Abstract

This is a sequel to the paper [4], in which we introduced Drinfeld modular polynomials of higher rank, using an analytic construction. These polynomials relate the isomorphism invariants of Drinfeld $F_q[T]$-modules of rank $r \geq 2$ linked by isogenies of a specified type.

In the current paper, we give an algebraic construction of greater generality, and prove a generalization of the Kronecker congruences relations, which describe what happens when modular polynomials associated to $P$-isogenies are reduced modulo a prime $P$. We also correct an error in [4].

1 Isomorphism invariants

Denote by $F_q$ the finite field of $q$ elements. Let $A = F_q[T]$ and $r \geq 2$ a positive integer. Let $g_1, \ldots, g_{r-1}$ be algebraically independent over $k = F_q(T)$, and let $B = A[g_1, \ldots, g_{r-1}] = F_q[T, g_1, \ldots, g_{r-1}]$. Denote by $\tau : x \mapsto x^q$ the $q$-Frobenius, and for any ring $R$ we denote by $R\{\tau\}$ the ring of twisted polynomials in $\tau$ with coefficients in $R$, subject to the commutation relations $\tau a = a^q \tau$ for all $a \in R$.

Let $\varphi : A \to B\{\tau\}$ be the Drinfeld $A$-module of rank $r$ of generic characteristic determined by

$$\varphi_T = T + g_1 \tau + \cdots + g_{r-1} \tau^{r-1} + \tau^r.$$ 

We think of $\varphi$ as the monic generic Drinfeld $A$-module of rank $r$. A general reference for Drinfeld modules is [5, §4].

The group $F_{q^r}^*$ acts on $B \otimes_{F_q} F_{q^r}$ via

$$\lambda*(g_i \otimes 1) = g_i \otimes \lambda^{q^i-1}, \quad i = 1, 2, \ldots, r - 1,$$

and we denote by

$$C := (B \otimes_{F_q} F_{q^r})^{F_{q^r}} \cap B$$

the subring of invariants with coefficients in $F_q$. Equivalently, $C$ consists of those polynomials in $B$ whose monomials are of the form $f(T)g_1^{e_1}g_2^{e_2} \cdots g_{r-1}^{e_{r-1}}$ satisfying $f(T) \in A = F_q[T]$ and

$$\sum_{k=1}^{r-1} e_k (q^k - 1) \equiv 0 \mod q^r - 1.$$ 

Recall that an $A$-field is a field $L$ together with a ring homomorphism $\gamma : A \to L$. 

*Supported by the Alexander von Humboldt foundation, and by the NRF grant BS2008100900027.
Proposition 1.1 For every algebraically closed $A$-field $L$, there is a canonical bijection between the set of isomorphism classes of rank $r$ Drinfeld $A$-modules over $L$, and ring homomorphisms $m : C \to L$ satisfying $m|_A = \gamma$.

Proof.

Let $\psi : A \to L\{\tau\}$ be a rank $r$ Drinfeld $A$-module over the algebraically closed $A$-field $L$, then up to isomorphism we may assume that it is monic, i.e. that

$$\psi_T = \gamma(T) + a_1\tau + \cdots + a_{r-1}\tau^{r-1} + \tau^r, \quad a_i \in L.$$ 

We associate to $\psi$ the ring homomorphism

$$m_\psi : B \to L \quad \text{with} \quad m_\psi(g_i) = a_i \quad \text{and} \quad m|_A = \gamma.$$ 

Let $\iota : C \hookrightarrow B$ be the inclusion, then the homomorphism

$$m_\psi \circ \iota : C \to L$$

is invariant under isomorphisms of the Drinfeld module $\psi$.

Conversely, let $m : C \to L$ be a ring homomorphism with $m|_A = \gamma$. For each $i = 1, 2, \ldots, r - 1$ we have $g_i^{q^r - 1} \in C$, therefore we can extend $m$ to $B$ by defining $m(g_i)$ to be a chosen $(q^r - 1)$st root of $m(g_i^{q^r - 1})$ in $L$.

Each homomorphism $m : B \to L$ yields a Drinfeld module $\psi$ with

$$\psi_T = \gamma(T) + m(g_1)\tau + \cdots + m(g_{r-1})\tau^{r-1} + \tau^r.$$ 

Now let $\psi$ and $\tilde{\psi}$ be two Drinfeld modules such that $m_\psi \circ \iota = m_{\tilde{\psi}} \circ \iota$. We have to show that $\psi$ and $\tilde{\psi}$ are isomorphic over $L$.

The group $F_{q^r}^*$ acts on $B \otimes_{F_q} L = (B \otimes_{F_q} \mathbb{F}_{q^r}) \otimes_{\mathbb{F}_{q^r}} L$ by $\lambda \ast (g_i \otimes \iota) = g_i \otimes \lambda^{q^r - 1} \iota$ and $m_\psi$ extends to $m_\psi : B \otimes_{F_q} L \to L$ as

$$m_\psi(g_i \otimes \iota) = m_\psi(g_i)\iota.$$ 

Suppose that $\psi$ and $\tilde{\psi}$ are not isomorphic, then for each $\lambda \in F_{q^r}^*$, there is a $g_\lambda \in \{g_1, g_2, \ldots, g_{r-1}\}$ for which $m_\psi(\lambda \ast (g_\lambda \otimes 1)) \neq m_{\tilde{\psi}}(g_\lambda \otimes 1)$. We consider the element $f \in B \otimes_{F_q} L$ defined by

$$f = 1 \otimes 1 - \prod_{\lambda \in F_{q^r}^*} \frac{g_\lambda \otimes 1 - 1 \otimes m_\psi(\lambda \ast (g_\lambda \otimes 1))}{1 \otimes (m_\psi(g_\lambda \otimes 1) - m_\psi(\lambda \ast (g_\lambda \otimes 1)))}.$$ 

We evaluate

$$m_{\tilde{\psi}}(f) = 0 \quad \text{and} \quad m_\psi(\mu \ast f) = 1 \quad \text{for each} \quad \mu \in F_{q^r}^*.$$ 

This yields

$$1 = m_{\tilde{\psi}}(\prod_{\mu \in F_{q^r}^*} (\mu \ast f)) = (m_\psi \circ \iota)(\prod_{\mu \in F_{q^r}^*} (\mu \ast f)) = (m_{\tilde{\psi}} \circ \iota)(\prod_{\mu \in F_{q^r}^*} (\mu \ast f)) = 0,$$

a contradiction, which proves the proposition. □

Let $\psi$ be a rank $r$ Drinfeld $A$-module over the $A$-field $L$ given by

$$\psi_T = \gamma(T) + a_1\tau + \cdots + a_r\tau^r, \quad a_1, a_2, \ldots, a_r \in L \quad \text{and} \quad a_r \neq 0.$$
Denote by $\bar{L}$ the algebraic closure of $L$ and let $\delta \in \bar{L}$ be a $(q^r - 1)$st root of $a_r$. Then $\psi$ is isomorphic (over $\bar{L}$) to $\psi' := \delta \psi \delta^{-1}$, given by

$$\psi'_T = \gamma(T) + a'_1 \tau + \cdots + a'_{r-1} \tau^{r-1} + \tau^r, \quad a'_k = \delta^{1-q^k} a_k \text{ for } k = 1, 2, \ldots, r - 1.$$ 

Let $J = \sum_{i=1}^{n} f_i(T) g_{1}^{e_{i,1}} g_{2}^{e_{i,2}} \cdots g_{r-1}^{e_{i,r-1}} \in C$ be an invariant and set

$$J(\psi) := \sum_{i=1}^{n} \gamma(f_i(T)) (a'_1)^{e_{i,1}} (a'_2)^{e_{i,2}} \cdots (a'_{r-1})^{e_{i,r-1}}$$

$$= \sum_{i=1}^{n} \gamma(f_i(T)) a_1^{e_{i,1}} a_2^{e_{i,2}} \cdots a_{r-1}^{e_{i,r-1}} \delta^{\sum_{k=1}^{n} \sum_{k=1}^{r-1} e_{i,k}(1-q^k)}$$

$$= \sum_{i=1}^{n} \gamma(f_i(T)) a_1^{e_{i,1}} a_2^{e_{i,2}} \cdots a_{r-1}^{e_{i,r-1}} \delta^{-\sum_{i=1}^{n} \sum_{k=1}^{r-1} e_{i,k}(q^k-1)} \in L. $$

**Corollary 1.2** Let $\psi$ and $\tilde{\psi}$ be two rank $r$ Drinfeld $A$-modules over the $A$-field $L$. Then $\psi$ and $\tilde{\psi}$ are isomorphic over the algebraic closure $\bar{L}$ if and only if $J(\psi) = J(\tilde{\psi})$ for all $J \in C$.

**Proof.** Let $m_{\psi} : C \rightarrow \bar{L}$ be the homomorphism associated to the isomorphism class of $\psi$ by Proposition 1.1. Then $m_{\psi}(J) = J(\psi)$ for all $J \in C$ and the result follows. $\square$

**Remark 1.3** In fancier language, Proposition 1.1 states that Spec($C$) over Spec($A$) is the coarse moduli scheme parametrizing isomorphism classes of rank $r$ Drinfeld $A$-modules over algebraically closed $A$-fields. This was first shown by I.Y. Potemine in [6].

If $r = 2$, then in fact $C = A[j]$, where $j = q^{g+1} = g^{g+1}/\Delta$ is the usual $j$-invariant of $\psi_T = \gamma(T) + g\tau + \Delta \tau^2$.

In general, the ring $C$ is a finitely generated $A$-algebra, and an explicit set of generators is constructed in [6]. This means that one only needs a finite set of invariants in order to determine whether or not any two Drinfeld modules are isomorphic. For a given finite set of Drinfeld modules of generic characteristic, however, one can find a single invariant to distinguish between them.

**Proposition 1.4** Let $S$ be a finite set of pairwise non-isomorphic rank $r$ Drinfeld $A$-modules of generic characteristic. Then there exists $J \in C$ such that $J$ distinguishes $S$, i.e. $J(\varphi_1) \neq J(\varphi_2)$ for all $\varphi_1 \neq \varphi_2 \in S$.

**Proof.** We use induction on $n := |S|$. The result is clearly true for $n \leq 2$. Let $n \geq 3$, and suppose that the statement is true for sets of cardinality $n - 1$. Pick $\varphi_1 \in S$ and let $S_1 := S \setminus \{\varphi_1\}$. By the induction hypothesis, there exists $J_1 \in C$ which distinguishes $S_1$. If $J_1$ distinguishes $S$ then we’re done. If not, then there exists $\varphi_2 \in S$ such that $J_1(\varphi_1) = J_1(\varphi_2)$, and moreover $\{\varphi_1, \varphi_2\}$ is the only pair in $S$ on which $J_1$ takes the same value.

Pick $J_2 \in C$ which distinguishes $\{\varphi_1, \varphi_2\}$, and consider $J_a := J_1 + aJ_2$ for all $a \in A$. If $J_a$ distinguishes $S$ for some $a \in A$, then we’re done. If not, then there exists a pair $\psi_1, \psi_2 \in S$ for which $J_a(\psi_1) = J_a(\psi_2)$ for at least two distinct values of $a \in A$. From this, we easily deduce that $J_1(\psi_1) = J_1(\psi_2)$, which forces $\{\psi_1, \psi_2\} = \{\varphi_1, \varphi_2\}$, and $J_2(\psi_1) = J_2(\psi_2)$, which is a contradiction. $\square$
Remark 1.5 The conclusion of Proposition 1.4 can fail in special characteristic. For example, let $L = \mathbb{F}_2$ of characteristic $\ker \gamma = T \mathbb{F}_2[T]$ and $r = 3$. Then the three Drinfeld $F_2[T]$-modules defined over $L$ by

$$
\psi_1^T = \tau^3, \quad \psi_2^T = \tau + \tau^3, \quad \psi_3^T = \tau^2 + \tau^3
$$

are pair-wise non-isomorphic, as witnessed by the invariants $g_1^7, g_2^7 \in C$, but no single $J \in C$ can distinguish between all three since $J(\psi^i) \in \mathbb{F}_2$ for every $J \in C$ and $i = 1, 2, 3$.

2 Isogenies and modular polynomials

Let $N \in A$ be monic, then $\varphi_N$ applied to a variable $X$ defines an $F_q$-linear polynomial $\varphi_N(X) \in B[X]$ which is monic and separable over $B$ of degree $q^{r \deg N}$. Let $K = \text{Quot}(B) = F_q(T, g_1, \ldots, g_{r-1})$, denote by $K_N$ the splitting field of $\varphi_N(X)$ over $K$, and let $R_N$ be the integral closure of $B$ in $K_N$. Then the set $\varphi[N] \subset R_N$ of roots of $\varphi_N(X)$ is an $A$-module isomorphic to $(A/NA)^r$.

The Galois group $\text{Gal}(K_N/K)$ respects this $A$-module structure, and in fact it is shown in [3] that $\text{Gal}(K_N/K) \cong \text{Aut}(\varphi[N]) \cong \text{GL}_r(A/NA)$.

Let $f$ be an isogeny from $\varphi$ to another Drinfeld module $\varphi(f)$, defined over an extension of $K$. This means that

$$
f \varphi_T = \varphi_T(f) f.
$$

(1)

Write $f = f_0 + f_1 \tau + \cdots + f_d \tau^d$. Replacing $f$ by $f_d^{-1} f$ gives

$$(f_d^{-1} f) \varphi_T = (f_d^{-1} \varphi_T(f) f_d) (f_d^{-1} f),$$

so if we replace $\varphi(f)$ by an isomorphic Drinfeld module, we may assume that $f_d = 1$, i.e. $f$ is monic. In this case, there exists a monic $N \in A$ such that

$$\ker f \subset \varphi[N],$$

and so $f \in R_N\{\tau\}$. Now comparing the coefficients of the highest powers of $\tau$ in (1) shows that $\varphi_T(f) \in R_N\{\tau\}$ is also monic. For any invariant $J \in C$ we find that $J(\varphi(f)) \in R_N$.

Definition 2.1 Any isogeny $f$ of $\varphi$ satisfying $f \subset \varphi[N]$ is called an $N$-isogeny.

Denote by $I_N$ the set of all monic $N$-isogenies $f \in R_N\{\tau\}$, as above. Since any such $f$ is determined by its kernel, the set $I_N$ is finite.

Definition 2.2 Let $J \in C$ be an invariant. We call

$$
\Phi_{J,N}(X) := \prod_{f \in I_N} \left(X - J(\varphi(f))\right) \in R_N[X]
$$

the full modular polynomial of level $N$ associated to $J$. 

Definition 2.3 Let $H \subset \varphi[N] \cong (A/NA)^r$ be an $A$-submodule. Any isogeny $f \in I_N$ for which $\ker f$ is an element of the $\text{GL}_r(A/NA)$ orbit of $H$ is called an isogeny of type $H$.

Let $J \in C$ be an invariant. Then we call

$$\Phi_{J,H}(X) := \prod_{f \in I_N \text{ of type } H} (X - J(\varphi(f))) \in R_N[X]$$

the modular polynomial of type $H$ associated to $J$.

Proposition 2.4 Let $H \subset \varphi[N]$ be an $A$-submodule, and $J \in C$. Then $\Phi_{J,H}(X) \in C[X]$. Furthermore, if $J \in C$ distinguishes the Drinfeld modules $\{\varphi^f \mid f \text{ of type } H\}$, then $\Phi_{J,H}(X)$ is irreducible over $K$.

Proof. By construction, $\Phi_{J,H}(X) \in R_N[X]$ and $\text{Gal}(K_N/K)$ permutes the roots of $\Phi_{J,H}(X)$, so its coefficients lie in $R_N \cap K = B$.

We next show that $\Phi_{J,H}(X) \in C[X]$. Let $\lambda \in \mathbb{F}_q^*$ and consider the isomorphic Drinfeld module $\psi := \lambda^{-1}\varphi\lambda$, so

$$\psi_T = T + a_1\tau + \cdots + a_{r-1}\tau^{r-1} + \tau^r,$$

with each $a_i = \lambda^{q^i-1}g_i \in \mathbb{F}_q[T, g_1, \ldots, g_{r-1}] \cong B \otimes_{\mathbb{F}_q} \mathbb{F}_q^r$.

We note that $\psi[N] = \lambda^{-1}(\varphi[N])$, and so every $N$-isogeny $f : \varphi \to \varphi^f$ of type $H \subset \varphi[N]$ corresponds to an $N$-isogeny $\lambda^{-1}f : \psi \to \psi^{(\lambda^{-1}f)\lambda} = \lambda^{-1}\varphi^f\lambda$ of type $\lambda^{-1}H \subset \psi[N]$.

Thus, if we specialise the coefficients of $\Phi_{J,H}(X)$ via $g_i \mapsto a_i = \lambda^{q^i-1}g_i$, we obtain the monic polynomial $\Phi_{J(\psi),H}(X)$ whose roots are precisely the $J(\psi^{(\lambda^{-1}f)\lambda})$ for $f \in I_N$ of type $H$. But $J(\psi^{(\lambda^{-1}f)\lambda}) = J(\lambda^{-1}\varphi^f\lambda) = J(\varphi^f)$, so $\Phi_{J(\psi),H}(X) = \Phi_{J,H}(X)$ and we have shown that the coefficients of $\Phi_{J,H}(X)$ are $\mathbb{F}_q^*$-invariant in $B \otimes_{\mathbb{F}_q} \mathbb{F}_q^r$. Thus $\Phi_{J,H}(X) \in C[X]$.

Lastly, the condition on $J$ ensures a one-to-one correspondence between the roots of $\Phi_{J,H}(X)$ and $\{\varphi^f \mid f \text{ of type } H\}$. Since $\text{Gal}(K_N/K) \cong \text{GL}_r(A/NA)$ acts transitively on these roots, $\Phi_{J,H}(X)$ is irreducible over $K$. $\square$

Corollary 2.5 The full modular polynomial satisfies $\Phi_{J,N}(X) \in C[X]$, and if $J$ distinguishes the Drinfeld modules $\{\varphi^f \mid f \in I_N\}$, then the $K$-irreducible factors of $\Phi_{J,N}(X)$ are precisely the $\Phi_{J,H}(X)$ for various types $H \subset \varphi[N]$. $\square$

When $r = 2$, then $C = A[j]$ and $\Phi_{j,(A/NA)}(X) = \Phi_N(j, X) \in A[j, X]$ is the usual Drinfeld modular polynomial constructed in [2].

Let $\psi$ be a rank $r$ Drinfeld $A$-module defined over an $A$-field $L$. Then the coefficients of $\Phi_{J,H}(X) \in C[X]$ can be applied to $\psi$ (equivalently, $m_\psi$ from Proposition 1.1 can be applied to each coefficient), resulting in a polynomial

$$\Phi_{J(\psi),H}(X) \in L[X],$$

whose roots are precisely the $J(\psi^f)$ for $N$-isogenies $f : \psi \to \psi^f$ of type $H$, which we will prove below. If $N$ is not prime to the characteristic $\ker(\gamma)$ of $\psi$, then we need to make the notion of “$N$-isogeny of type $H$” more precise.

For our purposes we define a level-$N$ structure on $\psi$ to be a surjective $A$-module homomorphism

$$\mu : \varphi[N] \to \psi[N] \subset \hat{L}.$$
When $N$ is prime to the characteristic $\ker(\gamma)$ of $\psi$, then $\mu$ is an isomorphism. If $\mu$ and $\mu'$ are two level-$N$ structures on $\psi$, then there is a $\sigma \in \GL_r(A/NA)$ such that $\mu' = \mu \circ \sigma$.

Let $H \subset \varphi[N]$ be an $A$-submodule. Then an isogeny $f : \psi \to \psi'(f)$ is said to be of type $H$ if $f(X) = \prod_{h \in H'}(X - \mu(h))$, where $H' \subset \varphi[N]$ is an element of the $\GL_r(A/NA)$-orbit of $H$. The set of isogenies of $\psi$ of type $H$ is independent of the chosen level structure $\mu$. We have

**Proposition 2.6** Let $\psi$ be a rank $r$ Drinfeld $A$-module over the $A$-field $L$, let $J \subset C$ be an invariant and $H \subset \varphi[N]$ an $A$-submodule. Then

$$\Phi_{J(\psi),H}(X) = \prod_{f \text{ of type } H} (X - J(\psi'(f))) \in L[X].$$

**Proof.** We have

$$\varphi_T(X) = \prod_{u \in \varphi[T]} (X - u) = TX + g_1 X^q + \cdots + g_{r-1} X^{q^{r-1}} + X^q,$$

so the $g_i \in \mathbb{F}_q[u : u \in \varphi[T]]$ are polynomials over $\mathbb{F}_q$ in the $u$'s. Moreover, these polynomials are invariant under the $\GL_r(A/TA)$-action on $\varphi[T]$.

Next, let $f : \varphi \to \varphi'(f)$ be an isogeny of type $H$, then for a suitable $H' \subset \varphi[N]$ we have

$$f(X) = \prod_{h \in H'} (X - h) = f_0 X + f_1 X^q + \cdots + f_{d-1} X^{q^{d-1}} + X^q,$$

where $d = \dim_{\mathbb{F}_q}(H)$. Again, we see that the $f_i \in \mathbb{F}_q[h : h \in H']$ are polynomials over $\mathbb{F}_q$ in the $h$'s.

Write $\varphi'(f) = T + g'_1 \tau + \cdots + g'_r \tau^{r-1} + \tau$, then comparing coefficients of $\tau^{d-1}, \tau^{d-2}, \ldots, \tau^{d-r+1}$ in $f \cdot \varphi = \varphi_T'(f) \cdot f$, we obtain

$$g'_i \in \mathbb{F}_q[T, g_1, \ldots, g_{r-1}, f_1, \ldots, f_{d-1}] \subset \mathbb{F}_q[u, h : u \in \varphi[T], h \in H'].$$

As a result

$$J(\varphi'(f)) \in \mathbb{F}_q[u, h : u \in \varphi[T], h \in H'],$$

but $J \subset C \subset \mathbb{F}_q[T, g_1, \ldots, g_{r-1}]$, so in fact $J(\varphi'(f)) \in \mathbb{F}_q[u : u \in \varphi[T]]$.

Now, replacing $\psi$ by an isomorphic Drinfeld module over $\bar{L}$ if necessary, we may assume that

$$\psi_T = \gamma(T) + a_1 \tau + \cdots + a_{r-1} \tau^{r-1} + \tau, \quad a_1, \ldots, a_{r-1} \in \bar{L},$$

is monic. Let $M = \lcm(T, N)$ and let $\mu : \varphi[M] \to \psi[M]$ be a level-$M$ structure on $\psi$. By the same arguments as above, replacing each $u$ by $\mu(u)$ and each $h$ by $\mu(h)$, we find that each

$$J(\psi'(f)) \in \mathbb{F}_q[\mu(u) : u \in \varphi[T]]$$

is the same polynomial as $J(\varphi'(f))$, but with each $u$ replaced by $\mu(u)$.

Applying the map $\mu$ to the polynomials $g_i \in \mathbb{F}_q[u : u \in \varphi[T]]$, each $g_i$ is mapped to $a_i$, hence $\mu$ coincides there with the homomorphism $m_\psi : C \to \bar{L}$ from Proposition 1.1. Thus, for each isogeny $f$ of type $H$, we obtain

$$m_\psi(J(\varphi'(f))) = J(\psi'(f)),$$

which completes the proof. \qed
3 Correction to [4]

In [4] we gave an analytic construction of modular polynomials of type \((A/NA)^{r-1}\). These polynomials also classify incoming isogenies \(\varphi' \rightarrow \varphi\) with kernels isomorphic to \(A/NA\), whereas the point of view of the present article is to classify modular polynomials by the kernels of the dual, outgoing isogenies \(f : \varphi \rightarrow \varphi'\), which explains the shift in terminology from type \(A/NA\) to type \((A/NA)^{r-1}\).

Theorem 1.1 of [4] claims that the polynomials \(\Phi_{J(A/NA)^{r-1}}(X)\) are irreducible, but this is only true if \(J \in C\) distinguishes the set of Drinfeld modules \(\{\varphi(f) \mid f \text{ of type } (A/NA)^{r-1}\}\), i.e. when \(\Phi_{J(A/NA)^{r-1}}(X)\) has distinct roots. Such invariants \(J \in C\) always exist, by Proposition 1.4.

4 Reduction mod \(P\) and Kronecker congruence relations

In this section, we let \(N = P \in A\) be a monic prime, and we study the reduction of modular polynomials modulo \(P\). When we reduce polynomials in \(R_P[X]\), then we are actually reducing modulo a chosen prime of \(R_P\) extending \(PB\) (remember that \(R_P\) is integral over \(B\)), but we will still write \(mod\ P\) for ease of notation.

Define \(F_P := A/PA\). We start with the following basic result.

**Proposition 4.1** We have
\[
\varphi_P \equiv \tilde{\varphi}_P \cdot \tau^{\deg(P)} \mod P,
\]
where \(\tilde{\varphi}_P \in (B \otimes_A F_P)\{\tau\}\) is not divisible by \(\tau\).

In other words, \(\varphi\) has ordinary reduction at every prime \(P\).

We will give two proofs of this result, starting with a conceptual proof.

**Proof.** Denote by \(\tilde{\varphi} : A \rightarrow (B \otimes_A F_P)\{\tau\}\) the reduction of \(\varphi\) modulo \(P\). We have \(\tilde{\varphi}[P] \cong (A/PA)^{r-h}\), where \(h\) is the height of \(\varphi\) (see [5, §4.5]). The linear term of \(\varphi_P\) is \(r\), so \(\tilde{\varphi}_P\) is divisible by \(\tau\) and thus \(h \geq 1\). We will show that \(h = 1\) by constructing a specialization of \(\varphi\) with ordinary reduction at a prime above \(P\).

Recall that \(k = F_q(T)\) and let \(F/k\) be a separable extension of degree \(r\) which has only one place above the place of \(k\) with uniformizer \(1/T\) (i.e. \(F/k\) is purely imaginary) and in which \(P\) splits completely (such a field exists, by [1, Chapter X, Theorem 6]). Denote by \(R\) the integral closure of \(A\) in \(F\), and let \(\psi\) be a rank 1 Drinfeld \(R\)-module, which is automatically a rank \(r\) Drinfeld \(A\)-module with complex multiplication by \(R\) (for example, let \(\psi\) be the Drinfeld module corresponding to the lattice \(R\) in the algebraic closure of \(F_q((\frac{1}{T}))\)). Let \(PR = p_1p_2\cdots p_r\) be the factorization of \(PR\) in \(R\). Let \(L/F\) be a finite extension over which \(\psi\) is defined, let \(\mathfrak{P}_1\) be a place of \(L\) above \(p_1\), and denote by \(\mathcal{O}_{\mathfrak{P}_1}\) the valuation ring of \(\mathfrak{P}_1\). Since all rank 1 Drinfeld modules have potential good reduction by [5, Cor. 4.10.4], we may write
\[
\psi_T = T + a_1\tau + a_2\tau^2 + \cdots + a_r\tau^r, \quad \text{with} \quad a_1, \ldots, a_{r-1} \in \mathcal{O}_{\mathfrak{P}_1}, \quad a_r \in \mathcal{O}_{\mathfrak{P}_1}^*.
\]

After possibly replacing \(L\) by a finite extension and \(\psi\) by an isomorphic Drinfeld module, we may assume furthermore that \(a_r = 1\), so that \(\psi\) is the image of \(\varphi\) under the specialization \(g_i \mapsto a_i, \ i = 1, 2, \ldots, r - 1\).
Consider the coefficient of equality if and only if $m$ was used in the construction of $\psi$ monomials in $(T,g)$, whereas all other terms have strictly smaller degree in $g$.

One of the terms of $\psi$ can be written uniquely in the form $T^a g^b \tau^c$ and we set $\deg_{g_1}(m) := b$ and $\deg_{\tau}(m) := c$.

By induction on $i$, one readily shows that

$$\deg_{g_1}(m) \leq \frac{q^{\deg_{\tau}(m)} - 1}{q - 1},$$

with equality if and only if $m$ is simple.

Now suppose $P = \sum_{i=0}^s a_i T_i$, with $a_s = 1$, is our monic prime in $A$ of degree $s$. We consider the coefficient $b_s(T,g_1)$ of $\tau^s$ in

$$\psi_P = \sum_{i=0}^s a_i (\psi_T)^i = \sum_{j=0}^{rs} b_j(T,g_1) \tau^j.$$ 

One of the terms of $b_s(T,g_1)$ is $g_1^{(q^s-1)/(q-1)}$, arising from the monomial $(g_1 \tau)^s$ in $(\psi_T)^s$, whereas all other terms have strictly smaller degree in $g_1$, since they arise from non-simple monomials in $(\psi_T)^i$ with $i \leq s$. It follows that $b_s(T,g_1)$ does not vanish modulo $P$, and so the reduction of $\psi$ modulo $P$ has height 1, as required. \qed

**Corollary 4.2** There exists a unique monic $P$-isogeny $f_0$ of $\varphi$ satisfying

1. $f_0 \equiv \tau^{\deg P} \mod P$,
2. $U_0 := \ker f \cong A/PA = \mathbb{F}_P$ as $A$-modules, and
3. $f_0 \varphi = \varphi(f_0) f_0$, where

$$\varphi(f_0) = T + g_1^{[P]} \tau + \cdots + g_s^{[P]} \tau^{r-1} + \tau^r \mod P.$$

**Proof.** Let $U_0 = \ker (\varphi[P] \rightarrow \varphi[P])$ denote the kernel of reduction modulo $P$. Then by Proposition 4.1, $U_0 \cong A/PA$, and

$$f_0(X) := \prod_{u_0 \in U_0} (X - u_0) \equiv X^{[P]} \mod P.$$ 

It is now easy to verify that $f_0$ has all the required properties. \qed

Since the kernel of any $P$-isogeny $f$ is an $\mathbb{F}_P$-vector space, its kernel $U := \ker f$ satisfies either $U_0 \cap U = \{0\}$, in which case we call $f$ ordinary, or else $U_0 \subset U$, in which case we call $f$ special. Equivalently, $f$ is ordinary if the reduction of $f$ modulo $P$ is separable, and special otherwise.
Definition 4.3 Let $H \subset \varphi[P]$ be an $A$-submodule and $J \in C$ an invariant. We define the following factors of the modular polynomial $\Phi_{J,H}(X)$:

\[
\Phi^\text{spec}_{J,H}(X) := \prod_{f \in I_P \text{ special of type } H} \left( X - J(\varphi(f)) \right) \in R_P[X], \quad \text{and}
\]

\[
\Phi^\text{ord}_{J,H}(X) := \prod_{f \in I_P \text{ ordinary of type } H} \left( X - J(\varphi(f)) \right) \in R_P[X].
\]

Clearly $\Phi_{J,H}(X) = \Phi^\text{spec}_{J,H}(X) \cdot \Phi^\text{ord}_{J,H}(X)$.

We are now ready to prove our main result.

Theorem 4.4 (Kronecker Congruence Relations) Let $P \in A$ be a monic prime, $J \in C$ an invariant and $1 \leq s < r$. Then

1. $\Phi^\text{ord}_{J,(A/PA)^s}(X) \equiv \left( \Phi^\text{spec}_{J,(A/PA)^{s+1}}(X|P) \right)^{|P|^{s-1}} \mod P$, and

2. $\Phi_{J,(A/PA)^s}(X) \equiv \Phi^\text{spec}_{J,(A/PA)^s}(X) \cdot \left( \Phi^\text{spec}_{J,(A/PA)^{s+1}}(X|P) \right)^{|P|^{s-1}} \mod P$.

Furthermore,

3. The reductions of $\Phi^\text{spec}_{J,(A/PA)^s}(X)$ and $\Phi^\text{ord}_{J,(A/PA)^s}(X)$ modulo $P$ lie in $(C \otimes_A \mathbb{F}_P)[X]$ for every $s = 1, \ldots, r$.

Proof. Let $1 \leq s < r$. Let $f_U$ and $f_{\bar{U}}$ be two ordinary $P$-isogenies of type $H \cong (A/PA)^s$ with kernels $U$ and $\bar{U}$, respectively. We call $f_U$ and $f_{\bar{U}}$ equivalent if $U + U_0 = \bar{U} + U_0$. This way each equivalence class contains $|P|^s$ elements, since the kernel of each isogeny in the equivalence class of $f_U$ is obtained by adding elements of $U_0$ to each of the $s$ basis vectors of $U$. The $P$-isogeny $f_{U+U_0}$ with kernel $U + U_0$ is then special of type $(A/PA)^{s+1}$, and moreover each special isogeny of type $(A/PA)^{s+1}$ arises from an equivalence class of ordinary isogenies of type $(A/PA)^s$ in this way.

We see that

\[
f_{U+U_0}(X) = \prod_{u \in U} \prod_{u_0 \in U_0} (X - u - u_0) = \prod_{u \in U} (X - u)^{|P|} \equiv f_U(X)^{|P|} \equiv \tau^\text{deg } P (f_U(X)) \mod P.
\]

Thus, for the corresponding isogenous Drinfeld modules,

\[
\varphi(U+U_0) \cdot \tau^\text{deg } P \cdot f_U \equiv \varphi(U+U_0) \cdot f_{U+U_0} = f_{U+U_0} \cdot \varphi \equiv \tau^\text{deg } P \cdot f_U \cdot \varphi = \tau^\text{deg } P \cdot \varphi(U) \cdot f_U \mod P,
\]

and we obtain

\[
\varphi(U+U_0) \cdot \tau^\text{deg } (P) \equiv \tau^\text{deg } (P) \cdot \varphi(U) \mod P.
\]

For any invariant $J \in C$ we now have

\[
J(\varphi(U+U_0)) \equiv J(\varphi(U)|P|) \mod P.
\]
If we combine these results, we calculate
\[
\left( \Phi_{J,(A/PA)^s}^\text{ord}(X) \right)^{|P|} \equiv \prod_{f_U \text{ ordinary of type } (A/PA)^s} \left( X^{|P|} - J((\varphi(U))^{|P|}) \right) \mod P
\]
\[
\equiv \prod_{f_U(U_0)} \left( X^{|P|} - J((\varphi(U+U_0))^{|P|}) \right)^{|P|^{s}} \mod P
\]
\[
\equiv \left( \Phi_{J,(A/PA)^{s+1}}^\text{spec}(X) \right)^{|P|^{s}} \mod P,
\]
from which (1.) follows.

Next, (2.) follows from (1.) and \( \Phi_{J,(A/PA)^s}(X) = \Phi_{J,(A/PA)^s}^\text{spec}(X) \cdot \Phi_{J,(A/PA)^s}^\text{ord}(X) \).

It remains to prove (3.). If \( s = r \), then
\[
\Phi_{J,(A/PA)^r}(X) = \Phi_{J,(A/PA)^r}^\text{spec}(X) = X - J,
\]
since the only isogeny of type \( (A/PA)^r \) is the endomorphism \( \varphi_N \), and of course
\[
\Phi_{J,(A/PA)^r}^\text{ord}(X) = 1.
\]
Now suppose that \( \Phi_{J,(A/PA)^s}(X) \mod P \in (C \otimes_A \mathbb{F}_p)[X] \) for some \( 1 \leq s \leq r \). Since also \( \Phi_{J,(A/PA)^{s-1}}(X) \mod P \in (C \otimes_A \mathbb{F}_p)[X] \), it follows from (2.), with \( s \) replaced by \( s - 1 \), that \( \Phi_{J,(A/PA)^{s-1}}(X) \mod P \in (C \otimes_A \mathbb{F}_p)[X] \). Indeed, if this were not the case, consider its highest coefficient not in \( C \otimes_A \mathbb{F}_p \) and remember that all our polynomials are monic.

Lastly, it follows from (1.) that now also \( \Phi_{J,(A/PA)^s}^\text{ord}(X) \mod P \in (C \otimes_A \mathbb{F}_p)[X] \).

**Question 4.5** Suppose that \( J \) distinguishes the reduced Drinfeld modules \( \varphi^{(f)} \) for special isogenies \( f \in I_p \). Is \( \Phi_{J,(A/PA)^s}(X) \) irreducible modulo \( P \)?

5 Examples

**Example 1.** \( s = 1 \): In this case
\[
\Phi_{J,(A/PA)\text{spec}}(X) = X - J((\varphi(f_0))) = X - J^{[P]}],
\]
by Corollary 4.2, so
\[
\Phi_{J,(A/PA)}(X) \equiv (X - J^{[P]}) \cdot \Phi_{J,(A/PA)^2}(X^{[P]}) \mod P.
\]

**Example 2.** \( s = r - 1 \): We have
\[
\Phi_{J,(A/PA)^r}\text{spec}(X) = X - J((\varphi^N)) = X - J,
\]
so
\[
\Phi_{J,(A/PA)^r-1}(X) \equiv \Phi_{J,(A/PA)^r-1}(X) \cdot \left( X^{[P]} - J \right)^{|P|^{r-2}} \mod P.
\]

**Example 3.** \( r = 2 \): This is a combination of examples 1 and 2 above, and gives the classical result (see [2]):
\[
\Phi_{J,(A/PA)}(X) \equiv (X - J^{[P]}) \cdot (X^{[P]} - J) \mod P.
\]
Example 4. Now suppose that $r = 3$, $P = T$ and $A = \mathbb{F}_2[T]$, see [4]. In this case,

$$C = \frac{A[J_{07}, J_{12}, J_{41}, J_{70}]}{(J_{07}J_{41} - J_{12}^3, J_{12}J_{70} - J_{41}^2)},$$

where $J_{ij} = g_1^ig_2^j$. In [4] we computed $\Phi_{J,(A/TA)^2}(X)$ for $J \in \{J_{07}, J_{12}, J_{41}, J_{70}\}$ (they are denoted $P_{J,T}(X)$ in that paper). Reducing these modulo $T$, one obtains, for example,

$$\Phi_{J_{12},(A/TA)^2}(X) \equiv \Phi_{J_{12},(A/TA)^2}^{\text{spec}}(X) \cdot (X^2 + J_{12})^2 \mod T$$

where

$$\Phi_{J_{12},(A/TA)^2}^{\text{spec}}(X) \equiv X^3 + (J_{07}J_{12} + J_{12}^3 + J_{70})X^2 + (J_{07}J_{41} + J_{12}J_{41}J_{70} + J_{41} + J_{70}^2)X$$

$$+ (J_{07}J_{12}J_{41} + J_{12}^2J_{70} + J_{12}J_{70}^2 + J_{41}^2 + J_{70}) \mod T.$$

A similar computation, carried out with the help of Heriniaina Razafinjatovo, confirms that

$$\Phi_{J_{12},(A/TA)}(X) \equiv (X + J_{12}^2) \cdot \Phi_{J_{12},(A/TA)^2}^{\text{spec}}(X^2) \mod T,$$

with $\Phi_{J_{12},(A/TA)^2}^{\text{sep}}(X)$ as above.

References

[1] E. Artin and J. Tate, Class Field Theory, AMS Chelsea, 2008.

[2] S. Bae, On the modular equation for Drinfeld modules of rank 2, *J. Number Theory* 42 (1992), 123–133.

[3] F. Breuer, Explicit Drinfeld moduli schemes and Ahyankar’s Generalized Iteration conjecture, *preprint* (2015); arXiv:1503.06420 [math.NT]

[4] F. Breuer, H.-G. Rück, Drinfeld modular polynomials in higher rank, *J. Number Theory* 129 (2009), 59–83.

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

[6] I.Y. Potemine, Minimal terminal $\mathbb{Q}$-factorial models of Drinfeld coarse moduli schemes, *Math. Phys. Anal. Geom.* 1 (1998), 171–191.

Department of Mathematical Sciences
University of Stellenbosch
Stellenbosch, 7600
South Africa
fbreuer@sun.ac.za

Institut für Mathematik
Universität Kassel,
Kassel, 34132
Germany
rueck@mathematik.uni-kassel.de