + g_\psi\iota_n^q,\\
\tau^{i+2} &: \Delta_\phi^{q^i}\iota_i + g_\phi^{q^{i+1}}\iota_{i+1} + \omega^{q^{i+2}}\iota_{i+2} = \Delta_\psi\iota_i^{q^2} + g_\psi\iota_{i+1}^q + \omega\iota_{i+2}, \text{ for } i \in [0, n-2],\\
\tau^1 &: g_\phi\iota_0 + \omega^q\iota_1 = g_\psi\iota_0^q + \omega\iota_1.
\end{aligned}$$

Now, our strategy diverges from previous methods. In [JN19] and [CGS20], one uses these equations from τ^{n+2} to τ^2, in this order, to recursively find candidate solutions for ι_n to ι_1, in this

order. At each step, there are either 0 or q possible solutions for ι_i [LS22, Lemma 4.2], forming a tree that can explored. Each leaf of the tree then provides a solution if it also satisfies the final equation from τ^1. It was heuristically argued in [LS22] that this tree has exponential size in n, and that successful leaves are rare, leading to an exponential running time.

5. Acknowledgements

The author is supported by the Agence Nationale de la Recherche under grants ANR MELODIA (ANR-20-CE40-0013) and ANR CIAO (ANR-19-CE48-0008).

References

[CGS20] Perlas Caranay, Matthew Greenberg, and Renate Scheidler. Computing modular polynomials and isogenies of rank two drinfeld modules over finite fields. In *75 Years of Mathematics of Computation: Symposium on Celebrating 75 Years of Mathematics of Computation, November 1-3, 2018, the Institute for Computational and Experimental Research in Mathematics (ICERM)*, volume 754, page 283. American Mathematical Soc., 2020.

[JN19] Antoine Joux and Anand Kumar Narayanan. Drinfeld modules may not be for isogeny based cryptography. Cryptology ePrint Archive, Report 2019/1329, 2019. `https://ia.cr/2019/1329`.

[LS22] Antoine Leudière and Pierre-Jean Spaenlehauer. Hard homogeneous spaces from the class field theory of imaginary hyperelliptic function fields. Cryptology ePrint Archive, Report 2022/349, 2022. `https://ia.cr/2022/349`.