Appendix to: Abelian varieties over finite fields with commutative endomorphism algebra: theory and algorithms

Jonas Bergström, Valentijn Karemaker, and Stefano Marseglia

This document contains auxiliary material to the content of the main article. It is thought as a guide to the Magma code contained in the repository [1]. The reference to the main article can be recognized by the use of arabic numerals, while in this document we use roman numerals for lemmas, thorems and remarks, and letters for the algorithms.

The notation is the same as in the main article, see in particular Section 6. It is recalled at the end of the document, for convenience.

Local-local part of Dieudonné modules

The next lemma is used in Algorithm 1 of the main article and Remark IV.

Lemma I. *Let $\widetilde{\mathfrak{P}}_{\nu,1},\dots,\widetilde{\mathfrak{P}}_{\nu,g_\nu}$ be the maximal ideals of $\mathcal{O}_{\widetilde{A}}$ extending a place ν of E_p. Fix an index i and consider the natural surjective ring homomorphism*

$$\varphi : \mathcal{O}_{\widetilde{A}} \twoheadrightarrow \frac{\mathcal{O}_{\widetilde{A}}}{\widetilde{\mathfrak{P}}^2_{\nu,i}\cdot\prod_{j\neq i}\widetilde{\mathfrak{P}}_{\nu,j}} \simeq \frac{\mathcal{O}_{\widetilde{A}}}{\widetilde{\mathfrak{P}}^2_{\nu,i}} \times \prod_{i\neq j}\frac{\mathcal{O}_{\widetilde{A}}}{\widetilde{\mathfrak{P}}_{\nu,j}}.$$

Pick $b_i \in \widetilde{\mathfrak{P}}_{\nu,i}\setminus\widetilde{\mathfrak{P}}^2_{\nu,i}$ and let $t_{\nu,i}$ be an element of $\mathcal{O}_{\widetilde{A}}$ such that $\varphi(t_{\nu,i})$ equals the class of b_i in the i-th component and the class of 1 in every other component. Then the image of $t_{\nu,i}$ via the natural ring homomorphism $\mathcal{O}_{\widetilde{A}} \to \mathcal{O}_{\widetilde{A},\widetilde{\mathfrak{P}}_{\nu,j}} \simeq \mathcal{O}_{A,\mathfrak{P}_{\nu,j}}$ is a uniformizer if $j=i$ and a unit otherwise.

Proof. The statement is an application of Nakayama's lemma and the Chinese remainder theorem. □

The next algorithm computes a set of representatives of the W'_R-isomorphism classes of fractional W'_R-ideals, summarizing Subsection 6.2 of the main article.

Algorithm A.
Input: The order R.
Output: A set of fractional $\widetilde{W}_R$-ideals representing $\mathcal{W}(W'_R)$.

(1) Compute the orders $\mathcal{O}_{\widetilde{A}}$ and $\widetilde{W}_R$;

(2) Compute the set $\widetilde{\mathfrak{p}}_1,\dots,\widetilde{\mathfrak{p}}_n$ of maximal ideals of $\widetilde{W}_R$ that lie below the maximal ideals of $\mathcal{O}_{\widetilde{A}}$ extending the places of E_p with slope in $(0,1)$;

(3) Set $k = \mathrm{val}_p([\mathcal{O}_{\widetilde{A}} : \widetilde{W}_R])$;

(4) For each $\widetilde{\mathfrak{p}}_i$ compute a set $\mathcal{W}_i$ of representatives of $\mathcal{W}(\widetilde{W}_R + \widetilde{\mathfrak{p}}_i^k\mathcal{O}_{\widetilde{A}})$, for example, using [2, Algorithm ComputeW];

(5) Construct a set of representatives of $\mathcal{W}(W'_R)$ by combining the sets $\mathcal{W}_1,\dots,\mathcal{W}_n$, using Lemma 3.7.

Theorem II. *Algorithm A is correct.*

Proof. This is an immediate consequence of Lemma 6.3 and Proposition 3.10. □

The following lemma gives details about the computation of the quotient of local unit groups $\mathcal{O}_A^\times/S^\times$, using global representatives, discussed in Remark 6.6 in Step 3, see Subsection 6.3.

Lemma III. *Let* $\widetilde{\mathfrak{f}}$ *be the conductor of* $\widetilde{S}$ *in* $\mathcal{O}_{\widetilde{A}}$ *and* $\widetilde{\mathfrak{p}}_1,\dots,\widetilde{\mathfrak{p}}_r$ *the maximal ideals of* $\widetilde{S}$ *corresponding to the finitely many maximal ideals of* S*. For* $i=1\dots,r$*, set* k_i *to be the smallest integer greater than or equal to* $\mathrm{val}_p(|\widetilde{S}/\widetilde{\mathfrak{f}}|)/\mathrm{val}_p(|\widetilde{S}/\widetilde{\mathfrak{p}}_i|)$*. Then the natural ring homomorphism*

$$\widetilde{S}\longrightarrow \frac{\mathcal{O}_{\widetilde{A}}}{\widetilde{\mathfrak{f}}+\prod_{i=1}^r\widetilde{\mathfrak{p}}_i^{k_i}\mathcal{O}_{\widetilde{A}}}$$

has kernel $\widetilde{\mathfrak{f}}+\prod_{i=1}^r\widetilde{\mathfrak{p}}_i^{k_i}$ *and it induces a group isomorphism*

$$\frac{\mathcal{O}_{A'}^\times}{S^\times}\simeq\frac{\left(\dfrac{\mathcal{O}_{\widetilde{A}}}{\widetilde{\mathfrak{f}}+\prod_{i=1}^r\widetilde{\mathfrak{p}}_i^{k_i}\mathcal{O}_{\widetilde{A}}}\right)^\times}{\left(\dfrac{\widetilde{S}}{\widetilde{\mathfrak{f}}+\prod_{i=1}^r\widetilde{\mathfrak{p}}_i^{k_i}}\right)^\times}.$$

Proof. For $i=1,\dots,r$, we have $\widetilde{\mathfrak{p}}_i^{k_i}\widetilde{S}_{\widetilde{\mathfrak{p}}_i}\subseteq\widetilde{\mathfrak{f}}_{\widetilde{\mathfrak{p}}_i}$ and hence also $\widetilde{\mathfrak{p}}_i^{k_i}\mathcal{O}_{\widetilde{A},\widetilde{\mathfrak{p}}_i}\subseteq\widetilde{\mathfrak{f}}_{\widetilde{\mathfrak{p}}_i}\mathcal{O}_{A,\widetilde{\mathfrak{p}}_i}=\widetilde{\mathfrak{f}}_{\widetilde{\mathfrak{p}}_i}$. The kernel of the homomorphism in the statement is

$$\widetilde{S}\cap(\widetilde{\mathfrak{f}}+\prod_{i=1}^r\widetilde{\mathfrak{p}}_i^{k_i}\mathcal{O}_{\widetilde{A}});$$

we now show that it equals $\widetilde{\mathfrak{f}}+\prod_{i=1}^r\widetilde{\mathfrak{p}}_i^{k_i}$. It suffices to check the equality locally at every maximal ideal of $\widetilde{S}$. Let $\mathfrak{p}$ be a maximal ideal not in the set $\{\widetilde{\mathfrak{p}}_1,\dots,\widetilde{\mathfrak{p}}_r\}$. Then

$$\left(\widetilde{\mathfrak{f}}+\prod_{i=1}^r\widetilde{\mathfrak{p}}_i^{k_i}\right)_{\mathfrak{p}}=\widetilde{S}_{\mathfrak{p}}=\left(\widetilde{S}\cap(\widetilde{\mathfrak{f}}+\prod_{i=1}^r\widetilde{\mathfrak{p}}_i^{k_i}\mathcal{O}_{\widetilde{A}})\right)_{\mathfrak{p}},$$

while

$$\left(\widetilde{\mathfrak{f}}+\prod_{i=1}^r\widetilde{\mathfrak{p}}_i^{k_i}\right)_{\widetilde{\mathfrak{p}}_i}=\widetilde{\mathfrak{f}}_{\widetilde{\mathfrak{p}}_i}=\left(\widetilde{S}\cap(\widetilde{\mathfrak{f}}+\prod_{i=1}^r\widetilde{\mathfrak{p}}_i^{k_i}\mathcal{O}_{\widetilde{A}})\right)_{\widetilde{\mathfrak{p}}_i}$$

for $i=1,\dots,r$.

For the second part of the statement, we observe that the decomposition $S\simeq\oplus_{\mathfrak{p}}S_{\mathfrak{p}}$, where the direct sum is over the finitely many maximal ideals $\mathfrak{p}$ of S, induces a decomposition $\mathcal{O}_{A'}\simeq\oplus_{\mathfrak{p}}\mathcal{O}_{A',\mathfrak{p}}$. If $\mathfrak{p}$ does not lie above the conductor $\mathfrak{f}$ of S in $\mathcal{O}_{A'}$ then $S_{\mathfrak{p}}=\mathcal{O}_{A',\mathfrak{p}}$. Hence we have the following isomorphism:

$$\frac{\mathcal{O}_{A'}^\times}{S^\times}\simeq\bigoplus_{\mathfrak{f}\subseteq\mathfrak{p}}\frac{\mathcal{O}_{A',\mathfrak{p}}^\times}{S_{\mathfrak{p}}^\times}. \tag{1}$$

For $\mathfrak{p}$ lying above the conductor $\mathfrak{f}$, there is a natural bijection between the finite set of primes of $\mathcal{O}_{A',\mathfrak{p}}$ and the set of maximal ideals of $\mathcal{O}_{A',\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}}$, where $\mathfrak{f}_{\mathfrak{p}}$ is the completion of $\mathfrak{f}$ at $\mathfrak{p}$. Hence the map

$$\mathcal{O}_{A',\mathfrak{p}}^\times\to\left(\frac{\mathcal{O}_{A',\mathfrak{p}}}{\mathfrak{f}_{\mathfrak{p}}}\right)^\times$$

induced by taking quotients is surjective. The composition

$$\mathcal{O}_{A',\mathfrak{p}}^\times\to\left(\frac{\mathcal{O}_{A',\mathfrak{p}}}{\mathfrak{f}_{\mathfrak{p}}}\right)^\times\to\frac{(\mathcal{O}_{A',\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}})^\times}{(S_{\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}})^\times}$$

has kernel $S_{\mathfrak{p}}^\times$. Therefore, by Equation (1), we get

$$\frac{\mathcal{O}_{A'}^\times}{S^\times}\simeq\bigoplus_{\mathfrak{f}\subseteq\mathfrak{p}}\frac{(\mathcal{O}_{A',\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}})^\times}{(S_{\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}})^\times}. \tag{2}$$

The argument used above shows that, for each i, we have isomorphisms

$$\frac{S_{\mathfrak{p}_i}}{\mathfrak{f}_{\mathfrak{p}_i}}\simeq\frac{\widetilde{S}_{\widetilde{\mathfrak{p}}_i}}{\widetilde{\mathfrak{f}}_{\widetilde{\mathfrak{p}}_i}}\simeq\frac{\widetilde{S}_{\widetilde{\mathfrak{p}}_i}}{\left(\widetilde{\mathfrak{f}}+\prod_{i=1}^r\widetilde{\mathfrak{p}}_i^{k_i}\right)_{\widetilde{\mathfrak{p}}_i}}, \tag{3}$$

inducing

$$\frac{\mathcal{O}_{A',\mathfrak{p}_i}}{\mathfrak{f}_{\mathfrak{p}_i}} \simeq \frac{\mathcal{O}_{\widetilde{A},\widetilde{\mathfrak{p}}_i}}{\widetilde{\mathfrak{f}}_{\widetilde{\mathfrak{p}}_i}} \simeq \frac{\mathcal{O}_{\widetilde{A},\widetilde{\mathfrak{p}}_i}}{\left(\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i} \mathcal{O}_{\widetilde{A}}\right)_{\widetilde{\mathfrak{p}}_i}}. \tag{4}$$

We conclude by combining Equations (3), (4) and (2) and the fact that we have canonical ring isomorphisms

$$\frac{\widetilde{S}}{\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i}} \simeq \prod_{i=1}^{r} \frac{\widetilde{S}_{\widetilde{\mathfrak{p}}_i}}{\left(\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i}\right)_{\widetilde{\mathfrak{p}}_i}}$$

and

$$\frac{\mathcal{O}_{\widetilde{A}}}{\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i} \mathcal{O}_{\widetilde{A}}} \simeq \prod_{i=1}^{r} \frac{\mathcal{O}_{\widetilde{A},\widetilde{\mathfrak{p}}_i}}{\left(\widetilde{\mathfrak{f}} + \prod_{i=1}^{r} \widetilde{\mathfrak{p}}_i^{k_i} \mathcal{O}_{\widetilde{A}}\right)_{\widetilde{\mathfrak{p}}_i}}.$$

□

The next remark explains how to scale fractional ideals in $\widetilde{A}$ using only elements coming from E. This is used to push all candidates of the representatives of the isomorphism classes $W'_R\{F', V'\}$-ideals into the finite quotient Q_{m_0} in Algorithm 2, while keeping m_0 small for efficiency reasons.

Remark IV. In Step 3 of Algorithm 2, we need to scale each $\widetilde{W_R}$-ideal $\widetilde{I}_k$ inside $\widetilde{J}$ by some element x of $\widetilde{\Delta}(E^\times)$, that is, $x \in \widetilde{\Delta}^{-1}(C)$, where $C = (\widetilde{J} : \widetilde{I}_k)$. Moreover, it is desirable to try to minimize $w = \mathrm{val}_p(\exp(\widetilde{J}/x\widetilde{I}_k))$, in order to keep the parameter m_0 as low as possible, since m_0 determines the size of the quotients appearing in the rest of the algorithm. One possibility is to compute $v = \mathrm{val}_p(\exp(\widetilde{I}_k + \widetilde{J}/\widetilde{J}))$ and $y = [p^v\widetilde{I}_k + \widetilde{J} : \widetilde{J}]$, which is coprime to p. Then $x = p^v y$ is the *integer* in $\widetilde{\Delta}^{-1}(C)$ giving the smallest possible value of w. Another possibility (dropping the restriction of x being an integer) is to use the fact that C is a fractional $\mathcal{O}_{\widetilde{A}}$-ideal. Compute the uniformizers $t_{\nu_1}, \ldots, t_{\nu_n}$ of the places $\nu_1, \ldots, \nu_n$ of E above p For each ν_i, let M_i be the maximum value of $\mathrm{val}_{\widetilde{\mathfrak{P}}}(C)$ for $\widetilde{\mathfrak{P}}$ ranging over the maximal ideals of $\mathcal{O}_{\widetilde{A}}$ above ν_i. Then set $x' = \widetilde{\Delta}(t_{\nu_1}^{M_1} \cdots t_{\nu_n}^{M_n})$, $y = [x'\widetilde{I}_k + \widetilde{J} : \widetilde{J}]$ and finally $x = x'y$. The second method might give smaller values of w but requires more expensive computations. Similar considerations apply in Step 2 if one is using the method described in Remark 6.11 for computing F_{m_0} and V_{m_0}.

Algorithm A above and Algorithms 1 and 2 from the main article are combined in the Magma intrinsic `IsomorphismClassesDieudonneModulesCommEndAlg`, which returns representatives of the isomorphism classes of local-local parts, that is, $\mathcal{W}(W'_R)$. The representatives are global objects: if $\{M_1, \ldots, M_n\}$ is a set of fractional W'_R-ideals representing $\mathcal{W}(W'_R)$, the intrinsic returns a set of fractional $\widetilde{W_R}$-ideals $\{\widetilde{M}_1, \ldots, \widetilde{M}_n\}$ satisfying $\widetilde{M}_{i,\widetilde{\mathfrak{p}}}$, where $\widetilde{\mathfrak{p}}$ is the local-local maximal ideal of R above p.

Tate modules and non-local-local part of Dieudonné modules

Denote by $\mathfrak{X}_\pi^{\{0\}}$ and $\mathfrak{X}_\pi^{\{1\}}$ the local-reduced and reduced-local parts of $\mathfrak{X}_{\pi,p}$. In the main article, we explain that the computation of $\prod_{\ell \neq p} \mathfrak{X}_{\pi,\ell}$ as well as $\mathfrak{X}_\pi^{\{0\}}$ and $\mathfrak{X}_\pi^{\{1\}}$ can be done in terms of fractional R-ideals, see Theorem 3.12 and Proposition 6.1. The outputs of these local computations can be glued into a unique fractional R-ideal using Lemma 3.7. This procedure is summarized in the next algorithm, which is implemented in the Magma intrinsic `IsomorphismClassesAwayFromLocalLocalCommEndAlg`.

Algorithm B.
Input: The order $R = \mathbb{Z}[\pi, q/\pi]$.
Output: A sequence of fractional R-ideals representing the elements of $\prod_{\ell \neq p} \mathfrak{X}_{\pi,\ell} \times \mathfrak{X}_\pi^{\{0\}} \times \mathfrak{X}_\pi^{\{1\}}$.

(1) Compute the set $\{\mathfrak{l}_1, \ldots, \mathfrak{l}_n\}$ of maximal ideals of R, which either divide the conductor $(R : \mathcal{O})$ and do not contain p, or is in $\mathcal{P}_{R_p}$ with slope in $\{0, 1\}$.

(2) For $i = 1, \ldots, n$ do the following:

  (i) Set $k_i = \mathrm{val}_{\ell_i}([\mathcal{O} : R])$ where ℓ_i is the rational prime below $\mathfrak{l}_i$;

(ii) Compute a set of representatives $\mathcal{R}^{\mathfrak{l}_i}$ of $\mathcal{W}(R+\mathfrak{l}_i^{k_i}\mathcal{O})$, using, for example, [2, Algorithm ComputeW];

(3) Initialize an empty list $\mathcal{R}^{\mathtt{out}}$.

(4) For each sequence $(I^{\mathfrak{l}_1},\dots,I^{\mathfrak{l}_n})$ in $\prod_{i=1}^n \mathcal{R}^{\mathfrak{l}_i}$ do

(i) Compute using Lemma 3.7 a fractional R-ideal I such that $I_{\mathfrak{l}_i} = I^{\mathfrak{l}_i}$ for each $i = 1,\dots,n$;

(ii) Add I to $\mathcal{R}^{\mathtt{out}}$;

(5) return $\mathcal{R}^{\mathtt{out}}$;

Theorem V. *Algorithm B is correct.*

Proof. For the maximal ideals not containing p, the result follows from Theorem 3.12. For the local-reduced and reduced-local maximal ideals $\mathfrak{l}_i$, the chosen value of k_i ensures that $\mathfrak{l}_i^{k_i}\mathcal{O}\subseteq R$ by Remark 3.11. The result then follows from Propositions 3.10 and 6.1. □

Isomorphism classes in $\mathcal{A}_\pi$

The remaining algorithms, when combined with Algorithms A and B above and Algorithms 1 and 2 from the main article, allow us to compute the set $\mathcal{A}_\pi^{\mathrm{isom}}$ of isomorphism classes of abelian varieties in the isogeny class $\mathcal{A}_\pi$ together with their endomorphism rings. These algorithms are used to produce the examples in Section 7 of the main article. The following lemma and algorithm compute the endomorphism rings of the abelian varieties in $\mathcal{A}_\pi$, which are uniquely determined by the isomorphism classes of their local parts.

Lemma VI. *Let $\mathfrak{p}_1,\dots,\mathfrak{p}_n$ be maximal ideals of R, let $S_1,\dots,S_n$ be overorders of R, and let $k_1,\dots,k_n$ be positive integers such that for each i we have $\mathfrak{p}_i^{k_i}\mathcal{O}_{E,\mathfrak{p}_i}\subseteq S_{i,\mathfrak{p}_i}$. Define*

$$S = \cap_{i=1}^n (S_i + \mathfrak{p}_i^{k_i}\mathcal{O}_E).$$

Then S is an overorder of R such that $S_{\mathfrak{p}_i} = S_{i,\mathfrak{p}_i}$ for every i and $S_{\mathfrak{q}} = \mathcal{O}_{E,\mathfrak{q}}$ for every other maximal ideal $\mathfrak{q}$ of R.

Proof. The statement follows immediately after localization. □

Algorithm C.
Input: A pair $(\widetilde{I},\widetilde{M}')$ where: $\widetilde{I}$ is a fractional R-ideal representing a class in $\prod_{\ell\neq p}\mathfrak{X}_{\pi,\ell}\times\mathfrak{X}_\pi^{\{0\}}\times\mathfrak{X}_\pi^{\{1\}}$, as from the output of Algorithm B; $\widetilde{M}'$ is a fractional $\widetilde{W}_R$-ideal representing an isomorphism class of $W'_R\{F',V'\}$-ideal, as from the output of Algorithm 2 from the main article.
Output: An overorder S of R which is the endomorphism ring any abelian variety whose Tate modules and Dieudonné modules are determined by the isomorphism class of the pair $(\widetilde{I},\widetilde{M}')$.

(1) Set $T_1 = (\widetilde{I}:\widetilde{I})$;

(2) Set $T_2 = \widetilde{\Delta}^{-1}\left((\widetilde{M}':\widetilde{M}')\right)$;

(3) Let $\mathcal{P}_{\mathrm{sing}}$ be the set of maximal ideals of R which are singular;

(4) For each $\mathfrak{p}\in\mathcal{P}_{\mathrm{sing}}$, set $S^{\mathfrak{p}} = T_2$ if $\mathfrak{p}$ is in $\mathcal{P}_{R_p}^{(0,1)}$, and set $S^{\mathfrak{p}} = T_1$ otherwise.

(5) Use Lemma VI to compute the order S which is locally equal to $S^{\mathfrak{p}}$ for each $\mathfrak{p}\in\mathcal{P}_{\mathrm{sing}}$ and maximal at every order maximal ideal;

(6) Return S.

Theorem VII. *Algorithm C is correct.*

Proof. The result follows from Lemma VI. □

The next and final algorithm combines all the previous ones to compute representatives of $\mathcal{A}_\pi^{\mathrm{isom}}$. It is implemented as the Magma intrinsic `IsomorphismClassesCommEndAlg`.

Algorithm D.
Input: An isogeny class $\mathcal{A}_\pi$ of abelian varieties with commutative endomorphism ring.
Output: A set of representatives of the isomorphism classes of in the category $\mathcal{C}_\pi$ (see Definition 5.1).

(1) Compute the order $R = \mathbb{Z}[\pi, q/\pi]$;

(2) Initialize an empty list $\mathcal{R}^{\texttt{out}}$;

(3) Run Algorithm B and let $\mathcal{R}^{\texttt{not-loc-loc}}$ be the output;

(4) Run Algorithm 2 and let $\mathcal{R}^{(0,1)}$;

(5) For each pair $(\widetilde{I}, \widetilde{M}')$ in $\mathcal{R}^{\texttt{not-loc-loc}} \times \mathcal{R}^{(0,1)}$, do the following:

  (1) Use Algorithm C to compute the endomorphism ring S of $(\widetilde{I}, \widetilde{M}')$;

  (2) Compute a set of representatives $J_1, \dots, J_s$ of the class group $\mathrm{Cl}(S)$ of S;

  (3) For $j = 1, \dots, s$, append $(\widetilde{I}, \widetilde{M}', J_j)$ to $\mathcal{R}^{\texttt{out}}$.

(6) Return $\mathcal{R}^{\texttt{out}}$.

Remark VIII. The output of Algorithm D is a list of vectors of data representing the local parts of the computation and the action of the class group. We now explain how to glue these data into a pair (I, M) belonging to the category $\mathcal{C}_\pi$ which is equivalent to $\mathcal{A}_\pi$ by Theorem 5.2 of the main article. Recall, this is the same as saying that I is a fractional R-ideal, M is a fractional W_R-ideal, and we have the compatibility condition $i_p(I)R_p = \Delta^{-1}(M)$, where $i_p\colon E \to E_p$ is the natural embedding.

Let $Y = (\widetilde{I}, \widetilde{M}', J_j)$ be an element of the output of Algorithm D. Let $\mathcal{P}$ be the set of maximal ideals of R that are either above p, or coprime to p and singular. For each $\mathfrak{p}$ in $\mathcal{P}$, set $I^{\mathfrak{p}} = \widetilde{\Delta}^{-1}(\widetilde{M}')$ if $\mathfrak{p}$ is the unique local-local maximal ideal of R, and set $I^{\mathfrak{p}} = \widetilde{I}$ otherwise. Use Lemma 3.7 to construct a fractional R-ideal I_Y whose localization at $\mathfrak{p}$ is $I^{\mathfrak{p}}$ for each $\mathfrak{p} \in \mathcal{P}$. Similarly, construct a fractional W_R-ideal M_Y whose localization at $\mathfrak{p}$ is $\widetilde{\Delta}(I^{\mathfrak{p}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for $\mathfrak{p} \in \mathcal{P}_{R_p}^{\{0\}} \sqcup \mathcal{P}_{R_p}^{\{1\}}$ and $\widetilde{M}' \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for $\mathfrak{p} \in \mathcal{P}_{R_p}^{(0,1)}$. The association

$$(\widetilde{I}, \widetilde{M}', J_j) \longmapsto (I_Y J_j, M_Y \Delta(J_j \otimes_{\mathbb{Z}} \mathbb{Z}_p))$$

induces a bijection between the output of Algorithm D and the isomorphism classes of $\mathcal{C}_\pi$.

An analogous procedure is implemented in the intrinsic `GeneralizedDeligneModule`, with the difference that the second output is a global fractional $\widetilde{W}_R$-ideal instead of a local fractional W_R-ideal.

Theorem IX. *Algorithm D is correct.*

Proof. The result follows from Theorem 4.9 as well as Theorem 3.12, combined with the fact that a fractional ideal in E is determined by its localizations together with an element of the Picard group. ☐

Remark X. We could theoretically, in several of the algorithms presented above, use the duality of Subsection 4.3.2 to only make computations for places ν of E_p with slope in $[0, 1/2]$. This is not something that we have extensively implemented in practice, since we do not believe it would significantly improve the efficiency of our algorithms.

Notation

- $\mathbb{F}_q$, a finite field with $q = p^a$ elements of characteristic p.
- $\mathcal{A}_\pi$, an isogeny class of abelian varieties over $\mathbb{F}_q$ with commutative endomorphism algebra $E = \mathbb{Q}[\pi]$, where π is the Frobenius endomorphism.
- $\mathcal{A}_\pi^{\mathrm{isom}}$, the set of $\mathbb{F}_q$-isomorphism classes in $\mathcal{A}_\pi$.

- $\mathfrak{X}_\pi = \mathfrak{X}_{\pi,p} \times \prod_{\ell \neq p} \mathfrak{X}_{\pi,\ell}$, where $\mathfrak{X}_{\pi,p}$ (resp. $\mathfrak{X}_{\pi,\ell}$) is the set of isomorphism classes of Dieudonné modules (resp. ℓ-Tate modules) in $\mathcal{A}_\pi$.
- for an order S and a set $\mathcal{T}$ of maximal ideals of S: $\mathcal{W}(S)_{\mathcal{T}}$, the set of fractional S-ideals modulo the relation $I_\mathfrak{m} \simeq_\mathfrak{m} J_\mathfrak{m}$ for all $\mathfrak{m} \in \mathcal{T}$; see Definition 3.1 (also for variants).
- $h(x)$, the square-free characteristic polynomial of π.
- $\mathcal{O}_E$, the maximal order of E.
- $E_p = E \otimes_Q \mathbb{Q}_p = \prod_{\nu|p} E_\nu$.
- $R = \mathbb{Z}[\pi, q/\pi]$; $R_p = R \otimes_\mathbb{Z} \mathbb{Z}_p$.
- $L = \mathbb{Q}_p(\zeta_{q-1})$, the unramified extension of $\mathbb{Q}_p$ of degree a.
- $W = \mathcal{O}_L = \mathbb{Z}_p[\zeta_{q-1}]$.
- σ, the Frobenius automorphism of $L/\mathbb{Q}_p$.
- for a place ν of E_p: e_ν, the ramification index; f_ν, the inertia degree; $g_\nu = \gcd(a, f_\nu)$; $s(\nu) = \mathrm{val}_\nu(\pi)/ae_\nu$, the slope.
- τ_ν, the Frobenius automorphism of LE_ν/E_ν.
- $\mathfrak{p}_{E_\nu}$ (respectively $\mathfrak{p}_{LE_\nu}$), the maximal ideal of $\mathcal{O}_{E_\nu}$ (respectively $\mathcal{O}_{LE_\nu}$).
- $A = \prod_{\nu|p} A_\nu$, where $A_\nu = \prod_{j=1}^{g_\nu} LE_\nu$.
- $\Delta : E_p \hookrightarrow A$, induced by the diagonal embeddings $E_\nu \hookrightarrow A_\nu$.
- $F_\nu \colon A_\nu \to A_\nu$, an additive map satisfying the Frobenius property, that is, $F_\nu^a = \Delta_{|E_\nu}(\pi_\nu)$ and $F_\nu \lambda = \lambda^\sigma F_\nu$, for every $\lambda \in L$.
- $F = (F_\nu)_{\nu|p}$ acting of $A = \prod_{\nu|p} A_\nu$.
- F_ν with the Frobenius property is of W-type if $F_\nu(z) = \alpha_\nu \cdot z^\sigma$, where $\alpha_\nu = (1, \ldots, 1, u_\nu) \in A_\nu$ with $N_{LE_\nu}(u_\nu) = \pi_\nu$; see Definition 4.4.
- $V = pF^{-1}$.
- $W_R = W \otimes_{\mathbb{Z}_p} R$.
- for $* = \{0\}, (0,1)$ or $\{1\}$: $\mathcal{P}^*_{R_p}$, the set of maximal ideal of R_p below a place ν with $s(\nu) \in *$.
- $R_p = R_p^{\{0\}} \sqcup R_p^{(0,1)} \sqcup R_p^{\{0\}}$, where $R_p^* = R_p \cap \prod_{\nu : s(\nu) \in *} E_\nu$.
- for $* = \{0\}, (0,1)$ or $\{1\}$: E^*, A^*, W_R^*, F^*, V^*, etc. denote the $*$-part of the corresponding object.
- for the local-local part (i.e the $(0,1)$-part), we use also $'$: E', A', W_R', F', V', etc.
- Υ, the set of Δ'-isomorphism classes of fractional $W_R'\{F', V'\}$-ideals with multiplicator ring $\mathcal{O}_{A'}$; see Definition 4.20.
- $\mathcal{C}_\pi$, a category of pairs (I, M) where I is a fractional R-ideal in E, and M is a $W_R\{F,V\}$-ideal such that $\Delta^{-1}(M) = i_p(I)R_p$; morphisms are $\mathrm{Hom}_{\mathcal{C}_\pi}((I,M),(J,N)) = \{\alpha \in E | \alpha I \subseteq J, \Delta(i_p(\alpha))M \subseteq N\}$; see Definition 5.1.
- $\widetilde{A}$ (resp. $\widetilde{A'}$, $\widetilde{W}_R$, etc.), the 'global version' of A (resp. A', W_R, etc.); see Subsection 6.1.

References

[1] Stefano Marseglia, `https://github.com/stmar89/IsomClAbVarFqCommEndAlg`, The examples in this paper were computed using the code at commit c25be473adfeb1dba9932d47961e54649889fa78.

[2] ———, *Local isomorphism classes of fractional ideals of orders in étale algebras*, J. Algebra **673** (2025), pp. 77–102.

Matematiska institutionen, Stockholms Universitet, SE-106 91 Stockholm, Sweden
Email address: jonasb@math.su.se

Mathematisch Instituut, Universiteit Utrecht, Postbus 80010, 3508 TA Utrecht, The Netherlands
Email address: v.z.karemaker@uu.nl

Mathematisch Instituut, Universiteit Utrecht, Postbus 80010, 3508 TA Utrecht, The Netherlands
Laboratoire GAATI, Université de la Polynésie française, BP 6570 – 98702 Faaa, Polynésie française
Laboratoire Jean Alexandre Dieudonné, Université Côte Azur, 06108 Nice Cedex 2, France
Email address: stefano.marseglia@univ-cotedazur.fr