The Generalised Tate Pairing over any field

Jonathan Komada Eriksen

Abstract. We generalise a pairing on elliptic curves over finite fields, called the generalised Tate pairing, which is defined in terms of an arbitrary endomorphism of the curve, with certain trace requirements. We rederive this pairing from group cohomology, which allows us to generalise the pairing to principally polarized abelian varieties over any field, endomorphisms of any trace, and prove perfectness using a general duality theorem.

1. Introduction

For an abelian variety A defined over a field k, there exists several pairings on various groups related to the group of points on A. Two important examples of this are m-Weil pairing, which for $m \in \mathbb{N}$ defines a perfect pairing

$$e_m : A[m] \times \widehat{A}[m] \to \mu_m,$$

and the Lichtenbaum-Tate pairing (also just commonly referred to as the Tate-pairing), which is a pairing

$$T_m : A(k)/[m]A(k) \times \widehat{A}(k)[m] \to k^\times/(k^\times)^m.$$

When $k = \mathbb{F}_q$ is a finite field, the Tate-pairing is well known to be a perfect pairing whenever $m \mid q - 1$. Further, still assuming finite fields, Bruin [1] shows that the Lichtenbaum-Tate pairing (composed with the identification $(-)^{\frac{q-1}{m}} : k^\times/(k^\times)^m \xrightarrow{\sim} \mu_m$) can be defined in terms of the Weil pairing and the q-power Frobenius endomorphism as

$$T_m([P], Q) = e_m(\pi_q(R) - R, Q)$$

for some point $R \in A$ satisfying $[m]R = P$. Building on this, Castryck, Houben, Merz, Mula, van Buuren and Vercauteren [2] recently defined another pairing as follows: given an elliptic curve E over $\mathbb{F}_q$, and an endomorphism $\sigma \in \mathrm{End}(E)$ satisfying $\mathrm{trd}(\sigma) \equiv 0 \pmod{m, \mathrm{nrd}(\sigma)}$, they define the generalised m-Tate pairing as

$$\begin{aligned} T_m^\sigma : \ker\sigma/[m]\ker\sigma \times (\ker\sigma)[m] &\to \mu_m \\ T_m^\sigma(P, Q) &= e_m(\sigma(R), Q) \end{aligned}$$

Mathematics Subject Classification 2020: 11G10.
Keywords: Abelian Varieties.

where R is again defined as any point satisfying $[m]R = P$.

This pairing has recently led to works on other pairings in cryptography, especially those useful in the construction and cryptanalysis of isogeny-based cryptography. The generalised Tate pairing was originally introduced to show that certain variants of the vectorisation problem admit a polynomial-time algorithm [2, Section 6.1]. A different generalisation of the Tate pairing was constructed by Stange [12], and subsequently applied to vectorisation by Macula and Stange [5]. On the constructive side, Robert has shown that the Weil and Tate pairings on abelian varieties in general come from a richer geometric structure [9,10], which has been shown to have many applications, including both faster algorithms for computing them [8], and completely novel side-channel attacks on classical elliptic curve cryptography [10, Section 6.4].

Contributions. In this paper, we revisit the generalised Tate pairing. Although Bruin's formula for the Tate pairing clearly only makes sense over finite fields, this restriction does not seem necessary for the generalised Tate pairing. To prove results for the general case, we rederive the generalised Tate pairing from the group cohomology of $\widehat{\mathbb{Z}}$, analogous to how the Tate pairing can be derived from the Galois cohomology of $\mathbb{F}_q$. We show that this construction agrees with the one in [2].

2. Preliminaries

Throughout the paper, we make the convention $0 \notin \mathbb{N}$. For an abelian group M, we denote the multiplication-by-m map as $[m] : M \to M$. Given any endomorphism $\psi : M \to M$, we denote the image of ψ by ψM, and the kernel of ψ by $M[\psi]$ (except the kernel of $[m]$, which we simply denote as $M[m]$). For a general introduction to abelian varieties, we refer to the notes by Milne [6].

Profinite group cohomology. We will first recall the basic definitions of profinite group cohomology. Standard references include [7] and [11], however we also recommend [4] for a friendly introduction. Note that all three references introduce group cohomology with Galois cohomology as the motivation; this will not be the case for us.

A topological group G is a group equipped with a topology, so that the group operations are continuous. A profinite group G is a topological group that is isomorphic to an inverse limit $\varprojlim_{i \in I} G_i$ (in the category of topological groups) of finite groups G_i with the discrete topology. A discrete G-module M is a G-module that can be written as the union

$$M = \bigcup_{U \subset G} M^U$$

where U runs over the open subgroups of G, and

$$M^U = \{m \in M \mid \sigma \cdot m = m, \forall \sigma \in U\}$$

denotes the fixed points of U (this is equivalent to saying that the map $\sigma \to \sigma \cdot m$ is continuous when M is given the discrete topology). We also say that M is torsion if every element of M has finite order.

Given a (pro)finite group G and a (discrete) G-module M, the inhomogeneous n-cochains for G, with values in M, which we denote by $\mathscr{C}^n(G, M)$, are defined as the group of (continuous) maps $f : G^n \to M$ for $n \geq 0$, and $\mathscr{C}^0(G, M) = M$ for $n = 0$. For any n, one can define certain boundary maps $d^n : \mathscr{C}^n(G, M) \to \mathscr{C}^{n+1}(G, M)$, and subsequently the group of inhomogeneous n-cocycles are defined as $\mathscr{Z}^n(G, M) := \ker d^n$, and the group of inhomogeneous n-coboundaries as $\mathscr{B}^n(G, M) := \operatorname{im} d^{n-1}$. This defines the nth-cohomology group as

$$H^n(G, M) := \mathscr{Z}^n(G, M)/\mathscr{B}^n(G, M).$$

Explicitly, the first boundary maps are given as $d^0(m)(\sigma) = \sigma \cdot m - m$, and $d^1(f)(\sigma, \tau) = f(\sigma) + \sigma \cdot f(\tau) - f(\sigma\tau)$. We will not need the higher degrees.

Cohomology of $\widehat{\mathbb{Z}}$. We now specialise to the case relevant for this paper. The profinite integers are defined as the inverse limit

$$\widehat{\mathbb{Z}} := \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z},$$

It is topologically generated by a canonical element $\gamma \in \widehat{\mathbb{Z}}$, i.e. $\overline{\langle \gamma \rangle} = \widehat{\mathbb{Z}}$. In this paper, we work with $\widehat{\mathbb{Z}}$-modules and related cohomology groups. It can be shown that the action of $\widehat{\mathbb{Z}}$ on a discrete $\widehat{\mathbb{Z}}$-module is uniquely defined by defining the action of γ.

The $\widehat{\mathbb{Z}}$-modules we consider admit a simple description by the following proposition.

Proposition 2.1. *Let γ be a topological generator of $\widehat{\mathbb{Z}}$, and let M be a discrete, torsion $\widehat{\mathbb{Z}}$-module, whose action is given by $\gamma \cdot m = \alpha(m)$ for some automorphism $\alpha : M \to M$. Then*

$$H^k(\widehat{\mathbb{Z}}, M) \simeq \begin{cases} M[\alpha - 1] & \text{for } k = 0, \\ M/(\alpha - 1)M & \text{for } k = 1, \\ 0 & \text{for } k \geq 2. \end{cases}$$

and the isomorphism for $k = 1$ is given by ev_γ, i.e. evaluating in γ.

Proof. See [7, Proposition 1.7.7]. ∎

The cup-product is, for any n, m, defined on the level of cochains as a map $\mathscr{C}^n(G, N) \times \mathscr{C}^m(G, M) \to \mathscr{C}^{n+m}(G, N \otimes M)$, which induces a bilinear map $H^n(G, N) \times H^m(G, M) \to H^{n+m}(G, N \otimes M)$. Explicitly for $n = 1, m = 0$ (which, again, is the only case we will need), the formula is given as

$$\begin{aligned} \smile : \mathscr{C}^1(G, N) \times \mathscr{C}^0(G, M) &\to \mathscr{C}^1(G, N \otimes M) \\ (f, m) &\to ((f \smile m)(\sigma) = f(\sigma) \otimes m) \end{aligned}$$

Given an abelian group M, we define $M^\vee := \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$. If M is a finite G-module, then $M^\vee$ also carries a natural structure of a G-module via the action $(\tau \cdot \phi)(m) = \phi(\tau^{-1} \cdot m)$. By giving $\mathbb{Q}/\mathbb{Z}$ a trivial $\widehat{\mathbb{Z}}$-module structure, we can post-compose the cup-product with the evaluation map, i.e. the homomorphism (of $\widehat{\mathbb{Z}}$-modules)

$$\begin{aligned} \mathrm{ev} : M \otimes M^\vee &\to \mathbb{Q}/\mathbb{Z} \\ \mathrm{ev}(m \otimes \phi) &= \phi(m) \end{aligned}$$

induces a homomorphism (of abelian groups)

$$\mathrm{ev}_* : H^n(\widehat{\mathbb{Z}}, M \otimes M^\vee) \to H^n(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}),$$

and it is common to also refer to this composition as the cup product. Note also that by Proposition 2.1, $H^1(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Q}/\mathbb{Z}$. Our main Theorem (Theorem 4.4) will follow from the following duality theorem.

Theorem 2.2. *Given any finite $\widehat{\mathbb{Z}}$-module M, the cup product*

$$H^1(\widehat{\mathbb{Z}}, M) \times H^0(\widehat{\mathbb{Z}}, M^\vee) \to \mathbb{Q}/\mathbb{Z}$$

defines a perfect pairing.

Proof. See [7, Theorem 3.4.6], in particular [7, Chp. 3, §4, Excercise 3]. ∎

Of course, since the modules M are finite, the image really lies in $\frac{1}{m}\mathbb{Z}/\mathbb{Z}$, where m is the exponent of M. For the rest of this paper, $\mathbb{Q}/\mathbb{Z}$ will be considered a trivial $\widehat{\mathbb{Z}}$-module (like in Theorem 2.2), while μ_m will refer to the $\widehat{\mathbb{Z}}$-module $\mu_m(\overline{k})$, with a possibly non-trivial action. Note that whenever $\mathrm{char}(k)$ is coprime with m, we have an isomorphism $\mu_m(\overline{k}) \simeq \frac{1}{m}\mathbb{Z}/\mathbb{Z}$ of abelian groups. However, by the convention just established, this is only an isomorphism of $\widehat{\mathbb{Z}}$-modules if the action on μ_m is trivial.

3. The Generalised Tate Pairing from Group Cohomology

We now detail the construction of the generalised Tate pairing using the group cohomology of $\widehat{\mathbb{Z}}$. Throughout, we fix k to be a field, and let A/k be an abelian variety with a principal polarization $\mathcal{L}$. In the case that $\mathrm{char}(k) > 0$, we will throughout assume that the positive integer $m \in \mathbb{Z}_{>0}$ is coprime to $\mathrm{char}(k)$.

For any endomorphism α of $(A, \mathcal{L})$, i.e. an endomorphism $\alpha \in \mathrm{End}(A)$ such that there exists an integer d satisfying $[d] = \alpha^\dagger \circ \alpha$, where $\dagger$ refers to the rosati involution defined by $\mathcal{L}$, recall that $\deg(\alpha) = d^g$, where $g = \dim A$. We now start by forming the abelian group

$$A[\alpha^\infty - 1] := \bigcup_{n \in \mathbb{N}} A[\alpha^n - 1]$$

We can give $A[\alpha^\infty - 1]$ the structure of a $\widehat{\mathbb{Z}}$-module as follows: any $P \in A[\alpha^\infty - 1]$ is contained in $A[\alpha^n - 1]$ for some[1] finite n. Given $m = (m_1, m_2, \dots) \in \widehat{\mathbb{Z}}$, we may thus define $m \cdot P = \alpha^{m_n}(P)$. Notice that this is independent of choice of n by definition of $\widehat{\mathbb{Z}}$.

We will now prove some of the basic properties of this $\widehat{\mathbb{Z}}$-module. To prepare this, we start with a standard lemma.

Lemma 3.1. *Let A/k be a principally polarized abelian variety, and let $\alpha \in \mathrm{End}(A)$ satisfy $\alpha^\dagger\alpha = [d]$, where $d > 1$. Then $\alpha^n - 1$ is an isogeny for all $n \in \mathbb{N}$.*

Proof. Take any prime $\ell \neq \mathrm{char}(k)$ with $\gcd(\ell, \deg(\alpha)) = 1$, and consider the action of α on the rational ℓ-adic Tate-module, $V_\ell(A) = T_\ell(A) \otimes \mathbb{Q}$. Since an endomorphism is an isogeny if and only if it acts invertibly on $V_\ell(A)$, the result follows if we can show that

$$\det(\alpha^n - 1) = \prod_{i=1}^{2g} (\lambda_i^n - 1)$$

is non-zero, where λ_i denotes the eigenvalues of α. However, this follows immidiately from the fact that $\alpha^\dagger\alpha = [d]$ implies that all eigenvalues satisfy $|\lambda_i| = \sqrt{d} > 1$. ∎

Lemma 3.2. *Let γ be a topological generator of $\widehat{\mathbb{Z}}$. The action defined above is the unique continuous action extending the action $\gamma \cdot P = \alpha(P)$, and makes $A[\alpha^\infty - 1]$ into a discrete $\widehat{\mathbb{Z}}$-module. Furthermore, assuming $\deg(\alpha) > 1$, or k is a finite field, $A[\alpha^\infty - 1]$ is additionally torsion.*

In either case, for any $m \in \mathbb{Z}$ satisfying $\gcd(m, \deg(\alpha)) = 1$, we have $A[m] \subseteq A[\alpha^\infty - 1]$, and $[m]A[\alpha^\infty - 1] = A[\alpha^\infty - 1]$.

Proof. It is clear that the action defined extends the action $\gamma \cdot P = \alpha(P)$, and by definition, $A[\alpha^\infty - 1] = \bigcup_{n\in\mathbb{N}} A[\alpha^n - 1] = \bigcup_{n\in\mathbb{N}} A[\alpha^\infty - 1]^{n\widehat{\mathbb{Z}}}$, thus $A[\alpha^\infty - 1]$ is discrete.

Next, assuming $\deg(\alpha) > 1$, Lemma 3.1 tells us that $A[\alpha^n - 1]$ is finite for all n, and thus $A[\alpha^\infty - 1]$ is torsion. In the case that $\deg(\alpha) = 1$, it is an automorphism of $(A, \mathcal{L})$ (with inverse given by $\alpha^\dagger$), and thus it is of finite order [6, Proposition 14.4]. When α has finite order, we have $A[\alpha^\infty - 1] = A(\overline{k})$, which is still torsion if k is a finite field.

The second statement follows from the fact that when $\gcd(\deg(\alpha), m) = 1$, α acts as an automorphism on $A[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2g}$, where $g = \dim A$ (this also shows surjectivity of $[m]$, since for any P satisfying $\alpha^n(P) = P$, this implies that α^n acts invertibly on $[m]^{-1}(P)$). ∎

Next, given any $m \in \mathbb{Z}$ coprime to $\deg(\alpha)$, the last part of the lemma above shows that the Kummer sequence for $A[\alpha^\infty - 1]$ looks like

$$0 \longrightarrow A[m] \longrightarrow A[\alpha^\infty - 1] \xrightarrow{[m]} A[\alpha^\infty - 1] \longrightarrow 0$$

[1] Of course, there are infinitely many choices of n.

Applying group cohomology then gives the long exact sequence

$$0 \longrightarrow H^0(\widehat{\mathbb{Z}}, A[m]) \longrightarrow H^0(\widehat{\mathbb{Z}}, A[\alpha^\infty - 1]) \longrightarrow H^0(\widehat{\mathbb{Z}}, A[\alpha^\infty - 1])$$
$$\xrightarrow{\ \delta\ } H^1(\widehat{\mathbb{Z}}, A[m]) \longrightarrow H^1(\widehat{\mathbb{Z}}, A[\alpha^\infty - 1]) \longrightarrow \cdots$$

where the connecting homomorphism δ can be explicitly defined by sending $P \in A[\alpha - 1] = H^0(\widehat{\mathbb{Z}}, A[\alpha^\infty - 1])$ to the cocycle class $[\eta \to \eta \cdot R - R]$ for some $R \in A[\alpha^\infty - 1]$ satisfying $[m]R = P$.

It is classical that $H^1(\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q), A)$ vanishes. Below, we prove the generalisation we need, showing that it follows easily from Proposition 2.1.

Lemma 3.3. *Assume* $\deg(\alpha) > 1$. *Then* $H^1(\widehat{\mathbb{Z}}, A[\alpha^\infty - 1]) = 0$

Proof. By combining Proposition 2.1 and Lemma 3.2, we have

$$H^1(\widehat{\mathbb{Z}}, A[\alpha^\infty - 1]) = A[\alpha^\infty - 1]/(\alpha - 1)A[\alpha^\infty - 1].$$

Let $P \in A[\alpha^\infty - 1]$, and let $Q \in A$ such that $\alpha(Q) - Q = P$ (which exists since isogenies are surjective). We need to show that $Q \in A[\alpha^\infty - 1]$ too.

Since $P \in A[\alpha^\infty - 1]$, there exists some n such that $(\alpha^n - 1)(\alpha - 1)(Q) = (\alpha^n - 1)(P) = 0$. Set $R = (\alpha^n - 1)(Q)$. Since $\alpha - 1$ and $\alpha^n - 1$ commute, we have $\alpha(R) = R$. Further, since R is in the kernel of $\alpha - 1$, R has finite order, so say $[d]R = 0$. Then

$$\begin{aligned}(\alpha^{nd} - 1)(Q) &= (\alpha^{n(d-1)} + \alpha^{n(d-2)} + \cdots + 1)(\alpha^n - 1)(Q) \\ &= (\alpha^{n(d-1)} + \alpha^{n(d-2)} + \cdots + 1)(R) = [d]R = 0\end{aligned}$$

and we are done. ∎

We can thus conclude that the connecting homomorphism induces an isomorphism

$$\delta : A[\alpha - 1]/[m]A[\alpha - 1] \xrightarrow{\sim} H^1(\widehat{\mathbb{Z}}, A[m])$$

whenever α has infinite order, or even any α such that $\alpha - 1$ is an isogeny (e.g. not $\alpha = [1]$) over finite fields (this follows directly from the fact that isogenies are surjective). Also simply using the definition to identify $H^0(\widehat{\mathbb{Z}}, A[m]) = A[m, \alpha - 1]$, the cup-product induces a bilinear map

$$\begin{aligned}A[\alpha - 1]/[m]A[\alpha - 1] \times A[m, \alpha - 1] &\to H^1(\widehat{\mathbb{Z}}, A[m] \otimes A[m]) \\ (P, Q) &\to \delta(P) \smile Q\end{aligned}$$

Next, consider the polarized m-Weil pairing

$$\begin{aligned} e_{m,\mathcal{L}} : A[m] \times A[m] &\to \mu_m \\ e_{m,\mathcal{L}}(P,Q) &= e_m(P, \mathcal{L}(Q)) \end{aligned}$$

which is still a perfect pairing since $\mathcal{L}$ is an isomorphism. We would now want to apply the polarized Weil pairing to land in the nicer group $H^1(\widehat{\mathbb{Z}}, \mu_m)$. However, for this map to define a map in cohomology, this requires the Weil pairing to be $\widehat{\mathbb{Z}}$-equivariant, i.e. $A[m] \otimes A[m] \to \mu_m$ must be a map of $\widehat{\mathbb{Z}}$-modules.

Luckily, we are free to give μ_m the structure of a $\widehat{\mathbb{Z}}$-module, to make this pairing equivariant. The action of $\widehat{\mathbb{Z}}$ on $A[m] \otimes A[m]$ is given by

$$\gamma \cdot (P \otimes Q) = \alpha(P) \otimes \alpha(Q),$$

and from basic properties of the Weil pairing, we have that

$$\begin{aligned} e_{m,\mathcal{L}}(\alpha(P), \alpha(Q)) &= e_m(\alpha(P), \mathcal{L} \circ \alpha(Q)) \\ &= e_m(P, \widehat{\alpha} \circ \mathcal{L} \circ \alpha(Q) \\ &= e_{m,\mathcal{L}}(P, [d]Q) = e_{m,\mathcal{L}}(P,Q)^d \end{aligned}$$

for $\alpha^\dagger \circ \alpha = [d]$, and thus we can define the action by $\gamma \cdot \zeta = \zeta^d$ for all $\zeta \in \mu_m$ (this is really an action, since we already assumed $\gcd(m,d) = 1$). Finally, let $\lambda := d - 1$. By a direct application of Proposition 2.1, we get the isomorphism $H^1(\widehat{\mathbb{Z}}, \mu_m) \simeq \mu_m / \mu_m^\lambda$ by ev_γ.

We summarize:

Definition 3.4. Let k be a field, and let $(A, \mathcal{L})$ be a principally polarized abelian variety defined over k. Given an endomorphism α of $(A, \mathcal{L})$ with $\alpha^\dagger \circ \alpha = [d]$, $d > 1$ (or any α such that $\alpha - 1$ is an isogeny, when k is a finite field), and $m \in \mathbb{Z}$ satisfying $\gcd(d, m) = 1$, the generalised m-Tate pairing is given by

$$\begin{aligned} T^\alpha_{m,\mathcal{L}} : A[\alpha - 1]/[m]A[\alpha - 1] \times A[m, \alpha - 1] &\to \mu_m / \mu_m^\lambda \\ T^\alpha_{m,\mathcal{L}}(P,Q) &= [e_{m,\mathcal{L}}(\delta_P(\gamma), Q)] \end{aligned}$$

where $\lambda := d - 1$, and $\delta_P(\eta) = \eta \cdot R - R$ for some $R \in A[\alpha^\infty - 1]$ with $[m]R = P$.

Example 3.5. When $k = \mathbb{F}_q$, and α is the Frobenius, the above is really (a polarized version of) Bruin's formula for the Lichtenbaum-Tate pairing.

Example 3.6. Another familiar example comes when one considers $\alpha = [m + 1]$. Since

$$A[m]/[m]A[m] = A[m]$$

and $\delta_P([m+1]) = [m+1]R - R = [m]R + R - R = P$, we see that this case simply reduces to the usual polarized m-Weil pairing.

Remark 3.7. There is a well-defined pairing that is independent of polarization, first discussed by Galbraith, Gilchrist and Robert [3], which coincides with the pairing defined above in certain cases. Set $\beta = \alpha - 1$, and recall that there is a pairing [3, Appendix A]

$$T_m^\beta : A[\beta]/[m]A[\beta] \times \widehat{A}[m, \widehat{\beta}] \to \mu_m,$$

again defined as $T_m^\beta(P, Q) = e_m(\delta_P(\gamma), Q)$ (note that we have swapped the arguments compared to [3]). In fact, in the $\gcd(\deg(\alpha), m) = 1$ case, this pairing is always perfect (this follows from [3, Remark A.1]). Composing with a principal polarization then gives

$$H_{\mathcal{L},m}^\alpha : A[\alpha - 1]/[m]A[\alpha - 1] \times A[m, \alpha^\dagger - 1] \to \mu_m,$$

and $A[m, \alpha^\dagger - 1]$ coincides with $A[m, \alpha - 1]$ when $d \equiv 1 \pmod m$, for $\alpha^\dagger \circ \alpha = [d]$ (e.g. [3, Example A.1]).

4. Perfectness of the generalised Tate pairing.

We now compare with the original definition of the generalised Tate pairing Castryck, Houben, Merz, Mula, van Buuren and Vercauteren [2]. We will show that Definition 3.4 specialises to their definition for $\sigma = \alpha - 1$. After that, we derive the conditions for when the pairing is perfect.

We start with the following Lemma, which will justify the choice of m in the following.

Lemma 4.1. *Let m' be an integer, such that $\gcd(\deg(\alpha - 1), m) \mid m' \mid m$. Then*

$$j_{m',m} \circ T_{m',\mathcal{L}}^\alpha = T_{m,\mathcal{L}}^\alpha$$

where $j_{m',m} : \mu_{m'}/\mu_{m'}^\lambda \to \mu_m/\mu_m^\lambda$ denotes the map induced by the inclusion $\mu_{m'} \hookrightarrow \mu_m$.

Proof. We can start by verifying that the domains are equal: We have equality $A[m, \alpha - 1] = A[m', \alpha - 1]$, as well as $[m]A[\alpha - 1] = [m']A[\alpha - 1]$, thus it is also clear that the image of $T_{m,\mathcal{L}}^\alpha$ lies in the image of $\mu_{m'}$ in μ_m/μ_m^λ, i.e. $\mu_{m'}/(\mu_{m'} \cap \mu_m^\lambda)$. By inspecting Definition 3.4, we see that the only thing we need to prove is that

$$e_{m,\mathcal{L}}(\delta_P(\gamma), Q) = e_{m',\mathcal{L}}(\delta'_P(\gamma), Q),$$

where we can set $\delta_P(\gamma) = \alpha(R) - R$, and $\delta'_P(\gamma) = \alpha([m/m']R) - [m/m']R$ for $R \in A[\alpha^\infty - 1]$ satisfying $[m]R = P$. But this equality follows from a standard compatibility on the Weil-pairing, which states that

$$e_{\psi\circ\phi,\mathcal{L}}(P, Q) = e_{\psi,\mathcal{L}}(\phi(P), Q)$$

(apply this with $\psi = [m']$ and $\phi = [m/m']$), see [2, Lemma 3.1]. ∎

Remark 4.2. Note that the map $j_{m',m}$ above need not be injective (its kernel is given by $(\mu_{m'} \cap \mu_m^\lambda)/\mu_{m'}^\lambda$), and thus a pairing that is not degenerate for m' might end up being degenerate for m.

Let $\overline{T}_m^\sigma$ denote the generalised Tate pairing as defined in [2] (i.e., not as in Definition 3.4). For an elliptic curve E, let $\mathcal{L}_0 : E \simeq \widehat{E}$ denote the canonical polarization. Note that, since we are in dimension 1, we have $\alpha^\dagger \circ \alpha = [\deg(\alpha)]$.

Proposition 4.3. *Let E be an elliptic curve, defined over a finite field $\mathbb{F}_q$. Let $\alpha \in \mathrm{End}(E)$, and let $m \in \mathbb{Z}$ such that $\deg(\alpha) \equiv 1 \pmod{\gcd(\deg(\alpha-1), m)}$. Then $T^\alpha_{m',\mathcal{L}_0}$ equals $\overline{T}_m^\sigma$ for $\sigma = \alpha - 1$, and $m' = \gcd(\deg(\alpha-1), m)$ (with the arguments swapped).*

Proof. The domain and explicit formula of $T^\alpha_{m',\mathcal{L}_0}$ agrees with that of $\overline{T}_m^\sigma$ by the proof of Lemma 4.1, so we only need to check the codomain. The codomain agrees when $\lambda \equiv 0 \pmod{m'}$ (after after identifying the image $\mu_{m'} \hookrightarrow \mu_m$). But this is the same as requiring that $\mathrm{tr}(\sigma) \equiv 0 \pmod{m'}$, as

$$\begin{aligned} \lambda = \deg(\alpha) - 1 &\equiv (\deg(\sigma) + 1 + \mathrm{tr}(\sigma)) - 1 \pmod{m'} \\ &\equiv \mathrm{tr}(\sigma) \pmod{m'} \end{aligned}$$

since we are assuming $m' = \gcd(\deg(\sigma), m)$. ∎

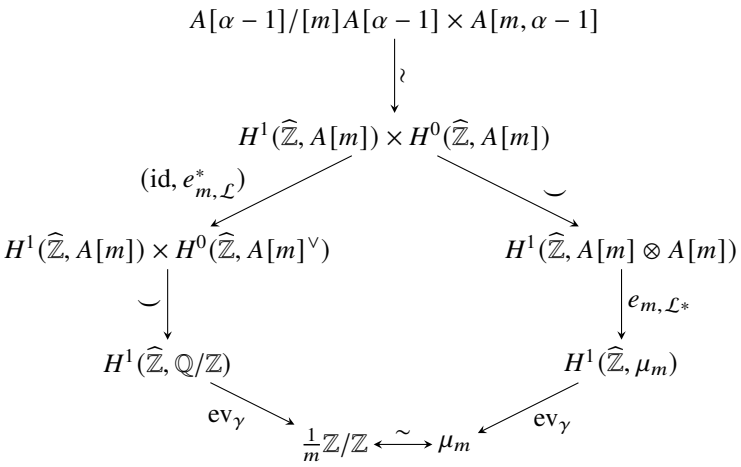
While [2] only define the generalised Tate pairing for $\mathrm{tr}(\sigma) \equiv 0 \pmod{\gcd(\deg(\sigma), m)}$, or equivalently, $\deg(\alpha) \equiv 1 \pmod{\gcd(\deg(\alpha-1), m)}$, we get a well-defined pairing regardless. However, as we now show, this condition is indeed precisely what is needed to prove that their the pairing is perfect. Note that by Remark 4.2 and Proposition 4.3, we can and need only prove perfectness for $\deg(\alpha) \equiv 1 \pmod{m}$ to get the analoguous for $\overline{T}_m^\sigma$. Notice that this requirement generalises the requirement for when the Lichtenbaum-Tate pairing is perfect, and further, that this is exactly when it coincides with the perfect pairing mentioned in Remark 3.7.

Theorem 4.4. *Assume $d \equiv 1 \pmod{m}$ for $\alpha^\dagger \circ \alpha = [d]$, and that m is coprime to $\mathrm{char}(k)$. Then, the generalised Tate-pairing $T^\alpha_{m,\mathcal{L}}$ is a perfect pairing.*

Proof. By unraveling the definitions, we see that this allows us to apply Theorem 2.2 when the hypothesis on d is satisfied. Very explicitly, recall that the polarized m-Weil pairing defines an isomorphism of abelian groups $e^*_{m,\mathcal{L}} : A[m] \xrightarrow{\sim} A[m]^\vee$, while the canonical action of G on $M^\vee$ for any G-module M is given by $\tau \cdot f(m) = f(\tau^{-1} \cdot m)$. Combining this, we see that

$$\begin{aligned} e^*_{m,\mathcal{L}}(\gamma \cdot Q) &= e^*_{m,\mathcal{L}}(\alpha(Q)) \\ &= e_{m,\mathcal{L}}(-, \alpha(Q)) \\ &= e_{m,\mathcal{L}}(\alpha^{-1}(-), Q)^d \\ &= \gamma \cdot e^*_{m,\mathcal{L}}(Q)^d \end{aligned}$$

thus, we may upgrade this to an isomorphism of $\widehat{\mathbb{Z}}$-modules if and only if $d \equiv 1 \pmod{m}$, in which case $e^*_{m,\mathcal{L}}$ induces an isomorphism $H^n(\widehat{\mathbb{Z}}, A[m]) \simeq H^n(\widehat{\mathbb{Z}}, A[m]^\vee)$ for all n (which we also denote by $e^*_{m,\mathcal{L}}$ by abuse of notation). Now, we have defined the generalised m-Tate pairing as the composition of maps on the right of the diagram



The composition on the left is a perfect pairing by Theorem 2.2, and by fixing the correct generator of μ_m (which induces a fixed isomorphism $\frac{1}{m}\mathbb{Z}/\mathbb{Z} \simeq \mu_m$), we see that the diagram commutes, simply by inspecting the maps (both the compositions result in the formula from Definition 3.4). ∎

Acknowledgements. The idea for this note came after a fruitful conversation with Krijn Reijnders, which the author is thankful for. Further, thank you to Wouter Castryck for several helpful comments and suggestions. Finally, a large thanks to the anonymous reviewer whose suggestions and corrections improved the paper significantly.

Funding. This work is supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement ISOCRYPT – No. 101020788), by the Research Council KU Leuven grant C14/24/099 and by CyberSecurity Research Flanders with reference number VOEWICS02.

References

[1] Peter Bruin. The tate pairing for abelian varieties over finite fields. *Journal de theorie des nombres de Bordeaux*, 23(2):323–328, 2011.

[2] Wouter Castryck, Marc Houben, Simon-Philipp Merz, Marzio Mula, Sam van Buuren, and Frederik Vercauteren. Weak instances of class group action based cryptography via self-pairings. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III*, volume 14083 of *Lecture Notes in Computer Science*, pages 762–792. Springer, 2023.

[3] Steven D. Galbraith, Valerie Gilchrist, and Damien Robert. Improved algorithms for ascending isogeny volcanoes, and applications. In Daniel Escudero and Ivan Damgård, editors, *Progress in Cryptology - LATINCRYPT 2025 - 9th International Conference on Cryptology and Information Security in Latin America, Medellín, Colombia, October 1-3, 2025, Proceedings*, volume 16129 of *Lecture Notes in Computer Science*, pages 174–208. Springer, 2025.

[4] Pierre Guillot. *A gentle course in local class field theory: local number fields, Brauer groups, Galois cohomology*. Cambridge University Press, 2018.

[5] Joseph Macula and Katherine E Stange. Extending class group action attacks via sesquilinear pairings. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 371–395. Springer, 2024.

[6] James S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[7] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323. Springer Science & Business Media, 2013.

[8] Giacomo Pope, Krijn Reijnders, Damien Robert, Alessandro Sferlazza, and Benjamin Smith. Simpler and faster pairings from the montgomery ladder. *IACR Communications in Cryptology*, 2025(2), 2025.

[9] Damien Robert. The geometric interpretation of the tate pairing and its applications. *IACR Cryptol. ePrint Arch.*, page 177, 2023.

[10] Damien Robert. Fast pairings via biextensions and cubical arithmetic. *IACR Cryptol. ePrint Arch.*, page 517, 2024.

[11] Jean-Pierre Serre. *Cohomologie galoisienne*, volume 5. Springer Science & Business Media, 1994.

[12] Katherine E Stange. Sesquilinear pairings on elliptic curves. *arXiv preprint arXiv:2405.14167*, 2024.

Jonathan Komada Eriksen
COSIC, KU Leuven, Kasteelpark Arenberg 10, 3001 Heverlee, Belgium;
jonathke@esat.kuleuven.be
Author IDs: zbMATH eriksen.jonathan-komada MR 1601928 ORCID 0009-0000-3040-2965