Contemporary Mathematics
Volume **754**, 2020
https://doi.org/10.1090/conm/754/15148

Computing modular polynomials and isogenies of rank two Drinfeld modules over finite fields

Perlas Caranay, Matthew Greenberg, and Renate Scheidler

Abstract. We present algorithms for computing j-invariants, modular polynomials and explicit isogenies for ordinary rank 2 Drinfeld modules over finite fields and describe how Drinfeld modular polynomials can be used to compute isogeny graphs and endomorphism rings of ordinary rank 2 Drinfeld modules. Our technique for computing Drinfeld modular polynomials is based on the traditional analytic approach for obtaining classical modular polynomials. Our ideas for generating isogeny graphs and finding endomorphism rings for rank 2 Drinfeld modules closely follows the work of Kohel and Fouquet. All our algorithms were implemented in SAGE and numerical examples are included.

1. Introduction and motivation

Drinfeld modules represent the function field analogue of the theory of complex multiplication for number fields. They were introduced as "elliptic modules" by Drinfeld [**13**] in the 1970s in the course of proving the Langlands conjectures for the general linear group GL(2) over global function fields. Drinfeld modules of rank 2 in particular exhibit surprisingly similar behaviour to elliptic curves: they are classified as ordinary or supersingular, support isogenies and their duals, and their endomorphism rings have an analogous structure. Their isomorphism classes are parameterized by j-invariants which are the roots of the corresponding Drinfeld modular polynomial, and the ordinary components of their isogeny graphs take the shape of a volcano. The rich analytic and algebraic theory of Drinfeld modules has undergone extensive investigation; see, for example, Gekeler [**20**–**24**, **26**], Goss [**27**–**29**] and Hayes [**33**] for a by-no-means complete list of references. However, as far as the authors are aware, little if anything about Drinfeld modules has been explored from a computational perspective. Along with [**39**, **40**], this paper represents a first systematic foray in this direction, in the hope that complementing the theoretical exploration of Drinfeld modules with algorithms and concrete numerical data will lead to a better understanding of these objects and their behaviour. Motivated by significant advances over the past two decades on computing modular polynomials and endomorphism rings of elliptic curves, we explore the analogous algorithmic aspects of rank 2 Drinfeld modules over finite fields.

2010 *Mathematics Subject Classification.* Primary 11G09, 11Y16, 11Y40.

Key words and phrases. Rank 2 Drinfeld module, j-invariant, isogeny, Drinfeld modular polynomial, isogeny volcano, endomorphism ring, algorithms and computations.

The third author was supported by NSERC of Canada.

Similar to the setting of elliptic curves, the ℓ-th Drinfeld modular polynomial parameterizes pairs of ℓ-isogenous Drinfeld modules in terms of their j-invariants. There is a sizable body of literature on computing j-functions and modular polynomials for elliptic curves — see [**9**, **14**, **15**] to cite just a few sources — and Sutherland has computed an extensive database of them [**45**]. However, except for a few sporadic small examples [**3**, **43**], no analogous computations have been performed for Drinfeld modules. Our main contribution is a pair of explicit algorithms for computing rank 2 Drinfeld module j-invariants and Drinfeld modular polynomials, based on their description in [**3**] combined with the traditional analytic approach for computing classical j-invariants and modular polynomials. The first of these algorithms computes the Laurent series expansion of the j-function up to arbitrary precision. This expansion is then employed to compute the Drinfeld modular polynomial. Not surprisingly, as in the classical case, the main challenge here is rapid coefficient growth. However, the precise growth rate appears to be different from the classical setting, representing one instance where Drinfeld modules exhibit subtle and rather mysterious differences in behaviour compared to their elliptic curve counterparts. We also present a technique for computing explicit isogenies of Drinfeld modules. It is based on symbolic computation and is entirely different from elliptic curve techniques such as Vélu's formulas [**48**] for which we know of no Drinfeld module analogue. Another symbolic approach described herein efficiently computes dual isogenies of Drinfeld modules.

Isogeny graphs are closely related to modular polynomials and play a prominent role in computing the endomorphism ring of an elliptic curve [**4**, **36**] and in point counting [**16**, **17**]. Algorithms involving isogeny graphs associated to elliptic curves can be found in [**6**, **16**, **17**, **36**, **38**, **47**] and other sources, but the concept is entirely new in the Drinfeld module setting. We describe isogeny graphs of rank 2 Drinfeld modules which turn out to be structurally virtually identical to their elliptic curve counterparts; in particular, their ordinary components are volcanoes whose shape is determined by a result analogous to Kohel's Theorem [**36**, Prop. 23]. Following the methods of [**16**, **36**], we describe how isogeny volcanos and endomorphism rings of ordinary rank 2 Drinfeld modules can be computed from Drinfeld modular polynomials.

All our algorithms are accompanied by a comprehensive analysis of their asymptotic run time and storage requirements. We also provide an exact precision analysis of our method for computing j-invariants and determine the precise accuracy required to compute modular polynomials. We implemented our algorithms in SAGE [**44**] and provide numerical examples here; in the interest of space, these examples are much smaller than what our algorithms can generally handle and are included predominantly for illustrative purposes. Our source code is available on GitHub at [**7**]. Any underlying theoretical results on Drinfeld modules that were required in our algorithmic exploration and have not appeared in previous literature were carefully and rigorously adapted from the classical to the Drinfeld module setting; detailed descriptions and proofs can be found in the first author's doctoral dissertation [**8**].

Although our algorithms borrow extensively from methodology for elliptic curves, their basic computational building blocks and complexity analysis tools are quite different from the classical setting. Our computations involve non-prime finite fields and polynomials over finite fields, so all our estimates are governed by

a non-archimedean discrete valuation, rather than the standard archimedean absolute value. On a more mundane level, there is only one positive integer of any given absolute value, whereas for any $n \in \mathbb{N}$, there are q^n monic polynomials in $\mathbb{F}_q[T]$ of absolute value q^n. Most importantly, there are subtle theoretical differences between elliptic curves and Drinfeld modules, such as unexpected parameter dependencies. For example, the Frobenius norm for an elliptic curve over $\mathbb{F}_p$ is p, regardless of the curve, whilst in the rank 2 Drinfeld module case, this quantity depends on the leading coefficient of the Drinfeld module. Arguably the most significant difference is the fact that the coefficients of the Drinfeld j-function and the Drinfeld modular polynomial depend on the size of the base field and seem to grow notably faster than their classical counterparts, which has significant ramifications for complexity estimates.

2. Background on Drinfeld modules

We only consider the simplest setting of rank 2 Drinfeld modules over finite fields; the reader is referred to [**30**, Ch. 4] for a comprehensive treatment of Drinfeld modules of arbitrary rank over more general fields. Throughout, we adopt the following notation that is widely used in the literature on Drinfeld modules:

- $\mathbb{F}_q$ is a finite field of order q;
- $\mathbf{A} = \mathbb{F}_q[T]$ is the polynomial ring in the indeterminate T over $\mathbb{F}_q$;
- $\mathbf{A}^+ \subset \mathbf{A}$ is the set of monic polynomials in $\mathbf{A}$;
- $|a| = q^{\deg_T(a)}$ for any non-zero $a \in \mathbf{A}$;
- P is a fixed monic irreducible polynomial in $\mathbf{A}$ of degree d;
- $\mathbb{L} = \mathbf{A}/P\mathbf{A} \cong \mathbb{F}_{q^d}$;
- τ is the q-th power Frobenius map on some fixed algebraic closure $\overline{\mathbb{L}}$ of $\mathbb{L}$, defined via $\tau(\alpha) = \alpha^q$ for all $\alpha \in \overline{\mathbb{L}}$;
- $\mathbb{L}\{\tau\}$ is the ring of twisted polynomials in τ over $\mathbb{L}$ with the commutation rule $\tau\alpha = \alpha^q\tau$ for $\alpha \in \mathbb{L}$.

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

$$\varphi : \mathbf{A} \to \mathbb{L}\{\tau\} , \quad a \mapsto \varphi_a ,$$

satisfying the following two conditions:

(1) For all $a \in \mathbf{A}$, the constant term of φ_a is the image of a (also denoted a for simplicity) under the natural map from $\mathbf{A}$ into $\mathbb{L}$;
(2) $\varphi_a \notin \mathbb{L}$ for some $a \in \mathbf{A}$, i.e. $\varphi(\mathbf{A}) \not\subset \mathbb{L}$.

As is standard in the literature, the image $\varphi(a)$ of any $a \in \mathbf{A}$ is denoted φ_a. The $\mathbb{F}_q$-algebra homomorphic property implies that φ is uniquely defined by the image φ_T of T. The *rank* of φ is the degree of φ_T as a polynomial in τ. In our computations, we will focus exclusively on Drinfeld modules of rank $r = 2$.

Since the constant coefficient of any image φ_a is a, we see that Drinfeld modules are injective maps. The term *module* in this context arises from the action of $\mathbf{A}$ on $\mathbb{L}$ defined via $a\alpha = \varphi_a(\alpha)$ for $a \in \mathbf{A}$ and $\alpha \in \mathbb{L}$. This imposes an $\mathbf{A}$-module structure on $\mathbb{L}$ different from the normal one.

In the most general context, Drinfeld modules are defined over any extension $\mathbb{L}$ of $\mathbb{F}_q$ with a fixed $\mathbb{F}_q$-algebra homomorphism from $\mathbf{A}$ into $\mathbb{L}$ called a *structure map*. Here, we only consider the simplest case $\mathbb{L} = \mathbf{A}/P\mathbf{A}$, where the structure map is reduction modulo P. In our discussion of the analytic theory later on, we will also

require Drinfeld modules over an algebraically closed, complete extension field $\mathbf{C}$ of $\mathbb{F}_q(T)$, where the structure map is inclusion.

For any rank r Drinfeld module φ over $\mathbb{L}$ and any non-zero $a \in \mathbf{A}$, the roots of the polynomial $\varphi_a \in \mathbb{L}\{\tau\}$ in some fixed algebraic closure $\overline{\mathbb{L}}$ of $\mathbb{L}$ form the *a-torsion points* of φ, denoted

$$\varphi[a] = \ker \varphi_a = \{\lambda \in \overline{\mathbb{L}} \mid \varphi_a(\lambda) = 0\} \ .$$

They form a free $\mathbf{A}/a\mathbf{A}$-module of rank r when P does not divide a and rank less than r otherwise.

Let φ, ψ be Drinfeld modules over $\mathbb{L}$. A *morphism* (over $\mathbb{L}$) from φ to ψ, denoted $u : \varphi \longrightarrow \psi$, is a polynomial $u(\tau) \in \mathbb{L}\{\tau\}$ such that

$$u\varphi_a = \psi_a u$$

for all $a \in \mathbf{A}$. Since φ and ψ are $\mathbb{F}_q$-algebra homomorphisms, u is a morphism if and only if $u\varphi_T = \psi_T u$. It is important to note that, throughout this paper, morphisms will be defined over $\mathbb{L}$ unless specifically stated otherwise; the generalization to morphisms over $\overline{\mathbb{L}}$ is straightforward. An *endomorphism* is a morphism from a Drinfeld module to itself. An invertible morphism is an *isomorphism*; it is simply a non-zero element of $\mathbb{L}$. Isomorphism imposes an equivalence relation on the set of Drinfeld modules over $\mathbb{L}$ of fixed rank.

A non-zero morphism of Drinfeld modules is an *isogeny*. It is easy to see that isogenies preserve the rank of a Drinfeld module. Every isogeny $u : \varphi \longrightarrow \psi$ has a unique *dual* isogeny $\hat{u} : \psi \longrightarrow \varphi$ such that

$$\hat{u}u = \varphi_{\mathfrak{n}} \ , \quad u\hat{u} = \psi_{\mathfrak{n}} \tag{2.1}$$

for some non-zero $\mathfrak{n} \in \mathbf{A}$ that is unique up to multiples in $\mathbb{F}_q^*$. Consequently, isogeny is an equivalence relation on the set of Drinfeld modules over $\mathbb{L}$ of a fixed rank, with every isogeny class partitioned into isomorphism classes. Two Drinfeld modules are *isogenous* if there exists an isogeny from one to the other.

For the remainder of this section, we restrict to Drinfeld modules of rank 2, which we write in the form

$$\varphi = (g, \Delta) \quad \text{where} \quad \varphi_T = T + g\tau + \Delta\tau^2 \ , \tag{2.2}$$

with $g \in \mathbb{L}$ and $\Delta \in \mathbb{L}^*$. The *j-invariant* of φ is the quantity

$$j = j(\varphi) = \frac{g^{q+1}}{\Delta} \in \mathbb{L} \ .$$

Every $j \in \mathbb{L}$ occurs as the j-invariant of some rank 2 Drinfeld module φ; for example, $\varphi = (0, \Delta)$ when $j = 0$ and $\varphi = (1, j^{-1})$ otherwise. Two rank 2 Drinfeld modules over $\mathbb{L}$ are isomorphic over $\overline{\mathbb{L}}$ if and only if they have the same j-invariant. Thus, the elements of $\mathbb{L}$ are in one-to-one correspondence with the $\overline{\mathbb{L}}$-isomorphism classes of rank 2 Drinfeld modules over $\mathbb{L}$. Note that in contrast to the j-invariant of an elliptic curve $y^2 = x^3 + Ax + B$ of discriminant Δ, defined to be $j = -1728(4A)^3/\Delta$, the exponent $q+1$ of g in the numerator of a rank 2 Drinfeld module j-invariant depends on the size of the base field. We will see that this dependence on q recurs as a fundamental distinction between rank 2 Drinfeld modules and elliptic curves throughout both theory and computation.

A rank 2 Drinfeld module φ is said to be *supersingular* if its P-torsion $\varphi[P]$ is trivial and *ordinary* otherwise; in the latter case, $\varphi[P]$ is isomorphic to $\mathbf{A}/P\mathbf{A}$ as an $\mathbf{A}$-module. The *Hasse invariant* $H(\varphi) \in \mathbf{A}$ of φ is the coefficient of τ^d in

the polynomial $\varphi_P \pmod P$. It vanishes if and only if φ is supersingular. Drinfeld modules φ with $j(\varphi) = 0$ are ordinary if and only if P has even degree ([**20**, Thm. 5.9]).

Let $u : \varphi \to \psi$ be an isogeny of rank 2 Drinfeld modules, with dual isogeny $\hat{u}$ as given in (2.1). Then $\varphi_{\mathfrak{n}}$ and $\psi_{\mathfrak{n}}$ are analogues of the multiplication-by-$\mathfrak{n}$ maps for elliptic curves. The polynomial $\mathfrak{n} \in \mathbf{A}$ is the *(isogeny) degree* of u (and of $\hat{u}$), and satisfies $\deg_\tau(u) = \deg_\tau(\hat{u}) = \deg_T(\mathfrak{n})$. The isomorphisms from φ to ψ are precisely the isogenies of constant degree $\mathfrak{n} \in \mathbb{F}_q^*$, i.e. the elements of $\mathbb{L}^*$. For any $\mathfrak{n} \in \mathbf{A}$, two rank 2 Drinfeld modules φ, ψ over $\mathbb{L}$ are $\mathfrak{n}$-*isogenous* if there exists an $\mathfrak{n}$-*isogeny* between them, i.e. an isogeny $u : \varphi \to \psi$ of degree $\mathfrak{n} \in \mathbf{A}$.

As a concrete family of examples, we provide an explicit characterization and construction for isogenies of a given linear degree $\mathfrak{n}$ on rank 2 Drinfeld modules. The special case $\mathfrak{n} = T$ was handled previously by Schweizer [**43**].

PROPOSITION 2.1. *Let $\mathfrak{n} \in \mathbf{A}$ 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 $\mathfrak{n}$-isogeny on the rank 2 Drinfeld module $\varphi = (g, \Delta)$ over $\mathbb{L}$ if and only if $\Delta\alpha^{q+1} + g\alpha + \mathfrak{n} = 0$. In this case, u maps φ to the Drinfeld module $\psi = (g', \Delta')$ over $\mathbb{L}$, with $g' = g^q - \alpha\Delta + \alpha^{q^2}\Delta^q$ and $\Delta' = \Delta^q$. Moreover, the dual isogeny of u is $\hat{u} = \Delta\tau + g + \Delta\alpha^q$.*

PROOF. Suppose first that $u = \tau - \alpha$ is an $\mathfrak{n}$-isogeny on the rank 2 Drinfeld module $\varphi = (g, \Delta)$. Then the dual isogeny of u is of the form $\hat{u} = \Delta\tau + \beta$ for some $\beta \in \mathbb{L}$. Comparing coefficients in the identity $\varphi_{\mathfrak{n}} = \hat{u}u$ yields $\beta = g + \Delta\alpha^q = -\mathfrak{n}/\alpha$, so $\Delta\alpha^{q+1} + g\alpha + \mathfrak{n} = 0$ as asserted.

Conversely, suppose $\Delta\alpha^{q+1} + g\alpha + \mathfrak{n} = 0$. Put $u = \tau - \alpha$, $\varphi = (g, \Delta)$ and $\psi = (g', \Delta')$ where $g' = g^q - \alpha\Delta + \alpha^{q^2}\Delta^q$ and $\Delta' = \Delta^q \in \mathbb{L}^*$. Then φ, ψ are Drinfeld modules over $\mathbb{L}$ and $u \in \mathbb{L}\{\tau\}$. It is easy to verify that $u\varphi_{\mathfrak{n}} = \psi_{\mathfrak{n}}u$, so u is an $\mathfrak{n}$-isogeny on φ whose dual is again readily seen to be $\hat{u} = \Delta\tau + g + \Delta\alpha^q$. □

EXAMPLE 2.2. We provide three small numerical examples that illustrate Proposition 2.1. Let $q = 3$, $P(T) = T^5 + 2T + 1$ and $\mathbb{L} = \mathbf{A}/P\mathbf{A}$.

(1) The T-isogeny $u = \tau - \alpha$ with $\alpha = T^3 + 2T + 2$ sends the Drinfeld module $\varphi = (T^2, T^3)$ over $\mathbb{L}$ to the Drinfeld module $\psi = (2T^4 + T^2, 2T^4 + T + 2)$ over $\mathbb{L}$. Its dual is $\hat{u} = T^3\tau + T^4 + T^2 + T$. Here, $T^3\alpha^4 + T^2\alpha + T = 0$.
(2) The $(T + 1)$-isogeny $u = \tau - \alpha$ with $\alpha = T^2 + 2$ maps $\varphi = (T^2, T^2 + 2T)$ to $\psi = (2T^4 + 2T + 2, 2T^3 + T^2 + 2T)$. Its dual is $\hat{u} = (T^2 + 2T)\tau + T^4 + T^3 + T^2 + T$, and we have $(T^2 + 2T)\alpha^4 + T^2\alpha + T + 1 = 0$.
(3) The polynomial $u = \tau - \alpha$ with $\alpha = T^3 + T$ is a $(T + 2)$-isogeny from $\varphi = (T^3, T^4 + 1)$ to $\psi = (2T^4 + 1, T^4 + T^3 + T^2 + 1)$ with dual $\hat{u} = (T^4 + 1)\tau + T^3 + 2T^2 + 2T + 1$, and we have $(T^4 + 1)\alpha^4 + T^3\alpha + T + 2 = 0$.

We revisit such explicit symbolic isogeny computation in Section 8. Another method of constructing isogenies of Drinfeld modules over finite fields is given in [**49**, Sec. 2] using *kernel lattices*.

Just like elliptic curves, Drinfeld modules have a comprehensive analytic theory. Here, the analogue of the complex numbers is the algebraically closed complete field $\mathbf{C} = (\overline{\mathbf{K}_\infty})_\infty$, obtained by taking the completion of $\mathbf{K} = \mathbb{F}_q(T)$ at the infinite place, then taking the algebraic closure of the resulting complete field, and finally taking the completion at the infinite place again. The theory of Drinfeld modules over $\mathbf{C}$ is described, for instance, in [**30**], [**32**, Ch. 4] or [**42**, Ch. 13]. A detailed

discussion of the coefficients g and Δ of a rank 2 Drinfeld module over $\mathbf{C}$ can be found in [**22**, **23**, **25**] and [**27**].

The coefficients g and Δ of a rank 2 Drinfeld module $\varphi = (g, \Delta)$ over $\mathbf{C}$ are Drinfeld modular forms of respective weights $q-1$ and q^2-1 (see, for example, [**23**]), hence the j-invariant $j = g^{q+1}/\Delta$ of φ is a modular function. As such, all these quantities have Laurent series expansions, the Drinfeld module analogue of Fourier expansions. A detailed derivation of these expansions was given in [**8**, Section 5.4]. Here, the canonical uniformizer corresponding to the classical quantity $\exp(2\pi i z)$ is the function

$$t = t(z) = \frac{1}{\overline{\pi} z} \prod_{a \in \mathbf{A} \setminus \{0\}} \left(1 - \frac{z}{a}\right)^{-1} ,$$

where $\bar{\pi}$ serves as a normalizing factor analogous to the complex number $2\pi i$ in the classical case; see [**30**, Ch. 3] for a detailed computation of $\overline{\pi}$. For brevity, put

$$t_a = t(az) \qquad (a \in \mathbf{A} \setminus \{0\}) . \tag{2.3}$$

By [**23**] (see [**3**, Theorem 1.2] for the explicit expressions given here), the normalized coefficients $\bar{g}, \bar{\Delta}$ of φ have t-expansions

$$\begin{aligned} \bar{g}(z) &= \bar{\pi}^{1-q} g(z) = 1 - [1] \sum_{a \in \mathbf{A}^+} t_a^{q-1} , \\ \bar{\Delta}(z) &= \bar{\pi}^{1-q^2} \Delta(z) = -\bar{g}^q \sum_{a \in \mathbf{A}^+} t_a^{q-1} - [2] \sum_{a \in \mathbf{A}^+} t_a^{q^2-1} + \sum_{a \in \mathbf{A}^+} t_a^{q^2-q} , \end{aligned} \tag{2.4}$$

where we recall that $\mathbf{A}^+$ is the set of all monic polynomials in $\mathbf{A}$ and

$$[i] = T^{q^i} - T \in \mathbf{A} \qquad (i \in \mathbb{N}) \tag{2.5}$$

is the product of all monic irreducible polynomials in $\mathbf{A}$ whose degree divides i. The expansions in (2.4) only contain powers of t whose exponent is divisible by $q-1$. Putting

$$s = t^{q-1} ,$$

the t-expansions of $\bar{g}$ and $\bar{\Delta}$ over $\mathbf{A}$ are in fact s-expansions given as follows:

$$\begin{aligned} \bar{g}(s) &= 1 - [1]s - [1]s^{q^2-q+1} + [1]s^{q^2} - [1]\left([1] + \alpha\right) s^{q^2+1} + \dots , \\ \bar{\Delta}(s) &= -s + s^q - [1]s^{q+1} - s^{q^2-q+1} + s^{q^2} - \left([1] - [1]^q + \alpha\right) s^{q^2+1} + \dots , \end{aligned}$$

with $\alpha = 1$ if $q = 2$ and $\alpha = 0$ otherwise. The s-expansion of $j(z)$ is thus of the form

$$j(s) = \frac{\bar{g}(s)^{q+1}}{\bar{\Delta}(s)} = \sum_{i=0}^{\infty} a_i s^{i-1} , \qquad a_i \in \mathbf{A} , \quad a_0 = -1 . \tag{2.6}$$

The strong dependence of the s-expansions of g, Δ and j on q, the size of the base field, represents a subtle distinction from the elliptic curve scenario. Moreover, as q grows, these power series become sparser.

Similar to the classical setting, the j-invariant of a rank 2 Drinfeld module over $\mathbf{C}$ gives rise to a modular polynomial; see [**1**] for an analytic treatment of these objects. For $\mathfrak{n} \in \mathbf{A}$, the $\mathfrak{n}$-*th Drinfeld modular polynomial* $\Phi_{\mathfrak{n}}(X, j)$ is the minimal polynomial of $j(\mathfrak{n}z)$ over the function field $\mathbf{C}(j)$. Its coefficients are power series in s over $\mathbf{A}$. The roots of $\Phi_{\mathfrak{n}}(X, j)$ are precisely the j-invariants of rank 2 Drinfeld modules that are $\mathfrak{n}$-isogenous over $\mathbf{C}$ via an isogeny whose kernel is isomorphic to $\mathbf{A}/\mathfrak{n}\mathbf{A}$ as an $\mathbf{A}$-submodule of $\mathbf{C}$. As a polynomial in two variables X, Y, $\Phi_{\mathfrak{n}}(X, Y)$

has coefficients in $\mathbf{A}$ and is symmetric in X and Y, i.e. $\Phi_{\mathfrak{n}}(X,Y) = \Phi_{\mathfrak{n}}(Y,X)$. In our context, we restrict to the case where $\mathfrak{n} = \ell$ is a monic irreducible polynomial. In this case, $\Phi_\ell(X,Y)$ has degree $q^{\deg_T(\ell)}+1$ in both X and Y, with leading terms $X^{q^{\deg_T(\ell)+1}}$ and $Y^{q^{\deg_T(\ell)+1}}$. We compute the coefficients of $\Phi_\ell(X,Y)$ in $\mathbf{A}$ from the identity

$$\Phi_\ell(j(\ell z), j(z)) = 0\ , \tag{2.7}$$

where the s-expansions of $j(z)$ and $j(\ell z)$ over $\mathbf{A}$ are evaluated to sufficiently high precision. A complete analogue of Deuring's Lifting Theorem for elliptic curves holds for Drinfeld modules as well, see [**2**, Thm. 3.4]. Hence, two rank 2 Drinfeld modules over $\mathbb{L}$ are ℓ-isogenous if and only if $\Phi_\ell(X,Y)$ vanishes over $\mathbb{L}$ when evaluated at their two respective j-invariants.

3. Endomorphism rings and isogeny graphs in rank 2

As in the classical setting, the endomorphisms of a Drinfeld module φ over $\mathbb{L}$ form a ring under addition and composition, called the *endomorphism ring* of φ and denoted $\mathrm{End}_{\mathbb{L}}(\varphi)$. By identifying $\mathbf{A}$ with $\varphi(\mathbf{A})$, we see that $\mathrm{End}_{\mathbb{L}}(\varphi)$ contains an embedded copy of $\mathbf{A}$. Endomorphisms and isogenies of rank 2 Drinfeld modules over $\mathbb{L} = \mathbf{A}/P\mathbf{A}$ were investigated in detail by Gekeler in [**20**, **24**, **26**]; see also Yu [**49**]. They showed that $\mathrm{End}_{\mathbb{L}}(\varphi)$ is a free $\mathbf{A}$-module of rank at most 4 that contains the q^d-th power Frobenius

$$F = \tau^d\ ,$$

where $d = \deg_T(P)$. By [**34**] (see also [**8**, Thm. 6.3.9] for a proof of this identity), the characteristic polynomial of F is

$$P_\varphi(X) = X^2 - (-1)^d \left(\frac{\Delta}{P}\right)_{q-1}^{-1} H(\varphi)X + (-1)^d \left(\frac{\Delta}{P}\right)_{q-1}^{-1} P \in \mathbf{A}[X], \tag{3.1}$$

where $H(\varphi)$ is the Hasse invariant of φ and $(\Delta/P)_{q-1} \equiv \Delta^{(q^d-1)/(q-1)} \pmod P$ is the $(q-1)$-st power residue symbol of Δ in $\mathbb{L}$. Fast algorithms for computing $P_\varphi(X)$ can be found in [**39**, **40**]. Note that the constant coefficient of $P_\varphi(X)$ depends on φ which represents another difference to elliptic curves over a prime field $\mathbb{F}_p$, where this term is always p, independent of the curve. By [**24**, Thm. 3.5], two Drinfeld modules φ and ψ over $\mathbb{L}$ are isogenous if and only if $P_\varphi(X) = P_\psi(X)$.

An *imaginary quadratic function field* is a quadratic extension of $\mathbb{F}_q(T)$ in which the infinite place of $\mathbb{F}_q(T)$ is either ramified or inert. In analogy to the elliptic curve setting, when φ is ordinary, the roots of $P_\varphi(X)$ define an order in an imaginary quadratic function field $\mathcal{K}/\mathbb{F}_q(T)$ called the *Frobenius order* and denoted $\mathbf{A}[F]$. Then $\mathrm{End}_{\mathbb{L}}(\varphi)$ is isomorphic to an order $\mathcal{O}_\varphi$ of $\mathcal{K}$, called the *endomorphism order* of φ, that contains $\mathbf{A}[F]$. Moreover, all endomorphisms of an ordinary rank 2 Drinfeld module over $\mathbb{L}$ are defined over $\mathbb{L}$. Hence, in order to characterize the endomorphism ring of an ordinary rank 2 Drinfeld module φ, it suffices to identify the *conductor* of the associated endomorphism order $\mathcal{O}_\varphi$ in $\mathcal{K}$, i.e. the unique monic polynomial f_φ such that $\mathcal{O}_\varphi = \mathbf{A} + f_\varphi \mathcal{O}_\mathcal{K}$, where $\mathcal{O}_\mathcal{K}$ is the maximal order of $\mathcal{K}$. Note that f_φ divides the conductor f_F of $\mathbf{A}[F]$.

For completeness, we mention that if φ is ordinary with $j(\varphi) = 0$ (i.e. P has even degree), then $\mathcal{O}_\varphi = \mathbb{F}_{q^2}[T]$ and $\mathcal{K} = \mathbb{F}_{q^2}(T)$ [**2**, Rem. 3.3]. Moreover, the endomorphism ring of a supersingular rank 2 Drinfeld module φ is isomorphic to either an imaginary quadratic order or a maximal order in a quaternion algebra; see

[**49**, Props. 4 and 5] and [**8**, Thm. 6.4.2] for details and proofs. The full endomorphism ring of φ, i.e. the ring of endomorphisms of φ defined over $\overline{\mathbb{L}}$, is a maximal quaternion order if and only if φ is supersingular; see [**20**, Thm. 5.3].

In his doctoral dissertation [**36**], Kohel gave an algorithm for finding the endomorphism ring of an elliptic curve E over a finite field. When E is ordinary, the algorithm finds, for each prime ℓ dividing the Frobenius conductor, the exact power of ℓ dividing the conductor of the endomorphism order of E. This is accomplished by following a suitable path of ℓ-isogenies starting at E and ending at an elliptic curve whose endomorphism order is the Frobenius order. Following Kohel's characterization of all possible isogeny configurations and paths, Fouquet in her thesis [**16**] (see also [**17**]) described the complete ℓ-isogeny graph containing E and first coined the term *volcano* to visualize its structure. A careful and thorough analysis of Kohel's and Fouquet's reasoning, undertaken in [**8**, Chap. 7], reveals that the entire isogeny graph framework carries over to the setting of rank 2 Drinfeld modules.

For a monic irreducible polynomial $\ell \in \mathbf{A}$ distinct from P, the *ℓ-isogeny graph* $G_\ell(\mathbb{L})$ is defined as follows. The vertex set of $G_\ell(\mathbb{L})$ is $\mathbb{L}$, interpreted as the set of j-invariants — or equivalently, $\overline{\mathbb{L}}$-isomorphism classes — of rank 2 Drinfeld modules over $\mathbb{L}$. For any two vertices $j, j' \in \mathbb{L}$, an edge from j to j' is placed in $G_\ell(\mathbb{L})$ if and only if $\Phi_\ell(j, j') = 0$, and the number of edges from j to j' is the multiplicity of j as a root of $\Phi_\ell(X, j')$. In this way, $G_\ell(\mathbb{L})$ is a disconnected directed graph that may contain loops and multiple edges. Each connected component of $G_\ell(\mathbb{L})$ contains j-invariants of exclusively ordinary or supersingular Drinfeld modules.

Henceforth, we only consider the ordinary connected components of $G_\ell(\mathbb{L})$ not containing 0. Here, the edge multiplicities between any two vertices are symmetric, so we consider edges undirected by virtue of identifying each ℓ-isogeny with its dual. In any such component G, two j-invariants are adjacent if and only if the corresponding endomorphism orders are equal or the conductor of one is the product of ℓ and the conductor of the other. Then G takes on the beautiful shape of a *volcano*. The subgraph C of G consisting of the ℓ-isogenies joining isomorphism classes of Drinfeld modules with identical endomorphism orders is a (possibly degenerate) cycle called the *crater* of G. Its length is equal to the order of the ideal class of a prime ideal lying above ℓ in any of the endomorphism orders associated to vertices in C. Each vertex in C is the root of a (possibly degenerate) complete tree of the same height, called a *side* of G. The leaf nodes comprise the *floor* of G. The vertices at level i correspond precisely to those endomorphism orders whose conductor has ℓ-adic valuation i. Thus, vertices on the crater C correspond to endomorphism orders whose conductor is not a multiple of ℓ, and endomorphism orders of vertices on the floor of G have conductors whose ℓ-adic valuation matches that of the conductor of the Frobenius order. The number of neighbours of each vertex j in G is precisely the number of roots of $\Phi_\ell(X, j)$ in $\mathbb{L}$ which is 0, 1, 2 or $|\ell| + 1$, where $|\ell| = q^{\deg_T(\ell)}$; see [**8**, Table 7.3, p. 174] for details. As a result, the graph G is almost regular; if $G \setminus C$ is non-empty, then every internal vertex of G has degree $|\ell| + 1$. An example can be found in Figure 7.1.

All Drinfeld modules whose j-invariants are contained in G are isogenous over $\mathbb{L}$. So the number of vertices in G is bounded above by the size of the corresponding isogeny class, which is equal to the *Hurwitz class number* of the associated Frobenius

order $\mathbf{A}[F]$ ([**49**, Cor. to Prop. 7] and [**26**, Prop. 6.8]). This is the quantity

$$\mathcal{H}(\mathbf{A}[F]) = \sum_{f|f_F} h(\mathcal{O}_f) = h(\mathcal{O}_\mathcal{K}) \sum_{f|f_F} |f| \prod_{Q|f} \left(1 - \frac{\chi_\mathcal{K}(Q)}{|Q|}\right) . \tag{3.2}$$

Here, f_F is the Frobenius conductor, $\mathcal{O}_f$ is the order of conductor f in $\mathcal{K}$, $h(\mathcal{O}_f)$ is its ideal class number, $\mathcal{O}_\mathcal{K}$ is the maximal order of $\mathcal{K}$, $\chi_\mathcal{K}(Q) \in \{-1, 0, 1\}$ is the Kronecker symbol of Q (see, for example, [**26**, Sec. 7.6]), and the product in (3.2) runs over all the monic irreducible divisors Q of f. The second identity in (3.2) uses the fact that all orders in $\mathcal{K}$ have unit group $\mathbb{F}_q^*$, as $\mathcal{K}$ is imaginary. Since $|Q| \geq q$, $|\chi_\mathcal{K}(Q)| \leq 1$ for every Q dividing f, and the number of Q dividing f is at most $\deg_T(f)$, each term under the sum in (3.2) is bounded above by $(q+1)^{\deg_T(f)}$. Moreover, for each i with $0 \leq i \leq \deg_T(f_F)$, the number of monic factors of f_F of degree i is at most $\binom{\deg_T(f_F)}{i}$. It follows that

$$\begin{aligned}
\sum_{f|f_F} |f| \prod_{Q|f} \left(1 - \frac{\chi_\mathcal{K}(Q)}{|Q|}\right) &\leq \sum_{f|f_F} (q+1)^{\deg_T(f)} \\
&\leq \sum_{i=0}^{\deg_T(f_F)} \binom{\deg_T(f_F)}{i} (q+1)^i \\
&= (q+2)^{\deg_T(f_F)} .
\end{aligned}$$

By [**42**, Props. 14.6 and 14.7], we have $h(\mathcal{O}_\mathcal{K}) = 2^{1-c} h(\mathcal{K})$ where $h(\mathcal{K})$ is the degree zero divisor class number of $\mathcal{K}$ and c is the parity of $d = \deg_T(P)$, i.e. $c = 0$ if d is even and $c = 1$ if d is odd. The upper Hasse-Weil bound (see, for example, [**42**, Prop. 5.11]) asserts that $h(\mathcal{K}) \leq (\sqrt{q}+1)^{2g}$, where g is the genus of $\mathcal{K}$. Since $d = 2\deg(f_F) + 2g + 2 - c$, we obtain

$$\begin{aligned}
\mathcal{H}(\mathbf{A}[F]) &\leq 2^{1-c}(\sqrt{q}+1)^{2g}(q+2)^{\deg_T(f_F)} \\
&< 2^{1-c}(\sqrt{q}+1)^{2g+2\deg_T(f_F)} \\
&= 2^{1-c}(\sqrt{q}+1)^{d-2+c} . \qquad (3.3)
\end{aligned}$$

This estimate is an improvement over [**8**, Thm. 8.4.3].

4. Analyzing algorithms for Drinfeld modules

The remainder of this paper is devoted to computational aspects of rank 2 Drinfeld modules. In the next several sections, we present four algorithms for rank 2 Drinfeld modules that compute, respectively:

(1) the s-expansion of the j-function over $\mathbf{C}$ to a given precision (Section 5);
(2) the ℓ-th Drinfeld modular polynomial (Section 6);
(3) the collection of all isogenies of a given degree between two given rank 2 Drinfeld modules over $\mathbb{L}$ (Section 8);
(4) the dual isogeny of any given isogeny over $\mathbb{L}$ (Section 9).

In Section 7, we also describe how the modulo P reduction of the ℓ-th Drinfeld modular polynomial can be utilized to generate the full isogeny volcano and compute the endomorphism ring of an ordinary rank 2 Drinfeld module over $\mathbb{L}$ with non-zero j-invariant. Asymptotic run time and memory estimates are provided for all our procedures. All our algorithms were implemented in SAGE [**44**]; the code is available at [**7**]. We include a number of supporting numerical examples here.

We explain briefly how to measure the asymptotic time and space complexity of our algorithms. For consistency, we state all complexity results in terms of operations (for time) and elements (for space) in $\mathbb{F}_q$. Recall that $|a| = q^{\deg_T(a)}$ for any non-zero $a \in \mathbf{A}$. Our run times and space requirements are written as functions of q, $|P|$, $|\mathsf{n}|$, $\deg_T(P) = d$ and $\deg_T(\mathsf{n})$, where n is the degree of the isogeny under consideration. For our asymptotics, we assume $|P| \to \infty$ or $|\mathsf{n}| \to \infty$ or both; this includes the case $q \to \infty$. The complexity of Algorithm 5.1 is also a function of the precision N of the approximation to the j-invariant computed. We leave explicit dependencies on q in our formulas, so our O-constants are true constants, with no hidden dependencies on any parameters, including q.

In our algorithms, we perform arithmetic in the rings $\mathcal{R} = \mathbb{F}_q, \mathbb{L}$, $\mathbf{A}$, and the ring of truncated power series in s over $\mathbf{A}$. We denote by $M(n)$ the number of $\mathbb{F}_q$-operations required to multiply two polynomials of degree n with coefficients in $\mathbb{F}_q$; so $M(n) = O(n^2)$ for naive multiplication and $M(n) = O(n \log n)$ for fast arithmetic [**31**]. Using Newton iteration, this is also the cost of polynomial division with remainder when the numerator has degree n [**19**, Thm. 9.6]. One multiplication and one division in $\mathbb{L}$ each have cost $O(M(d))$ where $d = \deg_T(P)$. Computing q-th powers of polynomials over $\mathbb{F}_q$ is free; for elements in $\mathbb{L}$, this operation has cost $O(M(d))$. Multiplying two truncated power series over $\mathbf{A}$ of degree N in s for which each coefficient in $\mathbf{A}$ has T-degree bounded by n has cost $M(N)M(n)$. Evaluating a polynomial of degree n over some coefficient ring $\mathcal{R}$ can be done in $O(n)$ operations over $\mathcal{R}$ using Horner's method. We denote the number of $\mathbb{F}_q$-operations needed to find a root of a polynomial of degree n over $\mathbb{L} \cong \mathbb{F}_{q^d}$ by $R(n, d)$. Rabin's probabilistic algorithm [**41**] for example accomplishes this in an expected $O(M(d)nd \log d \log\log d \log q)$ $\mathbb{F}_q$-operations. Finally, every element of $\mathbb{L}$ requires storage of d elements in $\mathbb{F}_q$.

5. Computing the j-function over C

For a Laurent series in s over $\mathbf{A}$ given by

$$f(s) = \sum_{i=m}^{\infty} c_i s^i \qquad (m \in \mathbb{Z},\ c_i \in \mathbf{A},\ c_m \neq 0)\ ,$$

an *approximation of $f(s)$ to precision $N \in \mathbb{Z}$* is a Laurent polynomial $f_N(s) \in \mathbf{A}[s, s^{-1}]$ such that the coefficients of s^i in $f_N(s)$ and $f(s)$ agree for $m \leq i \leq N$. We use the notation $f_N(s) \equiv f(s) \pmod{s^{N+1}}$, keeping in mind that negative powers of s may appear in this congruence.

In this section, we present an algorithm for computing an approximation $j_N(s)$ to any precision N of the Laurent series expansion (2.6) of $j(s)$, along with an exact precision analysis and an asymptotic complexity estimate. The desired approximation $j_N(s)$ is obtained by generating approximations $\bar{g}_{N+2}(s)$ of $\bar{g}(s)$ and $\bar{\Delta}_{N+2}(s)$ of $\bar{\Delta}(s)$ from (2.4), and then computing the first $N+2$ coefficients of the quotient $\bar{g}_{N+2}^{q+1}/\bar{\Delta}_{N+2}$. In order to find $\bar{g}_{N+2}(s)$ and $\bar{\Delta}_{N+2}(s)$, we need to ascertain how many terms t_a^{q-1}, $t_a^{q^2-1}$, $t_a^{q^2-q}$, with $a \in \mathbf{A}^+$, need to be included in the sums appearing in (2.4). To that end, we use the results of [**23**, Sect. 4] to find the s-expansion of t_a^{q-1} and determine the truncation point.

When $a = 1$, we have $t_a^{q-1} = t^{q-1} = s$, so let $a \in \mathbf{A}$ be monic and non-constant. Then $t_a = t^{|a|} f_a(t)^{-1}$, where $f_a(X)$ is the *a-th inverse cyclotomic polynomial*.

Putting $h_a(s) = f_a(t)$, we obtain

$$t_a^{q-1} = \frac{s^{|a|}}{h_a(s)^{q-1}} = \frac{s^{|a|}h_a(s)}{1-(1-h_a(s))^q} = s^{|a|}h_a(s)\sum_{i=0}^{\infty}(1-h_a(s))^{qi} \ . \tag{5.1}$$

Let $m = \deg_T(a)$. Then

$$h_a(s) = \sum_{i=0}^{m}\beta_i s^{\frac{q^m-q^i}{q-1}} \in \mathbf{A}[s] \ , \tag{5.2}$$

where

$$\beta_0 = a, \qquad \beta_i = \frac{\beta_{i-1}^q - \beta_{i-1}}{[i]} \qquad (1 \le i \le m) \ ,$$

with $[i]$ given by (2.5). We have $\beta_m = 1$ and $\deg_T(\beta_i) \le (m-i)q^i$ for $0 \le i \le m$. A computationally more efficient way to compute the polynomials β_i is as follows. Write $a = \sum_{k=0}^{m} A_k T^k$ with $A_k \in \mathbb{F}_q$ and $A_m = 1$. Then

$$\beta_i = \sum_{k=i}^{m} A_k f_{i,k} \qquad (0 \le i \le m) \ , \tag{5.3}$$

where

$$f_{0,k} = T^k \ , \qquad f_{i,k} = \frac{f_{i-1,k}^q - f_{i-1,k}}{[i]} \quad (1 \le i \le k-1) \ , \qquad f_{k,k} = 1 \ , \tag{5.4}$$

for $0 \le k \le m$. We have $\deg_T(f_{i,k}) = (k-i)q^i$ for $0 \le i \le k \le m$; see [**8**, Appendix A.2] for a proof of (5.3) and the degree formula. Note that the polynomials $f_{i,k}$ only depend on q and are independent of a, hence they can be precomputed.

By [**23**, Eq. (10.10)], we have

$$\sum_{\substack{a\in\mathbf{A}^+\\ \deg_T(a)=m}} t_a^{q-1} = s^{\frac{q^{2m+1}+1}{q+1}} + \text{ higher order terms} \ .$$

Hence, in order to obtain approximations of $\bar{g}$ and $\bar{\Delta}$ to sufficient precision, we need to include in the computation of $\bar{g}_{N+2}$ and $\bar{\Delta}_{N+2}$ all monic polynomials a of degree m such that $(q^{2m+1}+1)/(q+1) \le N+2$. This yields an optimal degree bound of

$$\lambda = \left\lfloor \frac{\log_q\left(q(N+2)+N+1\right)-1}{2} \right\rfloor \ . \tag{5.5}$$

By (2.4), approximations of $\bar{g}$ and $\bar{\Delta}$ to precision $N+2$ are thus given by

$$\bar{g}_{N+2}(s) \equiv 1 - [1] \sum_{\substack{a\in\mathbf{A}^+\\ \deg_T(a)\le\lambda}} t_a^{q-1} \pmod{s^{N+3}} \ , \tag{5.6}$$

$$\begin{aligned}\bar{\Delta}_{N+2}(s) \equiv -\bar{g}_{N+2}^q \sum_{\substack{a\in\mathbf{A}^+\\ \deg_T(a)\le\lambda}} t_a^{q-1} - [2] \sum_{\substack{a\in\mathbf{A}^+\\ \deg_T(a)\le\lambda}} t_a^{q^2-1} \\ + \sum_{\substack{a\in\mathbf{A}^+\\ \deg_T(a)\le\lambda}} t_a^{q^2-q} \pmod{s^{N+3}} \ .\end{aligned} \tag{5.7}$$

Algorithm 5.1 computes an approximation of $j(s)$ to any given precision N. Its cost is analyzed in Theorem 5.1. We assume that the polynomials $f_{i,k}$ in (5.4) have been precomputed.

Algorithm 5.1 Computing an approximation to the j-function

Input: A prime power q and a non-negative integer N.
Output: An approximation $j_N(s)$ of the j-function $j(s)$ to precision N.

1: Compute λ as given in (5.5).
2: **for all** monic polynomials $a \in \mathbf{A}$ with $\deg(a) \leq \lambda$ **do**
3: Compute $h_a(s)$ using (5.2) and (5.3).
4: Compute $t_a^{q-1} \leftarrow s^{|a|} h_a(s)/h_a(s)^q \pmod{s^{N+3}}$.
5: Compute $t_a^{q^2-q} \leftarrow (t_a^{q-1})^q \pmod{s^{N+3}}$.
6: Compute $t_a^{q^2-1} \leftarrow t_a^{q-1} t_a^{q^2-q} \pmod{s^{N+3}}$.
7: **end for**
8: Compute $\bar{g}_{N+2}$ using (5.6).
9: Compute $\bar{g}_{N+2}^{q+1} \leftarrow \bar{g}_{N+2}\bar{g}_{N+2}^q \pmod{s^{N+3}}$.
10: Compute $\bar{\Delta}_{N+2}$ using (5.7).
11: Compute $j_N(s) \leftarrow \bar{g}_{N+2}^{q+1}/\bar{\Delta}_{N+2} \pmod{s^{N+3}}$.
12: **return** $j_N(s)$.

THEOREM 5.1. *Algorithm* 5.1 *computes the j-invariant to precision N in*

$$O\left(\sqrt{N}M(N)^2 + M(N)M(qN)\right)$$

operations in $\mathbb{F}_q$ and requires storage of $O(qN^2)$ elements of $\mathbb{F}_q$, as $q, N \longrightarrow \infty$. Here, $M(n)$ is the number of $\mathbb{F}_q$-operations required to multiply two polynomials in $\mathbb{F}_q[T]$ of degree n.

PROOF. The first summand in the run time estimate arises from steps 2-7 and the second summand from steps 9-11; the cost of step 8 is negligible in light of step 4. Again following [**23**], we note that the coefficient of s^i in the power series expansions of $h_a(s)$ and t_a has degree at most i in T; the same is thus true for $h_a(s)^{-q}$ (since the constant term of $h_a(s)$ is 1) and for powers of t_a. The coefficient of s^i in the power series expansions of $\bar{g}$, $\bar{g}^q$, $\bar{g}^{q+1}$, $\bar{\Delta}/s$, $s/\bar{\Delta}$ and j has degree at most qi in T; see [**3**].

The most expensive among steps 2-7 is step 6 which uses the result from step 4; the cost of steps 3 and 5 is negligible in comparison. Here, we multiply two truncated power series of precision $N+2$, each of whose coefficients has degree at most $N+2$, for a total cost of $M(N+2)^2$ operations in $\mathbb{F}_q$. The number of loop iterations is the same as the number of monic polynomials in $\mathbf{A}$ of T-degree at most λ, i.e.

$$\sum_{i=0}^{\lambda} q^i = \frac{q^{\lambda+1}-1}{q-1},$$

which is bounded, up to a constant, by $\sqrt{N}$. Hence the overall cost of steps 2-7 is $O(\sqrt{N}M(N)^2)$ operations in $\mathbb{F}_q$.

For the product $\bar{g}_{N+2}\bar{g}_{N+2}^q \pmod{s^{N+3}}$ in step 9, we multiply two truncated power series of length $N+3$, where the largest degree of any coefficient is $q(N+2)$. So this step requires $O(M(N)M(qN))$ operations in $\mathbb{F}_q$. The most expensive term to

compute in step 10 is the middle term in (5.7), also with a cost of $O(M(N)M(qN))$ operations in $\mathbb{F}_q$. The division step 11 has same cost as step 10.

Finally, Algorithm 5.1 stores truncated power series of precision at most $N+2$ with coefficients whose T-degree is at most $q(N+1)$. The total space requirement is thus $O(qN^2)$ elements in $\mathbb{F}_q$. □

Note that $O(qN^2)$ is in fact the size of the output of Algorithm 5.1. Our computations show that the bound λ in (5.5) is optimal; including only polynomials of degree $\leq \lambda - 1$ produced errors in the coefficients of $j_N(s)$.

We implemented Algorithm 5.1 in SAGE [**44**] and used it to compute j-functions over $\mathbb{F}_q$ for all prime powers $q \leq 100$. For the primes $q = 2, 3, 5, 7$, we used a degree bound of $\lambda = 2$, whereas for all other prime powers $q \leq 100$, we used $\lambda = 1$. Note that over $\mathbb{F}_7$, the algorithm produces the j-invariant to precision 2099 when the bound $\lambda = 2$ is used. For our largest prime $q = 97$, $\lambda = 1$ guarantees correctness to precision 9311. Thus, very few polynomials $a \in \mathbf{A}^+$ are needed to obtain $j_N(s)$ to quite high precision. Table 5.1 lists the j-functions to precision 9 for the primes $q = 2, 3, 5$ and to precision 13 for $q = 7$. Note the increasing level of sparsity, as q increases, of both $j(s)$ as a Laurent series in s and of its coefficients as polynomials in T.

TABLE 5.1. j-function approximations for q = 2,3,5, and 7

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

6. Computing Drinfeld modular polynomials

As in the analytic approach for computing classical modular polynomials — see, for example, the comments by Cohen [**10**] and Elkies [**14**] — the main obstacle to computing Drinfeld modular polynomials is the rapid growth of the size of the coefficients of both the j-function and the modular polynomial, along with the large number of coefficients of $j(s)$ required in the computation of the ℓ-th modular polynomial $\Phi_\ell(X,Y)$ as $|\ell|$ increases. Storage space for $\Phi_\ell(X,Y)$ is an additional resource issue that must be taken into account.

Throughout this section, let $\ell \in \mathbf{A}$ be a monic irreducible polynomial distinct from P. Our algorithm for computing the rank 2 Drinfeld modular polynomial $\Phi_\ell(X,Y)$ over $\mathbb{L}$ is based on the method of Bae-Lee [**3**] which uses the coefficients

of the j-invariant's s-expansion, combined with linear algebra. It follows the classical idea of obtaining the coefficients of $\Phi_\ell(X,Y)$ from (2.7), where the quantities $j(z)$ and $j(\ell z)$ in (2.7) are replaced by respective approximations to sufficient precision in s. Our main contributions here include analyses of the required precision for the Laurent series expansion of j and of the complexity, along with a SAGE implementation of the algorithm. To the best of our knowledge, this is the only general approach for computing Drinfeld modular polynomials to date; special cases were completed in [**43**] ($\ell = T$, $2 \leq q \leq 5$), [**3**, Example 4.6] ($\ell = T$, $q = 3$) and [**3**, Example 4.7] ($\deg(\ell) = 1$, $q = 2$). An analysis for computing modular polynomials attached to higher rank Drinfeld modules was given in [**5**], along with computations for rank 3 over $\mathbb{F}_3$ and the polynomial $\ell = T$.

We give a brief account of the construction in [**3**]. For brevity, put

$$L = \frac{(|\ell|+1)(|\ell|+2)}{2} .$$

Writing

$$\Phi_\ell(X,Y) = X^{|\ell|+1} + Y^{|\ell|+1} + \sum_{\mu=0}^{|\ell|}\sum_{\nu=0}^{\mu} w_{\mu,\nu} X^\mu Y^\nu + \sum_{\mu=1}^{|\ell|}\sum_{\nu=0}^{\mu-1} w_{\mu,\nu} X^\nu Y^\mu , \tag{6.1}$$

we need to compute the L coefficients $w_{\mu,\nu} \in \mathbf{A}$ for $0 \leq \nu \leq \mu \leq |\ell|$. Expanding (2.7) using (6.1) yields a linear system of L equations whose unknowns are the quantities $w_{\mu,\nu}$ and whose coefficients are polynomials in the coefficients of the s-expansions of $j(z)$, $j(\ell z)$ and their powers. Write these s-expansions as

$$j(\ell z) = \sum_{i=0}^{\infty} b_i s^{i-|\ell|} , \qquad j(z)^e = \sum_{i=0}^{\infty} a_i(e) s^{i-e} , \qquad j(\ell z)^e = \sum_{i=0}^{\infty} b_i(e) s^{i-e|\ell|}$$

for $1 \leq e \leq |\ell|+1$, and recall the s-expansion of $j(s)$ given in (2.6). Then $a_i(1) = a_i$ and $b_i(1) = b_i$ for all $i \geq 0$. The quantities $a_i(e)$ and $b_i(e)$ can be recursively obtained as

$$a_i(e) = \sum_{k=0}^{i} a_k(e-1) a_{i-k} , \qquad b_i(e) = \sum_{k=0}^{i} b_k(e-1) b_{i-k} \tag{6.2}$$

for $e \geq 1$. Define the sets

$$W = \{(\mu,\nu) \mid |\ell| \geq \mu \geq 0, \mu \geq \nu \geq 0\} ,$$
$$V = \{(k,h) \mid 0 \leq k \leq |\ell|, k \leq h \leq |\ell|\} ,$$

both of cardinality L. Here, W is the set of all pairs (μ,ν) for which we need to compute $w_{\mu,\nu}$ and V is the set of all pairs (k,h) that give the indices $i = k|\ell| + h$ of the coefficients $a_i(e)$ and $b_i(e)$ appearing in this computation.

For notational convenience, put $a_i = 0$ for $i < 0$. Then the aforementioned linear system can be written in matrix-vector form as $\mathbf{Mx} = \mathbf{y}$. Here, $\mathbf{x}$ is the column vector consisting of the unknown polynomials $w_{\mu,\nu} \in \mathbf{A}$ where (μ,ν) runs through the pairs in W in reverse lexicographic order, and $\mathbf{y} = (y_i)_{1 \leq i \leq L}$ is the column vector consisting of the polynomials

$$b_{k|\ell|+h}(|\ell|+1) + a_{k|\ell|+h-|\ell|^2+1}(|\ell|+1) ,$$

where (k,h) runs through the pairs in V in lexicographic order. The matrix $\mathbf{M} = (m_{ij})$ is given as follows. Let (k,h) be the i-th element in V in lexicographic

order and (μ,ν) the j-th element in W in reverse lexicographic order. Then

$$m_{i,j} = \begin{cases} c_{k|\ell|+h-|\ell|^2-|\ell|+\mu|\ell|+\nu}(\nu,\mu) + c_{k|\ell|+h-|\ell|^2-|\ell|+\nu|\ell|+\mu}(\mu,\nu) & \text{if } \mu \neq \nu, \\ c_{k|\ell|+h-|\ell|^2-|\ell|+\mu|\ell|+\nu}(\nu,\mu) & \text{if } \mu = \nu, \end{cases}$$

where

$$c_n(\mu,\nu) = \begin{cases} 0 & \text{if } n < 0\,, \\ \displaystyle\sum_{l=0}^{n} a_l(\mu) b_{n-l}(\nu) & \text{if } n \geq 0\,, \end{cases}$$

with particular values $c_0(0,0) = 1$ and $c_n(\mu,0) = a_n(\mu)$, $c_n(0,\nu) = b_n(\nu)$ for $n \geq 0$. Then $\mathbf{M}$ is a lower triangular square matrix of size L whose diagonal entries are all ± 1 as $c_0(\mu,\nu) = (-1)^{\mu+\nu}$. Hence, the unknown coefficients $w_{\mu,\nu}$ of $\Phi_\ell(X,Y)$ can be determined iteratively via forward substitution:

$$\begin{aligned} w_{|\ell|,|\ell|} &= \frac{y_1}{m_{1,1}}\,, \\ w_{|\ell|,|\ell|-1} &= \frac{y_2 - m_{2,1} w_{|\ell|,|\ell|}}{m_{2,2}}\,, \\ &\vdots \\ w_{0,0} &= \frac{y_L - \left(m_{L,1} w_{|\ell|,|\ell|} + m_{L,2} w_{|\ell|,|\ell|-1} + \cdots + m_{L,L-1} w_{1,0}\right)}{m_{L,L}}\,. \end{aligned} \tag{6.3}$$

The formulas in (6.3) involve the coefficients $a_i(e), b_i(e)$ for $0 \leq i \leq |\ell|^2 + |\ell|$ and $1 \leq e \leq |\ell| + 1$. By (6.2), it is thus sufficient to precompute a_i and b_i for $0 \leq i \leq |\ell|^2+|\ell|$, so we generate approximations of the s-expansions of $j(z)$ and $j(\ell z)$ to respective precisions $|\ell|^2 + |\ell| - 1$ and $|\ell|^2$. The former can be obtained via Algorithm 5.1. For the latter, we replace $s = s(z)$ in $j(z)$ by $s(\ell z) = t_\ell^{q-1}$ as given in (5.1) (with $a = \ell$) and evaluate the expression

$$s^{|\ell|} j(\ell z) = \frac{s^{|\ell|}}{t_\ell^{q-1}} \sum_{i=0}^{\infty} a_i t_\ell^{(q-1)i} = h_\ell(s)^{q-1} \sum_{i=0}^{\infty} a_i \left(s^{|\ell|} h_\ell(s) \sum_{k=0}^{\infty} (1 - h_\ell(s))^{rk} \right)^i$$

modulo $s^{|\ell|^2+|\ell|+1}$. Algorithm 6.1 presents the procedure described above in algorithmic form.

THEOREM 6.1. *Algorithm* 6.1 *computes the coefficients* $w_{\mu,\nu}$ *of the modular polynomial* $\Phi_\ell(X,Y)$ *as given in* (6.1) *in*

$$O\left(|\ell|^6 M(q|\ell|^2)\right)$$

$\mathbb{F}_q$*-operations and requires storage of* $O(q|\ell|^6)$ *elements of* $\mathbb{F}_q$*, as* $|\ell| \longrightarrow \infty$*. Here,* $M(n)$ *is the number of* $\mathbb{F}_q$*-operations required to multiply two polynomials in* $\mathbb{F}_q[T]$ *of degree* n*.*

PROOF. We will see that the run time and required space are dominated by steps 5-15. By [**3**, Lem. 3.1], we have $\deg_T(a_i(e)) \leq qi$; similarly, $\deg_T(b_i(e)) \leq qi$ for all $i \geq 0$ and $e \geq 1$. It follows that the cost of each exponentiation in steps 2 and 3 is $O\left(M(|\ell|^2)M(q|\ell|^2)\right)$ operations in $\mathbb{F}_q$, for a total cost of $O\left(|\ell|M(|\ell|^2)M(q|\ell|^2)\right)$ operations in $\mathbb{F}_q$ for steps 1-4. For $1 \leq e \leq |\ell| + 1$ and

Algorithm 6.1 Computing the modular polynomial $\Phi_\ell(X,Y)$

Input: A prime power q, a monic irreducible polynomial $\ell \in \mathbb{F}_q[T]$, an approximation $\sum_{i=0}^{|\ell|^2+|\ell|} a_i s^{i-1}$ of $j(z)$ to precision $|\ell|^2+|\ell|-1$, and an approximation $\sum_{i=0}^{|\ell|^2+|\ell|} b_i s^{i-|\ell|}$ of $j(\ell z)$ to precision $|\ell|^2$.

Output: The coefficients $w_{\mu,\nu}$ of the modular polynomial $\Phi_\ell(X,Y)$ as given in (6.1).

for $e = 2$ to $|\ell|+1$ **do**
  Compute $j(z)^e \equiv \sum_{i=0}^{|\ell|^2+|\ell|} a_i(e) s^{i-e} \pmod{s^{|\ell|^2+\ell}}$ via (6.2)
  Compute $j(\ell z)^e \equiv \sum_{i=0}^{|\ell|^2+|\ell|} b_i(e) s^{i-e|\ell|} \pmod{s^{|\ell|^2+1}}$ via (6.2).
end for
for $\mu = 0$ to $|\ell|$ **do**
  for $\nu = 0$ to $|\ell|$ **do**
    $c_0(\mu,\nu) \leftarrow (-1)^{\mu+\nu}$
    for $i = 1$ to $|\ell|^2+|\ell|$ **do**
      $c_i(\mu,\nu) \leftarrow 0$
      for $n = 0$ to i **do**
        $c_i(\mu,\nu) \leftarrow c_i(\mu,\nu) + a_n(\mu) b_{i-n}(\nu)$
      end for
    end for
  end for
end for
Construct the ordered sets
  $W = \{(\mu,\nu) \mid |\ell| \geq \mu \geq 0, \mu \geq \nu \geq 0\}$ in reverse lexicographic order
  $V = \{(k,h) \mid 0 \leq k \leq |\ell|, k \leq h \leq |\ell|\}$ in lexicographic order
for $i = 1$ to $(|\ell|+1)(|\ell|+2)/2$ **do**
  Let (k,h) be the i-th element in V (in lexicographic order).
  if $k|\ell| + h < |\ell|^2 - 1$ **then**
    $y_i \longleftarrow b_{k|\ell|+h}(|\ell|+1)$
  else
    $y_i \longleftarrow b_{k|\ell|+h}(|\ell|+1) + a_{k|\ell|+h-|\ell|^2+1}(|\ell|+1)$.
  end if
end for
for $i = 1$ to $(|\ell|+1)(|\ell|+2)/2$ **do**
  for $j = 1$ to i **do**
    Let (k,h) be the i-th element in V (in lexicographic order)
    Let (μ,ν) be the j-th element in W (in reverse lexicographic order).
    if $\mu = \nu$ **then**
      $m_{i,j} \leftarrow c_{k|\ell|+h-|\ell|^2-|\ell|+\mu|\ell|+\mu}(\mu,\mu)$
    else
      $m_{i,j} \leftarrow c_{k|\ell|+h-|\ell|^2-|\ell|+\mu|\ell|+\nu}(\nu,\mu) + c_{k|\ell|+h-|\ell|^2-|\ell|+\nu|\ell|+\mu}(\mu,\nu)$
    end if
  end for
end for
Compute $w_{\mu,\nu}$, $(\mu,\nu) \in W$ (in reverse lexicographic order) via (6.3)
return $w_{\mu,\nu}$, $0 \leq \nu \leq \mu \leq |\ell|$.

$0 \le i \le |\ell|^2 + |\ell|$, each coefficient $a_i(e), b_i(e)$ requires storage of $qi+1$ elements of $\mathbb{F}_q$. So steps 1-4 require space

$$2\,(|\ell|+1)\sum_{i=0}^{|\ell|^2+|\ell|}(qi+1) = O(q|\ell|^5)\ .$$

The innermost loop (steps 10-12) inside steps 5-15 executes

$$(|\ell|+1)^2(|\ell|^2+|\ell|)(|\ell|^2+|\ell|+1)/2$$

times, and each iteration performs multiplication of two polynomials of degree at most $q(|\ell|^2+|\ell|)$, for a total cost of $O(|\ell|^6 M(q|\ell|^2))$ operations in $\mathbb{F}_q$. Since $\deg_T(a_n(\mu)) \le qn$ and $\deg_T(b_{i-n}(\nu)) \le q(i-n)$, we see that $\deg_T(c_i(\mu,\nu)) \le qi$ for $0 \le \mu, \nu \le |\ell|$ and $0 \le i \le |\ell|^2+|\ell|$. It follows that we store $(|\ell|+1)^2(|\ell|^2+|\ell|+1)$ polynomials $c_i(\mu,\nu)$ in steps 5-15, each of degree at most $q(|\ell|^2+|\ell|)$. The total storage requirement for these steps is thus $O(q|\ell|^6)$ elements in $\mathbb{F}_q$.

Steps 16-24 and 25-35 require negligible run time and storage compared to steps 5-15. Step 36 computes $(|\ell|+1)^2$ quantities $w_{\mu,\nu}$, among which $w_{0,0}$ is the most costly, requiring $(|\ell|+1)(|\ell|+2)/2-1$ polynomial multiplications and additions. Moreover, for all i,j, we have $\deg_T(m_{i,j}) \le q(|\ell|^2+|\ell|)$ and $\deg_T(w_{\mu,\nu}) \le q|\ell|(|\ell|+1)^2/2$ by (6.4) below (see [**3**, Cor. 3.8]). Hence, these loops require a total of $O(|\ell|^4 M(q|\ell|^3))$ operations in $\mathbb{F}_q$ and storage of $O(q|\ell|^6)$ elements in $\mathbb{F}_q$. For both schoolbook and fast multiplication, this run time estimate does not exceed $O(|\ell|^6 M(q|\ell|)^2)$. □

On first glance, the complexity of Algorithm 6.1 as determined in Theorem 6.1 looks significantly higher than the asymptotic run time estimates for computing classical modular polynomials. Assuming fast multiplication techniques, it amounts to $O(q|\ell|^{8+\varepsilon})$ operations in $\mathbb{F}_q$. In contrast, Elkies [**14**] estimated the run time of the analytic method for computing the classical ℓ-th modular polynomial to be $O(\ell^{4+\varepsilon})$ arithmetic operations; this estimate was subsequently refined to $O(\ell^{4.5+\varepsilon})$ bit operations by Charles-Lauter [**9**]. Enge [**15**] and Bröker-Lauter-Sutherland [**6**] introduced methods with expected run time $O(\ell^{3+\varepsilon})$ under reasonable assumptions. The reason for this significant discrepancy between classical and Drinfeld modular polynomial computation arises from the different growth rates of the coefficients of $\Phi_\ell(X,Y)$ and of j and its powers in the two settings.

In the elliptic curve setting, a lower bound of $\Omega(\sqrt{ei})$ on the bit length of the i-th Fourier coefficient of $j(z)^e$ is given in [**9**], whereas for Drinfeld modules, the analogous coefficients are estimated to have a degree that grows as qi. For e and i of magnitudes ℓ and ℓ^2, respectively, the classical bound is of order $\ell^{3/2}$, whereas in the Drinfeld module setting, the maximum coefficient degree is obtained for $i = |\ell|^2+|\ell|$ (independent of e) and has degree of order $q|\ell|^2$. Moreover, the s-expansions of $\bar{g}$ and $\bar{\Delta}$ seem to grow sparser as q increases, and sparsity was not taken into account in our run time estimates.

Another major difference is in the behaviour of the modular polynomial itself. The *logarithmic height* of the Drinfeld modular polynomial $\Phi_\ell(X,Y)$ is the quantity

$$H = \max_{(\mu,\nu)\in W}\{\deg_T(w_{\mu,\nu})\}\ ;$$

it is the natural analogue of the classical logarithmic height. Bae-Lee [**3**] proved

$$\frac{|\ell|}{q} \leq H \leq \frac{q|\ell|(|\ell|+1)^2}{2} , \tag{6.4}$$

which necessitates up to $O(q|\ell|^5)$ elements in $\mathbb{F}_q$ to store $\Phi_\ell(X,Y)$. In stark contrast, the logarithmic height of the classical ℓ-th modular polynomial is asymptotic to $6\ell\log(\ell)$ (see Cohen [**10**]). This yields an upper bound of order $B=\ell^3$ (discounting log factors) on the size of this polynomial, so the complex analytic approach for computing the modular polynomial has run time $O(B^{1.5+\varepsilon})$ and the algorithms of [**15**] and [**6**] are essentially optimal, with a quasilinear run time of $O(B^{1+\varepsilon})$. Assuming the corresponding best known approximate coefficient bound of $|\ell|^3$ as given in (6.4) estimates the size of the ℓ-th Drinfeld modular polynomial as $B=|\ell|^5$ and the run time of Algorithm 6.1 as $O(B^{1.6+\varepsilon})$. Exact degree bounds on the coefficients of $\Phi_\ell(X,Y)$ are not known. Our computations strongly suggest that at least for linear ℓ, we have $H=q(|\ell|^2+|\ell|)$.

Example 6.2 lists three Drinfeld modular polynomials produced by our SAGE implementation of Algorithm 6.1. Recall from Section 2 that, for $\ell \neq P$, two rank 2 Drinfeld modules over $\mathbb{L}$ are ℓ-isogenous over $\mathbb{L}$ if and only if the modular polynomial $\Phi_\ell(X,Y)$ vanishes in $\mathbb{L}$ when evaluated at their respective j-invariants.

EXAMPLE 6.2. Let $q=3$, $P(T)=T^5+2T+1$ and $\mathbb{L}=\mathbb{F}_3[T]/P\mathbb{F}_3[T]$.

(1) Recall from Example 2.2 that the rank 2 Drinfeld modules $\varphi=(T^2,T^3)$ and $\psi=(2T^4+T^2,2T^4+T+2)$ are isogenous via the T-isogeny $u=\tau-(T^3+2T+2)$. The two respective j-invariants are $j(\varphi)=T+2$ and $j(\psi)=2T^4+T^3+2T^2+T+2$. Over $\mathbb{L}$, we have

$$\begin{aligned}\Phi_T(X,T+2) = X^4 &+ (2T^3+1)X^3 + (T^3+2T^2+1)X^2 \\ &+ (T^3+2T^2+T+1)X + 2T^3+T^2+2T+1 .\end{aligned}$$

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

$$\begin{aligned} &T^4+T^2+T+2 , && T^4+T^3+2T^2 , \\ &2T^4+2T^3+T^2+T+1 , && 2T^4+T^3+2T^2+T+2=j(\psi) .\end{aligned}$$

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

(2) The rank 2 Drinfeld module $\varphi=(T^2,T^2+2T)$ is $(T+1)$-isogenous to $\psi=(2T^4+2T+2,2T^3+T^2+2T)$ via the $(T+1)$-isogeny $u=\tau-(T^2+2)$. The two respective j-invariants are $j(\varphi)=T^2$ and $j(\psi)=T^4+2T^3+T^2$. The polynomial

$$\begin{aligned}\Phi_{T+1}(X,T^2) = X^4 &+ (2T^4+T^3+2T+1)X^3 + (2T^4+2T^3+2T^2)X^2 \\ &+ (2T^3+2T^2+2T+1)X + T^2\end{aligned}$$

over $\mathbb{L}$ has two roots in $\mathbb{L}$, namely $2T^3+T$ and $j(\psi)=T^4+2T^3+T^2$.

(3) From Example 2.2, $\varphi=(T^3,T^4+1)$ and $\psi=(2T^4+1,T^4+T^3+T^2+1)$ are $(T+2)$-isogenous via $u=\tau-(T^3+T)$. We have

$$\begin{aligned} j(\varphi) &= T^4+T^3+T^2+2T+2 , \\ j(\psi) &= 2T^4+2T^3+2T+2 ,\end{aligned}$$

and

$$\Phi_{T+2}(X, j(\varphi)) = X^4 + (T^4 + 2T^3 + 2T^2 + 1)X^3 + (2T^4 + T + 2)X^2 + (2T^4 + T^3 + 2T^2 + T)X + T^4 + T^2 + 2T \ .$$

This polynomial has four roots in $\mathbb{L}$, namely

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

In Example 6.2, we observed the vanishing of the modular polynomial Φ_ℓ on the pairs of ℓ-isogenous j-invariants introduced independently in Example 2.2. This serves as a check on the correctness of our algorithms. Using Algorithm 6.1, we computed all the Drinfeld modular polynomials for the following parameters:

(1) $\ell = T$ and all prime powers q with $2 \leq q \leq 25$;
(2) $\ell = T + \varepsilon$ with $\varepsilon \in \mathbb{F}_q^*$ for all primes q with $2 \leq q \leq 23$;
(3) all monic irreducible polynomials $\ell \in \mathbf{A}$ of degree 2 for $q = 2, 3, 5$.

Examples can be found in [**8**, Sec. A.1]. In all our numerical examples for linear ℓ, the logarithmic height H of $\Phi_\ell(X, Y)$ was equal to $q^2(q+1) = q(|\ell|^2 + |\ell|)$. Our computations agree with the numerical examples of [**3**] and [**43**]. In addition to Example 6.2, we verified ℓ-isogeny via the modular polynomial test for many Drinfeld modules obtained from Proposition 2.1. This verification was performed for $q = 3, 5, 7$, $\ell = T + \varepsilon$ with $\varepsilon \in \mathbb{F}_q$, and monic irreducible polynomials of degrees d with $2 \leq d \leq 5$. We also verified that all the modular polynomials we computed satisfy the *Kronecker congruence* (see [**1**])

$$\Phi_\ell(X, j) \equiv (X - j^{|P|})(X^{|P|} - j) \pmod{\ell} \ .$$

7. Applications: Computing isogeny volcanoes and endomorphism rings

As before, let $\ell \in \mathbf{A}$ be a monic irreducible polynomial different from P, and let $\varphi = (g, \Delta)$ be an ordinary rank 2 Drinfeld module over $\mathbb{L}$ with $j(\varphi) \neq 0$. Two applications that utilize the reduction modulo P of the ℓ-th modular polynomial $\Phi_\ell(X, Y)$ over $\mathbb{L}$ are to compute the isogeny volcano containing $j(\varphi)$ and the endomorphism order of φ. By (6.4), storing $\Phi_\ell(X, Y) \pmod{P}$ requires up to $O(|\ell|^2 \min\{q|\ell|^3, d\})$ elements in $\mathbb{F}_q$.

The isogeny volcano G of φ is generated through a relatively straightforward graph generation algorithm using repeated root finding. It maintains a subset of $\mathbb{L}$ of visited vertices (initialized to only contain $j(\varphi)$), a subset of $\mathbb{L}$ of unvisited vertices (initialized to contain the set of roots of $\Phi_\ell(X, j(\varphi))$ in $\mathbb{L}$ distinct from $j(\varphi)$, with multiplicities), and a set of edges (initialized as empty). At every stage, the algorithm computes all the roots of $\Phi_\ell(X, u)$ in $\mathbb{L}$ where u is unvisited. All these roots are marked as unvisited, u is flagged as visited, and for every root j, we add as many edges $\{j, u\}$ as the multiplicity of the root j of $\Phi_\ell(X, u)$, provided no such edges are as yet present. The algorithm terminates if either a root 0 is encountered or all roots in $\mathbb{L}$ have been visited. The space requirement of this procedure is determined by the size of $\Phi_\ell(X, Y) \pmod{P}$ and the size of the output G which is bounded by (3.3). The asymptotic run time is at most $O\left((\sqrt{q}+1)^{d-2+c} R(|\ell|, d) M(d)\right)$ where $R(|\ell|, d)$ accounts for finding roots of $\Phi_\ell(X, u)$ and the $M(d)$ term converts arithmetic in $\mathbb{L}$ to arithmetic in $\mathbb{F}_q$.

In practice, assuming that $\Phi_\ell(X,Y) \pmod P$ is a known input to this algorithm is problematic. Unlike Sutherland's extensive online table of classical modular polynomials [**45**], there is no readily available database of Drinfeld modular polynomials.

We implemented isogeny volcano computation in SAGE [**44**] and produced a substantial collection of examples; see [**8**, Sect. 8.4 and Appendix B]. For illustrative purposes, we include a small example here.

EXAMPLE 7.1. Let $q = 3$, $P(T) = T^7 + 2T^2 + 1$ and $\ell = T$. Figure 7.1 depicts the T-isogeny volcano for the ordinary Drinfeld module $\varphi = (T, T^3 + 2T^2 + 2T)$ over $\mathbb{L} = \mathbb{F}_3[T]/P\mathbb{F}_3[T]$ whose j-invariant is

$$j(\varphi) = 2T^6 + 2T^4 + 2T^3 + T^2 + 2T + 2 \ .$$

Its crater has length 3, each of its internal vertices has 4 neighbours, and each of its 3 sides is a complete ternary tree of height 2. This isogeny volcano was produced by our SAGE implementation and was also drawn using SAGE.

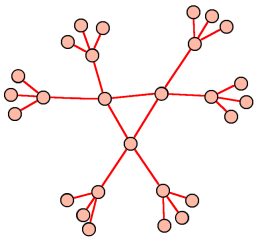

FIGURE 7.1. Arial view of the T-isogeny volcano containing $j = 2T^6 + 2T^4 + 2T^3 + T^2 + 2T + 2$ over $\mathbb{L} = \mathbb{F}_3[T]/P\mathbb{F}_3[T]$ with $P(T) = T^7 + 2T^2 + 1$.

The reduction $\pmod P$ of $\Phi_\ell(X,Y)$ can also be used to compute endomorphism rings. The concept behind Kohel's algorithm for finding the endomorphism order of an elliptic curve is to locate it in its connected component of the isogeny graph, thereby generating a small subgraph of this component in the process. In the context of point counting, the search was subsequently refined by Fouquet [**16**, **17**] who exploited the fact that every vertex j in a volcano is adjacent to at most two other vertices on or closer to the crater, and hence to at least one vertex that is closer to the floor. Combining their two approaches leads to a technique for finding the endomorphism ring of a rank 2 Drinfeld module.

Let φ be an ordinary rank 2 Drinfeld module that is not isogenous to one with j-invariant 0. Then its endomorphism ring $\mathrm{End}_{\mathbb{L}}(\varphi)$ is isomorphic to an imaginary quadratic order $\mathcal{O}_\varphi$ that is uniquely determined by its conductor f_φ in the associated maximal order. The conductor f_φ is in turn determined by the ℓ-adic valuations $v_\ell(f_\varphi)$ for each monic irreducible polynomial ℓ dividing the Frobenius conductor f_F. Entirely analogous to the elliptic curve setting, we find each $v_\ell(f_\varphi)$ as the level where $j(\varphi)$ is situated inside its ℓ-isogeny volcano $G \subset G_\ell(\mathbb{L})$. The height of G is $n = v_\ell(f_F)$. Any path of isogenies from $j(\varphi)$ to the floor of G has length $m = v_\ell(f_F/f_\varphi)$, so $v_\ell(f_\varphi) = n - m$. Fouquet's idea was to grow three simultaneous ℓ-isogeny paths in G starting at $j(\varphi)$. If $j(\varphi)$ is located in the crater of G, then at least one of these paths moves down from level 0 to level 1; otherwise,

at least two of the paths move down a level. Avoiding backtracking ensures that at least one of the three paths is a direct path from $j(\varphi)$ to the floor of G. We stop growing a path if either its length exceeds the height n or visits a vertex of degree 1, in which case the floor of G is reached.

The paths are grown similar to the isogeny volcano construction and require the polynomial $\Phi_\ell(X,Y) \pmod P$. At every vertex j in a path, we compute the roots of $\Phi_\ell(X,j)$ in $\mathbb{L}$ and choose as the next vertex one of these roots that is not already contained in this path. The first path to reach the floor has length $n-m \le n \le (d-1)/2$. Hence, the asymptotic run time of this procedure is bounded by $O\left(dR(|\ell|,d)M(d)\right)$. The paths need storage of at most $3d(d-1)/2$, which is vastly dominated by the size of $\Phi_\ell(X,Y) \pmod P$. We give a small example to illustrate the strategy.

EXAMPLE 7.2. Let $q=3$, $P(T)=T^{11}+2T^2+1$ and $\ell=T$. Let $\varphi=(g,\Delta)$ be the ordinary rank 2 Drinfeld module over $\mathbb{L}=\mathbb{F}_3[T]/P\mathbb{F}_3[T]$ given by

$$g = T^{10}+T^8+T^7+T^5+T^4+T^3+2T+2\ , \qquad \Delta = T^3\ ,$$

with j-invariant

$$j_0 = j(\varphi) = 2T^9+T^8+T^7+2T^6+T^3+2T^2+2T\ .$$

The Frobenius polynomial associated to φ is

$$P_\varphi(X) = X^2-(2T^4+2T^2+2)X+(T^{11}+2T^2+1)$$

and has discriminant $2T^6(T^2+T+2)(T^3+2T^2+2T+2)$. Hence, the Frobenius conductor is $f_F = T^3$, so no T-isogeny path starting at j_0 should grow beyond length 3. Using the procedure described above, we obtain the following paths P_1, P_2, P_3 from j_0 to the floor of the isogeny volcano containing j_0:

$$\begin{aligned}
P_1:\quad & j_0 = 2T^9+T^8+T^7+2T^6+T^3+2T^2+2T\ ,\\
& j_1 = T^9+2T^6+T^5+2T^4+T^3+2T+1\ ,\\
& j_2 = T^5+2T^4+2T^3+2T^2+2\ ,\\
& j_3 = T^9+2T^8+T^7+T^5+T^3+2T^2+1\ ,\\[1ex]
P_2:\quad & j_0 = 2T^9+T^8+T^7+2T^6+T^3+2T^2+2T\ ,\\
& j_1 = T^9+T^8+T^7+2T^6+2T^5+T^3+2T^2+1\ ,\\[1ex]
P_3:\quad & j_0 = 2T^9+T^8+T^7+2T^6+T^3+2T^2+2T\ ,\\
& j_1 = 2T^7+T^6+2T^5+T^4+2T^3+2T\ .
\end{aligned}$$

Both P_2 and P_3 are of length 1. So $\nu_T(f_\varphi) = 3-1 = 2$, and hence $f_\varphi = T^2$. Thus, j_0 is located at level 2 of the volcano, see Figure 7.2. It follows that P_2 and P_3 both went straight down to the floor, whereas P_1 moved up to level 1.

We note that a method for computing endomorphism rings of Drinfeld modules of arbitrary rank was given in [**18**]. It finds the desired endomorphism ring modulo that of Frobenius by entirely different means. Another approach for arbitrary rank can be found in [**37**].

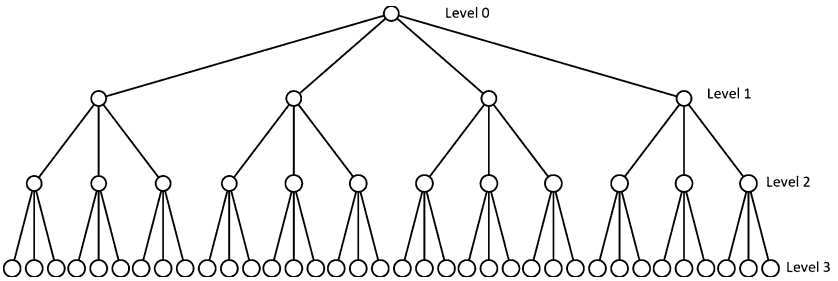

FIGURE 7.2. Profile view of the T-isogeny volcano containing $j = 2T^9+T^8+T^7+2T^6+T^3+2T^2+2T$ over $\mathbb{L} = \mathbb{F}_3[T]/P\mathbb{F}_3[T]$ with $P(T) = T^{11}+2T^2+1$.

8. Computing explicit isogenies

It is possible to establish $\mathfrak{n}$-isogeny between two given rank 2 Drinfeld modules directly and construct an $\mathfrak{n}$-isogeny between them if one exists. For any one pair of Drinfeld modules with parameters of modest size, this method of isogeny detection may be preferable over resorting to modular polynomials. However, when processing many Drinfeld modules at once, for example in ℓ-isogeny volcano or endomorphism ring computation, this method is not efficient.

Let $\varphi = (g, \Delta)$ and $\psi = (g', \Delta')$ be two rank 2 Drinfeld modules over $\mathbb{L}$. We may assume that φ and ψ are not isomorphic as this can easily be checked: by [**20**, Lem. 4.1], φ and ψ are isomorphic if and only if there exists $c \in \mathbb{L}^*$ such that $g = c^{q-1}g'$ and $\Delta = c^{q^2-1}\Delta'$. The brute-force approach now described finds all the $\mathfrak{n}$-isogenies $u : \varphi \to \psi$ over $\mathbb{L}$ or establishes that no such $\mathfrak{n}$-isogeny exists.

For brevity, put $k = \deg_T(\mathfrak{n})$. A (hypothetical) $\mathfrak{n}$-isogeny $u : \varphi \to \psi$ is a polynomial in $\mathbb{L}\{\tau\}$ of degree k given by

$$u = \sum_{i=0}^{k} u_i \tau^i \qquad (u_i \in \mathbb{L},\ u_k \neq 0)\ .$$

The coefficients of u can be determined symbolically from the identity $u\varphi_T = \psi_T u$. By comparing coefficients of the powers of τ in this identity, we obtain a system of $k+3$ equations

$$\begin{aligned}
u_0 T &= T u_0\ , \\
u_0 g + u_1 T^q &= T u_1 + g' u_0^q\ , \\
u_0 \Delta + u_1 g^q + u_2 T^{q^2} &= \Delta' u_0^{q^2} + g' u_1^q + T u_2\ , \\
&\vdots \\
u_{k-2}\Delta^{q^{k-2}} + u_{k-1} g^{q^{k-1}} + u_k T^{q^k} &= \Delta' u_{k-2}^{q^2} + g' u_{k-1}^q + T u_k\ , \\
u_{k-1}\Delta^{q^{k-1}} + u_k g^{q^k} &= \Delta' u_{k-1}^{q^2} + g' u_k^q\ , \\
u_k \Delta^{q^k} &= \Delta' u_k^{q^2}\ ,
\end{aligned} \tag{8.1}$$

in the unknowns u_i for $i = 0, 1, \ldots, k$. We solve the last $k+1$ equations of (8.1). The last equation forces

$$u_k^{q^2-1} = y \quad \text{with} \quad y = \Delta^{q^k}/\Delta' \,.$$

Thus, a necessary condition for the existence of an n-isogeny $u : \varphi \to \psi$ over $\mathbb{L}$ is the existence of a (q^2-1)-st root of y in $\mathbb{L}$. One can *a priori* verify the existence of such a root by checking whether $y^{(q^d-1)/e} = 1$ in $\mathbb{L}$, where

$$e = \gcd(q^d - 1, q^2 - 1) = \begin{cases} q-1 & \text{if } d \text{ is odd}\,, \\ q^2-1 & \text{if } d \text{ is even}\,. \end{cases}$$

Furthermore, if y has a (q^2-1)-st root in $\mathbb{L}$, then it has exactly e such roots in $\mathbb{L}$. We may choose any one of them, since all the roots just differ by a factor that is a root of unity in $\mathbb{L}$. For example, we can make a canonical choice by requiring u_k to be monic as a polynomial in $\mathbf{A}$ modulo P.

By virtue of (8.1), we rule out non-existence of u, and compute its coefficients if an n-isogeny $u : \varphi \to \psi$ exists, by finding the roots in $\mathbb{L}$ of the following polynomials:

$$\begin{aligned} &\text{For } u_k\text{:} && \Delta' X^{q^2-1} - \Delta^{q^k} = 0 \quad (u_k \text{ monic}). \\ &\text{For } u_{k-1}\text{:} && \Delta' X^{q^2} - \Delta^{q^{k-1}} X + g' u_k^q - u_k g^{q^k} = 0\,. \\ &\text{For } u_{k-i}\ (2 \le i \le k)\text{:} && \Delta' X^{q^2} - \Delta^{q^{k-i}} X + T u_{k+2-i} + g' u_{k+1-i}^q \\ &&& \quad - u_{k+1-i} g^{q^{k+1-i}} - u_{k+2-i} T^{q^{k+2-i}} = 0\,. \end{aligned} \tag{8.2}$$

Any $(k+1)$-tuple $(u_0, u_1, \ldots, u_k) \in \mathbb{L}^{k+1}$ obtained from (8.2) gives rise to possible coefficients of u. Any such $(k+1)$-tuple over $\mathbb{L}$ whose first two entries satisfy the second equation of (8.1) defines an n-isogeny $u : \varphi \to \psi$. Here, each of the equations for $u_{k-1}, \ldots, u_0$ has up to q^2 roots, and for each root $u_{k-i} \in \mathbb{L}$, we need to solve the entire collection of polynomial equations for which u_{k-i} and u_{k-i+1} appear in the constant coefficient and for which u_{k-i-1} is a potential root. To exhaust all possibilities, we grow a tree. The root of this tree is the unique monic (q^2-1)-st root u_k of y, i.e. the unique monic root of the first polynomial in (8.2), provided it belongs to $\mathbb{L}$. The next level consists of the vertices u_{k-1}, connected to u_k by an edge, where u_{k-1} is a root of the second polynomial in (8.2) that belongs to $\mathbb{L}$. In general, level i consists of vertices of the form $u_{k-i} \in \mathbb{L}$. Every such vertex determines a unique polynomial appearing in (8.2) for which u_{k-i} and its parent u_{k-i+1} appear in the constant coefficient. If this polynomial has roots $u_{k-i-1} \in \mathbb{L}$, then all these roots are added as vertices at the next level and connected to u_{k-i} by edges. If at any level no vertices are added, then no n-isogeny from φ to ψ exists and we abort.

Once all the equations are solved, the tree is complete. For each edge (u_0, u_1), we check that u_0 and u_1 satisfy the second equation of (8.1). If yes, then the corresponding $(k+1)$-tuple $(u_0, u_1, \ldots, u_k)$, where u_i is the parent of u_{i-1} for $1 \le i \le k$, represents the coefficients of an n-isogeny from φ to ψ. This process is presented in Algorithm 8.1.

In the case when $\mathsf{n} = \ell$ is monic and irreducible, and φ, ψ are ordinary, we know from the structure of ℓ-isogeny volcanoes that there is almost always at most one ℓ-isogeny from φ to ψ; in the rare cases where φ and ψ lie on a crater of size at most 2, there may be 2 such isogenies, arising from a double edge or a double

loop if $\varphi = \psi$. Unfortunately, we do not know *a priori* which is the correct path through the tree; this may not become evident until the validity is established with the test of whether u_0 and u_1 satisfy the second equation in (8.1).

Algorithm 8.1 Computing explicit isogenies

Input: A prime power q, a monic irreducible polynomial $P \in \mathbb{F}_q[T]$ of degree d, a polynomial $\mathsf{n} \in \mathbb{F}_q[x]$ of degree $k \geq 1$ with $P \nmid \mathsf{n}$, and two Drinfeld modules $\varphi = (g, \Delta)$, $\psi = (g', \Delta')$ over the field $\mathbb{L} = \mathbb{F}_q[T]/P\mathbb{F}_q[T]$.

Output: A list of $(k+1)$-tuples $(u_0, u_1, \ldots, u_k)$ such that $u = \sum_{i=0}^{k} u_i \tau^i$ is an n-isogeny from φ to ψ, or statement that no n-isogeny from φ to ψ exists.

$y \leftarrow \Delta^{q^k}/\Delta'$.
$e \leftarrow q-1$ if d is odd; $e \leftarrow q^2-1$ if d is even.
if $y^{(q^d-1)/e} \neq 1$ **then**
    return "No n-isogeny exists."
end if
$u_k \leftarrow$ the unique monic root of $X^{q^2-1} - y \pmod{P}$ in $\mathbb{L}$.
$E \leftarrow \{\}$, $V \leftarrow \{u_k\}$.
$R \leftarrow \{\text{roots of } \Delta' X^{q^2} - \Delta^{q^{k-1}} X + g' u_k^q - u_k g^{q^k}\}$ in $\mathbb{L}$
if $R = \{\}$ **then**
    return "No n-isogeny exists."
end if
for all $u_{k-1} \in R$ **do**
    $V \leftarrow V \cup \{u_{k-1}\}$
    $E \leftarrow E \cup \{(u_k, u_{k-1})\}$
end for
for $i = 2$ to k **do**
    for all $u_{k+1-i} \in V$ **do**
        $R \leftarrow \{\text{roots of } \Delta' X^{q^2} - \Delta^{q^{k-i}} X + T u_{k+2-i} + g' u_{k+1-i}^q - u_{k+1-i} g^{q^{k+1-i}} - u_{k+2-i} T^{q^{k+2-i}}\}$ in $\mathbb{L}$.
        if $R = \{\}$ **then**
            return "No n-isogeny exists."
        end if
        for all $u_{k-i} \in R$ **do**
            $V \leftarrow V \cup \{u_{k-i}\}$
            $E \leftarrow E \cup \{(u_{k-i+1}, u_{k-i})\}$
        end for
    end for
end for
$L \leftarrow \{\}$.
for all leaf vertices $u_0 \in V$ **do**
    if $u_0 g + u_1 T^q = T u_1 + g' u_0^q$ (where u_1 is the parent of u_0) **then**
        $L \leftarrow L \cup \{(u_0, u_1, \ldots, u_k)\}$ where u_i is the parent of u_{i-1} for $1 \leq i \leq k$.
    end if
end for
return L

THEOREM 8.1. *For any two rank 2 Drinfeld modules φ, ψ over $\mathbb{L} = \mathbb{F}_q[T]/P\mathbb{F}_q[T]$ and any polynomial $\mathfrak{n} \in \mathbf{A}$ with $P \nmid \mathfrak{n}$, Algorithm 8.1 computes all the $\mathfrak{n}$-isogenies from φ to ψ, or ascertains that none exist, in*

$$O\left(|\mathfrak{n}|^2 R(q^2, d) M(d)\right)$$

$\mathbb{F}_q$-operations, as $|P|, |\mathfrak{n}| \longrightarrow \infty$. Here, $R(n, d)$ is the number of operations in $\mathbb{F}_{q^d}$ required to compute the roots of a degree n polynomial over $\mathbb{F}_{q^d}$, and $M(n)$ is the number of $\mathbb{F}_q$-operations required to multiply two polynomials in $\mathbb{F}_q[T]$ of degree n. The space requirement is $O(|\mathfrak{n}|^2 d)$ elements in $\mathbb{F}_q$.

PROOF. The worst case complexity scenario is if each polynomial equation in (8.2) has q^2 roots in $\mathbb{L}$. In that case, each internal vertex in the tree of coefficients yielding a potential isogeny has q^2 children. So the total number of root computations is equal to the number of vertices, which is

$$\sum_{i=0}^{k} q^{2i} = \frac{q^{2k+1} - 1}{q - 1} = O(|\mathfrak{n}|^2) \ .$$

For each node, the algorithm must find the root of a polynomial over $\mathbb{L}$ of degree q^2. This yields the run time result. Since each node is an element in $\mathbb{L}$, the tree requires storage of $O(|\mathfrak{n}|^2 d)$ elements in $\mathbb{F}_q$. □

We expect the complexity result in Theorem 8.1 to be a vast overestimate much of the time, since it is unlikely that each of the polynomials in (8.2) has q^2 roots in $\mathbb{L}$. In fact, in all our computations over $\mathbb{F}_3$ where the two input Drinfeld modules were *a priori* known to be ℓ-isogenous via the modular polynomial root test, every node in the tree only had $q = 3$ children.

Finally, Algorithm 8.1 can in fact find all the $\mathfrak{n}$-isogenies from φ to ψ over any extension field of $\mathbb{L}$. However, if we allow roots outside $\mathbb{L}$ in our tree, then the complexity estimate of Theorem 8.1 is no longer valid.

EXAMPLE 8.2. Let $q = 3$, $P(T) = T^9 + 2T^3 + 2T^2 + T + 1$, and $\mathfrak{n} = T^2 + 1$. Consider the ordinary rank 2 Drinfeld modules

$$\varphi = (T^2,\ T^7) \ , \qquad \psi = (T,\ 2T^6 + 2T^5 + 2T^4 + 2T^2 + T + 2)$$

over $\mathbb{L} = \mathbb{F}_3[T]/P\mathbb{F}_3[T]$. Their respective j-invariants are

$$j(\varphi) = T \ , \qquad j(\psi) = T^7 + T^6 + T^5 + 2T^3 + T^2 + T + 1 \ .$$

Note that φ and ψ are (T^2+1)-isogenous as $\Phi_{T^2+1}(j(\varphi), j(\psi)) = 0$. Algorithm 8.1 produces the (T^2+1)-isogeny $u = u_0 + u_1\tau + u_2\tau^2 \in \mathbb{L}\{\tau\}$ from φ to ψ, where

$$\begin{aligned} u_0 &= 2T^8 + T^7 + 2T^5 + 2T^4 + 2T^2 + T + 2 \ , \\ u_1 &= T^7 + T^6 + 2T^5 + T^4 + T^3 + T^2 + T + 2 \ , \\ u_2 &= T^8 + T^7 + 2T^6 + T^5 + 2T^4 + 2T^3 + T + 1 \ . \end{aligned}$$

9. Computing dual isogenies

Dual isogenies can also be found via symbolic computation, but far more efficiently. Given two rank 2 Drinfeld modules $\varphi = (g, \Delta)$ and $\psi = (g', \Delta')$ over $\mathbb{L}$

and an isogeny $u \in \mathbb{L}\{\tau\}$ of degree $\mathfrak{n} \in \mathbf{A}$ from φ to ψ, the dual isogeny $\hat{u}$ is characterized by the identity $\hat{u}u = \varphi_{\mathfrak{n}}$. Write

$$u = \sum_{i=0}^{k} u_i \tau^i \ , \qquad \hat{u} = \sum_{i=0}^{k} \hat{u}_i \tau^i \ , \qquad \varphi_{\mathfrak{n}} = \sum_{i=0}^{2k} n_i \tau^i \ ,$$

where $k = \deg_T(\mathfrak{n})$, $u_i, \hat{u}_i \in \mathbb{L}$ for $0 \le i \le k$, $n_i \in \mathbb{L}$ for $0 \le i \le 2k$, and $u_k \hat{u}_k n_{2k} \neq 0$. The coefficients n_i can be recursively determined as follows (see, for example, [**35**, Lem. 3.2.2]):

$$\begin{aligned} n_0 &= \mathfrak{n} \ , \qquad n_1 = \frac{g n_0^q - n_0 g}{T^q - T} \ , \\ n_i &= \frac{n_{i-1}^q g - n_{i-1} g^{q^{i-1}} + n_{i-2}^{q^2} \Delta - n_{i-2} \Delta^{q^{i-2}}}{T^{q^i} - T} \qquad (2 \le i \le 2k) \ . \end{aligned} \tag{9.1}$$

Comparing coefficients of the powers of τ in the identity $\varphi_{\mathfrak{n}} = \hat{u}u$ produces the following system of $2k+1$ linear equations in the unknowns $\hat{u}_0, \hat{u}_1, \ldots, \hat{u}_{2k}$:

$$\begin{aligned} n_0 &= \hat{u}_0 u_0 \ , \\ n_1 &= \hat{u}_0 u_1 + \hat{u}_1 u_0^q \ , \\ n_2 &= \hat{u}_0 u_2 + \hat{u}_1 u_1^q + \hat{u}_2 u_0^{q^2} \ , \\ &\vdots \\ n_k &= \hat{u}_0 u_k + \hat{u}_1 u_{k-1}^q + \cdots + \hat{u}_k u_0^{q^k} \ , \\ n_{k+1} &= \hat{u}_1 u_k^q + \hat{u}_2 u_{k-1}^{q^2} + \cdots + \hat{u}_k u_1^{q^k} \ , \\ &\vdots \\ n_{2k} &= \hat{u}_k u_k^{q^k} \ . \end{aligned}$$

A solution can be obtained recursively from the first $k+1$ of these equations via

$$\begin{aligned} \hat{u}_0 &= n_0 u_0^{-1}, \\ \hat{u}_j &= \left(n_j - \sum_{i=0}^{j-1} \hat{u}_i u_{m-i}^{q^i} \right) u_0^{-q^j}, \qquad (1 \le j \le k) \ . \end{aligned} \tag{9.2}$$

In algorithmic form, this simple procedure can be summarized as follows.

Algorithm 9.1 Computing a dual isogeny

Input: A prime power q, a monic irreducible polynomial $P \in \mathbb{F}_q[T]$ of degree d, a Drinfeld module $\varphi = (g, \Delta)$ over $\mathbb{L} = \mathbb{F}_q[T]/P\mathbb{F}_q[T]$, and an isogeny $u = \sum_{i=0}^{k} u_i \tau^i$ of degree $\mathfrak{n}$ on φ such that $P \nmid \mathfrak{n}$ and $k = \deg_T(\mathfrak{n})$.

Output: The dual isogeny $\hat{u} = \sum_{i=0}^{k} \hat{u}_i \tau^i$.

1: Compute the first $k+1$ polynomials $n_0, n_1, \ldots, n_k \in \mathbb{L}$ defined in (9.1).
2: Compute the polynomials $\hat{u}_0, \hat{u}_1, \ldots, \hat{u}_k \in \mathbb{L}$ defined in (9.2)
3: **return** $\hat{u} = \sum_{i=0}^{k} \hat{u}_i \tau^i$.

THEOREM 9.1. *For any rank 2 Drinfeld module φ over $\mathbb{L} = \mathbb{F}_q[T]/P\mathbb{F}_q[T]$, any polynomial $\mathfrak{n} \in \mathbf{A}$ with $P \nmid \mathfrak{n}$, and any $\mathfrak{n}$-isogeny u defined on φ, Algorithm 9.1 computes the dual isogeny $\hat{u}$ of u in*

$$O\left(\deg_T(\mathfrak{n})^2 M(d)\right)$$

$\mathbb{F}_q$-operations, as $|P|, |\mathfrak{n}| \longrightarrow \infty$, with a storage requirement of $O(\deg_T(\mathfrak{n})d)$ elements in $\mathbb{F}_q$. Here, $M(n)$ is the number of $\mathbb{F}_q$-operations required to multiply two polynomials in $\mathbb{F}_q[T]$ of degree n.

PROOF. Step 1 computes $k+1$ elements in $\mathbb{L}$, where each such element needs a fixed number of multiplications and exponentiations by q. So the cost of step 1 is $O(kM(d))$ operations in $\mathbb{F}_q$ and $O(kd)$ space. Step 2 computes k elements in $\mathbb{L}$, and the number of operations in $\mathbb{L}$ required to compute the j-th such element is $O(j)$. Hence this step has a computational cost of $O(k^2M(d))$ operations in $\mathbb{F}_q$, requiring storage of $O(kd)$ elements in $\mathbb{F}_q$. □

EXAMPLE 9.2. Consider the (T^2+1)-isogeny u computed in Example 8.2. Algorithm 9.1 computes the dual of u as $\hat{u} = \hat{u}_0 + \hat{u}_1\tau + \hat{u}_2\tau^2 \in \mathbb{L}\{\tau\}$ where

$$\begin{aligned}
\hat{u}_0 &= 2T^6 + 2T^5 + T^4 + 2T^3 + 2T + 1 \ , \\
\hat{u}_1 &= T^8 + T^7 + 2T^6 + 2T^5 + 2T^4 + 2 \ , \\
\hat{u}_2 &= T^8 + T^7 + T^6 + 2T^5 + T^4 + T^3 + 2T^2 + 1 \ .
\end{aligned}$$

10. Current and future work

Exploration into computations on rank 2 Drinfeld modules is still very much in its infancy. In terms of generating modular polynomials, we are as yet a long way away from producing comprehensive tables like those for classical modular polynomials supplied by Sutherland [**45**]. Endomorphism ring computation for Drinfeld modules also lags behind what can be accomplished for elliptic curves. An optimized high-speed implementation will narrow that gap.

Not surprisingly, among the algorithms presented here, our method for computing Drinfeld modular polynomials is the most costly due to the size of the polynomials involved in the computation. The gap in the complexity estimate between this algorithm and its classical counterpart is somewhat vexing. Using the methodology and coefficient bounds of Bae-Lee [**3**], it appears that our estimate cannot be improved. Perhaps taking sparsity of the j-expansions in s and its coefficients in T into account would help, but such an analysis seems challenging. On the other hand, it is possible that this issue simply represents a fundamental difference between the behaviour of classical and Drinfeld modular polynomials. As mentioned earlier, while the logarithmic height of the classical modular polynomial $\Phi_\ell(X,Y)$ grows quasilinearly in ℓ, the growth of the coefficients of the ℓ-th Drinfeld modular polynomial is between linear and cubic [**3**]. In all our examples with $\deg_T(\ell) = 1$, the logarithmic height H of $\Phi_\ell(X,Y)$ was $H = q(|\ell|^2 + |\ell|) = q^3 + q^2$. For all the examples with $\deg_T(\ell) = 2$ that we computed, the height stayed below $q(|\ell|^2 + |\ell|)$. This matter clearly warrants further investigation. Our computations are as yet too modest to observe consistent behaviour here, let alone formulate a hypothesis. A fast implementation that is able to produce larger volumes of data will shed more light on this question.

As a start, we opted to adopt the standard analytic approach for computing classical modular polynomials to the Drinfeld module setting. There are other techniques such as computing the modular polynomial modulo many small primes and then lifting it via Chinese Remaindering (see, for example [**6**, **9**, **46**]) or Enge's evaluation-interpolation method [**15**]. Work on exploring these algorithms in the context of Drinfeld modules is currently in progress. In addition, *Hilbert class polynomials* play a crucial role in the elliptic curve analogues of many of the algorithms under consideration here, and their computation is closely linked to obtaining modular polynomials and isogeny volcanoes. The Drinfeld analogue would be the polynomial $H_{\mathcal{O}}(X) \in \mathbf{A}[X]$ whose roots are the j-invariants of rank 2 Drinfeld modules with endomorphism orders isomorphic to $\mathcal{O}$. While Gekeler [**20**] and Hayes [**33**] laid the theoretical ground work, and singular moduli were discussed, for example, in [**11**, **12**], there has to date been no investigation of Hilbert class polynomials for Drinfeld modules to the best of our knowledge. We intend to fill this gap.

Our treatment did not extend to supersingular rank 2 Drinfeld modules, nor to those with j-invariant 0. An investigation of these cases is currently underway. Kohel [**36**, Chap. 7] showed that the ℓ-isogeny subgraph of supersingular elliptic curves over a finite field is connected and gave an algorithm for computing four $\mathbb{Z}$-linearly independent endomorphisms of a given curve. We expect that the ℓ-isogeny graph of a supersingular rank 2 Drinfeld module will look similar and Kohel's work can be adapted to this setting. We are also exploring ways of computing the endomorphism ring of a supersingular rank 2 Drinfeld module. In [**4**], Bisson and Sutherland presented two index calculus algorithms for computing the endomorphism ring of an ordinary elliptic curve. Under reasonable smoothness assumptions, both methods have sub-exponential run time. The approach seems to lend itself well to adaptation to rank 2 Drinfeld modules over $\mathbb{F}_q$. However, the run time will likely generally be exponential in the size of q, since the corresponding smoothness parameter only bounds the degrees of polynomial factors in relations, but not their coefficients in $\mathbb{F}_q$. Recent computational advances in the context of isogenies and endomorphisms of Abelian surfaces also lead to the natural questions of analogous notions and computations on Drinfeld modules of higher rank.

Isogeny volcanoes for Drinfeld modules give rise to a number of open questions as well. We did not attempt to use Proposition 2.1 for generating isogeny volcanoes. The explicit construction of a linear n-isogeny defined on $\varphi = (g, \Delta)$ over $\mathbb{L}$ relies on the existence of a root of the polynomial $\Delta X^{q+1} + gX + \mathsf{n}$ in $\mathbb{L}$. For the case $\mathsf{n} = \ell$ monic and irreducible, it is conceivable that the entire ℓ-isogeny volcano of φ can be constructed using this approach. It may then be possible to adapt classical methods that compute $\Phi_\ell(X, Y)$ from the ℓ-isogeny volcano, such as the algorithms described in [**6**], to the Drinfeld module setting. Moreover, isogeny volcanoes of Drinfeld modules may have other applications. In the elliptic curve setting, isogeny graphs can be used to detect supersingularity, see [**47**]; the same may be true for Drinfeld modules. Fouquet and Morain [**16**, **17**] employed isogeny volcanoes for point counting on elliptic curves; it is unclear if there is a corresponding application for Drinfeld modules.

This last point leads back to the broader tantalizing question of similarities and differences between elliptic curves and rank 2 Drinfeld modules. A crucial distinction between the two classes of objects is that the geometric structure and properties of elliptic curves do not appear to carry over to Drinfeld modules; in

this context, their otherwise close resemblance seems to come to an abrupt end. There is no notion of "points" on Drinfeld modules, and the fundamental point counting formula $\#E(\mathbb{F}_p) = p + 1 - a_p$, where a_p is the trace of Frobenius, has no meaning here. Vélu's formulas for constructing cyclic isogenies seem to have no obvious Drinfeld module analogue either, and conversely, our construction of Algorithm 8.1 appears to not be applicable to elliptic curves. On the other hand, Drinfeld modules do support a notion of torsion points — the roots of any image φ_a for $a \in \mathbf{A}$; see Section 2 — so perhaps further analogies extending to the geometry of elliptic curves could be discovered. Possible starting points might be Yu's kernel lattice construction of isogenies [**49**, Sec. 2] or divisibility properties and kernels of polynomials in $\mathbb{L}\{\tau\}$.

Acknowledgment

The authors sincerely thank the three anonymous referees for their helpful comments.

References

[1] S. Bae, *On the modular equation for Drinfel′d modules of rank* 2, J. Number Theory **42** (1992), no. 2, 123–133, DOI 10.1016/0022-314X(92)90016-I. MR1183371
[2] S. Bae and J. K. Koo, *On the singular Drinfel′d modules of rank* 2, Math. Z. **210** (1992), no. 2, 267–275, DOI 10.1007/BF02571797. MR1166525
[3] S. Bae and S. Lee, *On the coefficients of the Drinfeld modular equation*, J. Number Theory **66** (1997), 85–101.
[4] G. Bisson and A. V. Sutherland, *Computing the endomorphism ring of an ordinary elliptic curve over a finite field*, J. Number Theory **131** (2011), no. 5, 815–831, DOI 10.1016/j.jnt.2009.11.003. MR2772473
[5] F. Breuer and H.-G. Rück, *Drinfeld modular polynomials in higher rank*, J. Number Theory **129** (2009), no. 1, 59–83, DOI 10.1016/j.jnt.2008.07.010. MR2468471
[6] R. Bröker, K. Lauter, and A. V. Sutherland, *Modular polynomials via isogeny volcanoes*, Math. Comp. **81** (2012), no. 278, 1201–1231, DOI 10.1090/S0025-5718-2011-02508-1. MR2869057
[7] P. Caranay, `DModules`. GitHub repository. `https://github.com/pcaranay/DModules`.
[8] P. Caranay, *Computing isogeny volcanoes of rank two Drinfeld modules*, Ph.D. Thesis, Calgary, Canada, 2018. `https://prism.ucalgary.ca/handle/1880/106320`.
[9] D. Charles and K. Lauter, *Computing modular polynomials*, LMS J. Comput. Math. **8** (2005), 195–204, DOI 10.1112/S1461157000000954. MR2166572
[10] P. Cohen, *On the coefficients of the transformation polynomials for the elliptic modular function*, Math. Proc. Cambridge Philos. Soc. **95** (1984), no. 3, 389–402, DOI 10.1017/S0305004100061697. MR755826
[11] D. R. Dorman, *On singular moduli for rank* 2 *Drinfel′d modules*, Compositio Math. **80** (1991), no. 3, 235–256. MR1134255
[12] D. R. Dorman, *Factorization of Drinfel′d singular moduli*, p-adic methods in number theory and algebraic geometry, Contemp. Math., vol. 133, Amer. Math. Soc., Providence, RI, 1992, pp. 75–79, DOI 10.1090/conm/133/1183971. MR1183971
[13] V. G. Drinfel'd, *Elliptic modules*, Math. USSR Sbornik **23** (1974), no. 4, 561–592.
[14] N. D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 21–76. MR1486831
[15] A. Enge, *Computing modular polynomials in quasi-linear time*, Math. Comp. **78** (2009), no. 267, 1809–1824, DOI 10.1090/S0025-5718-09-02199-1. MR2501077
[16] M. Fouquet, *Anneau d'endomorphismes et cardinalité des courbes elliptiques: aspects algorithmiques*, Ph.D. Thesis, Palaiseau, France, 2001.

[17] M. Fouquet and F. Morain, *Isogeny volcanoes and the SEA algorithm*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 276–291, DOI 10.1007/3-540-45455-1_23. MR2041091

[18] S. Garai and M. Papikian, *Computing endormorphism rings and Frobenius matrices of Drinfeld modules*, 2019. https://arxiv.org/abs/1908.01805v1.

[19] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, 2nd ed., Cambridge University Press, Cambridge, 2003. MR2001757

[20] E.-U. Gekeler, *Zur Arithmetik von Drinfel′d-Moduln* (German), Math. Ann. **262** (1983), no. 2, 167–182, DOI 10.1007/BF01455309. MR690193

[21] E.-U. Gekeler, *A product expansion for the discriminant function of Drinfel′d modules of rank two*, J. Number Theory **21** (1985), no. 2, 135–140, DOI 10.1016/0022-314X(85)90046-0. MR808282

[22] E.-U. Gekeler, *Drinfel′d modular curves*, Lecture Notes in Mathematics, vol. 1231, Springer-Verlag, Berlin, 1986. MR874338

[23] E.-U. Gekeler, *On the coefficients of Drinfel′d modular forms*, Invent. Math. **93** (1988), no. 3, 667–700, DOI 10.1007/BF01410204. MR952287

[24] E.-U. Gekeler, *On finite Drinfel′d modules*, J. Algebra **141** (1991), no. 1, 187–203, DOI 10.1016/0021-8693(91)90211-P. MR1118323

[25] E.-U. Gekeler, *A survey on Drinfeld modular forms*, Turkish J. Math. **23** (1999), no. 4, 485–518. MR1780937

[26] E.-U. Gekeler, *Frobenius distributions of Drinfeld modules over finite fields*, Trans. Amer. Math. Soc. **360** (2008), no. 4, 1695–1721, DOI 10.1090/S0002-9947-07-04558-8. MR2366959

[27] D. Goss, *Von Staudt for $\mathbb{F}_q[T]$*, Duke Math. J. **45** (1978), no. 4, 885–910.

[28] D. Goss, *The algebraist's upper half-plane*, Bull. Amer. Math. Soc. (N.S.) **2** (1980), no. 3, 391–415, DOI 10.1090/S0273-0979-1980-14751-5. MR561525

[29] D. Goss, *Modular forms for $\mathbf{F}_r[T]$*, J. Reine Angew. Math. **317** (1980), 16–39, DOI 10.1515/crll.1980.317.16. MR581335

[30] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 35, Springer-Verlag, Berlin, 1996. MR1423131

[31] D. Harvey and J. V. D. Hoeven, *Polynomial multiplication over finite fields in time $O(n \log n)$*. https://hal.archives-ouvertes.fr/hal-02070816.

[32] D. R. Hayes, *A brief introduction to Drinfel′d modules*, The arithmetic of function fields (Columbus, OH, 1991), Ohio State Univ. Math. Res. Inst. Publ., vol. 2, de Gruyter, Berlin, 1992, pp. 1–32. MR1196509

[33] D. R. Hayes, *Explicit class field theory in global function fields*, Studies in algebra and number theory, Adv. in Math. Suppl. Stud., vol. 6, Academic Press, New York-London, 1979, pp. 173–217. MR535766

[34] L.-C. Hsia and J. Yu, *On characteristic polynomials of geometric Frobenius associated to Drinfeld modules*, Compositio Math. **122** (2000), no. 3, 261–280, DOI 10.1023/A:1002015330987. MR1781330

[35] F. Jung, *Characteristische Polynome von Drinfeld-Moduln*, Master's Thesis, Germany, 2000. https://www.math.uni-sb.de/ag/gekeler/PERSONEN/Jung/Download/Dip_FJung.ps.

[36] D. R. Kohel, *Endomorphism rings of elliptic curves over finite fields*, ProQuest LLC, Ann Arbor, MI, 1996. Thesis (Ph.D.)–University of California, Berkeley. MR2695524

[37] N. Kuhn and R. Pink, *Finding endomorphisms of Drinfeld modules*, 2016. https://arxiv.org/abs/1608.02788v1.

[38] D. Moody, *Computing isogeny volcanoes of composite degree*, Appl. Math. Comput. **218** (2012), no. 9, 5249–5258, DOI 10.1016/j.amc.2011.11.008. MR2870046

[39] Y. Musleh, *Fast algorithms for finding the characteristic polynomial of a rank-2 Drinfeld module*, Doctoral dissertation, University of Waterloo (Canada), 2018. https://hdl.handle.net/10012/13889

[40] Y. Musleh and É. Schost, *Computing the characteristic polynomial of a finite rank two Drinfeld module*, ISSAC'19—Proceedings of the 2019 ACM International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2019, pp. 307–314, DOI 10.1145/3326229.3326256. MR4007474

[41] M. O. Rabin, *Probabilistic algorithms in finite fields*, SIAM J. Comput. **9** (1980), no. 2, 273–280, DOI 10.1137/0209024. MR568814

[42] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR1876657
[43] A. Schweizer, *On the Drinfel′d modular polynomial* $\Phi_T(X, Y)$, J. Number Theory **52** (1995), no. 1, 53–68, DOI 10.1006/jnth.1995.1055. MR1331765
[44] W. A. Stein et al., *Sage Mathematics Software (Version 7.6)*, The Sage Development Team, 2017. `http://www.sagemath.org`.
[45] A. Sutherland, *Modular polynomials*. `https://math.mit.edu/~drew/ClassicalModPolys.html`.
[46] A. V. Sutherland, *On the evaluation of modular polynomials*, ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 1, Math. Sci. Publ., Berkeley, CA, 2013, pp. 531–555, DOI 10.2140/obs.2013.1.531. MR3207430
[47] A. V. Sutherland, *Isogeny volcanoes*, ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 1, Math. Sci. Publ., Berkeley, CA, 2013, pp. 507–530, DOI 10.2140/obs.2013.1.507. MR3207429
[48] J. Vélu, *Isogénies entre courbes elliptiques* (French), C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241. MR294345
[49] J.-K. Yu, *Isogenies of Drinfel′d modules over finite fields*, J. Number Theory **54** (1995), no. 1, 161–171, DOI 10.1006/jnth.1995.1108. MR1352643

Department of Mathematics & Statistics, University of Calgary, 2500 University Drive NW, Calgary, Alberta, Canada T2N 1N4
Email address: `pcabarrubias@yahoo.com`

Department of Mathematics & Statistics, University of Calgary, 2500 University Drive NW, Calgary, Alberta, Canada T2N 1N4
Email address: `mgreenbe@ucalgary.ca`

Department of Mathematics & Statistics, University of Calgary, 2500 University Drive NW, Calgary, Alberta, Canada T2N 1N4
Email address: `rscheidl@ucalgary.ca`