Finding Endomorphisms of Drinfeld modules

Nikolas Kuhn
Dept. of Mathematics
ETH Zürich
Switzerland
nikolaskuhn@gmx.de

Richard Pink
Dept. of Mathematics
ETH Zürich
Switzerland
pink@math.ethz.ch

August 9, 2016

Abstract

We give an effective algorithm to determine the endomorphism ring of a Drinfeld module, both over its field of definition and over a separable or algebraic closure thereof. Using previous results we deduce an effective description of the image of the adelic Galois representation associated to the Drinfeld module, up to commensurability. We also give an effective algorithm to decide whether two Drinfeld modules are isogenous, again both over their field of definition and over a separable or algebraic closure thereof.

Contents

MSC classification: 11G09 (11R58, 11Y99)

1 Introduction

Given a Drinfeld A-module $\varphi\colon A \to K[\tau]$ over a field K, can one effectively determine its endomorphism ring $\mathrm{End}_K(\varphi)$?

Before answering this question, we must make it more precise. By definition $\mathrm{End}_K(\varphi)$ is the subset of elements of $K[\tau]$ which commute with φ_a for all $a \in A$. Thus one can write down individual endomorphisms, but what does it mean to know their totality? We think it means three things: Firstly, since $\mathrm{End}_K(\varphi)$ is a finitely generated projective A-module, one should have a finite set of generators. Secondly, one should know all A-linear relations between them, in other words, one should have a finite presentation of $\mathrm{End}_K(\varphi)$ as an A-module. Thirdly, one should be able to express any given endomorphism as an A-linear combination of the generators. Applying this to the product of any two generators, this yields an explicit description of the ring structure of $\mathrm{End}_K(\varphi)$, using which many questions about $\mathrm{End}_K(\varphi)$ as an A-algebra reduce to finite calculations over A.

To answer the question we must also clarify which algebraic calculations we assume that one can already perform within A and within K. By definition, the coefficient ring A underlying a Drinfeld module is a finitely generated normal integral domain of transcendence degree 1 over a finite prime field $\mathbb{F}_p$ of order p. So we assume that A is given by explicit finite sets of generators and relations. We also assume that K is the fraction field of an integral domain that is given by explicit finite sets of generators and relations over $\mathbb{F}_p$. For calculations within A and K we then have all the standard procedures from algorithmic commutative algebra at our disposal. Of course, one cannot effectively construct, or calculate within, a separable or algebraic closure $K^{\mathrm{sep}} \subset \overline{K}$ of K. But one can calculate in any finite extension of K and enlarge that extension whenever necessary.

The assumption that K is finitely generated over $\mathbb{F}_p$, however, introduces a new problem. Namely, while there exists a finite field extension K' of K with $\mathrm{End}_{\overline{K}}(\varphi) = \mathrm{End}_{K'}(\varphi)$, there is no a priori choice for it. To determine $\mathrm{End}_{\overline{K}}(\varphi)$ we must therefore also specify such an extension K'.

With these provisos we can now say that $\mathrm{End}_K(\varphi)$ and $\mathrm{End}_{\overline{K}}(\varphi)$ can be effectively determined: see Theorems 6.9 and 6.8.

Our algorithm for this has essentially two parts. One process goes through all integers $d \geqslant 0$ and finds all endomorphisms of degree d by solving finitely many polynomial equations. Eventually it will find a finite set of generators, but knowing when that happens requires other information. It is not hard to see that it suffices to know the rank of the endomorphism ring over A. So in addition to the first process, we start another process in parallel that tries to prove that the right number of A-linearly independent endomorphisms has already been found. When that succeeds, it kills the first process and stops with the correct answer.

The second process uses the Galois representation on the $\mathfrak{p}$-adic Tate module of φ for a suitable prime $\mathfrak{p}$ of A. By the Tate conjecture for Drinfeld modules, proved by Taguchi [18], [19], [20] and Tamagawa [21], this representation determines the endomorphism ring to a large extent; in particular, it determines its rank over A. Though the Galois representation

can be studied only indirectly, the associated characteristic polynomials of Frobeniuses can be computed effectively. The second process limits the possible endomorphisms by searching for characteristic polynomials that are sufficiently independent of each other in some sense.

For Drinfeld modules of generic characteristic, the endomorphism ring is always commutative, and the program outlined above suffices to determine it effectively. In special characteristic the endomorphism ring can be non-commutative, and we must wrestle with additional technical difficulties. The problem is that there may exist more endomorphisms when A is replaced by a smaller admissible coefficient ring. This puts additional constraints on the Galois representation.

In fact, by results of the second author and others [11], [12], [14], [13], [2], the knowledge of the endomorphism rings of certain Drinfeld modules obtained from φ by varying the ring of coefficients A determines the image of the Galois representation up to commensurability, even for the whole adelic Galois representation associated to φ. We therefore set up things to compute all this information as well and are thereby able to effectively determine the image of Galois up to commensurability: see Theorem 6.12.

In special characteristic we treat the isotrivial case, where φ is isomorphic over $\overline{K}$ to a Drinfeld module defined over a finite field, separately. In the non-isotrivial case we first use the method sketched above to find a maximal commutative subring A' of $\mathrm{End}_{\overline{K}}(\varphi)$. For technical reasons we replace φ by an isogenous Drinfeld module, after which A' is an admissible coefficient ring and φ extends to a Drinfeld A'-module with $\mathrm{End}_{\overline{K}}(\varphi') = A'$. In a second step we then find the unique smallest admissible coefficient ring $B \subset A'$ such that the center of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$ is B, whose existence is guaranteed by Pink [12, Thm. 1.2].

Our algorithm for this again has two parts. One process computes the traces of Frobeniuses in the adjoint representation, whose values generate the fraction field of B by Pink [12, Thm. 1.3]. It thus constructs an increasing sequence of subrings B_k of A' with $B_k = B$ for all sufficiently large k, but again it does not know when that occurs. In addition to the first process, we therefore run another process in parallel that tries to prove that B has been reached. This process is started as soon as the first B_k is infinite, and it simply goes through all integers $d \geqslant 0$ and finds all endomorphisms of degree d of $\varphi'|B_k$ over $\overline{K}$. This process knows whether $B_k = B$ has been reached by computing the ranks of B_k and of the submodule of $\mathrm{End}_{\overline{K}}(\varphi'|B_k)$ that is generated by the endomorphisms already found. When that occurs, it kills the first process and stops with the correct answer. Using the knowledge of B one can then find the endomorphism ring of the original Drinfeld module φ.

In all this, we do not care about computational efficiency; we only try to keep the code short and well-organized. An actual implementation should probably retain intermediate information and reuse it later. Also, simply searching for all endomorphisms of small degree seems a brute force approach. In Section 7 we discuss some ideas which might speed up the search by finding a priori candidates for the generators of the endomorphism ring.

A natural related question, kindly raised by Peter Jossen, is whether one can effectively decide whether two given Drinfeld A-modules φ and ψ over K are isogenous over K, re-

spectively over $\overline{K}$. Using the same methods as for endomorphisms, we answer this question affirmatively and show that $\mathrm{Hom}_K(\varphi,\psi)$ and $\mathrm{Hom}_{\overline{K}}(\varphi,\psi)$ can be effectively determined: see Section 8.

With effectiveness established, one may ask whether there exist any kinds of a priori bounds on the endomorphism ring, say on its rank and its discriminant over A, for instance in terms of the height of the Drinfeld module. (For abelian varieties over number fields such bounds are due to Masser and Wüstholz [10].) This article has nothing to contribute to this question, but it may be an interesting one for someone to pursue in the future.

Also, we have not tried to actually implement the proposed algorithms and can therefore not show any nice examples.

The article grew out of the master thesis of the first author [8].

2 Endomorphisms and image of Galois

In this section we review known facts about endomorphisms and Galois representations associated to Drinfeld modules and deduce some consequences. For the general theory of Drinfeld modules see Drinfeld [3], Deligne and Husemöller [1], Hayes [5], or Goss [4].

Basics: Let $\mathbb{F}_p$ denote the finite field of prime order p. Let F be a finitely generated field of transcendence degree 1 over $\mathbb{F}_p$, and let A be the subring of elements of F which are regular outside a fixed place ∞ of F. We call such A an admissible coefficient ring.

Let K be another finitely generated field over $\mathbb{F}_p$ with separable, respectively algebraic closures $K^{\mathrm{sep}} \subset \overline{K}$. Write $\mathrm{End}(\mathbb{G}_{a,K}) = K[\tau]$ with $\tau(x) = x^p$. Consider a Drinfeld A-module $\varphi\colon A \to K[\tau]$, $a \mapsto \varphi_a$ of rank r with characteristic ideal $\mathfrak{p}_0 \subset A$. Recall that φ has generic characteristic if $\mathfrak{p}_0 = (0)$ and special characteristic otherwise. We call φ isotrivial if, over some finite extension of K, it is isomorphic to a Drinfeld A-module defined over a finite field; this can happen only in special characteristic.

Endomorphisms: By definition $\mathrm{End}_K(\varphi)$ is the centralizer of $\varphi(A)$ in $K[\tau]$. This is a finitely generated projective A-module, and $\mathrm{End}^\circ_K(\varphi) := \mathrm{End}_K(\varphi) \otimes_A F$ is a division algebra over F of finite dimension dividing r^2. There exists a subfield $K' \subset K^{\mathrm{sep}}$ finite over K such that $\mathrm{End}_{\overline{K}}(\varphi) = \mathrm{End}_{K'}(\varphi)$. In generic characteristic the endomorphism ring is always commutative.

Good reduction: Choose a normal integral domain $R \subset K$ which is finitely generated over $\mathbb{F}_p$ with $\mathrm{Quot}(R) = K$, such that φ extends to a Drinfeld A-module over $\mathrm{Spec}\, R$. For any maximal ideal $\mathfrak{m} \subset R$ let $\varphi_\mathfrak{m}$ denote the resulting Drinfeld A-module over the finite residue field $k_\mathfrak{m} := R/\mathfrak{m}$. It is known that any endomorphism of φ over K already has coefficients in R; so reduction modulo $\mathfrak{m}$ induces a natural homomorphism of A-algebras

$$\mathrm{End}_K(\varphi) \longrightarrow \mathrm{End}_{k_\mathfrak{m}}(\varphi_\mathfrak{m}). \tag{2.1}$$

Moreover, the degree in τ of an endomorphism is preserved under reduction; hence the homomorphism is injective.

Frobenius: The element $\mathrm{Frob}_\mathfrak{m} := \tau^{[k_\mathfrak{m}/\mathbb{F}_p]}$ lies in the center of $k_\mathfrak{m}[\tau]$ and therefore in $\mathrm{End}_{k_\mathfrak{m}}(\varphi_\mathfrak{m})$. In fact, the center of $\mathrm{End}^\circ_{k_\mathfrak{m}}(\varphi_\mathfrak{m})$ is the field extension $F(\mathrm{Frob}_\mathfrak{m})$ of F that is generated by $\mathrm{Frob}_\mathfrak{m}$. Moreover, let $d_\mathfrak{m}$ denote the dimension of $F(\mathrm{Frob}_\mathfrak{m})$ over F, and let $e_\mathfrak{m}^2$ be the dimension of $\mathrm{End}^\circ_{k_\mathfrak{m}}(\varphi_\mathfrak{m})$ over $F(\mathrm{Frob}_\mathfrak{m})$; then we have $d_\mathfrak{m} e_\mathfrak{m} = r$.

Let $\min_\mathfrak{m}(X)$ denote the minimal polynomial of $\mathrm{Frob}_\mathfrak{m}$ over F; by construction it is irreducible and monic of degree $d_\mathfrak{m}$. Since $\mathrm{Frob}_\mathfrak{m}$ lies in an A-algebra of finite rank, this polynomial actually has coefficients in A. Define $\mathrm{char}_\mathfrak{m}(X) := \min_\mathfrak{m}(X)^{e_\mathfrak{m}}$, which is a monic polynomial in $A[X]$ of degree r, called the characteristic polynomial of $\mathrm{Frob}_\mathfrak{m}$.

Tate modules: For any maximal ideal $\mathfrak{p} \neq \mathfrak{p}_0$ of A the $\mathfrak{p}$-adic Tate module $T_\mathfrak{p}(\varphi)$ is a free module of rank r over the completion $A_\mathfrak{p}$. It is naturally endowed with an action of $\mathrm{End}_K(\varphi)$ and a continuous action of the Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. These actions commute with each other, and each helps in understanding the other.

Let R^{sep} denote the integral closure of R in K^{sep}. For any maximal ideal $\mathfrak{m} \subset R$ choose a maximal ideal $\mathfrak{m}^{\mathrm{sep}} \subset R^{\mathrm{sep}}$ which contains $\mathfrak{m}$. Then its residue field $k_\mathfrak{m}^{\mathrm{sep}} := R^{\mathrm{sep}}/\mathfrak{m}^{\mathrm{sep}}$ is a separable closure of $k_\mathfrak{m}$. For any maximal ideal $\mathfrak{p}$ of A different from the characteristic ideal of $\varphi_\mathfrak{m}$ this choice induces a natural isomorphism $T_\mathfrak{p}(\varphi) \cong T_\mathfrak{p}(\varphi_\mathfrak{m})$. This isomorphism is compatible with the action of endomorphisms via the reduction homomorphism (2.1). It is also compatible with the action of the decomposition group at $\mathfrak{m}^{\mathrm{sep}}$; namely, the inertia group acts trivially on $T_\mathfrak{p}(\varphi)$, and the isomorphism is equivariant under the action of the Frobenius at $\mathfrak{m}$. Moreover, the characteristic polynomial of this Frobenius in its action on the Tate module is precisely the characteristic polynomial $\mathrm{char}_\mathfrak{m}(X)$ defined above.

Adelic Galois representation: The product $T_{\mathrm{ad}}(\varphi) = \prod_{\mathfrak{p}\neq\mathfrak{p}_0} T_\mathfrak{p}(\varphi)$ is a free module of rank r over $A_{\mathrm{ad}} = \prod_{\mathfrak{p}\neq\mathfrak{p}_0} A_\mathfrak{p}$, called the prime-to-$\mathfrak{p}_0$ adelic Tate module of φ. It again carries natural commuting actions of $\mathrm{End}_K(\varphi)$ and of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. The latter corresponds to a continuous homomorphism

$$\rho_{\mathrm{ad}}\colon \mathrm{Gal}(K^{\mathrm{sep}}/K) \;\to\; \mathrm{Aut}_{A_{\mathrm{ad}}}(T_{\mathrm{ad}}(\varphi)) \;\cong\; \mathrm{GL}_r(A_{\mathrm{ad}}). \tag{2.2}$$

The image of ρ_{ad} is determined up to commensurability by endomorphisms, as described below.

Isogenies: A non-zero homomorphism between two Drinfeld A-modules is called an isogeny. With an isogeny, we can often reduce ourselves to Drinfeld A'-modules of smaller rank for a larger ring A', using the following fact:

Proposition 2.3 *(Hayes [5, Prop. 3.2], Devic-Pink [2, Prop. 4.3]) Let A^- be a commutative A-subalgebra of $\mathrm{End}_K(\varphi)$. Then its normalization A' is an admissible coefficient ring, and there exist a Drinfeld A'-module $\varphi'\colon A' \to K[\tau]$ and an isogeny $h\colon \varphi \to \varphi'|A$ over K. Moreover, we have $\mathrm{rank}(\varphi) = \mathrm{rank}_A(A') \cdot \mathrm{rank}(\varphi')$.*

For the remainder of the present section we fix a maximal commutative subring A^- of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ and a subfield $K' \subset K^{\mathrm{sep}}$ which is finite over K such that $A^- \subset \mathrm{End}_{K'}(\varphi)$. Set $F' := \mathrm{Quot}(A^-)$ and let $A' \subset F'$ be the normalization of A^-. Using Proposition 2.3 over K'

we choose a Drinfeld A'-module $\varphi'\colon A' \to K'[\tau]$ and an isogeny $h\colon \varphi \to \varphi'|A$ over K'. Then $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi') = A'$. Moreover φ is of special characteristic, respectively isotrivial, if and only if φ' is so. Set $r' := \mathrm{rank}(\varphi')$ and consider the adelic Galois representation associated to φ':

$$\rho'_{\mathrm{ad}}\colon \mathrm{Gal}(K^{\mathrm{sep}}/K') \;\to\; \mathrm{Aut}_{A'_{\mathrm{ad}}}(T_{\mathrm{ad}}(\varphi')) \;\cong\; \mathrm{GL}_{r'}(A'_{\mathrm{ad}}). \tag{2.4}$$

Generic characteristic: Here the image of Galois is described by:

Theorem 2.5 *(Pink-Rütsche [13]) If φ has generic characteristic, the image of ρ'_{ad} is an open subgroup of $\mathrm{GL}_{r'}(A'_{\mathrm{ad}})$, and the image of ρ_{ad} is commensurable with the subgroup*

$$\mathrm{Cent}_{\mathrm{GL}_r(A_{\mathrm{ad}})}(\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)).$$

Special characteristic: Here the endomorphism ring may be non-commutative; moreover, there may exist an admissible coefficient ring $B \subsetneqq A$ with $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi) \subsetneqq \mathrm{End}_{K^{\mathrm{sep}}}(\varphi|B)$, which puts additional constraints on the image of Galois. If φ is isotrivial, the image of ρ_{ad} is commensurable with the pro-cyclic subgroup generated by the image of Frobenius. Otherwise:

Theorem 2.6 *(Pink [12, Thm. 1.2]) If φ is non-isotrivial of special characteristic, there exists a unique admissible coefficient ring $B \subset A'$ with the properties:*

(a) The center of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$ is B.

(b) For every admissible coefficient ring $B' \subset A'$ we have $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B') \subset \mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$.

In almost all cases this subring B can be characterized independently using traces of Frobenius. In fact B is determined by the subfield $E := \mathrm{Quot}(B)$ of $F' := \mathrm{Quot}(A')$, because $B = A' \cap E$. Choose a normal integral domain $R' \subset K'$ which is finitely generated over $\mathbb{F}_p$ with $\mathrm{Quot}(R') = K'$, such that φ' extends to a Drinfeld A'-module over $\mathrm{Spec}\, R'$. For any maximal ideal $\mathfrak{m}' \subset R'$ let $\varphi'_{\mathfrak{m}'}$ denote the resulting Drinfeld A'-module over the finite residue field $k_{\mathfrak{m}'} := R'/\mathfrak{m}'$. Write the characteristic polynomial of $\mathrm{Frob}_{\mathfrak{m}'}$ associated to φ' in the form $\sum_{i=0}^{r'} a_i X^i$ with $a_i \in F'$, or in the form $\prod_{i=1}^{r'}(X - \alpha_i)$ over an algebraic closure of F', and set

$$t_{\mathfrak{m}'} \;:=\; \frac{a_1 a_{r'-1}}{a_0} \;=\; \sum_{i=1}^{r'}\sum_{j=1}^{r'} \frac{\alpha_i}{\alpha_j} \;\in\; F'. \tag{2.7}$$

Thus $t_{\mathfrak{m}'}$ is the trace of $\mathrm{Frob}_{\mathfrak{m}'}$ in the adjoint representation on $\mathrm{End}_{A'_{\mathfrak{p}'}}(T_{\mathfrak{p}'}(\varphi'))$ for any maximal ideal $\mathfrak{p}'$ different from the characteristic of $\varphi'_{\mathfrak{m}'}$. Let $E^{\mathrm{trad}} \subset F'$ be the subfield generated by the elements $t_{\mathfrak{m}'}$ for all $\mathfrak{m}'$.

Theorem 2.8 *(Pink [12, Thm. 1.3]) In the situation of Theorem 2.6, we have either*

(c) $E^{\mathrm{trad}} = E$, or

(c') $p = \mathrm{rank}(\varphi') = 2$ *and* $E^{\mathrm{trad}} = \{e^2 \mid e \in E\}$.

To describe the image of Galois let r'' be the rank and $\mathfrak{q}_0 \subset B$ the characteristic ideal of $\varphi'|B$. For any maximal ideal $\mathfrak{q} \neq \mathfrak{q}_0$ of B let $D_\mathfrak{q}$ denote the commutant of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$ in $\mathrm{End}_{B_\mathfrak{q}}(T_\mathfrak{q}(\varphi'|B)) \cong \mathrm{Mat}_{r''\times r''}(B_\mathfrak{q})$, which is an order in a central simple algebra over $\mathrm{Quot}(B_\mathfrak{q}) = E_\mathfrak{q}$. Let $D_\mathfrak{q}^1$ denote the multiplicative group of elements of $D_\mathfrak{q}$ of reduced norm 1, which is a subgroup of $\mathrm{SL}_{r''}(B_\mathfrak{q})$. Choose an element $b_0 \in B$ that generates a power of $\mathfrak{q}_0$, view it as a scalar in $\prod_{\mathfrak{q}\neq\mathfrak{q}_0} \mathrm{GL}_{r''}(B_\mathfrak{q})$, and let $\overline{\langle b_0\rangle}$ denote the closure of the subgroup generated by it. Let $K'' \subset K^{\mathrm{sep}}$ be a finite extension of K' over which all elements of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$ are defined.

Theorem 2.9 *(Devic-Pink [2, Thm. 1.2]) In the situation of Theorem 2.6, the image of* $\mathrm{Gal}(K^{\mathrm{sep}}/K'')$ *in the adelic Galois representation associated to* $\varphi'|B$ *is contained in* $\prod_{\mathfrak{q}\neq\mathfrak{q}_0} D_\mathfrak{q}^\times$ *and commensurable with*

$$\overline{\langle b_0\rangle} \cdot \prod_{\mathfrak{q}\neq\mathfrak{q}_0} D_\mathfrak{q}^1.$$

The images of Galois for φ' and φ up to commensurability can be determined from the image for $\varphi'|B$ as explained in Devic-Pink [2, §6.2]. Specifically, by [2, Prop. 6.7] the characteristic ideal $\mathfrak{p}_0' \subset A'$ of φ' is the unique maximal ideal of A' above $\mathfrak{q}_0$. For each maximal ideal $\mathfrak{q} \neq \mathfrak{q}_0$ of B there is a natural Galois equivariant isomorphism

$$T_\mathfrak{q}(\varphi'|B) \;\cong\; \prod_{\mathfrak{p}'|\mathfrak{q}} T_{\mathfrak{p}'}(\varphi'). \tag{2.10}$$

This induces a natural embedding

$$D_\mathfrak{q} \;\hookrightarrow\; \prod_{\mathfrak{p}'|\mathfrak{q}} \mathrm{End}_{A'_{\mathfrak{p}'}}(T_{\mathfrak{p}'}(\varphi')) \;\cong\; \prod_{\mathfrak{p}'|\mathfrak{q}} \mathrm{Mat}_{r'\times r'}(A'_{\mathfrak{p}'}). \tag{2.11}$$

Via Theorem 2.9 this determines the action of Galois on the Tate modules of φ'. A similar reduction process yields the action on the Tate modules of φ.

We will use Theorem 2.8 to bound E and B from below, so the case (c') might cause us problems. But we can avoid these using the following additional result:

Proposition 2.12 *In the situation of Theorem 2.6, if* $\mathrm{rank}(\varphi') = 2$*, then* $B = A'$.

Proof. To ease notation we replace K by K'. Let M denote the moduli scheme of Drinfeld A'-modules of rank 2, which is affine of relative dimension 1 over $\mathrm{Spec}(A')$. Since φ' is non-isotrivial, the associated K-valued point of M lies over a generic point of the special fiber $M_{\mathfrak{p}_0'}$ over $\mathrm{Spec}(A'/\mathfrak{p}_0')$. On the one hand this shows that after replacing K by a suitable subfield of K^{sep} we may assume that K has transcendence degree 1 over $\mathbb{F}_p$. On the other hand, since $M_{\mathfrak{p}_0'}$ is affine, there exists a place v of K with local ring $\mathcal{O}_v$ such that the

K-valued point does not extend to a morphism $\operatorname{Spec}\mathcal{O}_v \to M$. This means that φ' does not have potentially good reduction at v. After replacing K by a finite extension we may assume that φ' has semistable reduction at v. Thus after conjugating φ' by an element of $K^\times$ we may assume that its coefficients are integral at v and that its reduction has rank > 0.

Choose an extension of v to K^{sep} and let $\hat{\mathcal{O}}_v \subset K_v \subset K_v^{\mathrm{sep}}$ denote the corresponding completions of $\mathcal{O}_v \subset K \subset K^{\mathrm{sep}}$. Let $I_v \subset D_v \subset \mathrm{Gal}(K^{\mathrm{sep}}/K)$ denote the respective inertia and decomposition groups. Since φ' has rank 2, its Tate uniformization (see Drinfeld [3, §7]) must consist of a Drinfeld A'-module ψ_v of rank 1 over $\operatorname{Spec}\hat{\mathcal{O}}_v$ and an A'-lattice $\Lambda_v \subset K_v^{\mathrm{sep}}$ of rank 1 for the action of A' on K_v^{sep} via ψ_v. Here by definition an A'-lattice is a finitely generated projective A'-submodule whose intersection with any ball of finite radius is finite. This implies that any non-zero element of Λ_v has valuation < 0. Also, since Λ_v is finitely generated, after again replacing K by a finite extension we may assume that $\Lambda_v \subset K_v$.

Take any maximal ideal $\mathfrak{p}' \neq \mathfrak{p}'_0$ of A'. Then the Tate uniformization yields a natural D_v-equivariant short exact sequence

$$0 \longrightarrow T_{\mathfrak{p}'}(\psi_v) \longrightarrow T_{\mathfrak{p}'}(\varphi') \longrightarrow \Lambda_v \otimes_{A'} A'_{\mathfrak{p}'} \longrightarrow 0.$$

Here I_v acts trivially on the outer terms; so in a suitable basis its action on $T_{\mathfrak{p}'}(\varphi')$ corresponds to a homomorphism

$$I_v \longrightarrow U_{\mathfrak{p}'} := \begin{pmatrix} 1 & A'_{\mathfrak{p}'} \\ 0 & 1 \end{pmatrix} \subset \mathrm{GL}_2(A'_{\mathfrak{p}'}). \tag{2.13}$$

Let Δ denote the image of this homomorphism, viewed as a closed subgroup of the additive group of $A'_{\mathfrak{p}'}$. We claim that Δ is open in $A'_{\mathfrak{p}'}$.

To see this, we assume without loss of generality that the valuation v is normalized on K_v. Pick an element $\lambda \in \Lambda_v \smallsetminus \{0\}$ and set $c := -v(\lambda) \in \mathbb{Z}^{\geqslant 1}$. Recall that some power of $\mathfrak{p}'$ is principal, say $\mathfrak{p}'^k = (a')$ with $k > 0$ and $a' \in A'$. The Tate uniformization thus yields a natural D_v-equivariant isomorphism

$$\varphi'[\mathfrak{p}'^k] \;\cong\; \left\{x \in K_v^{\mathrm{sep}} \;\middle|\; \psi_{v,a'}(x) \in \Lambda_v\right\} \,/\, \Lambda_v.$$

Set $m := \dim_{\mathbb{F}_p}(A'/\mathfrak{p}'^k)$. Since ψ_v is a Drinfeld A'-module of rank 1 over $\hat{\mathcal{O}}_v$, we have $\psi_{v,a'} = \sum_{i=0}^m u_i \tau^i$ with $u_i \in \hat{\mathcal{O}}_v$ and $u_m \in \hat{\mathcal{O}}_v^\times$. Therefore any solution $x \in K_v^{\mathrm{sep}}$ of the equation $\psi_{v,a'}(x) = \lambda$ satisfies $p^m \cdot v(x) = v(\lambda) = -c$. It follows that the field extension $K_v(x)/K_v$ has ramification degree at least p^m/c. The image of I_v in the action on $\varphi'[\mathfrak{p}'^k]$ therefore also has order at least $p^m/c = |A'/\mathfrak{p}'^k|/c$. But this image is naturally isomorphic to the image of $\Delta \subset A'_{\mathfrak{p}'}$ in $A'/\mathfrak{p}'^k$, which therefore has index at most c. Repeating the calculation with $\mathfrak{p}'^{ki}$ in place of $\mathfrak{p}'^k$ shows that for every integer $i > 0$, the image of $\Delta \subset A'_{\mathfrak{p}'}$ in $A'/\mathfrak{p}'^{ki}$ has index at most c. Passing to the inverse limit over i we deduce that $\Delta \subset A'_{\mathfrak{p}'}$ itself has index at most c. It is therefore open, as claimed.

Now we can prove the proposition by contradiction. Suppose that $B \subsetneqq A'$, or equivalently $[F'/E] > 1$. Then we can find a maximal ideal $\mathfrak{q} \neq \mathfrak{q}_0$ of B and a maximal ideal $\mathfrak{p}'$

of A' above $\mathfrak{q}$ such that $[F'_{\mathfrak{p}'}/E_{\mathfrak{q}}] > 1$. We can also make $\mathfrak{q}$ avoid the finitely many primes of E where the central simple E-algebra $\mathrm{End}^{\circ}_{K^{\mathrm{sep}}}(\varphi'|B)$ is not split. Then its commutant $D_{\mathfrak{q}} \otimes_{B_{\mathfrak{q}}} E_{\mathfrak{q}}$ is also split, i.e., isomorphic to the ring of 2×2-matrices over $E_{\mathfrak{q}}$. Theorem 2.9 with the embedding (2.11) thus implies that the image $\Gamma_{\mathfrak{p}}$ of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ in the Galois representation on $T_{\mathfrak{p}'}(\varphi')$ is contained in a conjugate of $\mathrm{GL}_2(E_{\mathfrak{q}})$ in $\mathrm{GL}_2(F'_{\mathfrak{p}'})$. But by the claim above $\Gamma_{\mathfrak{p}}$ contains a conjugate of an open subgroup of $\left(\begin{smallmatrix} 1 & A'_{\mathfrak{p}'} \\ 0 & 1 \end{smallmatrix}\right)$. Together this is not possible with $[F'_{\mathfrak{p}'}/E_{\mathfrak{q}}] > 1$, yielding the desired contradiction. □

Independence of Frobeniuses: Next we will show that there exist Frobeniuses for φ' whose associated field extensions of F' are maximally independent. This requires some group theoretical preparation.

Consider a nonarchimedean local field L of equal characteristic p with algebraic closure $\overline{L}$. Recall that an element of $\mathrm{GL}_{r'}(L)$ is called regular semisimple if it has r' distinct eigenvalues in $\overline{L}$. Let us call an element totally split if its eigenvalues lie in L, respectively totally inert if its eigenvalues generate an unramified field extension of degree r' of L.

Lemma 2.14 *Every open subgroup of* $\mathrm{SL}_{r'}(L)$ *possesses an element* γ *such that, for any* $\delta \in \mathrm{GL}_{r'}(L)$ *sufficiently close to* γ*, every positive power of* δ *is regular semisimple and totally split. The same is true with totally inert in place of totally split.*

Proof. Let $\mathcal{O}_L$ denote the valuation ring of L and (π) its maximal ideal. Choose $i \geqslant 1$ such that the given subgroup contains all elements of $\mathrm{SL}_{r'}(\mathcal{O}_L)$ which are congruent to the identity matrix modulo (π^i). Let $\gamma_0 \in \mathrm{GL}_{r'}(\mathcal{O}_L)$ be the diagonal matrix with diagonal entries $1 + \pi^i, 1 + \pi^{i+1}, \ldots, 1 + \pi^{i+r'-1}$. Then $\gamma := \gamma_0^{r'} \det(\gamma_0)^{-1}$ lies in the given subgroup of $\mathrm{SL}_{r'}(L)$. By construction γ has r' distinct eigenvalues in L, which are all congruent to 1 modulo (π^i). For any $\delta \in \mathrm{GL}_{r'}(L)$ close to γ, the characteristic polynomial of δ is close to that of γ. But by Hensel's lemma split separable polynomials remain split separable under small deformations. Thus any $\delta \in \mathrm{GL}_{r'}(L)$ sufficiently close to γ has r' distinct eigenvalues in L, which are all congruent to 1 modulo (π^i). Moreover, if some positive power δ^n had two equal eigenvalues, two eigenvalues of δ would differ by a nontrivial root of unity congruent to 1 modulo (π), which does not exist. Thus δ^n is regular semisimple and totally split, as desired.

To prove the same assertion with totally inert in place of totally split, let L' be an unramified extension of degree r' of L with valuation ring $\mathcal{O}_{L'}$. Choose an element $\alpha \in \mathcal{O}_{L'}$ whose residue class generates the residue field extension k'/k and has trace $\mathrm{tr}_{k'/k}(\alpha) = 0$. Identify $\mathcal{O}_{L'}$ with a subring of the matrix ring $\mathrm{Mat}_{r' \times r'}(\mathcal{O}_L)$, and set $\gamma_0 := 1 + \pi^i \alpha \in \mathrm{GL}_{r'}(\mathcal{O}_L)$. Then $\det(\gamma_0) \equiv 1 + \pi^i \,\mathrm{tr}_{k'/k}(\alpha) \equiv 1$ modulo (π^{i+1}). Dividing one matrix column of γ_0 by this determinant yields an element $\gamma \in \mathrm{SL}_{r'}(\mathcal{O}_L)$ which is congruent to $1 + \pi^i \alpha$ modulo (π^{i+1}). Thus γ lies in the given subgroup. Consider any $\delta \in \mathrm{GL}_{r'}(\mathcal{O}_L)$ congruent to γ modulo (π^{i+1}). Then $(\delta - 1)/\pi^i$ has coefficients in $\mathcal{O}_L$ and is congruent to α modulo (π); hence its residue class generates k' over k. Thus the $\mathcal{O}_L$-subalgebra of $\mathrm{Mat}_{r' \times r'}(\mathcal{O}_L)$ generated by it is isomorphic to $\mathcal{O}_{L'}$. It follows that the L-subalgebra of $\mathrm{Mat}_{r' \times r'}(L)$ generated by δ is isomorphic to L'; hence δ is regular semisimple and totally

inert. Moreover, the ratio of any two distinct eigenvalues of δ is congruent to 1 modulo (π) and therefore not a root of unity. Thus any positive power δ^n is again regular semisimple and generates the same L-subalgebra, hence is again totally inert, as desired. $\square$

Now we return to Drinfeld modules of arbitrary characteristic, keeping the notation from before. For any maximal ideal $\mathfrak{m}'$ of R' we abbreviate $F'_{\mathfrak{m}'} := \mathrm{End}^{\circ}_{k^{\mathrm{sep}}_{\mathfrak{m}'}}(\varphi'_{\mathfrak{m}'})$.

Proposition 2.15 *There exist maximal ideals $\mathfrak{m}', \mathfrak{n}' \subset R'$, such that $F'_{\mathfrak{m}'}$ and $F'_{\mathfrak{n}'}$ are commutative and linearly disjoint over F', that is, their tensor product over F' is a field.*

Proof. If $r' = 1$, then $F'_{\mathfrak{m}'} = F'$ for all $\mathfrak{m}'$ and the assertion is trivial. So assume that $r' > 1$. Then φ' is not isotrivial. If φ' has special characteristic, let B, E, and $D_{\mathfrak{q}}$ be as above. Otherwise, set $B := A'$ and $E := F'$ and $D_{\mathfrak{q}} := \mathrm{Mat}_{r'\times r'}(B_{\mathfrak{q}})$.

Let $F'' \subset F'$ be the maximal subfield which is separable over E. Then there exist infinitely many maximal ideals $\mathfrak{q}$ of B which are totally split in F''. For almost all of these we also have $\mathfrak{q} \neq \mathfrak{q}_0$ and $D_{\mathfrak{q}} \cong \mathrm{Mat}_{r'\times r'}(B_{\mathfrak{q}})$. We select two distinct maximal ideals $\mathfrak{q}$ and $\mathfrak{q}'$ of B with these properties. Let

$$\tilde{\Gamma} \;\subset\; D_{\mathfrak{q}}^{\times} \times D_{\mathfrak{q}'}^{\times} \;\cong\; \mathrm{GL}_{r'}(B_{\mathfrak{q}}) \times \mathrm{GL}_{r'}(B_{\mathfrak{q}'})$$

denote the image of $\mathrm{Gal}(K^{\mathrm{sep}}/K'')$ in the Galois representation on $T_{\mathfrak{q}}(\varphi'|B) \times T_{\mathfrak{q}'}(\varphi'|B)$. Then Theorem 2.5, respectively 2.9, implies that $\tilde{\Gamma}$ contains an open subgroup of $\mathrm{SL}_{r'}(B_{\mathfrak{q}}) \times \mathrm{SL}_{r'}(B_{\mathfrak{q}'})$.

Lemma 2.16 *There exists a maximal ideal $\mathfrak{m}'$ of R' such that $F'_{\mathfrak{m}'}$ is commutative and any maximal ideal of A' above $\mathfrak{q}$ is totally split in $F'_{\mathfrak{m}'}$, while any maximal ideal of A' above $\mathfrak{q}'$ is totally inert in $F'_{\mathfrak{m}'}$.*

Proof. Using Lemma 2.14 choose an element $\gamma \in \mathrm{SL}_{r'}(B_{\mathfrak{q}})$ close to the identity element, such that for any $\delta \in \mathrm{GL}_{r'}(B_{\mathfrak{q}})$ sufficiently close to γ, every positive power of δ is regular semisimple and totally split. Likewise choose an element $\gamma' \in \mathrm{SL}_{r'}(B_{\mathfrak{q}'})$ close to the identity element, such that for any $\delta' \in \mathrm{GL}_{r'}(B_{\mathfrak{q}'})$ sufficiently close to γ', every positive power of δ' is regular semisimple and totally inert. As these elements can be chosen arbitrarily close to the identity element, we can require that $\tilde{\gamma} := (\gamma, \gamma')$ is an element of $\tilde{\Gamma}$. Since the images of Frobenius elements in $\mathrm{Gal}(K^{\mathrm{sep}}/K'')$ form a dense subset of $\tilde{\Gamma}$, there then exists a maximal ideal $\mathfrak{m}'$ of R' such that the image $\tilde{\delta} = (\delta, \delta')$ of $\mathrm{Frob}_{\mathfrak{m}'}$ satisfies the stated conditions, i.e., any positive power of δ is regular semisimple and totally spilt and any positive power of δ' is regular semisimple and totally inert. We claim that $\mathfrak{m}'$ has the desired properties.

To see this recall that $\mathrm{End}^{\circ}_{k^{\mathrm{sep}}_{\mathfrak{m}'}}(\varphi'_{\mathfrak{m}'}|B) = \mathrm{End}^{\circ}_{\ell_{\mathfrak{m}'}}(\varphi'_{\mathfrak{m}'}|B)$ for some finite field extension $\ell_{\mathfrak{m}'} \subset k^{\mathrm{sep}}_{\mathfrak{m}'}$ of $k_{\mathfrak{m}'}$, say of degree $n \geqslant 1$. Its center $E_{\mathfrak{m}'}$ is thus the field extension of E which is generated by $\mathrm{Frob}^n_{\mathfrak{m}'}$. Moreover, the minimal polynomial of $\mathrm{Frob}^n_{\mathfrak{m}'}$ over E is equal to that of δ^n and of δ'^n. As these elements are regular semisimple, it follows that $\mathrm{Frob}^n_{\mathfrak{m}'}$ is separable of degree r' over E. Thus $E_{\mathfrak{m}'}$ is separable of degree r' over E.

Next, the reduction of endomorphisms (2.1) induces a natural homomorphism of $E_{\mathfrak{m}'}$-algebras

$$E_{\mathfrak{m}'} \otimes_E \mathrm{End}^\circ_{K^{\mathrm{sep}}}(\varphi'|B) \longrightarrow \mathrm{End}^\circ_{k^{\mathrm{sep}}_{\mathfrak{m}'}}(\varphi'_{\mathfrak{m}'}|B). \tag{2.17}$$

Recall that $r' = \mathrm{rank}(\varphi')$, so that $r'' = \mathrm{rank}(\varphi'|B) = r'd$ with $d := [F'/E]$. Then $\mathrm{End}^\circ_{K^{\mathrm{sep}}}(\varphi'|B)$ is a central simple E-algebra of dimension d^2. On the other hand, since $E_{\mathfrak{m}'}$ is the center of $\mathrm{End}^\circ_{k^{\mathrm{sep}}_{\mathfrak{m}'}}(\varphi'_{\mathfrak{m}'}|B)$ and of degree r' over E, the equation $\mathrm{rank}(\varphi'|B) = r'' = r'd$ implies that $\dim_{E_{\mathfrak{m}'}}(\mathrm{End}^\circ_{k^{\mathrm{sep}}_{\mathfrak{m}'}}(\varphi'_{\mathfrak{m}'}|B)) \leqslant d^2$. Thus the source and target in (2.17) are central simple $E_{\mathfrak{m}'}$-algebras of dimension d^2, respectively $\leqslant d^2$; hence the homomorphism is an isomorphism.

Now observe that by the definition of endomorphisms $\mathrm{End}^\circ_{K^{\mathrm{sep}}}(\varphi')$ is simply the commutant of F' within $\mathrm{End}^\circ_{K^{\mathrm{sep}}}(\varphi'|B)$. The fact that $\mathrm{End}^\circ_{K^{\mathrm{sep}}}(\varphi') = F'$ thus means that F' is a maximal commutative subalgebra of $\mathrm{End}^\circ_{K^{\mathrm{sep}}}(\varphi'|B)$. Therefore the isomorphism (2.17) maps $E_{\mathfrak{m}'} \otimes_E F'$ isomorphically to a maximal commutative subalgebra of $\mathrm{End}^\circ_{k^{\mathrm{sep}}_{\mathfrak{m}'}}(\varphi'_{\mathfrak{m}'}|B)$. But again by the definition of endomorphisms $\mathrm{End}^\circ_{k^{\mathrm{sep}}_{\mathfrak{m}'}}(\varphi'_{\mathfrak{m}'})$ is simply the commutant of F' within $\mathrm{End}^\circ_{k^{\mathrm{sep}}_{\mathfrak{m}'}}(\varphi'_{\mathfrak{m}'}|B)$. As the center of $\mathrm{End}^\circ_{k^{\mathrm{sep}}_{\mathfrak{m}'}}(\varphi'_{\mathfrak{m}'}|B)$ is $E_{\mathfrak{m}'}$, this commutant is equal to the commutant of the image of $E_{\mathfrak{m}'} \otimes_E F'$, and hence equal to the image of $E_{\mathfrak{m}'} \otimes_E F'$. This shows that $F'_{\mathfrak{m}'} := \mathrm{End}^\circ_{k^{\mathrm{sep}}_{\mathfrak{m}'}}(\varphi'_{\mathfrak{m}'})$ is isomorphic to $E_{\mathfrak{m}'} \otimes_E F'$ over F'. In particular $F'_{\mathfrak{m}'}$ is commutative.

Finally, the fact that δ^n is totally split implies that $\mathfrak{q}$ is totally split in the field extension $E_{\mathfrak{m}'} = E(\mathrm{Frob}^n_{\mathfrak{m}'})$. It follows that any maximal ideal of A' above $\mathfrak{q}$ is totally split in $E_{\mathfrak{m}'} \otimes_E F' \cong F'_{\mathfrak{m}'}$. Likewise, the fact that δ'^n is totally inert implies that $\mathfrak{q}'$ is totally inert in $E_{\mathfrak{m}'}$. Since by assumption $\mathfrak{q}'$ is totally split in the maximal separable subextension of F'/E, every maximal ideal of A' above $\mathfrak{q}'$ has the same residue field as $\mathfrak{q}$. Thus every maximal ideal of A' above $\mathfrak{q}'$ is totally inert in $E_{\mathfrak{m}'} \otimes_E F' \cong F'_{\mathfrak{m}'}$. Therefore $\mathfrak{m}'$ has all the desired properties. □

To finish the proof of Proposition 2.15, choose any $\mathfrak{m}'$ as in Lemma 2.16. Applying Lemma 2.16 with the roles of $\mathfrak{q}$ and $\mathfrak{q}'$ reversed, we also choose a maximal ideal $\mathfrak{n}'$ of R such that $F'_{\mathfrak{n}'}$ is commutative and that any maximal ideal of A' above $\mathfrak{q}'$ is totally split in $F'_{\mathfrak{n}'}$, while any maximal ideal of A' above $\mathfrak{q}$ is totally inert in $F'_{\mathfrak{n}'}$. Together these properties imply that $F'_{\mathfrak{m}'}$ and $F'_{\mathfrak{n}'}$ are linearly disjoint over F', and we are done. □

3 Computer algebra prerequisites

In this section we briefly recall the methods from computer algebra which are used in the rest of the article. As a general reference, one can consult for example the book "Computational Commutative Algebra 1" by Kreuzer and Robbiano [7]. Many of the operations mentioned here are implemented in common computer algebra systems.

Representation of algebras and fields: Any finitely generated $\mathbb{F}_p$-algebra R can be represented as the quotient of a polynomial ring $\mathbb{F}_p[\underline{X}] := \mathbb{F}_p[X_1, \ldots, X_r]$ by a finitely

generated ideal J. Using Gröbner bases one can effectively decide whether J is prime, or equivalently whether R is integral. The localization of R with respect to finitely many elements $x_1, \ldots, x_s$ can be represented on the same footing as $R' := R[1/x_1 \cdots x_s] = R[Y]/(x_1 \cdots x_s Y - 1)$.

Any finitely generated field K over $\mathbb{F}_p$ can be represented as the field of fractions of $R := \mathbb{F}_p[\underline{X}]/J$ for a prime ideal J. Any calculation with ideals in $K[Y_1, \ldots, Y_s]$ reduces to one in $R'[Y_1, \ldots, Y_s]$ for a suitable localization R' of R.

Basic operations on elements: Let $R = \mathbb{F}_p[\underline{X}]/J$ be a finitely generated $\mathbb{F}_p$-algebra. Using a Gröbner basis of J, for every element of R one can compute its unique reduced representative with respect to this basis. Thus one can effectively decide whether two given elements of R are equal. If R is integral, one can therefore also decide whether two elements of its field of fractions are equal.

Using Gröbner bases one can also test whether a given element is contained in a given ideal of R. In particular, if R is integral, one can test whether one element divides another in R and, if so, determine the quotient. Thus one can decide whether an element of the field of fractions already lies in R.

Ideals and subrings: For any homomorphism $f\colon S \to R$ of finitely generated $\mathbb{F}_p$-algebras and any ideal J of R one can effectively determine the ideal $f^{-1}(J)$ of S. In particular, one can determine $\operatorname{Ker}(f)$ and hence obtain an explicit representation of $\operatorname{Im}(f) \cong S/\operatorname{Ker}(f)$. Applying this when S is a polynomial ring over $\mathbb{F}_p$, one can thus explicitly describe the subalgebra generated by finitely many given elements of R.

Furthermore, one can construct a sequence of all maximal ideals of R.

Normalization: If R is integral with field of fractions K, one can effectively describe the normalization R' of R together with the inclusions $R \hookrightarrow R' \hookrightarrow K$, see for example Singh-Swanson [16].

Field extensions: Let K be a field which is finitely generated over $\mathbb{F}_p$. Then for any irreducible polynomial $P \in K[X]$ one can write down a field extension of K generated by a root of P, namely as $K[X]/(P)$. Given an arbitrary polynomial $P \in K[X]$, one can effectively find its irreducible factors with multiplicities by Steel [17]. By iteration one can therefore effectively describe a splitting field of P over K.

For any field extension $K \subset L$ and any element $x \in L$, one can effectively decide whether x is algebraic over K and, if so, determine its minimal polynomial over K. By factoring a polynomial over L one can determine all its roots in L. In particular, one can therefore determine all conjugates of x over K in L.

Also, for any simple finite extension $K \subset K'$, one can effectively describe all homomorphisms $K' \to L$ over K, by mapping the generator of K' to roots of its minimal polynomial. By iteration over simple extensions, one can effectively describe all homomorphisms $K' \to L$ over K for any finite extension $K \subset K'$.

Moreover, one can effectively decide whether two field extensions K'/K and K''/K are linearly disjoint in that their tensor product $K' \otimes_K K''$ is a field. Indeed, if K'/K is simple,

this is equivalent to the minimal polynomial of the generator over K remaining irreducible over K''. The general case follows by iteration over simple extensions.

For any field K we let $K^{\mathrm{sep}} \subset \overline{K}$ denote a separable, respectively an algebraic closure of K. Though one cannot effectively construct these and compute in them, one can calculate in any finite extension and enlarge it whenever necessary. Throughout, all finite separable extensions of K are tacitly assumed to be contained in K^{sep}.

Solving polynomial equations: Let $\mathcal{S}$ be a system of finitely many polynomial equations in several variables over K which is known to have only finitely many solutions in $\overline{K}$. Then one can determine a finite extension K' of K such that all solutions of $\mathcal{S}$ lie in K' and one can find those solutions; Lazard [9] gives a possible way of doing this.

Intermediate fields: For any finite separable field extension $K \subset L$ one can effectively find a Galois closure $\tilde{L}$ and determine the Galois group of $\tilde{L}/K$. For every subgroup of this Galois group one can effectively determine generators of the associated intermediate field. In this way one can make a finite list of all intermediate fields of L/K.

More generally let L/K be an arbitrary finite field extension with maximal separable subextension L'/K. Then any intermediate field of L/K is a purely inseparable field extension of an intermediate field of L'/K. If K has transcendence degree 1 over $\mathbb{F}_p$, any purely inseparable extension is determined by its degree and generated by p-power roots; hence one can also make a finite list of all intermediate fields of L/K in this case.

Transcendence degree 1: We will often deal with finitely generated integral domains over $\mathbb{F}_p$ of transcendence degree 1. Any such ring B possesses a transcendent element t such that B is a finitely generated $\mathbb{F}_p[t]$-module. One can thus present B efficiently via a basis as $\mathbb{F}_p[t]$-module and a multiplication table with entries in $\mathbb{F}_p[t]$. For any other such element $t' \in B$ one can translate this presentation over $\mathbb{F}_p[t]$ into one over $\mathbb{F}_p[t']$, using commutative algebra over $\mathbb{F}_p[t, t']$.

In the same way one can describe any torsion free commutative or non-commutative B-algebra which is finitely generated as a B-module. This reduces many computations with modules and ideals to linear algebra over the principal ideal domain $\mathbb{F}_p[t]$.

Modules: For any finitely generated B-module M one can find its rank and the elementary divisors as an $\mathbb{F}_p[t]$-module. In particular, one can decide whether M is finite and, if so, make a list of its elements. If M is torsion free, for any submodule N of M one can effectively compute the saturation $\{m \in M \mid \exists\, b \in B \smallsetminus \{0\} \colon bm \in N\}$. In particular, for any $\mathrm{Quot}(B)$-subspace V of $M \otimes_B \mathrm{Quot}(B)$ one can determine $V \cap M$.

Admissible coefficient rings: Let F be the function field of an irreducible smooth projective curve C over $\mathbb{F}_p$. Let A be the subring of elements of F which are regular outside a fixed point ∞ of C. We call such A an admissible coefficient ring. For any ideal $\mathfrak{a} \subset A$, one can compute its prime factorization and the number $\dim_{\mathbb{F}_p}(A/\mathfrak{a})$. One can also compute the degree $\deg(\infty)$ of the residue field at ∞ over $\mathbb{F}_p$. For any integer $n \geqslant 0$, the finite set of elements a of A with $a = 0$ or $\dim_{\mathbb{F}_p}(A/Aa) \leqslant d$ is just the Riemann-Roch space $\Gamma\big(C, \mathcal{O}_C(\lfloor \frac{n}{\deg(\infty)} \rfloor \infty)\big)$, which can be effectively determined by Hess [6].

We finish this section with two more specialized facts.

Lemma 3.1 *For any simple finite field extension $F(x)$ of F, there exists an integer $m \geqslant 1$ such that $\bigcap_{n\geqslant 1} F(x^n) = F(x^m)$. Moreover, knowing the minimal polynomial of x over F one can effectively find such m as well as the minimal polynomial and the degree of x^m over F. In particular, one can effectively decide whether $F(x^n) = F(x)$ for all $n \geqslant 1$.*

Proof. Choose m such that $[F(x^m)/F]$ is minimal. Then for any $n \geqslant 1$, we have $F(x^m) = F(x^{nm}) \subset F(x^n)$. This proves the first statement of the lemma.

To find m effectively, note first that if $x = 0$, then $m = 1$ does the job. Otherwise, let $P(X)$ be the minimal polynomial of x over F. By looking at the coefficients of $P(X)$ one can find the largest power p^i such that $P(X) = Q(X^{p^i})$ for some polynomial $Q(X)$. Then $Q(X)$ is the minimal polynomial of x^{p^i} over F. After replacing x by x^{p^i} we can thus assume that $P(X) \notin F[X^p]$, in other words that $P(X)$ is separable. Let $\sigma_1, \ldots, \sigma_r$ be the pairwise distinct homomorphisms over F from $F(x)$ into a separable closure F^{sep} of F. Then $P(X) = \prod_{i=1}^r (X - \sigma_i(x))$. Consider the polynomial

$$Q(X) \ := \prod_{i\neq j} \Big(X - \frac{\sigma_i(x)}{\sigma_j(x)}\Big).$$

Being symmetric functions in $\sigma_1(x), \ldots, \sigma_r(x)$, the coefficients of Q lie in F and can be effectively computed from those of P. We can then effectively compute the factorization of $Q(X)$ into monic irreducible polynomials over F. By determining which of their coefficients are algebraic over $\mathbb{F}_p$ we can effectively decide which of these factors are defined over the constant field of F. From these we can effectively find a positive integer m such that all their roots are m-th roots of unity. This integer has the property that for all $n \geqslant 1$ and $i \neq j$, if $\sigma_i(x^n) = \sigma_j(x^n)$, then $\sigma_i(x^m) = \sigma_j(x^m)$. By Galois theory this implies that $F(x^m) \subset F(x^n)$, so m has the desired property.

Using symmetric functions again one can now effectively compute the polynomial $\prod_{i=1}^r (X - \sigma_i(x^m))$ in $F[X]$. As this is a power of the minimal polynomial of x^m over F, by factorization one can effectively determine this minimal polynomial, and hence also its degree. This proves the second statement of the lemma.

In particular, knowing the degrees of of the minimal polynomials of x and x^m over F one can effectively decide whether $F(x^m) = F(x)$. This implies the last statement. □

Computation in $K[\tau]$: As before let K be a finitely generated field over $\mathbb{F}_p$. By definition an element $u = \sum_{i=0}^n u_i \tau^i \in K[\tau]$ with $u_n \neq 0$ has degree $\deg_\tau(u) := n$, and the zero element has degree $-\infty$. This degree is additive in products, that is, for any $u, v \in K[\tau]$ we have $\deg_\tau(uv) = \deg_\tau(u) + \deg_\tau(v)$. Also, any left ideal of the ring $K[\tau]$ is principal, and $K[\tau]^\times = K^\times$.

Proposition 3.2 *For any elements $u, v \in K[\tau]$ with $v \neq 0$ there exist unique $q, r \in K[\tau]$ with $u = qv + r$ and $\deg_\tau(r) < \deg_\tau(v)$. Any finite subset of $K[\tau]$ possesses a greatest common right divisor and a least common left multiple, which are unique up to left multiplication by an element of $K^\times$. All of these can be computed effectively.*

Proof. For the first statement, that $K[\tau]$ is euclidean with respect to right division, see Goss [4, §1.6]. That q and r can be computed effectively is shown as in a commutative polynomial ring, for instance by induction on $\deg_\tau(u)$ and comparison of the highest coefficients. The corresponding euclidean algorithm yields the greatest common right divisor of any two, and consequently of any finite number of, elements of $K[\tau]$.

For the least common left multiple of a finite subset $\mathcal{S} \subset K[\tau]$ consider the left $K[\tau]$-module $M := \bigoplus_{u\in\mathcal{S}} K[\tau]/K[\tau]u$. The common left multiples of $\mathcal{S}$ are precisely those elements of $K[\tau]$ which annihilate the element $(1 + K[\tau]u)_{u\in\mathcal{S}}$ of M. Thus they form a left ideal of $K[\tau]$, which is therefore principal. Any generator of this ideal is a least common left multiple of $\mathcal{S}$. If $0 \in \mathcal{S}$, this least common left multiple is 0; otherwise its degree in τ is at most $\dim_K(M) = \sum_{u\in\mathcal{S}} \deg_\tau(u) < \infty$. In this case it can be determined by a bounded number of polynomial calculations over K. □

4 Bits of algorithms

Throughout this section we fix a Drinfeld A-module $\varphi\colon A \to K[\tau]$ over a finitely generated field K.

Proposition 4.1 *One can effectively determine the rank and height and characteristic ideal $\mathfrak{p}_0$ of φ, hence whether φ has generic or special characteristic, and whether φ is ordinary resp. isotrivial.*

Proof. Choose a non-constant $t \in A$ and write $\varphi_t = \sum_{i=0}^n x_i\tau^i$ with $x_n \neq 0$. By definition the rank of φ is the quotient $n/\dim_{\mathbb{F}_p}(A/At)$. By our computer algebra prerequisites, it can therefore be determined effectively. Also φ has generic characteristic if and only if x_0 is transcendental over $\mathbb{F}_p$. Specifically $\mathfrak{p}_0$ is defined as the kernel of the homomorphism $A \to K$, $a \mapsto d\varphi_a$. By our computer algebra prerequisites, it can be determined effectively.

If $\mathfrak{p}_0 \neq 0$, one can choose a new element $t \in \mathfrak{p}_0 \smallsetminus \{0\}$. Write $\varphi_t = \sum_{i=m}^n x_i\tau^i$ with $x_m \neq 0$, and write $At = \mathfrak{p}_0^k\mathfrak{a}$ for an ideal $\mathfrak{a}$ prime to $\mathfrak{p}_0$. Then by definition the height of φ is the quotient $m/\dim_{\mathbb{F}_p}(A/\mathfrak{p}_0^k)$, and φ is ordinary if and only if its height is 1. This can therefore also be determined effectively.

Next φ is isotrivial if and only if there exists $y \in \overline{K}^\times$ such that $y^{-1}\varphi_a y$ has coefficients in a finite field for every $a \in A$. We claim that it is enough to check this condition for the chosen element $t \in A$. Indeed, if it holds for t, after replacing φ by $y^{-1}\varphi y$ we may assume that φ_t has coefficients in a finite field $k \subset \overline{K}$. Setting $B' := \mathbb{F}_p[t]$, the restriction $\varphi|B'$ is then a Drinfeld B'-module defined over k. Thus there exists a finite extension $k' \subset \overline{K}$ of k with $\mathrm{End}_{\overline{K}}(\varphi|B') = \mathrm{End}_{k'}(\varphi|B') \subset k'[\tau]$. Since φ induces an embedding $A \hookrightarrow \mathrm{End}_{\overline{K}}(\varphi|B')$, it follows that φ itself is defined over k' and is therefore isotrivial, as claimed.

To test the condition for t, observe that $y^{-1}\varphi_t y = \sum_{i=0}^n x_i y^{q^i-1}\tau^i$. A direct calculation shows that there exists $y \in \overline{K}^\times$ such that all $x_i y^{q^i-1}$ are algebraic over $\mathbb{F}_p$ if and only if the ratios $x_i^{q^n-1}/x_n^{q^i-1}$ are algebraic over $\mathbb{F}_p$ for all $0 \leqslant i < n$. By our computer algebra prerequisites, this condition can be tested effectively. □

Proposition 4.2 *One can effectively find A' and φ' and h in Proposition 2.3, as well as an isogeny $h'\colon \varphi'|A \to \varphi$ over K and an element $a \in A \smallsetminus \{0\}$ with $h'h = \varphi_a$.*

Proof. We follow the construction in Devic-Pink [2, Prop. 4.3]. By our computer algebra prerequisites, one can effectively describe the normalization A' and, since A'/A^- is finite, find an element $a \in A \smallsetminus \{0\}$ satisfying $A'a \subset A^-$. Choose a system $\mathcal{R}$ of non-zero representatives of cosets of A' modulo A^-.

For simplicity we denote the given embedding $A^- \hookrightarrow \mathrm{End}_K(\varphi)$ by $a^- \mapsto \varphi_{a^-}$. Using Proposition 3.2, for any $a' \in \mathcal{R}$ one can effectively find the least common left multiple of φ_a and $\varphi_{a'a}$ in $K[\tau]$ and write it in the form $h_{a'}\varphi_{a'a}$ for some $h_{a'} \in K[\tau]$. Since A' is commutative, we have $\varphi_a\varphi_{a'a} = \varphi_{a'a}\varphi_a$. Thus this element is a common left multiple of $\varphi_{a'a}$ and φ_a, hence a left multiple of $h_{a'}\varphi_{a'a}$; hence φ_a is a left multiple of $h_{a'}$. Next, using Proposition 3.2 again one can effectively find the least common left multiple $h \in K[\tau]$ of the elements $h_{a'}$ for all $a' \in \mathcal{R}$. Since φ_a is already a common left multiple of these elements, it is a left multiple of h; in other words we have $\varphi_a = h'h$ for some $h' \in K[\tau]$.

This construction has the following effect. For any non-zero element $u \in K[\tau]$ consider the finite subgroup scheme $\ker(u)$ of $\mathbb{G}_{a,K}$. For any two non-zero elements $u, v \in K[\tau]$ with least common left multiple wv we then have $\ker(u) + \ker(v) = \ker(wv)$ and hence

$$v(\ker(u)) \;=\; v(\ker(u) + \ker(v)) \;=\; v(\ker(wv)) \;=\; \ker(w).$$

In the above construction we therefore have $\varphi_{a'a}(\ker(\varphi_a)) = \ker(h_{a'})$. Summing over all $a' \in \mathcal{R}$ implies that

$$\sum_{a' \in \mathcal{R}} \varphi_{a'a}(\ker(\varphi_a)) \;=\; \ker(h).$$

Thus h is the element f from the proof of [2, Prop. 4.3]. There we constructed a unique Drinfeld A'-module $\varphi'\colon A' \to K[\tau]$ such that h is an isogeny $\varphi \to \varphi'|A$. Since $h'h = \varphi_a$ with $a \neq 0$, it follows that h' is an isogeny $\varphi'|A \to \varphi$. To find φ' explicitly, for any element $a' \in A'$ we have $a'a \in A^-$ and can therefore calculate

$$\varphi'_{a'}h\varphi_a = \varphi'_{a'}\varphi'_a h = \varphi'_{a'a}h = h\varphi_{a'a}.$$

This means that $\varphi'_{a'}$ is the quotient of $h\varphi_{a'a}$ upon right division by $h\varphi_a$ in $K[\tau]$, which can again be computed explicitly by Proposition 3.2. □

Proposition 4.3 *Let $f \in \mathrm{End}_K(\varphi)$. As an element of the commutative subfield $F(f)$ of $\mathrm{End}^\circ_K(\varphi)$ of finite degree over F, it possesses a unique minimal polynomial $\min_f \in F[X]$. This polynomial has coefficients in A, and writing $\min_f(X) = X^k + a_1X^{k-1} + \ldots + a_k$, for each $1 \leqslant i \leqslant k$ we have*

$$\deg_\tau(\varphi_{a_i}) \leqslant i \cdot \deg_\tau(f),$$

with equality for $i = k$.

Proof. Since $\mathrm{End}_K(\varphi)$ is finitely generated as an A-module and A is integrally closed, the minimal polynomial has coefficients in A.

Let A' be the integral closure of $A[f]$ within $F' := F[f]$. By Proposition 2.3, this is an admissible coefficient ring and there exist a Drinfeld A'-module φ' and an isogeny $h\colon \varphi \to \varphi'|A$ over K. This induces an isomorphism of F-algebras $\varepsilon\colon \mathrm{End}_K^\circ(\varphi) \xrightarrow{\sim} \mathrm{End}_K^\circ(\varphi'|A)$ satisfying $\varepsilon(g)h = hg$ for all $g \in \mathrm{End}_K^\circ(\varphi)$; in particular $\varepsilon(f)h = hf$. Thus f and $\varepsilon(f) = \varphi'_f$ have the same degree in τ and the same minimal polynomial over F. After replacing φ by $\varphi'|A$, we may therefore assume that $A' \subset \mathrm{End}_K(\varphi)$.

Since $A \subset A'$ is an inclusion of admissible coefficient rings, there is a unique place ∞' of F' lying over ∞. For $f \in F'$ this implies that $\min_f$ has a unique slope at ∞. More precisely, let $\mathrm{ord}_{\infty'}$ be the normalized valuation on F' associated to ∞' and $\deg(\infty')$ the degree of its residue field over $\mathbb{F}_p$. Then by the definition of $\mathrm{rank}(\varphi')$ we have

$$\deg_\tau(\varphi'_{a'}) \;=\; \mathrm{rank}(\varphi') \cdot \dim_{\mathbb{F}_p}(A'/A'a') \;=\; -\mathrm{rank}(\varphi') \cdot \deg(\infty') \cdot \mathrm{ord}_{\infty'}(a')$$

for all $a' \in A'$. In other words $\deg_\tau(\varphi'_{a'}) = -v(a')$, where $v := \mathrm{rank}(\varphi') \cdot \deg(\infty') \cdot \mathrm{ord}_{\infty'}$ is a valuation on F' equivalent to $\mathrm{ord}_{\infty'}$. Now the slope of $\min_f$ with respect to v is $-v(f)$; hence for each i we have

$$\deg_\tau(\varphi_{a_i}) \;=\; \deg_\tau(\varphi'_{a_i}) \;=\; -v(a_i) \;\leqslant\; -i \cdot v(f) \;=\; i \cdot \deg_\tau(f),$$

with equality for $i = k$. □

Proposition 4.4 *For any $f \in \mathrm{End}_K(\varphi)$, one can effectively compute $\min_f$.*

Proof. Since $F[f]$ is a commutative subfield of $\mathrm{End}_K^\circ(\varphi)$, the degree k of $\min_f$ divides $\mathrm{rank}(\varphi)$. Write $\min_f(X) = X^k + a_1X^{k-1} + \ldots + a_k$ with $a_i \in A$. By the definition of $\mathrm{rank}(\varphi)$ and Proposition 4.3, for each $1 \leqslant i \leqslant k$ we then have $a_i = 0$ or

$$\dim_{\mathbb{F}_p}(A/Aa_i) = \frac{\deg_\tau(\varphi_{a_i})}{\mathrm{rank}(\varphi)} \leqslant \frac{i \cdot \deg_\tau(f)}{\mathrm{rank}(\varphi)}.$$

Thus each a_i lies in a finite set that can be effectively determined. For each choice of candidates for the a_i one can effectively compute $f^k + \varphi_{a_1} f^{k-1} + \cdots + \varphi_{a_k}$ in $K[\tau]$ and decide whether it is zero. Thus $\min_f$ can be computed by letting k run through the divisors of r in ascending order and checking all possible choices of coefficients a_i. □

Proposition 4.5 *If K is finite, one can effectively*

(a) find a finite separable extension K' of K such that $\mathrm{End}_{K'}(\varphi) = \mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$,

(b) compute the dimensions of $\mathrm{End}_{K^{\mathrm{sep}}}^\circ(\varphi)$ and of its center over F, and

(c) describe the center of $\mathrm{End}_{K^{\mathrm{sep}}}^\circ(\varphi)$ as an abstract field extension of F.

Proof. Set $\mathrm{Frob}_K := \tau^{[K/\mathbb{F}_p]}$. Then for any finite extension K_n/K of degree n, the center of $\mathrm{End}^\circ_{K_n}(\varphi)$ is a finite field extension of F that is generated by $\mathrm{Frob}_{K_n} := \tau^{[K_n/\mathbb{F}_p]} = \mathrm{Frob}_K^n$. As a special case of Proposition 4.4 one can effectively determine the minimal polynomial of Frob_K over F. Using Lemma 3.1, one can therefore effectively find an integer $m \geqslant 1$ such that $\bigcap_{n\geqslant 1} F(\mathrm{Frob}_K^n) = F(\mathrm{Frob}_K^m)$. Whenever $K_m \subset K_n$, it follows that $\mathrm{Frob}_{K_m} = \mathrm{Frob}_K^m$ lies in the center of $\mathrm{End}^\circ_{K_n}(\varphi)$. In particular, every element of $\mathrm{End}_{K_n}(\varphi)$ commutes with Frob_{K_m} and is therefore defined over K_m; in other words we have $\mathrm{End}_{K_n}(\varphi) = \mathrm{End}_{K_m}(\varphi)$. Varying n we deduce that $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi) = \mathrm{End}_{K_m}(\varphi)$, proving (a).

By Lemma 3.1 one can also effectively calculate the minimal polynomial of $\mathrm{Frob}_{K_m} = \mathrm{Frob}_K^m$ over F. This in turn determines the center $F(\mathrm{Frob}_{K_m})$ as an abstract field extension of F, proving (c). In particular, its dimension $d := \dim_F(F(\mathrm{Frob}_{K_m}))$ can be effectively computed. Moreover, let e^2 be the dimension of $\mathrm{End}^\circ_{K_m}(\varphi)$ over $F(\mathrm{Frob}_{K_m})$. Since K_m is finite, we then have $de = \mathrm{rank}(\varphi)$. Thus e can be effectively computed from d and $\mathrm{rank}(\varphi)$, which implies (b). □

Proposition 4.6 *One can effectively construct a normal integral domain $R \subset K$ which is finitely generated over $\mathbb{F}_p$ with $\mathrm{Quot}(R) = K$, such that φ extends to a Drinfeld A-module over $\mathrm{Spec}\, R$.*

Proof. By assumption K is given as the fraction field of a finitely generated integral domain R. For all elements a of a finite set of non-zero generators of the $\mathbb{F}_p$-algebra A, adjoin to R all coefficients of $\varphi_a \in K[\tau]$ as well as the inverses of their highest coefficients. Then R is still a finitely generated integral domain with $\mathrm{Quot}(R) = K$, and φ extends to a Drinfeld A-module over $\mathrm{Spec}\, R$. Finally, replace R by its normalization. By our computer algebra prerequisites, all these operations can be carried out effectively. □

Proposition 4.7 *For any maximal ideal $\mathfrak{m} \subset R$ one can effectively*

(a) determine the minimal and characteristic polynomials $\min_{\mathfrak{m}}$ and $\mathrm{char}_{\mathfrak{m}}$ of $\mathrm{Frob}_{\mathfrak{m}}$, and

(b) decide whether $\mathrm{End}^\circ_{k_{\mathfrak{m}}^{\mathrm{sep}}}(\varphi_{\mathfrak{m}})$ is commutative and in that case describe it as an abstract field extension of F.

Proof. For any $\mathfrak{m}$ we have an explicit description of the reduction $\varphi_{\mathfrak{m}}$ over the finite residue field $k_{\mathfrak{m}}$. By Proposition 4.4 we can therefore effectively determine the associated minimal polynomial of $\mathrm{Frob}_{\mathfrak{m}} := \tau^{[k_{\mathfrak{m}}/\mathbb{F}_p]}$ over F. Consequently we can also effectively determine the characteristic polynomial $\mathrm{char}_{\mathfrak{m}}(X) := \min_{\mathfrak{m}}(X)^{\mathrm{rank}(\varphi)/\deg(\min_{\mathfrak{m}})}$, proving (a). Part (b) is a direct consequence of Proposition 4.5 (b) and (c). □

5 Searching for endomorphisms

We keep (A, K, φ) as before.

Proposition 5.1 *For any integer $d \geqslant 0$, one can effectively determine a finite separable extension K' of K, such that all elements of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ of degree d in τ are defined over K', and determine these endomorphisms.*

Proof. Choose a finite set S of generators of the $\mathbb{F}_p$-algebra A. Then an element $u \in K[\tau]$ is an endomorphism of φ if and only if $u\varphi_a = \varphi_a u$ for all $a \in S$. With the Ansatz $u = \sum_{i=0}^{d} u_i \tau^i$ these equations amount to finitely many polynomial equations in the coefficients u_i. We also know that there are at most finitely many solutions. By our computer algebra prerequisites, one can therefore effectively describe all these solutions and a common field of definition K' for them. Since all endomorphisms over $\overline{K}$ are already defined over K^{sep}, one can choose K' separable over K. □

Next consider the natural A-algebra homomorphism

$$\mathrm{End}_{K^{\mathrm{sep}}}(\varphi) \to K^{\mathrm{sep}},\ u = \textstyle\sum_i u_i \tau^i \mapsto u_0. \tag{5.2}$$

Proposition 5.3 *Assume that φ has generic characteristic. Then:*

(a) The homomorphism (5.2) is injective.

(b) For any $u_0 \in K^{\mathrm{sep}}$, one can effectively decide whether there exists $u \in \mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ with lowest coefficient u_0 and, if so, find it.

(c) If $u \in \mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ has lowest coefficient $u_0 \in K$, then $u \in K[\tau]$.

Proof. By assumption the homomorphism is injective on A. Since $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ is an integral ring extension of A, the homomorphism is therefore injective.

Suppose that $u_0 \in K^{\mathrm{sep}}$ is the lowest coefficient of some element $u \in \mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$. Let $\min_u(X) \in A[X]$ be the minimal polynomial of u over A. Then $\min_u(u_0) = 0$, hence u_0 is integral algebraic over A, and by injectivity $\min_u$ is also the minimal polynomial of u_0 over A. Write $\min_u(X) = X^k + a_1 X^{k-1} + \ldots + a_k$ with $a_i \in A$. Then $\deg_\tau(u) = \deg_\tau(\varphi_{a_k})/k$ by Proposition 4.3. Here the right hand side depends only on the joint minimal polynomial of u and u_0; hence $\deg_\tau(u)$ is uniquely determined by u_0.

Now consider an arbitrary element $u_0 \in K^{\mathrm{sep}}$. By our computer algebra prerequisites one can effectively decide whether u_0 is algebraic over F and, if so, determine its minimal polynomial $\min_{u_0}$ over F. In particular, one can decide whether u_0 is integral over A, which is necessary for it to be the lowest coefficient of an endomorphism. If so, write $\min_{u_0}(X) = X^k + a_1 X^{k-1} + \ldots + a_k$ with $a_i \in A$; then we can also compute the number $d := \deg_\tau(\varphi_{a_k})/k$. By the above arguments any endomorphism $u \in \mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ with lowest coefficient u_0 then satisfies $\deg_\tau(u) = d$.

To see whether such u actually exists we use the ansatz $u = \sum_{i=0}^{d} u_i \tau^i$ with $u_i \in K^{\mathrm{sep}}$. Pick an arbitrary non-constant $t \in A$ and write $\varphi_t = \sum_{j=0}^{n} x_j \tau^j$. Expand the equation $u\varphi_t = \varphi_t u$ in the form

$$\sum_{i,j} u_i x_j^{p^i} \tau^{i+j} \;=\; \sum_i u_i \tau^i \sum_j x_j \tau^j \;=\; \sum_j x_j \tau^j \sum_i u_i \tau^i \;=\; \sum_{i,j} x_j u_i^{p^j} \tau^{i+j}.$$

Comparing the coefficients of τ^ℓ for each $0 < \ell \leqslant d$ yields an expression for $(x_0 - x_0^{p^\ell})u_\ell$ as a polynomial in $x_1, \ldots, x_n$ and $u_0, \ldots, u_{\ell-1}$. Since t is non-constant and φ has generic characteristic, the element x_0 is transcendental over $\mathbb{F}_p$. Thus $x_0 - x_0^{p^\ell} \neq 0$, and so we obtain explicit recursion relations for all u_ℓ in terms of the constant coefficient u_0. Plugging these into the equations obtained by comparing the coefficients of τ^ℓ for $\ell > d$ then yields explicit polynomial equations in u_0 over K. These equations are fulfilled if and only if the desired u exists, and in that case we can effectively find it. This proves (b).

Finally, the recursion relations show that $u \in K(u_0)[\tau]$ if it exists. In particular this implies (c). □

Now we fix a non-constant element $t \in A$ and set $\delta_t := \deg_\tau(\varphi_t) > 0$. We view $K^{\mathrm{sep}}[\tau]$ as an $\mathbb{F}_p[t]$-module via the multiplication $(a, u) \mapsto \varphi_a u$. Note that $K^{\mathrm{sep}}[\tau]$ is torsion free, so every finitely generated $\mathbb{F}_p[t]$-submodule is free.

Definition 5.4 *We call a sequence of non-zero elements $m_1, \ldots, m_n$ of $K^{\mathrm{sep}}[\tau]$* orthogonal *if for all $a_1, \ldots, a_n \in \mathbb{F}_p[t]$ we have*

$$\deg_\tau\Big(\sum_{i=1}^{n} \varphi_{a_i} m_i\Big) \;=\; \max\big\{\deg_\tau(\varphi_{a_i} m_i) \;\big|\; 1 \leqslant i \leqslant n\big\}.$$

Here $\deg_\tau(\varphi_{a_i} m_i) = \deg_t(a_i) \cdot \delta_t + \deg_\tau(m_i)$. In particular, we have $\deg_\tau(\varphi_{a_i} m_i) = -\infty$ if and only if $\deg_t(a_i) = -\infty$ if and only if $a_i = 0$. Thus the definition permits $\sum_{i=1}^n \varphi_{a_i} m_i$ to be zero only if all a_i are zero; hence any orthogonal sequence is $\mathbb{F}_p[t]$-linearly independent.

Proposition 5.5 *Given a finite extension K' of K and an $\mathbb{F}_p[t]$-submodule M of $K'[\tau]$ with an orthogonal basis $m_1, \ldots, m_n$, for any $f \in K'[\tau]$, one can effectively decide whether $f \in M$ and if so, one can effectively compute its coefficients with respect to that basis.*

Proof. If $f = \sum_i \varphi_{a_i} m_i$ with $a_i \in \mathbb{F}_p[t]$, by Definition 5.4 we must have $\deg_t(a_i) \cdot \delta_t + \deg_\tau(m_i) \leqslant \deg_\tau(f)$ for all i. Thus each $\deg_t(a_i)$ is bounded by an explicit number. Writing each $a_i = \sum_j a_{ij} t^j$ with finitely many $a_{ij} \in \mathbb{F}_p$ to be determined, the equation $f = \sum_i \varphi_{a_i} m_i$ is equivalent to finitely many linear equations in the a_{ij} with coefficients in K^{sep}. By our computer algebra prerequisites, one can effectively decide whether these have a solution in $\mathbb{F}_p$ and if so, find it. □

For any integer d let M_d denote the $\mathbb{F}_p[t]$-submodule of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi) \subset K^{\mathrm{sep}}[\tau]$ generated by all $u \in \mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ with $\deg_\tau(u) \leqslant d$. As there are only finitely many generators, this module is finitely generated. Recall that all finite separable extensions of K are tacitly assumed to be contained in K^{sep}.

Proposition 5.6 *For any $d \geqslant 0$, any finite separable extension K' of K, and any elements $m_1, \ldots, m_n \in \mathrm{End}_{K'}(\varphi)$ which form an orthogonal basis of M_{d-1}, one can effectively find $n' \geqslant n$, a finite separable extension K'' of K', and elements $m_{n+1}, \ldots, m_{n'} \in \mathrm{End}_{K''}(\varphi)$ of degree d such that $m_1, \ldots, m_{n'}$ is an orthogonal basis of M_d.*

Proof. First observe that, since M_{d-1} is generated by elements of degree $\leqslant d-1$, Definition 5.4 implies that $\deg_\tau(m_i) \leqslant d-1$ for all $1 \leqslant i \leqslant n$.

Next, applying Proposition 5.1 over K', we can effectively find a finite separable extension K'' of K' and elements $f_1, \ldots, f_k \in \mathrm{End}_{K''}(\varphi)$ which make up all elements of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ of degree d in τ. By definition, these together with $m_1, \ldots, m_n$ generate M_d. Using Proposition 5.5, for all $(\alpha_1, \ldots, \alpha_k) \in \mathbb{F}_p^k \smallsetminus \{(0, \ldots, 0)\}$ we can check whether $\sum_{j=1}^k \alpha_j f_j$ already lies in M_{d-1}. If it does, we can remove one generator f_j without changing the module M_d. After finitely many such operations and reordering $f_1, \ldots, f_k$, we may assume that we have constructed an integer $0 \leqslant \ell \leqslant k$ such that M_d is already generated by $m_1, \ldots, m_n, f_1, \ldots, f_\ell$ and that:

$$\text{For all } (\alpha_1, \ldots, \alpha_\ell) \in \mathbb{F}_p^\ell \smallsetminus \{(0, \ldots, 0)\} \text{ we have } \textstyle\sum_{j=1}^\ell \alpha_j f_j \notin M_{d-1}. \tag{5.7}$$

We claim that then $m_1, \ldots, m_n, f_1, \ldots, f_\ell$ are orthogonal.

To see this, set $n' := n+\ell$ and $m_{n+j} := f_j$ for all $1 \leqslant j \leqslant \ell$. For the sake of contradiction consider $a_1, \ldots, a_{n'} \in \mathbb{F}_p[t]$ such that

$$\deg_\tau\Big(\sum_{i=1}^{n'} \varphi_{a_i} m_i\Big) \;<\; D \;:=\; \max\big\{\deg_\tau(\varphi_{a_i} m_i) \;\big|\; 1 \leqslant i \leqslant n'\big\}. \tag{5.8}$$

Then the maximum D is attained for some $n < i \leqslant n'$, because otherwise the strict inequality would also hold with $a_{n+1}, \ldots, a_{n'}$ replaced by 0, contradicting the orthogonality of $m_1, \ldots, m_n$. Thus $D \geqslant d$.

For all $1 \leqslant i \leqslant n'$ we therefore have $D \geqslant \deg_\tau(m_i)$. Write $D = s_i\delta_t + \deg_\tau(m_i)$, so that $\deg_t(a_i) \leqslant s_i$. Dropping from $a_i \in \mathbb{F}_p[t]$ all terms of degree $< s_i$ in t then does not change the inequality (5.8). After doing this for all i we may assume that each $a_i = \alpha_i t^{s_i}$ for some $\alpha_i \in \mathbb{F}_p$, with $\alpha_i = 0$ if $s_i \notin \mathbb{Z}$.

If $D > d$, we have $s_i > 0$ for all i. This now means that all a_i are divisible by t. By the additivity of $\deg_\tau$ in products, the inequality (5.8) still holds after replacing each a_i by $t^{-1}a_i$. After repeating this a finite number of times, we can assume that $D = d$.

Then $s_i = 0$ for all $n < i \leqslant n'$. For these we then have $a_i =: \alpha_i \in \mathbb{F}_p$. Also, since the maximum in (5.8) is attained at some $n < i \leqslant n'$, at least one of these α_i is non-zero. On the other hand the inequality (5.8) now means that $\deg_\tau(m) < d$ for $m := \sum_{i=1}^{n'} \varphi_{a_i} m_i$. Since $m \in \mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$, it follows that $m \in M_{d-1}$. This in turn implies that

$$\sum_{j=1}^{\ell} \alpha_{n+j} f_j \;=\; \sum_{i=n+1}^{n'} \varphi_{a_i} m_i \;=\; m - \sum_{i=1}^{n} \varphi_{a_i} m_i \;\in\; M_{d-1}.$$

But this is a contradiction to (5.7).

This proves that $m_1, \ldots, m_n, f_1, \ldots, f_\ell$ are orthogonal. As any orthogonal sequence is $\mathbb{F}_p[t]$-linearly independent, and these elements generate M_d as an $\mathbb{F}_p[t]$-module; they form an orthogonal basis of M_d, as desired. □

Proposition 5.9 *For any d one can effectively determine a finite separable extension K' of K and elements $m_1, \dots, m_n \in \mathrm{End}_{K'}(\varphi)$ which form an orthogonal basis of M_d.*

Proof. For $d < 0$ we have $M_d = 0$ and the assertion is trivial. By induction on d the assertion thus follows from Proposition 5.6. □

Since $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ is finitely generated as a module over A and hence also over $\mathbb{F}_p[t]$, we have $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi) = M_d$ for all $d \gg 0$. Letting the procedure in Proposition 5.6 run inductively for $d \to \infty$, we will therefore eventually find an orthogonal basis of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ over $\mathbb{F}_p[t]$. However, knowing when we have reached that stage requires additional information. By the following proposition it suffices to know when M_d has the same rank as $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$:

Proposition 5.10 *For any d, if M_d has finite index in $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$, it is equal to $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$.*

Proof. Let $m_1, \dots, m_n$ be an orthogonal basis of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$. Since M_d is generated by elements of degree $\leqslant d$ and has finite index in $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$, for any $1 \leqslant i \leqslant n$ there exists an element $m \in M_d$ of degree $\leqslant d$, in whose expansion $m = \sum_{j=1}^{n} \varphi_{a_j} m_j$ with $a_j \in \mathbb{F}_p[t]$ the coefficient a_i is non-zero. By orthogonality we then have

$$d \geqslant \deg_\tau(m) \geqslant \deg_\tau(\varphi_{a_i} m_i) \geqslant \deg_\tau(m_i).$$

Thus the generators m_i of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ already lie in M_d; hence $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi) = M_d$. □

Proposition 5.11 *If the rank of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ over $\mathbb{F}_p[t]$ is given, one can effectively determine a finite separable extension K' of K and elements $m_1, \dots, m_n \in \mathrm{End}_{K'}(\varphi)$ which form an orthogonal basis of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$.*

Proof. Let the procedure in Proposition 5.6 run inductively for $d \to \infty$ until $\mathrm{rank}(M_d) = \mathrm{rank}(\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'))$. Then we are finished by Proposition 5.10. □

Remark 5.12 Given a finite extension K' of K and an orthogonal basis $m_1, \dots, m_n$ of $\mathrm{End}_{K'}(\varphi)$, we can effectively answer various elementary questions about this endomorphism ring. Namely, using Proposition 5.5 we can write each product $m_i m_j$ as an $\mathbb{F}_p[t]$-linear combination of $m_1, \dots, m_n$ and thus describe $\mathrm{End}_{K'}(\varphi)$ via a multiplication table. By solving linear equations over $\mathbb{F}_p[t]$ we can then, for instance, explicitly determine the commutant of any element, or of any finite number of elements, of $\mathrm{End}_{K'}(\varphi)$. In particular, we can explicitly determine the center of $\mathrm{End}_{K'}(\varphi)$. We can also find a finite presentation of $\mathrm{End}_{K'}(\varphi)$ as an A-module or as an A-algebra. Thus we can say that *we know* $\mathrm{End}_{K'}(\varphi)$.

Remark 5.13 Suppose that we are given a Drinfeld A-module φ' isogenous to φ and an orthogonal basis of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi')$. Then $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ and $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi')$ have the same rank over $\mathbb{F}_p[t]$; hence we can effectively find an orthogonal basis of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ using Proposition 5.11. But this seems wasteful. It is probably more economical to use given isogenies $\varphi \to \varphi' \to \varphi$ to find the endomorphisms of φ explicitly from those of φ'.

Proposition 5.14 *If K is finite, for any non-constant element $t \in A$ one can effectively find an orthogonal basis of* $\mathrm{End}_K(\varphi)$ *over* $\mathbb{F}_p[t]$.

Proof. Choose a basis $\{x_i \mid 1 \leqslant i \leqslant n\}$ of K over $\mathbb{F}_p$. Then $\{x_i\tau^j \mid 1 \leqslant i \leqslant n,\ 0 \leqslant j < n\}$ is a basis of $K[\tau]$ as a free module over its center $\mathbb{F}_p[\tau^n]$. For any $a \in A$ one can explicitly write φ_a as an $\mathbb{F}_p[\tau^n]$-linear combination of this basis. Doing this for finitely many generators of A as an $\mathbb{F}_p$-algebra, one can then explicitly determine their joint commutant in $K[\tau]$ by linear algebra over $\mathbb{F}_p[\tau^n]$. By definition this commutant is precisely $\mathrm{End}_K(\varphi)$. Thus one has an explicit basis of $\mathrm{End}_K(\varphi)$ as a module over $\mathbb{F}_p[\tau^n]$.

By another explicit calculation over $\mathbb{F}_p[\tau^n]$ one can determine the action of φ_t on this basis; in other words, one can determine $\mathrm{End}_K(\varphi)$ as a module over the polynomial ring in two variables $\mathbb{F}_p[\tau^n, t]$. That in turn yields a basis of $\mathrm{End}_K(\varphi)$ as a module over $\mathbb{F}_p[t]$. If this calculation is done carefully, say with a suitable Gröbner basis, the basis is already orthogonal; otherwise an orthogonal basis can be obtained from this one as in the proof of Proposition 5.6. □

6 Main algorithms

As before we fix a Drinfeld A-module $\varphi\colon A \to K[\tau]$ over a finitely generated field K. In this section we show that one can effectively determine the endomorphism ring $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ and, in the non-isotrivial special characteristic case, the admissible coefficient rings $B \subset A'$ and the Drinfeld A'-module φ' from Theorem 2.6 and the endomorphism ring $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$.

We begin by determining whether φ has generic or special characteristic and whether it is isotrivial, using Proposition 4.1. If φ is not isotrivial, we first find a maximal commutative subring of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$, whose normalization will be the ring A' below. We say that we *go up* with the coefficient ring.

Proposition 6.1 *If φ is not isotrivial, one can effectively find a finite separable extension K' of K, an admissible coefficient ring A' containing A, a Drinfeld A'-module φ' over K', and an isogeny $h\colon \varphi \to \varphi'|A$ over K', such that* $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi') = A'$.

Proof. Set $(A_0, K_0, \varphi_0) := (A, K, \varphi)$ and $n := 0$, and start processes (a) and (b) in parallel.

Process (a): Find endomorphisms: For each $d \geqslant 0$ use Proposition 5.1 to find all endomorphisms $f \in \mathrm{End}_{K^{\mathrm{sep}}}(\varphi_m)$ of degree d. For any such f use Proposition 4.4 to check whether f is scalar or not. If a non-scalar f is found, choose a finite separable extension K_{n+1} of K_n over which f is defined. Let A_{n+1} be the normalization of $A_n[f]$, and using Proposition 4.2 choose a Drinfeld A_{n+1}-module φ_{n+1} and an isogeny $\varphi_n \to \varphi_{n+1}|A_n$ over K_{n+1}. Then kill process (b), set $n := n + 1$, and restart both processes (a) and (b).

Process (b): Find Frobeniuses: Using Proposition 4.6 choose a finitely generated normal integral domain $R_n \subset K_n$ with $\mathrm{Quot}(R_n) = K_n$ over which φ_n has good reduction. For each maximal ideal $\mathfrak{m} \subset R_n$ use Proposition 4.7 (b) to decide whether $F_{n,\mathfrak{m}} := \mathrm{End}^{\circ}_{k_{\mathfrak{m}}^{\mathrm{sep}}}(\varphi_{n,\mathfrak{m}})$ is

commutative, and in that case describe it as an abstract field extension of $F_n := \mathrm{Quot}(A_n)$. As soon as a new such $F_{n,\mathfrak{m}}$ is found, check whether it and some previously found $F_{n,\mathfrak{m}'}$ are linearly disjoint over F_n. If no, continue with the next $\mathfrak{m}$. If yes, we know that $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi_n) = A_n$. Then kill process (a), set $(A', K', \varphi') := (A_n, K_n, \varphi_n)$, combine all isogenies from process (a) to an isogeny $h\colon \varphi \to \varphi'|A$ over K', and stop.

Effectivity: Process (a) constructs a sequence of Drinfeld modules of strictly decreasing rank. Thus eventually it continues forever with the same (A_n, K_n, φ_n). In that case we have $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi_n) = A_n$. Process (b) cannot terminate before that, because the rings $F_{n,\mathfrak{m}}$ all contain a subring isomorphic to $\mathrm{End}^{\circ}_{K^{\mathrm{sep}}}(\varphi_n)$ over F_n. But once (A_n, K_n, φ_n) remains constant, by Proposition 2.15 there exist maximal ideals $\mathfrak{m}$ and $\mathfrak{n}$ of R_n such that $F_{n,\mathfrak{m}}$ and $F_{n,\mathfrak{n}}$ are linearly disjoint over F_n. Thus process (b) terminates with a correct answer. □

Variation 6.2 In process (b) of Proposition 6.1, instead of checking for linear disjointness, for each $\mathfrak{m}$ make a list $\mathcal{L}_{\mathfrak{m}}$ of the finitely many isomorphism classes of field extensions E/F_n with $\mathrm{Hom}_{F_n}(E, F_{n,\mathfrak{m}}) \neq \varnothing$. For any new $\mathfrak{m}$ compare this list with all previously found lists $\mathcal{L}_{\mathfrak{m}'}$. If the intersection of these is the singleton $\{F_n\}$, kill process (a) and finish as before.

If φ is non-isotrivial of special characteristic, we must *go down* with the coefficient ring in order to discover more endomorphisms.

Proposition 6.3 *If φ is non-isotrivial of special characteristic, let (A', K', φ') be the data from Proposition 6.1. Then one can effectively find the admissible coefficient ring $B \subset A'$ from Theorem 2.6, a non-constant element $t \in B$, a finite separable extension K'' of K', and elements of $\mathrm{End}_{K''}(\varphi'|B)$ which form an orthogonal basis of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$ over $\mathbb{F}_p[t]$.*

Proof. Since φ' is non-isotrivial we have $\mathrm{rank}(\varphi') \geqslant 2$. If $\mathrm{rank}(\varphi') = 2$, then $B = \mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B) = A'$ by Proposition 2.12. In particular, for any non-constant element $t \in B$ we know the rank of B over $\mathbb{F}_p[t]$; hence we can effectively find an orthogonal basis over $\mathbb{F}_p[t]$ using Proposition 5.11.

So assume that $\mathrm{rank}(\varphi') > 2$. Then B is completely characterized by traces by Theorem 2.8. Start process (a).

Process (a): Find traces of Frobenius: Using Proposition 4.6 choose a finitely generated normal integral domain $R' \subset K'$ with $\mathrm{Quot}(R') = K'$ over which φ' has good reduction. Set $F' := \mathrm{Quot}(A')$ and $k := 0$ and $B_0 := \mathbb{F}_p$. For each maximal ideal $\mathfrak{m}' \subset R'$ use Proposition 4.7 (a) to compute the characteristic polynomial $\mathrm{char}_{\mathfrak{m}'} = \sum_{i=0}^{r'} a_i X^i \in F'[X]$ of $\mathrm{Frob}_{\mathfrak{m}'}$ associated to φ'. Using this, calculate the value $t_{\mathfrak{m}'} = a_1 a_{r'-1}/a_0 \in F'$ from (2.7). If $t_{\mathfrak{m}'} \notin \mathrm{Quot}(B_k)$, determine $B_{k+1} := A' \cap \mathrm{Quot}(B_k[t_{\mathfrak{m}'}]) \subset B$ and set $k := k+1$.

Keep repeating this forever with all $\mathfrak{m}'$. The first time that B_k becomes infinite, fix a non-constant element $t \in B_k$, set $B' := \mathbb{F}_p[t]$, and start process (b) in parallel.

Process (b): Find endomorphisms: For all integers d let M'_d denote the B'-submodule of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B')$ generated by all $u \in \mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B')$ with $\deg_\tau(u) \leqslant d$. Thus $M'_{-1} = 0$

with the trivial orthogonal basis. Using Proposition 5.6 inductively, for every $d \geqslant 0$ we can effectively construct a finite separable extension K'_d of K' and an orthogonal basis of M'_d contained in $\mathrm{End}_{K'_d}(\varphi'|B')$. If, with the current B_k from process (a), we have

$$\mathrm{rank}_{B'}(B_k) \cdot \mathrm{rank}_{B'}(M'_d) \;=\; \mathrm{rank}_{B'}(A')^2, \tag{6.4}$$

kill process (a) and stop, returning B_k and $K'' := K'_d$ and the given orthogonal basis of M'_d.

Effectivity: Process (a) produces an increasing sequence of normal subrings B_k of A'. By Theorem 2.8 this sequence eventually becomes stationary with $B_k = B$. In particular, from some point on B_k is infinite and hence an admissible coefficient ring. Process (b) then produces an increasing sequence of B'-submodules M'_d of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B')$ which eventually becomes stationary with $M'_d = \mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B')$. By Theorem 2.6 (b) we have $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B') \subset \mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$ and hence $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B') = \mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$. Thus at every step in process (b) we have

$$\mathrm{rank}_{B'}(B_k) \cdot \mathrm{rank}_{B'}(M'_d) \;\leqslant\; \mathrm{rank}_{B'}(B) \cdot \mathrm{rank}_{B'}(\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)),$$

with equality for all $k, d \gg 0$. But since B is the center of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$ by Theorem 2.6 (a), and A' is a maximal commutative subalgebra of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$, the right hand side of this inequality is equal to

$$\mathrm{rank}_{B'}(B)^2 \cdot \mathrm{rank}_B(\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)) \;=\; \mathrm{rank}_{B'}(B)^2 \cdot \mathrm{rank}_B(A')^2 \;=\; \mathrm{rank}_{B'}(A')^2.$$

Thus at every step in process (b) we have

$$\mathrm{rank}_{B'}(B_k) \cdot \mathrm{rank}_{B'}(M'_d) \;\leqslant\; \mathrm{rank}_{B'}(A')^2, \tag{6.5}$$

with equality for all $k, d \gg 0$. Comparing (6.5) with (6.4) shows that the process terminates and that upon termination we have $\mathrm{rank}_{B'}(B_k) = \mathrm{rank}_{B'}(B)$ and $\mathrm{rank}_{B'}(M'_d) = \mathrm{rank}_{B'}(\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B))$. The first of these equalities implies that $B_k = B$ because B_k is normal, and the second implies that $M'_d = \mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$ by Proposition 5.10. □

Variation 6.6 In process (a) of Proposition 6.3, in addition to $t_{\mathfrak{m}'}$ adjoin all coefficients of the characteristic polynomial of $\mathrm{Frob}_{\mathfrak{m}'}$ in the adjoint representation on $\mathrm{End}_{A'_{\mathfrak{p}'}}(T_{\mathfrak{p}'}(\varphi'))$. Like $t_{\mathfrak{m}'}$ these coefficients can be computed directly from the characteristic polynomial of $\mathrm{Frob}_{\mathfrak{m}'}$ on $T_{\mathfrak{p}'}(\varphi')$, and by the last sentence of Pink [12, Thm. 1.3], they also lie in $E^{\mathrm{trad}} = E$. In this way one can probably generate E faster.

Theorem 6.7 *One can effectively determine the rank of* $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ *over* A *and a finite separable extension* K'' *of* K *with* $\mathrm{End}_{K''}(\varphi) = \mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$.

Proof. First assume that φ has generic characteristic. Let (A', K', φ') be the data from Proposition 6.1. Then $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ is commutative, hence so is $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|A)$; hence the latter is equal to $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi') = A'$. Thus the rank of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ over A is equal to that of

$\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|A) = A'$ and can be determined from the knowledge of A'. Also, since φ' and the isogeny $\varphi \to \varphi'|A$ are defined over K', it follows that $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi) = \mathrm{End}_{K'}(\varphi)$. Thus the theorem holds with $K'' = K'$.

Next assume that φ is non-isotrivial of special characteristic. Let $(A', B, t, K'', \varphi')$ be the data from Propositions 6.1 and 6.3 and abbreviate $S := \mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|A)$. Then by Theorem 2.6 (b) we have $S \subset \mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$; hence S is simply the commutant of $\varphi'(A)$ in $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$. Choose finitely many generators of A as an $\mathbb{F}_p$-algebra. By Proposition 5.5 we can effectively express them as $\mathbb{F}_p[t]$-linear combinations of the orthogonal basis from Proposition 6.3. By Remark 5.12 we can therefore effectively determine S as an $\mathbb{F}_p[t]$-module. In particular, we can compute its rank over $\mathbb{F}_p[t]$. Although t does not necessarily lie in A, we nevertheless have $A \cup \mathbb{F}_p[t] \subset A' \subset S$. The multiplicativity of ranks thus implies that

$$\mathrm{rank}_A(S) \;=\; \mathrm{rank}_A(A') \cdot \mathrm{rank}_{A'}(S) \;=\; \mathrm{rank}_A(A') \cdot \frac{\mathrm{rank}_{\mathbb{F}_p[t]}(S)}{\mathrm{rank}_{\mathbb{F}_p[t]}(A')}.$$

Thus we can also compute the rank of S over A. As the rank of the endomorphism ring is invariant under isogenies, we have thereby computed the rank of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ over A. Moreover, since φ' and the isogeny $\varphi \to \varphi'|A$ are defined over K'', and $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B) = \mathrm{End}_{K''}(\varphi|B)$ by Proposition 6.3, it follows that $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi) = \mathrm{End}_{K''}(\varphi)$, as desired.

Finally assume that φ is isotrivial. Pick a non-constant $t \in A$ and write $\varphi_t = \sum_{i=0}^{n} x_i \tau^i$ with $x_n \neq 0$. Choose a finite extension K' of K containing an element y with $y^{1-q^n} = x_n$. Then $y^{-1}\varphi_t y$ has the highest term τ^n. Since φ is isotrivial, as in the proof of Proposition 4.1 it follows that the Drinfeld A-module $\psi := y^{-1}\varphi y$ is now defined over a finite subfield k of K'. In fact, such k can be described explicitly as the subfield generated by all coefficients of ψ_a for a finite set of generators a of A as an $\mathbb{F}_p$-algebra. Applying Proposition 4.5 to (k, ψ) in place of (K, φ), one can then effectively find a finite separable extension k' of k such that $\mathrm{End}_{k'}(\psi) = \mathrm{End}_{k^{\mathrm{sep}}}(\psi)$ and compute the rank of $\mathrm{End}_{k^{\mathrm{sep}}}(\psi)$ over A. For any finite extension K'' of K' containing a subfield isomorphic to k' we then have $\mathrm{End}_{K''}(\varphi) = \mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ and $\mathrm{rank}_A(\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)) = \mathrm{rank}_A(\mathrm{End}_{k^{\mathrm{sep}}}(\psi))$ and are done. □

Theorem 6.8 *For any non-constant element $t \in A$, one can effectively find a finite separable extension K'' of K and elements of $\mathrm{End}_{K''}(\varphi)$ which form an orthogonal basis of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ over $\mathbb{F}_p[t]$.*

Proof. From the knowledge of A we can determine the rank of A over $\mathbb{F}_p[t]$. Using Theorem 6.7 we can therefore effectively determine the rank of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ over $\mathbb{F}_p[t]$. We can then find the desired data by Proposition 5.11. (But in practice it might be more efficient to use the endomorphisms already found in Propositions 6.1 and 6.3; compare Remark 5.13.) □

Theorem 6.9 *(a) One can effectively determine the rank of $\mathrm{End}_K(\varphi)$ over A.*

(b) For any non-constant element $t \in A$, one can effectively find an orthogonal basis of $\mathrm{End}_K(\varphi)$ over $\mathbb{F}_p[t]$.

Proof. Maybe this can be achieved by carrying out the whole program over K instead of K^{sep}, but we deduce it from the orthogonal basis in Theorem 6.8, as follows. Let $m_1, \dots, m_n \in \mathrm{End}_{K''}(\varphi)$ be that basis. After replacing K'' by the subfield generated over K by the coefficients of all m_i, we can assume that K'' is galois over K. For any $\sigma \in \mathrm{Gal}(K''/K)$ and any i we can then express $\sigma(m_i)$ as an $\mathbb{F}_p[t]$-linear combination of $m_1, \dots, m_n$, using Proposition 5.5. In this way we can explicitly describe the action of $\mathrm{Gal}(K''/K)$ on $\mathrm{End}_{K''}(\varphi)$. By solving linear equations over $\mathbb{F}_p[t]$, we can then compute a basis of the submodule of invariants, which is precisely $\mathrm{End}_K(\varphi)$. In particular, we can determine the rank of $\mathrm{End}_K(\varphi)$ over $\mathbb{F}_p[t]$, and hence also over A. With a little more care we can make the basis orthogonal: Using the given orthogonal basis of $\mathrm{End}_{K''}(\varphi)$, for any d we can effectively find all elements of $\mathrm{End}_K(\varphi)$ of degree d, and can then find an orthogonal basis as in the proof of Proposition 5.6. □

Proposition 6.10 *One can effectively determine the isomorphism class of $T_{\mathrm{ad}}(\varphi)$ as a module over $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi) \otimes_A A_{\mathrm{ad}}$.*

Proof. Recall that $S := \mathrm{End}^{\circ}_{K^{\mathrm{sep}}}(\varphi)$ is a finite dimensional division algebra over F. Let Z denote its center. For any maximal ideal $\mathfrak{p} \neq \mathfrak{p}_0$ of A we then have $Z_{\mathfrak{p}} := Z \otimes_F F_{\mathfrak{p}} \cong \prod_{\mathfrak{P}} Z_{\mathfrak{P}}$, where the product is extended over all primes $\mathfrak{P}$ of Z above $\mathfrak{p}$. Also $S_{\mathfrak{p}} := S \otimes_F F_{\mathfrak{p}} \cong \prod_{\mathfrak{P}} S_{\mathfrak{P}}$ where each $S_{\mathfrak{P}} := S \otimes_Z Z_{\mathfrak{P}}$ is a central simple algebra over the field $Z_{\mathfrak{P}}$. The isomorphism class of any $S_{\mathfrak{P}}$-module is therefore determined by its dimension over $Z_{\mathfrak{P}}$.

The rational $\mathfrak{p}$-adic Tate module of φ is the $F_{\mathfrak{p}}$-vector space $V_{\mathfrak{p}}(\varphi) := T_{\mathfrak{p}}(\varphi) \otimes_{A_{\mathfrak{p}}} F_{\mathfrak{p}}$. Under the above decomposition of $Z_{\mathfrak{p}}$ it has the natural decomposition

$$V_{\mathfrak{p}}(\varphi) \;\cong\; V_{\mathfrak{p}}(\varphi'|A) \;=\; \prod_{\mathfrak{P}} V_{\mathfrak{P}}(\varphi'|A' \cap Z).$$

Here each factor $V_{\mathfrak{P}}(\varphi'|A' \cap Z)$ is a $Z_{\mathfrak{P}}$-vector space of dimension the rank of $\varphi'|A' \cap Z$, which is $\mathrm{rank}(\varphi)/[Z/F]$. Thus $V_{\mathfrak{p}}(\varphi)$ is a free module over $Z_{\mathfrak{p}}$ of rank $\mathrm{rank}(\varphi)/[Z/F]$. This therefore determines the isomorphism class of $V_{\mathfrak{p}}(\varphi)$ as a module over $S_{\mathfrak{p}}$.

Next, Theorem 6.8 and Remark 5.12 yield a finite separable extension K'' of K such that $\mathrm{End}_{K''}(\varphi) = \mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ and an explicit presentation of $\mathrm{End}_{K''}(\varphi)$ as an A-algebra. Using the reduced trace of S, one can find a maximal A-order $M \subset S$ containing $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$. For any maximal ideal $\mathfrak{p} \neq \mathfrak{p}_0$ of A the ring $M_{\mathfrak{p}} := M \otimes_A A_{\mathfrak{p}}$ is then a maximal order in $S_{\mathfrak{p}}$. In fact, we have $M_{\mathfrak{p}} \cong \prod_{\mathfrak{P}} M_{\mathfrak{P}}$ for maximal orders $M_{\mathfrak{P}}$ in $S_{\mathfrak{P}}$. Each $M_{\mathfrak{P}}$ is a matrix ring over a maximal $A_{\mathfrak{p}}$-order $M'_{\mathfrak{P}}$ in a division algebra over $F_{\mathfrak{p}}$. Here $M'_{\mathfrak{P}}$ is a (possibly non-commutative) discrete valuation ring, and so any finitely generated torsion free $M'_{\mathfrak{P}}$-module is free. It follows that any finitely generated $A_{\mathfrak{p}}$-torsion free $M_{\mathfrak{p}}$-module is projective, and so its isomorphism class is determined by the $S_{\mathfrak{p}}$-module obtained by base extension. In particular, we therefore know the isomorphism class of the $M_{\mathfrak{p}}$-submodule $\widetilde{T}_{\mathfrak{p}}$ of $V_{\mathfrak{p}}(\varphi)$ that is generated by $T_{\mathfrak{p}}(\varphi)$.

By analyzing the finite A-module $M/\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ one can construct a non-zero element $a \in A$ such that $a \cdot M \subset \mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$. For any maximal ideal $\mathfrak{p} \neq \mathfrak{p}_0$ with $\mathfrak{p} \nmid a$ we then have

$\mathrm{End}_{K^{\mathrm{sep}}}(\varphi) \otimes_A A_{\mathfrak{p}} = M_{\mathfrak{p}}$ and hence $\widetilde{T}_{\mathfrak{p}} = T_{\mathfrak{p}}(\varphi)$, which determines the isomorphism class of $T_{\mathfrak{p}}(\varphi)$ as a module over $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi) \otimes_A A_{\mathfrak{p}}$.

Now consider any maximal ideal $\mathfrak{p} \neq \mathfrak{p}_0$ with $\mathfrak{p}|a$ and set $n := \mathrm{ord}_{\mathfrak{p}}(a)$. By the definition of $\widetilde{T}_{\mathfrak{p}}$ we then have $\mathfrak{p}^n T_{\mathfrak{p}}(\varphi) \subset \mathfrak{p}^n \widetilde{T}_{\mathfrak{p}} = a \cdot M \cdot T_{\mathfrak{p}}(\varphi) \subset T_{\mathfrak{p}}(\varphi)$, and hence also $\mathfrak{p}^{2n} T_{\mathfrak{p}}(\varphi) \subset \mathfrak{p}^{2n} \widetilde{T}_{\mathfrak{p}} \subset \mathfrak{p}^n T_{\mathfrak{p}}(\varphi)$. But the group of $\mathfrak{p}^{2n}$-division points $\varphi[\mathfrak{p}^{2n}](K^{\mathrm{sep}}) \cong T_{\mathfrak{p}}(\varphi)/\mathfrak{p}^{2n} T_{\mathfrak{p}}(\varphi)$ and the action of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ on it can be determined by finite computation, and so can the subgroup $a \cdot M \cdot \varphi[\mathfrak{p}^{2n}](K^{\mathrm{sep}}) \cong \mathfrak{p}^n \widetilde{T}_{\mathfrak{p}}/\mathfrak{p}^{2n} T_{\mathfrak{p}}(\varphi)$. We can therefore find an explicit description of the $M_{\mathfrak{p}}$-module $\mathfrak{p}^n \widetilde{T}_{\mathfrak{p}}/\mathfrak{p}^{2n} \widetilde{T}_{\mathfrak{p}}$ and its $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi) \otimes_A A_{\mathfrak{p}}$-submodule $\mathfrak{p}^n T_{\mathfrak{p}}(\varphi)/\mathfrak{p}^{2n} \widetilde{T}_{\mathfrak{p}}$. Dividing by a, this determines the right hand side of the cartesian diagram

$$\begin{array}{ccc} \widetilde{T}_{\mathfrak{p}} & \longrightarrow & \widetilde{T}_{\mathfrak{p}}/\mathfrak{p}^n \widetilde{T}_{\mathfrak{p}} \\ \uparrow & & \uparrow \\ T_{\mathfrak{p}}(\varphi) & \longrightarrow & T_{\mathfrak{p}}(\varphi)/\mathfrak{p}^n \widetilde{T}_{\mathfrak{p}} \end{array} \tag{6.11}$$

up to isomorphism.

Note that we do not have an explicit description of $\widetilde{T}_{\mathfrak{p}}$, but know only its isomorphism class as a projective $M_{\mathfrak{p}}$-module. But for any positive integer k the natural homomorphism

$$\begin{array}{ccc} \mathrm{Aut}_{M'_{\mathfrak{P}}}\big((M'_{\mathfrak{P}})^{\oplus k}\big) & \longrightarrow & \mathrm{Aut}_{M'_{\mathfrak{P}}}\big((M'_{\mathfrak{P}})^{\oplus k}/\mathfrak{p}^n (M'_{\mathfrak{P}})^{\oplus k}\big) \\ \| & & \| \\ \mathrm{GL}_k(M'^{\mathrm{opp}}_{\mathfrak{P}}) & \longrightarrow & \mathrm{GL}_k\big(M'^{\mathrm{opp}}_{\mathfrak{P}}/\mathfrak{p} M'^{\mathrm{opp}}_{\mathfrak{P}}\big) \end{array}$$

is surjective. Thus for any finitely generated projective $M'_{\mathfrak{P}}$-module X, any automorphism of $X/\mathfrak{p}^n X$ lifts to an automorphism of X. The same then follows for $M_{\mathfrak{P}}$ and for $M_{\mathfrak{p}}$; hence any automorphism of the $M_{\mathfrak{p}}$-module $\widetilde{T}_{\mathfrak{p}}/\mathfrak{p}^n \widetilde{T}_{\mathfrak{p}}$ lifts to an automorphism of the $M_{\mathfrak{p}}$-module $\widetilde{T}_{\mathfrak{p}}$. This implies that in the diagram (6.11), the upper and right edges together are uniquely determined up to joint isomorphism! As the diagram is cartesian, this determines the isomorphism class of $T_{\mathfrak{p}}(\varphi)$ as a module over $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi) \otimes_A A_{\mathfrak{p}}$, as desired.

All in all we have seen that one can effectively determine the isomorphism class of $T_{\mathfrak{p}}(\varphi)$ as a module over $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi) \otimes_A A_{\mathfrak{p}}$ for all $\mathfrak{p} \neq \mathfrak{p}_0$, whence the proposition. □

Theorem 6.12 *One can effectively determine the image of the adelic Galois representation (2.2) up to commensurability and conjugation under* $\mathrm{GL}_r(A_{\mathrm{ad}})$.

Proof. If φ has generic characteristic, this follows by combining Theorem 6.8, Proposition 6.10, and Theorem 2.5.

If φ is non-isotrivial of special characteristic, by Propositions 6.1 and 6.3 one can effectively find the data (K', φ', f, B) described there, as well as an explicit presentation of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$. Let $\mathfrak{q}_0$ be the characteristic ideal of $\varphi'|B$, and set $B_{\mathrm{ad}} := \prod_{\mathfrak{q} \neq \mathfrak{q}_0} B_{\mathfrak{q}}$. Then by Proposition 6.10 one can effectively determine the isomorphism class of $T_{\mathrm{ad}}(\varphi'|B)$ as a module over $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B) \otimes_B B_{\mathrm{ad}}$. This yields an explicit description of the commutant $\prod_{\mathfrak{q} \neq \mathfrak{q}_0} D_{\mathfrak{q}}$ of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$ in $\mathrm{End}_{B_{\mathrm{ad}}}(T_{\mathrm{ad}}(\varphi'|B)) \cong \mathrm{Mat}_{r'' \times r''}(B_{\mathrm{ad}})$ and hence of the group

$\prod_{\mathfrak{q}\neq\mathfrak{q}_0} D_{\mathfrak{q}}^1$ of elements of reduced norm 1. With Theorem 2.9 one obtains a description of the image of Galois in the adelic Galois representation associated to $\varphi'|B$, up to commensurability and conjugation. The image of Galois for φ up to commensurability can be determined from this, as explained in Devic-Pink [2, §6.2].

If φ is isotrivial, find k and ψ as in the proof of Theorem 6.7, so that the image of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ is commensurable with the pro-cyclic group generated by Frob_k associated to ψ. By Proposition 6.10 one can compute the action of $\mathrm{Frob}_k \in \mathrm{End}_{k^{\mathrm{sep}}}(\psi)$ on $T_{\mathrm{ad}}(\psi) \cong T_{\mathrm{ad}}(\varphi)$ up to isomorphism. □

7 Variation

In this section we briefly discuss a different approach to making the search for endomorphisms effective by bounding the degrees of generators of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ via reduction. As outlined here, this approach succeeds only in a restricted class of cases in generic characteristic, namely when $\mathrm{End}_K^\circ(\varphi)$ is separable over F.

Proposition 7.1 *Let φ be a Drinfeld A-module over an arbitrary field L. Let v be a valuation on L with residue field ℓ_v where φ has good reduction φ_v. Then the natural reduction homomorphism*

$$\mathrm{End}_L(\varphi) \to \mathrm{End}_{\ell_v}(\varphi_v)$$

is injective and the torsion of its cokernel is primary to the characteristic ideal of φ_v.

Proof. The injectivity follows from the standard fact that the degree in τ of an endomorphism is preserved under reduction.

Let $\mathfrak{p}_v$ denote the characteristic ideal of φ_v. Extend v to a valuation on L^{sep}. Then the residue field of this extension is naturally a separable closure ℓ_v^{sep} of ℓ_v. After modifying φ by an isomorphism over L, we can assume that it has good reduction form, meaning that φ has coefficients in the valuation ring of v with highest coefficient a unit. Note that for any $a \in A \smallsetminus \mathfrak{p}_v$, the zeroth coefficient of φ_a is then also a unit in the valuation ring. It follows that the Newton polygon of $\varphi_a(X)/X$ with respect to v is a horizontal line, hence every non-zero element of $\varphi[a](L^{\mathrm{sep}})$ has valuation zero.

Consider an element $f_v \in \mathrm{End}_{\ell_v}(\varphi_v)$ and suppose there exists $a \in A \smallsetminus \mathfrak{p}_v$ such that $g_v := f_v\varphi_{v,a}$ is the reduction of some element $g \in \mathrm{End}_L(\varphi)$. We claim that then f_v must also lie in the image of the reduction homomorphism. Indeed, consider any $x \in \varphi[a](L^{\mathrm{sep}})$ and let $x_v \in \varphi_v[a](\ell_v^{\mathrm{sep}})$ denote its reduction. Then the reduction of $g(x)$ is $g_v(x_v) = f_v(\varphi_{v,a}(x_v)) = 0$; hence $g(x)$ has positive valuation. Since g is an endomorphism of φ, we have $g(x) \in \varphi[a](L^{\mathrm{sep}})$, and since every non-zero element of $\varphi[a](L^{\mathrm{sep}})$ has valuation zero, it follows that $g(x) = 0$. As x was arbitrary, we conclude that $\varphi[a](L^{\mathrm{sep}}) \subset \mathrm{Ker}(g)$. Using this and the fact that φ_a is separable, we see that g is right divisible by φ_a, in other words that $g = f\varphi_a$ for some $f \in L[\tau]$. It is straightforward to check that this f is an endomorphism of φ whose reduction is f_v.

Finally, let $h_v \in \mathrm{End}_{\ell_v}(\varphi_v)$ be such that for some non-zero $b \in A$ the product $h_v\varphi_{v,b}$ lies in the image of the reduction homomorphism. Write $bA = \mathfrak{p}_v^k\mathfrak{a}$ for some ideal $\mathfrak{a} \subset A$ not divisible by $\mathfrak{p}_v$ and pick any $a \in \mathfrak{a} \smallsetminus \mathfrak{p}_v$. Then for any $c \in \mathfrak{p}_v^k$, we have $b|ca$, and so $h_v\varphi_{v,c}\varphi_{v,a}$ lies in the image of the reduction homomorphism. Since $a \notin \mathfrak{p}_v$, by the above it follows that $h_v\varphi_{v,c}$ already lies in the image. Letting $c \in \mathfrak{p}_v^k$ vary, this shows that the image of h_v in the cokernel of the reduction homomorphism is annihilated by $\mathfrak{p}_v^k$. Letting h_v vary over all elements whose image in the cokernel is torsion finishes the proof. □

Proposition 7.2 *Let φ be a Drinfeld A-module over an arbitrary field L. Let v and v' be valuations on L with residue fields ℓ_v and $\ell_{v'}$ where φ has good reduction φ_v and $\varphi_{v'}$ with different characteristic ideals. Then the image of the natural reduction homomorphism*

$$\mathrm{End}_L(\varphi) \to \mathrm{End}_{\ell_v}(\varphi_v) \times \mathrm{End}_{\ell_{v'}}(\varphi_{v'})$$

is saturated, i.e., its cokernel is torsion free.

Proof. Let $\mathfrak{p}_v$ and $\mathfrak{p}_{v'}$ be the characteristic ideals of φ_v and $\varphi_{v'}$. By Proposition 7.1, the torsion part of the cokernel of the reduction homomorphism associated to v is $\mathfrak{p}_v$-primary, while the torsion part of the reduction homomorphism associated to v' is $\mathfrak{p}_{v'}$-primary. Using the facts that A is a Dedekind ring and that the endomorphism rings are torsion free, one can show that the product $\mathrm{End}_L(\varphi) \to \mathrm{End}_{\ell_v}(\varphi_v) \times \mathrm{End}_{\ell_{v'}}(\varphi_{v'})$ of the reduction homomorphisms has saturated image. This is an exercise in commutative algebra, which we leave to the reader. □

Now we return to a Drinfeld A-module $\varphi\colon A \to K[\tau]$ over a finitely generated field K. As before, let R be a finitely generated normal subring of K such that φ extends to a Drinfeld A-module over $\operatorname{Spec} R$.

Proposition 7.3 *For any maximal ideal $\mathfrak{m}$ where $\varphi_\mathfrak{m}$ is ordinary, $\mathrm{End}^\circ_{k_\mathfrak{m}^{\mathrm{sep}}}(\varphi_\mathfrak{m})$ is a finite separable field extension of F.*

Proof. The characteristic polynomial of $\mathrm{Frob}_\mathfrak{m}$ has precisely one root with multiplicity 1 in $\overline{F}$ which is not a unit above the characteristic ideal of $\varphi_\mathfrak{m}$. As the characteristic polynomial is a power of the minimal polynomial, it follows that the characteristic polynomial is already irreducible and separable. Thus $F(\mathrm{Frob}_\mathfrak{m})$ is a separable field extension of F of degree $\mathrm{rank}(\varphi_\mathfrak{m})$. Since $F(\mathrm{Frob}_\mathfrak{m})$ is the center of $\mathrm{End}^\circ_{k_\mathfrak{m}}(\varphi_\mathfrak{m})$, the formula $d_\mathfrak{m}e_\mathfrak{m} = \mathrm{rank}(\varphi_\mathfrak{m})$ implies that $\mathrm{End}^\circ_{k_\mathfrak{m}}(\varphi_\mathfrak{m}) = F(\mathrm{Frob}_\mathfrak{m})$, which is therefore commutative and separable over F. The same argument over a finite extension of $k_\mathfrak{m}$ proves the same for $\mathrm{End}^\circ_{k_\mathfrak{m}^{\mathrm{sep}}}(\varphi_\mathfrak{m})$. □

Proposition 7.4 *If φ has generic characteristic, the following conditions are equivalent:*

(a) $\mathrm{End}^\circ_K(\varphi)$ *is a finite separable field extension of F.*

(b) $\mathrm{End}^\circ_{K^{\mathrm{sep}}}(\varphi)$ *is a finite separable field extension of F.*

(c) There exists a maximal ideal $\mathfrak{m}$ of R such that the reduction $\varphi_\mathfrak{m}$ is ordinary.

Furthermore, each of the following conditions implies the ones above:

(d) The algebraic closure of F in K is separable over F.

(e) The rank of φ is not divisible by p.

Proof. Since φ has generic characteristic, $\mathrm{End}_K^\circ(\varphi)$ is commutative and thus a finite field extension of F. If it is separable, the set of maximal ideals of R where φ has ordinary reduction has positive Dirichlet density by [11, Thm. 0.3 (b)]. In particular it is non-empty, proving the implication (a)⇒(c).

Conversely, if φ has ordinary reduction at $\mathfrak{m}$, the endomorphism ring $\mathrm{End}_{k_\mathfrak{m}}^\circ(\varphi_\mathfrak{m})$ is a finite separable field extension of F by Proposition 7.3. The reduction of endomorphisms induces an F-algebra homomorphism $\mathrm{End}_K^\circ(\varphi) \to \mathrm{End}_{k_\mathfrak{m}}^\circ(\varphi_\mathfrak{m})$. As a subfield of a separable field extension $\mathrm{End}_K^\circ(\varphi)$ is therefore separable over F. This proves the implication (c)⇒(a).

Thus (a) and (c) are equivalent. Since $\mathrm{End}_{K^{\mathrm{sep}}}^\circ(\varphi) = \mathrm{End}_{K'}^\circ(\varphi)$ for some finite separable field extension K' of K, and the condition (c) is invariant under extending K, it follows that (a), (b), and (c) are all equivalent.

Next, in generic characteristic the natural homomorphism $\mathrm{End}_K(\varphi) \to K$, $u = \sum_{i=0}^d u_i\tau^i \mapsto u_0$ is injective and therefore extends to an F-algebra homomorphism $\mathrm{End}_K^\circ(\varphi) \to K$. Thus if the algebraic closure of F in K is separable over F, it follows that $\mathrm{End}_K(\varphi)$ is separable over F, in other words we have (d)⇒(a).

Finally, in generic characteristic the degree of the field extension $\mathrm{End}_K^\circ(\varphi)/F$ divides the rank of φ. If that is not divisible by p, it follows that $\mathrm{End}_K^\circ(\varphi)$ is separable over F; in other words we have (e)⇒(a). □

Lemma 7.5 *If φ has generic characteristic and $\mathrm{End}_K^\circ(\varphi)$ is separable over F, then there exist maximal ideals $\mathfrak{m}$ and $\mathfrak{n}$ of R, such that the reductions $\varphi_\mathfrak{m}$ and $\varphi_\mathfrak{n}$ are ordinary and have different characteristic ideals. Furthermore, one can effectively compute ideals $\mathfrak{m}$ and $\mathfrak{n}$ with these properties.*

Proof. By Proposition 7.4 there exists a maximal ideal $\mathfrak{m}$ with ordinary reduction. Going through all maximal ideals of R and applying Proposition 4.1, one can therefore effectively find such an $\mathfrak{m}$. Choose a non-zero element s in the characteristic ideal $\mathfrak{p}_\mathfrak{m}$ of $\varphi_\mathfrak{m}$. Since φ has generic characteristic, the image s' of s in R is again non-zero. The localization $R[1/s']$ is then again a finitely generated normal subring of K, and φ extends to a Drinfeld A-module over $\mathrm{Spec}\, R[1/s']$. Repeating the preceding argument, one can effectively find a maximal ideal of $R[1/s']$ where φ has ordinary reduction. Pulling this back to R yields a maximal ideal $\mathfrak{n}$ of R where φ has ordinary reduction and whose characteristic ideal $\mathfrak{p}_\mathfrak{n}$ does not contain s. Thus $\mathfrak{p}_\mathfrak{m} \neq \mathfrak{p}_\mathfrak{n}$, and we are done. □

If φ has generic characteristic and $\mathrm{End}_K^\circ(\varphi)$ is separable over F, we can now give a different method for computing $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$, which does not rely on Proposition 2.15.

Theorem 7.6 *If φ has generic characteristic and $\mathrm{End}_K(\varphi)$ is separable over A, one can effectively compute a finite separable extension K' of K such that $\mathrm{End}_{K'}(\varphi) = \mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$, and a finite generating set of $\mathrm{End}_{K'}(\varphi)$ as an A-module.*

Proof. Let $\mathfrak{m}$ and $\mathfrak{n}$ be as in Lemma 7.5. Then $\mathrm{End}_{k_\mathfrak{m}^{\mathrm{sep}}}(\varphi_\mathfrak{m})$ and $\mathrm{End}_{k_\mathfrak{n}^{\mathrm{sep}}}(\varphi_\mathfrak{n})$ are commutative by Proposition 7.3. They can be effectively computed by Proposition 4.5 (a) and Proposition 5.14.

Compute a finite list $\mathcal{L}_1$ of all F-subalgebras E of $\mathrm{End}^\circ_{k_\mathfrak{m}^{\mathrm{sep}}}(\varphi_\mathfrak{m}) \times \mathrm{End}^\circ_{k_\mathfrak{n}^{\mathrm{sep}}}(\varphi_\mathfrak{n})$ which are fields. This can be done by first finding all subfields of $\mathrm{End}^\circ_{k_\mathfrak{m}^{\mathrm{sep}}}(\varphi_\mathfrak{m})$ containing F and then determining all their F-embeddings into $\mathrm{End}^\circ_{k_\mathfrak{n}^{\mathrm{sep}}}(\varphi_\mathfrak{n})$. By our computer algebra prerequisites both these operations can be done effectively.

For each E in $\mathcal{L}_1$, find finitely many generators of $E \cap \mathrm{End}_{k_\mathfrak{m}^{\mathrm{sep}}}(\varphi_\mathfrak{m}) \times \mathrm{End}_{k_\mathfrak{n}^{\mathrm{sep}}}(\varphi_\mathfrak{n})$ as an A-module. Again, this is possible by our computer algebra prerequisites. Let $\mathcal{L}_2$ be the set of all elements of $\mathrm{End}_{k_\mathfrak{m}^{\mathrm{sep}}}(\varphi_\mathfrak{m}) \times \mathrm{End}_{k_\mathfrak{n}^{\mathrm{sep}}}(\varphi_\mathfrak{n})$ thus obtained as E varies.

For each x in $\mathcal{L}_2$, compute the minimal polynomial $\min_x$ of x over F. Choose a common splitting field K' of all these over K. Both steps are possible due to our computer algebra prerequisites. For each x determine all endomorphisms of φ over K' whose constant coefficient is a zero of $\min_x$, using Proposition 5.3. Let $\mathcal{L}_3$ be the set of all elements of $\mathrm{End}_{K'}(\varphi)$ thus obtained as x varies.

We claim that $\mathcal{L}_3$ generates $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ as an A-module. To see this, note first that since R is integrally closed with field of fractions K, the composite homomorphism $R \twoheadrightarrow k_\mathfrak{m} \hookrightarrow k_\mathfrak{m}^{\mathrm{sep}}$ can be extended to the valuation ring associated to some valuation v on K. Similarly, the reduction associated to $\mathfrak{n}$ comes from a valuation v' on K. Extend v and v' to valuations on K^{sep}, so that the residue fields of these extensions are $k_\mathfrak{m}^{\mathrm{sep}}$ and $k_\mathfrak{n}^{\mathrm{sep}}$, respectively. According to Proposition 7.2, the induced reduction homomorphism $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi) \to \mathrm{End}_{k_\mathfrak{m}^{\mathrm{sep}}}(\varphi_\mathfrak{m}) \times \mathrm{End}_{k_\mathfrak{n}^{\mathrm{sep}}}(\varphi_\mathfrak{n})$ is injective and has saturated image. It extends to a homomorphism $\mathrm{End}^\circ_{K^{\mathrm{sep}}}(\varphi) \to \mathrm{End}^\circ_{k_\mathfrak{m}^{\mathrm{sep}}}(\varphi_\mathfrak{m}) \times \mathrm{End}^\circ_{k_\mathfrak{n}^{\mathrm{sep}}}(\varphi_\mathfrak{n})$ of F-algebras, whose image E is a field and must therefore appear in the list $\mathcal{L}_1$. By saturatedness, the image of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ is equal to $E \cap \mathrm{End}_{k_\mathfrak{m}^{\mathrm{sep}}}(\varphi_\mathfrak{m}) \times \mathrm{End}_{k_\mathfrak{n}^{\mathrm{sep}}}(\varphi_\mathfrak{n})$. Therefore some subset $\{x_1, \ldots, x_n\}$ of $\mathcal{L}_2$ will generate this image as an A-module. By the construction of $\mathcal{L}_3$, each x_i is the reduction of an element of $\mathcal{L}_3$. This shows that $\mathcal{L}_3$ generates $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ as an A-module, as claimed. □

8 Comparing two Drinfeld modules

In this section we consider two Drinfeld A-modules φ and ψ over K with the same characteristic homomorphism $A \to K$ and hence the same characteristic ideal $\mathfrak{p}_0$. We will show that one can effectively decide whether φ and ψ are isogenous and determine all homomorphisms, both over $\overline{K}$ and over K.

By the Tate conjecture for A-motives, due to Taguchi [20] and Tamagawa [21] (see also Pink-Traulsen [15, Thm. 2.4]), for any prime $\mathfrak{p} \neq \mathfrak{p}_0$ of A we have a natural isomorphism

$$\mathrm{Hom}_K(\varphi, \psi) \otimes_A A_\mathfrak{p} \xrightarrow{\sim} \mathrm{Hom}_{A_\mathfrak{p}}(T_\mathfrak{p}(\varphi), T_\mathfrak{p}(\psi))^{\mathrm{Gal}(K^{\mathrm{sep}}/K)}. \tag{8.1}$$

In particular, as the right hand side does not change under inseparable extension, any homomorphism $\varphi \to \psi$ over $\overline{K}$ is already defined over K^{sep}. Thus φ and ψ are isogenous over $\overline{K}$ if and only if they are isogenous over K^{sep}.

Proposition 8.2 *Assume that for some prime $\mathfrak{p} \neq \mathfrak{p}_0$ of A, all $\mathfrak{p}$-torsion points of φ and ψ are defined over K. Then if φ and ψ are isogenous over K^{sep}, they are isogenous over K.*

Proof. Let K' be a finite separable extension of K over which φ and ψ are isogenous. After extending K' we may assume that K'/K is galois. Then

$$\mathrm{Hom}_K(\varphi, \psi) \;=\; \mathrm{Hom}_{K'}(\varphi, \psi)^{\mathrm{Gal}(K'/K)}.$$

By the isomorphism (8.1) for K' in place of K we have

$$\mathrm{Hom}_{K'}(\varphi, \psi) \otimes_A A_{\mathfrak{p}} \;\xrightarrow{\sim}\; \mathrm{Hom}_{A_{\mathfrak{p}}}(T_{\mathfrak{p}}(\varphi), T_{\mathfrak{p}}(\psi))^{\mathrm{Gal}(K^{\mathrm{sep}}/K')}.$$

The image of this isomorphism is a saturated $A_{\mathfrak{p}}$-submodule of $\mathrm{Hom}_{A_{\mathfrak{p}}}(T_{\mathfrak{p}}(\varphi), T_{\mathfrak{p}}(\psi))$ and hence a direct summand. The induced homomorphism

$$\mathrm{Hom}_{K'}(\varphi, \psi) \otimes_A A/\mathfrak{p} \;\longrightarrow\; \mathrm{Hom}_{A_{\mathfrak{p}}}(T_{\mathfrak{p}}(\varphi), T_{\mathfrak{p}}(\psi)) \otimes_A A/\mathfrak{p}$$

is therefore injective. By the construction of the Tate module $T_{\mathfrak{p}}(\varphi) \otimes_A A/\mathfrak{p}$ is naturally isomorphic to the group $\varphi[\mathfrak{p}]$ of $\mathfrak{p}$-torsion points of φ, and likewise for ψ. Thus we obtain a natural Galois equivariant injection

$$\mathrm{Hom}_{K'}(\varphi, \psi) \otimes_A A/\mathfrak{p} \;\hookrightarrow\; \mathrm{Hom}_{A/\mathfrak{p}}(\varphi[\mathfrak{p}], \psi[\mathfrak{p}]).$$

By assumption $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ acts trivially on the target group; hence $\mathrm{Gal}(K'/K)$ acts trivially on $\mathrm{Hom}_{K'}(\varphi, \psi) \otimes_A A/\mathfrak{p}$. Since $\mathrm{Gal}(K'/K)$ is a finite group, its action on $\mathrm{Hom}_{K'}(\varphi, \psi)$ thus factors through a p-group and is therefore unipotent. As $\mathrm{Hom}_{K'}(\varphi, \psi)$ is non-zero by assumption, so is consequently the submodule of $\mathrm{Gal}(K'/K)$-invariants. This means that $\mathrm{Hom}_K(\varphi, \psi)$ is non-zero, as desired. □

Choose a normal integral domain R that is finitely generated over $\mathbb{F}_p$ with $\mathrm{Quot}(R) = K$, such that φ and ψ extend to Drinfeld A-modules over $\mathrm{Spec}\, R$. For any maximal ideal $\mathfrak{m}$ of R let $\varphi_{\mathfrak{m}}$ and $\psi_{\mathfrak{m}}$ denote their reductions over $k_{\mathfrak{m}}$.

Proposition 8.3 *If φ and ψ are not isogenous over K, there exists a maximal ideal $\mathfrak{m} \subset R$ such that the characteristic polynomials of $\mathrm{Frob}_{\mathfrak{m}}$ associated to $\varphi_{\mathfrak{m}}$ and $\psi_{\mathfrak{m}}$ are different.*

Proof. Suppose to the contrary that for all $\mathfrak{m}$ the characteristic polynomials are equal. Pick a prime $\mathfrak{p} \neq \mathfrak{p}_0$ of A and consider the continuous representations of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ on the rational Tate modules $V_{\mathfrak{p}}(\varphi) := T_{\mathfrak{p}}(\varphi) \otimes_{A_{\mathfrak{p}}} F_{\mathfrak{p}}$ and $V_{\mathfrak{p}}(\psi) := T_{\mathfrak{p}}(\psi) \otimes_{A_{\mathfrak{p}}} F_{\mathfrak{p}}$. As the Frobenius elements are dense in $\mathrm{Gal}(K^{\mathrm{sep}}/K)$, it follows that any element of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ has the same characteristic polynomial on $V_{\mathfrak{p}}(\varphi)$ as on $V_{\mathfrak{p}}(\psi)$. By a general fact from representation theory (see Pink-Traulsen [15, Prop. 3.8]) the representations thus have a

common Jordan Hölder factor. But by Taguchi [18, Thm. 0.1], [19, Thm. 0.1] the representations are semisimple. Thus they posses an isomorphic direct summand, and in particular $\mathrm{Hom}_{A_\mathfrak{p}}(T_\mathfrak{p}(\varphi), T_\mathfrak{p}(\psi))^{\mathrm{Gal}(K^{\mathrm{sep}}/K)}$ is non-zero. By (8.1) it follows that $\mathrm{Hom}_K(\varphi, \psi)$ is non-zero, contrary to the assumption. □

Theorem 8.4 *One can effectively decide whether φ and ψ are isogenous over K.*

Proof. Again we start two processes in parallel:

Process (a): Find isogenies: For each $d \geqslant 0$ search for isogenies $\varphi \to \psi$ of degree d in τ. For this choose a finite set $\mathcal{S}$ of generators of the $\mathbb{F}_p$-algebra A. Then an element $u \in K[\tau]$ of degree d is an isogeny $\varphi \to \psi$ if and only if $u\varphi_a = \psi_a u$ for all $a \in \mathcal{S}$. With the Ansatz $u = \sum_{i=0}^{d} u_i \tau^i$ these equations amount to finitely many polynomial equations in the coefficients u_i. We also know that there are at most finitely many solutions. By our computer algebra prerequisites, one can therefore effectively describe all these solutions.

As soon as an isogeny $\varphi \to \psi$ is found, kill process (b) and stop with the answer "yes". Otherwise, repeat the calculation with $d + 1$ in place of d.

Process (b): Compare Frobeniuses: For each maximal ideal $\mathfrak{m} \subset R$ use Proposition 4.7 (a) to determine the characteristic polynomials of $\mathrm{Frob}_\mathfrak{m}$ associated to $\varphi_\mathfrak{m}$ and $\psi_\mathfrak{m}$. If they are different, kill process (a) and stop with the answer "no". Otherwise, repeat the calculation with the next $\mathfrak{m}$.

Effectivity: By Proposition 8.3 the algorithm terminates with the correct answer. □

Theorem 8.5 *One can effectively decide whether φ and ψ are isogenous over K^{sep}.*

Proof. Choose any prime $\mathfrak{p} \neq \mathfrak{p}_0$ of A. By solving the equations for the $\mathfrak{p}$-torsion points of φ and ψ one can find an explicit finite separable extension K' of K such that all these torsion points are defined over K'. Then Proposition 8.2 implies that φ and ψ are isogenous over K^{sep} if and only if they are isogenous over K'. This in turn can be effectively decided by Theorem 8.4. □

For the remaining results we view $K^{\mathrm{sep}}[\tau]$ as an $\mathbb{F}_p[t]$-module via the multiplication $(a, u) \mapsto \psi_a u$.

Theorem 8.6 *For any non-constant element $t \in A$, one can effectively find a finite separable extension K'' of K and elements of $\mathrm{Hom}_{K''}(\varphi, \psi)$ which form an orthogonal basis of $\mathrm{Hom}_{K^{\mathrm{sep}}}(\varphi, \psi)$ over $\mathbb{F}_p[t]$.*

Proof. Use Theorem 8.5 to decide whether φ and ψ are isogenous over K^{sep}. If not, then $\mathrm{Hom}_{K^{\mathrm{sep}}}(\varphi, \psi) = 0$ with the trivial basis. If yes, the rank of $\mathrm{Hom}_{K^{\mathrm{sep}}}(\varphi, \psi)$ over $\mathbb{F}_p[t]$ is equal to that of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$. The latter can be effectively determined by Theorem 6.7 and by computing the rank of A over $\mathbb{F}_p[t]$. To finish, observe that everything from Proposition 5.6 through Proposition 5.11 remains true with $M_d \subset \mathrm{Hom}_{K^{\mathrm{sep}}}(\varphi, \psi)$ in place of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ and, occasionally, ψ in place of φ. The analogue of Proposition 5.11 thus yields the desired orthogonal basis. (But again observe Remark 5.13.) □

Theorem 8.7 *For any non-constant element $t \in A$, one can effectively find an orthogonal basis of* $\mathrm{Hom}_K(\varphi, \psi)$ *over* $\mathbb{F}_p[t]$.

Proof. Use Theorem 8.4 to decide whether φ and ψ are isogenous over K. If not, then $\mathrm{Hom}_K(\varphi, \psi) = 0$ with the trivial basis. If yes, the rank of $\mathrm{Hom}_K(\varphi, \psi)$ over $\mathbb{F}_p[t]$ is equal to that of $\mathrm{End}_K(\varphi)$. The latter can be effectively determined by Theorem 6.9. To finish, apply the arguments from the proof of Theorem 6.9 to $\mathrm{Hom}_{K''}(\varphi, \psi)$ in place of $\mathrm{End}_{K''}(\varphi)$. □

References

[1] Deligne, P., Husemöller, D.: Survey of Drinfeld modules. in: *Current trends in arithmetical algebraic geometry* (Arcata, Calif., 1985), Contemp. Math., 67, Amer. Math. Soc., Providence, RI, 1987, 25–91.

[2] Devic, A., Pink, R.: Adelic openness for Drinfeld modules in special characteristic. *J. Number Theory* **132** (2012) 1583–1625.

[3] Drinfeld, V. G.: Elliptic modules (Russian), *Mat. Sbornik* **94** (1974), 594–627 translated in *Math. USSR Sbornik* **23** (1974), 561–592.

[4] Goss, D.: *Basic structures in function field arithmetic.* Springer-Verlag, 1996.

[5] Hayes, D. R.: Explicit class field theory in global function fields in: *Studies in algebra and number theory* Adv. in Math. Suppl. Stud. vol.6 New York: Academic Press (1979), 173–217.

[6] Hess, F.: Computing Riemann-Roch Spaces in Algebraic Function Fields and Related Topics. *J. Symbolic Computation* **33** no.4 (2002) 425–445.

[7] Kreuzer, M., Robbiano, L.: *Computational Commutative Algebra 1.* Springer-Verlag, Berlin-Heidelberg, 2000.

[8] Kuhn, N.: *Computing the endomorphism ring of a Drinfeld module in generic characteristic.* Master Thesis ETH Zürich, March 2016.

[9] Lazard, D.: Solving zero-dimensional algebraic systems. *J. Symbolic Computation* **13** no.2 (1992) 117–131.

[10] Masser, D. W., Wüstholz, G.: Endomorphism estimates for abelian varieties. *Math. Z. 215* (1994), no. 4, 641–653.

[11] Pink, R.: The Mumford-Tate conjecture for Drinfeld modules. *Publ. Res. Inst. Math. Sci.* **33** (1997), no. 3, 393–425.

[12] Pink, R.: The Galois representations associated to a Drinfeld module in special characteristic. II. Openness *J. Number Theory* **116**, no. 2 (2006) 348–372.

[13] Pink, R., Rütsche, E.: Adelic openness for Drinfeld modules in generic characteristic. *J. Number Theory* **129** no.4 (2009) 882–907.

[14] R. Pink and M. Traulsen, The Galois Representations Associated to a Drinfeld Module in Special Characteristic, III: Image of the Group Ring. *J. Number Theory* **116** no. 2 (2006), 373–395.

[15] Pink, R., Traulsen, M.: The Isogeny Conjecture for t-Motives Associated to Direct Sums of Drinfeld Modules. *J. Number Theory* **117** no. 2 (2006), 355–375.

[16] Singh, A., Swanson, I.: An algorithm for computing the integral closure. *Algebra Number Theory* **3** no.5 (2009) 587–595.

[17] Steel, A.: Conquering inseparability: primary decomposition and multivariate factorization over algebraic function fields of positive characteristic. *J. Symbolic Computation* **40** no.3 (2005) 1053–1075.

[18] Taguchi, Y.: Semisimplicity of the Galois representations attached to Drinfeld modules over fields of "finite characteristics". *Duke Math. J.* **62** (1991), 593–599.

[19] Taguchi, Y.: Semisimplicity of the Galois representations attached to Drinfeld modules over fields of "infinite characteristics". *J. Number Theory* **44** (1993), 292–314.

[20] Taguchi, Y.: The Tate conjecture for t-motives. *Proc. Amer. Math. Soc.* **123** No. 11 (1995), 3285–3287.

[21] Tamagawa, A.: The Tate conjecture for A-premotives. *Preprint*, 1994.