The Cokernel Pairing

Krijn Reijnders

COSIC, KU Leuven, Belgium

Abstract. We study a new pairing, beyond the Weil and Tate pairing. The Weil pairing is a non-degenerate pairing $E[m] \times E[m] \to \mu_m$, which operates on the kernel of $[m]$. Similarly, when $\mu_m \subseteq \mathbb{F}_q^*$, the Tate pairing is a non-degenerate pairing $E[m](\mathbb{F}_q) \times E(\mathbb{F}_q)/[m]E(\mathbb{F}_q) \to \mu_m$, which connects the kernel and the rational cokernel of $[m]$. We define a pairing

$$\langle \quad \rangle_m : E(\mathbb{F}_q)/[m]E(\mathbb{F}_q) \times E(\mathbb{F}_q)/[m]E(\mathbb{F}_q) \to \mu_m$$

on the rational cokernels of $[m]$, filling the gap left by the Weil and Tate pairing. When $E[m] \subseteq E(\mathbb{F}_q)$, this pairing is non-degenerate, and can be computed using three Tate pairings, and two discrete logarithms in μ_m, given a basis for $E[m]$. For $m = \ell$ prime, this pairing allows us to study $E(\mathbb{F}_q)/[\ell]E(\mathbb{F}_q)$ directly and to simplify the computation for a basis of $E[\ell^k]$, and more generally the Sylow ℓ-torsion. This finds natural applications in isogeny-based cryptography when computing ℓ^k-isogenies.

Keywords: pairings · isogenies · elliptic curves

1 Introduction

Pairings are ubiquitous in modern cryptography, from their first uses in the MOV-attacks [MOV91; FR94] to their applications in protocols [HSSI99; Jou04; BLS01; BF01; BKLS02; GHS02; Jou02; BGLS03; BLS04; Gal05; Ver09], exploiting their bilinearity and other unique characteristics. Most commonly, cryptography uses the Weil pairing [Wei40; Mil04] and the Tate pairing [Tat62; Lic69], and their variations [HSV06; Bru11]. For this work, we may think of the Weil pairing of degree m, for $m \in \mathbb{N}$, as the non-degenerate bilinear map

$$e_m : E[m] \times E[m] \to \mu_m,$$

where $E[m]$ is the m-torsion subgroup of an elliptic curve E over a finite field $\mathbb{F}_q$, and μ_m is the group of m-th roots of unity in $\mathbb{F}_q$. Similarly, we may think of the (reduced) Tate pairing of degree m as the bilinear map

$$t_m : E[m](\mathbb{F}_q) \times E(\mathbb{F}_q)/[m]E(\mathbb{F}_q) \to \mu_m,$$

which is non-degenerate when $\mu_m \subseteq \mathbb{F}_q^*$.

More recently, isogeny-based cryptrography often uses these pairings, as they find many natural applications in cryptonanalysis [CHMM+23; MS24] and core algorithm procedures [CJLN+17; ZSPD+18; KT18; Reij23; LWXZ24; CEMR24; DEFM+25]. It is not difficult to see why: Vélu's formulas [Vél71] allow us to compute an isogeny $\phi : E \to E'$ from a description of its kernel $G = \ker \phi$. Hence, given a point $P \in E$ of order n, we can compute a (cyclic) isogeny of degree n with kernel $G = \langle P \rangle$. As the complexity of these

E-mail: crypto.krijn@gmail.com (Krijn Reijnders)

*This work was supported in part 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 VR20192203. Date of this document: 2025-12-22.

formulas is $\mathcal{O}(|G|)$, or $\mathcal{O}(\sqrt{|G|})$ using $\sqrt{\text{é}}$lu [BDLS20], we improve the performance by factoring ϕ into prime-degree isogenies ϕ_i. As a result, we often want to compute isogenies of prime-power degree ℓ^k, which we may then describe by a point P of order ℓ^k, factored into k isogenies of degree ℓ. To find such points, or to describe them concisely, requires a basis of $E[\ell^k]$, where ℓ^k is such that there are no rational points of order ℓ^{k+1} on E. Equivalently, such points have no rational preimages under $[\ell]$ and we should look for such points in the set $E(\mathbb{F}_q) \setminus [\ell]E(\mathbb{F}_q)$.

This is where the Tate pairing comes in, as it allows us to identify points in $E(\mathbb{F}_q) \setminus [\ell]E(\mathbb{F}_q)$ if we have knowledge of the rational kernel $E[\ell](\mathbb{F}_q)$. It is no surprise that basis generation algorithms in the literature use the Tate pairing, whereas basis change algorithms use either the Tate or Weil pairing. Nevertheless, these pairing techniques only help us indirectly: the Tate pairing allows us to identify points in $E(\mathbb{F}_q) \setminus [\ell]E(\mathbb{F}_q)$, and the Weil pairing allows us to verify a basis for $E[\ell^k]$, but neither operates directly on the cokernel of $[\ell]$.

Contributions. This work introduces the cokernel pairing $\langle \quad \rangle_m$, which operates directly on the cokernel of $[m]$:

$$\langle \quad \rangle_m : E(\mathbb{F}_q)/[m]E(\mathbb{F}_q) \times E(\mathbb{F}_q)/[m]E(\mathbb{F}_q) \to \mu_m.$$

When $m = \ell$ is a (small) prime, this pairing allows us to find a basis for $E[\ell^k](\mathbb{F}_q)$ more directly: Our main theorem, Theorem 3.6, shows that $\langle P, Q\rangle_\ell \neq 1$ if and only if (the classes of) P and Q are a basis for $E(\mathbb{F}_q)/[\ell]E(\mathbb{F}_q)$. Among others, this implies that some multiple of P and Q are a basis for $E[\ell^k](\mathbb{F}_q)$, which is our main application of the cokernel pairing.

From a mathematical point of view, the cokernel pairing fills a symmetry gap: the Weil pairing e_m works with the kernel $E[m]$ for both arguments, the (reduced) Tate pairing t_m connects the rational kernel $E[m](\mathbb{F}_q)$ to the rational cokernel $E(\mathbb{F}_q)/[m]E(\mathbb{F}_q)$, and the cokernel pairing works with this rational cokernel for both arguments.

We provide a detailed explanation of the underlying dualities between several key objects, such as the m-torsion $E[m]$ and the Sylow m-torsion $\mathcal{S}_m(E)$, which expands on previous descriptions in the literature [Rob23; CR25; Reij25]. This deepened understanding of the duality between these objects helps us in developing practical applications of pairings.

For practical applications, we show how the cokernel pairing simplifies basis generation, state several methods to compute the cokernel pairing, and demonstrate these using concrete examples. Furthermore, we give concrete results that allow us to interpret the cokernel pairing in terms of other pairings. This leads to interesting open questions in many directions.

Remark 1. The cokernel pairing looks similar to a pairing defined by Tate for local fields, derived from cohomology, and we discuss the subtle differences in Section A. As far as we are aware, we are the first to introduce the cokernel pairing, and in particular, to study the cokernel pairing in the context of isogeny-based cryptography, where the Sylow ℓ-torsion is a remarkably central object. We hope that this work contributes to our understanding of this pairing and the Sylow ℓ-torsion.

Acknowledgements. We thank Damien Robert for insightful discussions on the cohomological interpretation of the cokernel pairing, and deeper insights into the dualities that appear in this context. We thank the whole ISOCRYPT team from KU Leuven for their support, feedback, and useful ideas.

2 Preliminaries

In this section, we introduce the necessary background on pairings, profiles, and the Sylow ℓ-torsion.

Notation. We denote the finite field of size q by $\mathbb{F}_q$, and we assume that $q = p^k$ for a prime p, the characteristic of $\mathbb{F}_q$. We denote the multiplicative group of non-zero elements of $\mathbb{F}_q$ by $\mathbb{F}_q^*$, which is a cyclic group of order $q-1$. We denote the algebraic closure of $\mathbb{F}_q$ by $\overline{\mathbb{F}_q}$ and the m-th roots of unity in $\mathbb{F}_q$ by μ_m.

For elliptic curves over $\mathbb{F}_q$, we denote the neutral element of E by $\mathbf{0}_E$, and π always denotes the Frobenius endomorphism $(x, y) \mapsto (x^q, y^q)$ with respect to $\mathbb{F}_q$. We use the word *rational* to refer to something defined over the base field $\mathbb{F}_q$, for example, E is rational when it is defined over $\mathbb{F}_q$, and $P \in E$ is rational when $P \in E(\mathbb{F}_q)$.

For an integer $m \in \mathbb{N}$, we denote the Weil pairing by e_m, the Tate pairing by T_m, and the reduced Tate pairing by t_m. We denote the Sylow m-torsion by $\mathcal{S}_m(E)$, which we describe in more detail in Section 2.4. We use the word *cofactor* with respect to some integer m to refer to the smallest integer h such that $[h]P \in \mathcal{S}_m(E)$ for all $P \in E(\mathbb{F}_q)$. When $|E(\mathbb{F}_q)| = N$ and $m = \ell$ prime, we may use[1] $h = N/\ell^{v_\ell(N)}$, where $v_\ell(N)$ is the ℓ-adic valuation of N. Simply put, for $N = \ell^k \cdot h$, we can use the cofactor h. We somewhat misuse the word *basis*, as we sometimes refer to a basis (P, Q) when these points are independent and generate a certain set, even though there are relations between the generated points, i.e., P and Q are only a generating set.

2.1 Pairings

In general, a pairing $A \times B \to C$ is a bilinear map between abelian groups A, B and C. In this work we are interested in abelian groups A and B that are subgroups or quotient groups of an elliptic curve E over a finite field $\mathbb{F}_q$, and similarly C is a subgroup or quotient group of $\mathbb{F}_q^*$. Central to this work are the subgroups and quotient groups derived from the multiplication-by-m endomorphisms $[m] : P \mapsto [m]P$, namely, the kernel

$$E[m] = \{P \in E \mid [m]P = \mathbf{0}_E\},$$

and, viewing $[m]$ as a map $E(\mathbb{F}_q) \to E(\mathbb{F}_q)$, the cokernel

$$E(\mathbb{F}_q)/[m]E(\mathbb{F}_q) = \{P + [m]E(\mathbb{F}_q) : P \in E(\mathbb{F}_q)\}.$$

For the rest of this section, we assume that m is a positive integer coprime to the characteristic of $\mathbb{F}_q$, and we let E be an elliptic curve over $\mathbb{F}_q$. Some results are specialized to the case where $m = \ell$ is a small odd prime, which is our main case of interest.

2.2 The Weil Pairing

The Weil pairing [Wei40] of degree m is a non-degenerate bilinear pairing

$$e_m : E[m] \times E[m] \to \mu_m. \tag{1}$$

More generally, for abelian varieties A, we can derive the Weil pairing as a pairing

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

where $\widehat{A}$ is the dual abelian variety of A [Sil10]. As elliptic curves are naturally isomorphic to their duals, we get a canonical principal polarization $E \to \widehat{E}$, which allows us to recover

[1] This may not be the smallest integer that clears all but the ℓ-torsion, but works for our needs.

the Weil pairing on E itself. Similarly, Jacobian varieties of non-singular curves with a rational point come equipped with such a principal polarization. In such cases, we may simply write e_m, with no need to specify the polarization $\lambda : A \to \widehat{A}$ against which we define the Weil pairing. More details can be found in the book by Edixhoven, Van der Geer, and Moonen [EVM12, Ch. 11].

The Generalized Weil Pairing. This generalized notion of the Weil pairing on abelian varities allows us to define the Weil-Cartier pairing [EVM12; Rob23] with respect to an m-isogeny $f : A \to B$. This results in a pairing $\ker f \times \ker \widehat{f} \to \mu_m$, where $\widehat{f} : \widehat{B} \to \widehat{A}$ is the dual isogeny.

2.3 The Tate Pairing

Assuming $\mu_m \subseteq \mathbb{F}_q^*$, the Tate-Lichtenbaum pairing [Tat62; Lic69] of degree m, hereafter simply the Tate pairing, is a non-degenerate bilinear pairing

$$T_m : E[m](\mathbb{F}_q) \times E(\mathbb{F}_q)/[m]E(\mathbb{F}_q) \to \mathbb{F}_q^*/\mathbb{F}_q^{*,m}. \tag{2}$$

This pairing was introduced in a cryptographic context by Frey and Rück [FR94]. For cryptographic purposes, working with equivalence classes in $\mathbb{F}_q^*$ is inconvenient. Hence, we may ‘reduce’ the Tate pairing by applying a final exponentiation by $\frac{q-1}{m}$, which maps to μ_m. This gives the reduced Tate pairing

$$t_m : E[m](\mathbb{F}_q) \times E(\mathbb{F}_q)/[m]E(\mathbb{F}_q) \to \mu_m. \tag{3}$$

The groups $\mathbb{F}_q^*/\mathbb{F}_q^{*,m}$ and μ_m are naturally dual to each other: when we view exponentiation by m as a map $\mathbb{F}_q^* \to \mathbb{F}_q^*$, the final reduction induces an isomorphism

$$\mathbb{F}_q^*/\mathbb{F}_q^{*,m} \xrightarrow{\sim} \mu_m, \quad z \mapsto z^{\frac{q-1}{m}}, \tag{4}$$

between the cokernel $\mathbb{F}_q^*/\mathbb{F}_q^{*,m}$ and the kernel μ_m We stress that, contrary to the Weil pairing, the Tate pairing crucially relies on the field of definition that we are working over, as is clear from its definition.

Link to the Weil Pairing. When $E[m] \subseteq E(\mathbb{F}_q)$, an alternative definition of the reduced Tate pairing can be obtained using a preimage R of Q, e.g., a point such that $[m]R = Q$. We get

$$t_m(P, Q) = e_m(P, \pi(R) - R). \tag{5}$$

Written in this way, we clearly see the arithmetic nature of the Tate pairing, as we take Frobenius π with respect to a field $\mathbb{F}_q$. If we compute the Tate pairing for the same points over a different field, we may get a different result. In particular, a non-trivial Tate pairing becomes trivial when we extend to the field of definition of R.

The Generalized Tate Pairing. Similar to the Weil pairing, we may also generalize the Tate pairing with respect to an m-isogeny $f : A \to B$ over $\mathbb{F}_q$. This results in the Tate-Cartier pairing, also known as the generalized f-Tate pairing or the Tate pairing associated to f. Bruin [Bru11] shows that this pairing between the rational kernel and rational cokernel of f is non-degenerate when $\ker f$ is annihilated by $[q-1]$, and gives a description as $\ker \widehat{f}\ (\mathbb{F}_q) \times \operatorname{coker} f\ (\mathbb{F}_q) \to \mathbb{F}_q^*$.

Computation of the Pairings. Miller’s algorithm [Mil04; FR94] computes both the Weil and Tate pairing efficiently, which generalize well to Jacobians. In recent work, Robert [Rob24] introduces *cubical arithmetic* to compute pairings on abelian varieties and Kummer varieties, generalizing previous work [LR16; Sta08; Sta11].

2.4 The Sylow ℓ-Torsion

The Sylow m-torsion $\mathcal{S}_m(E)$ is the subgroup of $E(\mathbb{F}_q)$ that contains all points whose orders divide some power of m, sometimes also denoted $E[m^\infty](\mathbb{F}_q)$. We mostly focus on the case where $m = \ell$ is a prime, in which case all points in $\mathcal{S}_\ell(E)$ are in the kernel of $[\ell^k]$ for some large enough k. We define the Sylow torsion generally for abelian varieties.

Definition 1. Let A be a g-dimensional abelian variety over $\mathbb{F}_q$ and ℓ a prime, coprime to p. The *Sylow ℓ-torsion* $\mathcal{S}_\ell(A)$ over $\mathbb{F}_q$ is the subgroup

$$\mathcal{S}_\ell(A) := A[\ell^\infty](\mathbb{F}_q) \cong \mathbb{Z}/\ell^{f_1}\mathbb{Z} \times \mathbb{Z}/\ell^{f_2}\mathbb{Z} \times \ldots \times \mathbb{Z}/\ell^{f_d}\mathbb{Z}$$

with $f_1, \ldots, f_d \in \mathbb{N}$ such that $f_1 \geq f_2 \geq \ldots f_d > 0$, and $d \leq 2g$. We say $\mathcal{S}_\ell(A)$ is *symmetric* when all f_i are equal, e.g. $\mathcal{S}_\ell(A) = A[\ell^{f_1}]$. When the Sylow ℓ-torsion is rank r, we refer to a set of r points as a *basis* of $\mathcal{S}_\ell(A)$ whenever their linear combinations generate all elements of $\mathcal{S}_\ell(A)$.

It is clear that $A[\ell](\mathbb{F}_q) \subseteq \mathcal{S}_\ell(A)$, and so d is equal to the rank of $A[\ell](\mathbb{F}_q)$. The exponent equals ℓ^{f_1}. Furthermore, an isogeny $f : A \to B$ gives us a homomorphism $\mathcal{S}_\ell(A) \to \mathcal{S}_\ell(B)$, which is an isomorphism whenever $\deg f$ is coprime to ℓ.

In the case of elliptic curves the rank d of $\mathcal{S}_\ell(E)$ is either 0, 1, or 2. In this paper we assume that $E[\ell]$ is rational, and so $d = 2$ in essentially all cases. Thus, on elliptic curves with $E[\ell]$ rational, a basis for the Sylow ℓ-torsion is simply a pair of points (P, Q) that generate all rational points of order ℓ^k for $0 \leq k \leq f_1$.

The Sylow ℓ-torsion is closely related to the rational cokernel $E(\mathbb{F}_q)/[\ell]E(\mathbb{F}_q)$ and the kernel $E[\ell]$. First, classes in the rational cokernel are in one-to-one correspondence with classes in $\mathcal{S}_\ell(E)/[\ell]\mathcal{S}_\ell(E)$ which comes down to 'ignoring' all other torsion, which we can formalize as multiplication by h, where h is the cofactor with respect to ℓ. Second, as $\mathcal{S}_\ell(E)/[\ell]\mathcal{S}_\ell(E)$ is dual to $E[\ell]$, we may associate a point $P_\ell \in E[\ell]$ to any class $P \in E(\mathbb{F}_q)/[\ell]E(\mathbb{F}_q)$.

Isogeny-based cryptography often works with supersingular curves $E/\mathbb{F}_{p^2}$ of order $(p+1)^2$, where the torsion structure is isomorphic to $\mathbb{Z}/(p+1)\mathbb{Z} \times \mathbb{Z}/(p+1)\mathbb{Z}$. In such cases, the Sylow ℓ-torsion is simply $\mathcal{S}_\ell(E) = E[\ell^f]$, where f is the largest integer such that $\ell^f \mid p+1$. In particular $\mathcal{S}_\ell(E)$ is symmetric, as it is isomorphic to $\mathbb{Z}/(\ell^f)\mathbb{Z} \times \mathbb{Z}/(\ell^f)\mathbb{Z}$.

2.5 The Tate Profile

When the Tate pairing of degree m is non-degenerate, we may study the cokernel $E(\mathbb{F}_q)/[m]E(\mathbb{F}_q)$ more precisely using a rational basis[2] $(P_1, \cdots, P_r)$ of $E[m](\mathbb{F}_q)$, and the map

$$t_{[m]} : E(\mathbb{F}_q) \to \mu_m^r, \quad Q \mapsto (t_m(P_1, Q), \cdots, t_m(P_r, Q)).$$

Following [Rob23; CR25; Reij25], we call $t_{[m]}$ the *Tate profile* of Q with respect to the basis $(P_1, \cdots, P_r)$. The profile is trivial if and only if $Q \in [m]E(\mathbb{F}_q)$, and whenever the profiles of a set $(Q_1, \ldots, Q_r)$ generate μ_m^r, the set generates the cokernel $E(\mathbb{F}_q)/[m]E(\mathbb{F}_q)$, which holds more generally for principally polarized abelian varieties too [Reij25, Thm. 1]. Under mild assumptions, $E[m] \xrightarrow{\sim} E(\mathbb{F}_q)/[m]E(\mathbb{F}_q) \xrightarrow{\sim} \mu_m^r$, and we should view the Tate profile as giving us a coordinate system on $E(\mathbb{F}_q)/[m]E(\mathbb{F}_q)$ through the map to μ_m^r. The rational kernel and cokernel are dual, hence isomorphic, but the isomorphism given by the profile crucially depends on a choice of basis.

[2] Clearly, for elliptic curves $E[m](\mathbb{F}_q)$ is at most rank 2. However, the approach in this section generalizes to abelian varieties of dimension g, where the rank is up to $2g$. Our phrasing accommodates this generalization.

3 The Cokernel Pairing

Before we introduce the cokernel pairing in Section 3.2, we explore the connection between the kernel $E[m]$ and the cokernel $E(\mathbb{F}_q)/[m]E(\mathbb{F}_q)$ in more detail. We are mostly interested in the case where $m = \ell$ is a small prime and $E[\ell]$ is rational, as studying the Sylow ℓ-torsion in this case is most interesting for our applications. Hence, we will focus on $m = \ell$ prime, and may sometimes switch to the more general case $m \in \mathbb{N}$ when this does not create extra difficulties or subtleties.

3.1 Connecting Kernel and Cokernel

The reduced Tate pairing, when defined as in Equation (5), relies on the preimages R_P of points P under $[\ell]$. We first analyze this map $P \mapsto \pi(R_P) - R_P$, before we analyze the cokernel pairing, to show that the map behaves well and naturally connects the kernel and cokernel of $[\ell]$.

Lemma 1. *Let E be an elliptic curve over $\mathbb{F}_q$. For $m \in \mathbb{N}$, assume $E[m] \subseteq E(\mathbb{F}_q)$, and let $P \in E(\mathbb{F}_q)$ with $R_P \in E(\overline{\mathbb{F}_q})$ such that $[m]R_P = P$. Then the map*

$$E(\mathbb{F}_q) \to E[m], \qquad P \mapsto \pi(R_P) - R_P$$

is a well-defined homomorphism with kernel $[m]E(\mathbb{F}_q)$. The map induces an isomorphism

$$\Phi_m : E(\mathbb{F}_q)/[m]E(\mathbb{F}_q) \xrightarrow{\sim} E[m]. \tag{6}$$

Proof. We have

$$[m](\pi(R_P) - R_P) = \pi([m]R_P) - [m]R_P = \pi(P) - P = \mathbf{0}_E,$$

and so we get $\Phi_m(P) \in E[m]$. Let $R, R' \in E(\overline{\mathbb{F}_q})$ such that $[m]R = P$ and $[m]R' = P$. Then $R' = R + T$ for some $T \in E[m]$. As $E[m] \subseteq E(\mathbb{F}_q)$, we have $\pi(T) = T$, and so

$$\pi(R') - R' = \pi(R) - R + \pi(T) - T = \pi(R) - R.$$

Thus, the map is well-defined. We get that $\Phi_m(P) = \mathbf{0}_E$ only if $\pi(R) = R$, which implies $R \in E(\mathbb{F}_q)$ and so $P = [m]R \in [m]E(\mathbb{F}_q)$, so $\ker \Phi_m = [m]E(\mathbb{F}_q)$. As both kernel and cokernel have the same size, we get the isomorphism $\Phi_m : E(\mathbb{F}_q)/[m]E(\mathbb{F}_q) \xrightarrow{\sim} E[m]$. □

When $m = \ell$ is prime, it is not too difficult to bound the extension degree in which such a preimage R lies, as the following result shows.

Corollary 1. *Let ℓ be a prime and $P \in E(\mathbb{F}_q)$. Let $R \in E(\overline{\mathbb{F}_q})$ such that $[\ell]R = P$. When $\Phi_\ell(P) = \mathbf{0}_E$, then $R \in E(\mathbb{F}_q)$. When $\Phi_\ell(P) \neq \mathbf{0}_E$, then $R \in E(\mathbb{F}_{q^\ell})$.*

Proof. When $\Phi_\ell(P) = \mathbf{0}_E$, this is immediate from Theorem 3.1. When $\Phi_\ell(P) \neq \mathbf{0}_E$, given that $\pi(R) - R$ is rational, we get $\pi\left(\pi(R) - R\right) = \pi(R) - R$ and so

$$\pi^2(R) - R = \pi\left(\pi(R) - R\right) + \pi(R) - R = [2](\pi(R) - R),$$

and by induction this gives $\pi^k(R) - R = [k](\pi(R) - R)$. Thus, for $k = \ell$ we find

$$\pi^\ell(R) - R = [\ell](\pi(R) - R) = \mathbf{0}_E,$$

that is, $\pi^\ell(R) = R$, so $R \in E(\mathbb{F}_{q^\ell})$. □

Assuming rational m-torsion, the endomorphism $[m]$ divides $\pi - 1$, and so we may also write Φ_m as the endomorphism $\frac{\pi-1}{m}$. As an isomorphism between the rational cokernel and the kernel, Φ_m identifies the 'position' of points in the Sylow m-torsion with respect to their position in $E[m]$. This is equivalent to the positioning given by the Tate profile $t_{[m]}$ with respect to some basis T_1, T_2 of the kernel, encoded as a value in μ_m^2. Furthermore, Φ_m is the curve equivalent to the 'reduction' map $\mathbb{F}_q^*/\mathbb{F}_q^{*,m} \xrightarrow{\sim} \mu_m$ from Equation (4).

3.2 The Cokernel Pairing

The definition of the reduced Tate pairing via Equation (5) motivates us to look at a pairing on the rational cokernels using the map Φ_m for a straightforward definition.

Definition 2. The *reduced cokernel pairing of degree m* is a pairing

$$\langle \quad \rangle_m : E(\mathbb{F}_q)/[m]E(\mathbb{F}_q) \times E(\mathbb{F}_q)/[m]E(\mathbb{F}_q) \to \mu_m.$$

Given $P, Q \in E(\mathbb{F}_q)$ as representants of their classes in $E(\mathbb{F}_q)/[m]E(\mathbb{F}_q)$, we define the cokernel pairing in terms of the Weil pairing e_m and the map Φ_m, by

$$\langle P, Q\rangle_m := e_m\left(\Phi_m(P), \Phi_m(Q)\right).$$

The (reduced) cokernel pairing is naturally connected to the Sylow m-torsion in the same way that the Weil pairing is naturally connected to $E[m]$, with the Tate pairing providing the bridge between these two. We first prove general properties of the cokernel pairing, before we dive deeper into this connection.

Proposition 1. *Assuming the m-torsion is rational, the reduced cokernel pairing of degree m is alternating, bilinear, non-degenerate, and compatible with isogenies $\phi : E \to E'$.*

- *For all $P, Q \in E(\mathbb{F}_q)$, we have $\langle P, Q\rangle_m = \langle Q, P\rangle_m^{-1}$.*
- *For all $P_1, P_2, Q \in E(\mathbb{F}_q)$, we have $\langle P_1 + P_2, Q\rangle_m = \langle P_1, Q\rangle_m \cdot \langle P_2, Q\rangle_m$, and similarly $\langle P, Q_1 + Q_2\rangle_m = \langle P, Q_1\rangle_m \cdot \langle P, Q_2\rangle_m$.*
- *For a given $P \in E(\mathbb{F}_q)$, if $\langle P, Q\rangle_m = 1$ for all $Q \in E(\mathbb{F}_q)$, then $P \in [m]E(\mathbb{F}_q)$, and mutatis mutandis for Q.*
- *For a separable isogeny $\phi : E \to E'$ over $\mathbb{F}_q$ and $P, Q \in E(\mathbb{F}_q)$, we have $\langle \phi(P), \phi(Q)\rangle_m = \langle P, Q\rangle_m^{\deg \phi}$.*

Proof. These properties are easily shown using the properties of the Weil pairing, and the map Φ_m. As the Weil pairing is alternating, we get the same for the cokernel pairing by

$$\langle P, Q\rangle_m = e_m\left(\Phi_m(P), \Phi_m(Q)\right) = e_m\left(\Phi_m(Q), \Phi_m(P)\right)^{-1} = \langle Q, P\rangle_m^{-1}.$$

Similarly, bilinearity follows by bilineairity of the Weil pairing and the fact that Φ_m is a homomorphism. For non-degeneracy, whenever $\langle P, Q\rangle_m = 1$ for all $Q \in E(\mathbb{F}_q)$, we must have by non-degeneracy of the Weil pairing that $\Phi_m(P) = \mathbf{0}_E$, which implies $P \in [m]E(\mathbb{F}_q)$ by Theorem 3.1. By the first property, the same holds for Q. Furthermore, when $P \in [m]E(\mathbb{F}_q)$ then $R \in E(\mathbb{F}_q)$, and so $\Phi_m(P) = \mathbf{0}_E$ which implies $\langle P, Q\rangle_m = 1$, and similarly for Q. Lastly, compatibility with isogenies follows from the compatibility of the Weil pairing with isogenies, together with the fact that $\phi(R_P)$ is a pre-image of $R_{\phi(P)}$. $\square$

The last property is interesting when $m \mid \deg \phi$, as we get $\langle \phi(P), \phi(Q)\rangle_m = 1$ for any $P, Q \in E(\mathbb{F}_q)$. Intuitively, either P or Q gets mapped to $[m]E'(\mathbb{F}_q)$, or we find that the $m^\bullet$-torsion of P and Q 'overlaps'. To make this more precise, we discuss the connection to the Sylow ℓ-torsion.

3.3 Connection to the Sylow ℓ-torsion

Let $m = \ell$ be prime. Recall that we may represent $\mathcal{S}_\ell(E)/[\ell]\mathcal{S}_\ell(E)$ by classes from $E(\mathbb{F}_q)/[\ell]E(\mathbb{F}_q)$, where $\mathcal{S}_\ell(E)$ is the Sylow ℓ-torsion of E, and that $\mathcal{S}_\ell(E)/[\ell]\mathcal{S}_\ell(E)$ is dual to the ℓ-torsion $E[m]$, with the map Φ_m giving us the isomorphism $\mathcal{S}_\ell(E)/[\ell]\mathcal{S}_\ell(E) \xrightarrow{\sim} E[\ell]$. This inspires the following definition.

Definition 3. A point $P \in E(\mathbb{F}_q) \setminus [\ell]E(\mathbb{F}_q)$ is *above* a point $P_\ell \in E[\ell]$ if $\Phi_\ell(P) = P_\ell$.

Assume $\mathcal{S}_\ell(E) \cong \mathbb{Z}/\ell^f\mathbb{Z} \times \mathbb{Z}/\ell^g\mathbb{Z}$, with $f \geq g > 0$. Understanding $\mathcal{S}_\ell(E)$ through the cokernel pairing will allow us to find a point of maximal order ℓ^f or a basis of points P, Q that allow us to compute any ℓ^g-isogeny. Note that a point $P \in E(\mathbb{F}_q) \setminus [\ell]E(\mathbb{F}_q)$ is not per se of order ℓ^f or ℓ^g, though one may use the Tate pairing to identify such points [Rob23; CR25]. For our purposes, we mainly need that some multiple of representants of generators $E(\mathbb{F}_q)/[\ell]E(\mathbb{F}_q)$ generate $\mathcal{S}_\ell(E)$ too [Reij25]. The following theorem is the crucial connection of $\mathcal{S}_\ell(E)$ to the cokernel pairing.

Theorem 1. *Let $P, Q \in E(\mathbb{F}_q)$, and let h be the cofactor of E with respect to ℓ. Then, $[h]P$ and $[h]Q$ generate $\mathcal{S}_\ell(E)$ if and only if $\langle P, Q\rangle_\ell = \zeta_\ell$ is a primitive ℓ-th root of unity.*

Proof. The proof is a combination of two insights: that Φ_ℓ gives us an isomorphism between $\mathcal{S}_\ell(E)/[\ell]\mathcal{S}_\ell(E)$ and $E[\ell]$, and that the Weil pairing $e_\ell(P', Q')$ is non-trivial if and only if P', Q' are a basis of $E[\ell]$.

If we have a basis P, Q of $\mathcal{S}_\ell(E)$, the points $\Phi_\ell(P)$ and $\Phi_\ell(Q)$ are non-trivial, otherwise P or Q has a rational preimage under $[\ell]$. Then, $\Phi_\ell(P)$ and $\Phi_\ell(Q)$ are independent, otherwise the classes $[P] = \lambda[Q]$ in $\mathcal{S}_\ell(E)/[\ell]\mathcal{S}_\ell(E)$ for some scalar λ, which implies P and Q are not a basis. Hence, $\langle P, Q\rangle_\ell = e_\ell\left(\Phi_\ell(P), \Phi_\ell(Q)\right) = \zeta_\ell \neq 1$.

Similarly, if $\langle P, Q\rangle_\ell \neq 1$ then $\Phi_\ell(P)$ and $\Phi_\ell(Q)$ are a basis of $E[\ell]$. Hence, the classes $[[h]P]$ and $[[h]Q]$ generate $\mathcal{S}_\ell(E)/[\ell]\mathcal{S}_\ell(E)$, which implies $[h]P$ and $[h]Q$ generate $\mathcal{S}_\ell(E)$. □

Thus, the cokernel pairing plays a dual role to the Weil pairing: whereas a Weil pairing of order ℓ implies a basis for $E[\ell]$, a non-trivial cokernel pairing of order ℓ implies a basis for $\mathcal{S}_\ell(E)$. More generally, for composite m, we want the cokernel pairing value to be a primitive m-th root of unity, similar to how the Weil pairing indicates a basis for $E[m]$ when the pairing is of order m. The isomorphism Φ_ℓ connects the dual objects $E[\ell]$ and $\mathcal{S}_\ell(E)/[\ell]\mathcal{S}_\ell(E)$, and the (reduced) Tate pairing allows us to transfer knowledge from one to the other. We have visualised this in Figure 1.

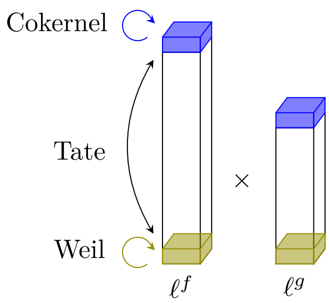

Figure 1: A visualisation of the Sylow ℓ-torsion, indicating in blue where the cokernel pairing operates and in olive the kernel $E[\ell]$ where the Weil pairing operates, with the Tate pairing transforming information from the kernel to the cokernel and back, as an elevator from the first to the top floor.

Remark 2. The cokernel pairing requires the assumption that $E(\mathbb{F}_q)$ has rational ℓ-torsion. This is not a strong restriction on the applicability of the cokernel pairing, as we need rational ℓ-torsion to ensure that $\mathcal{S}_\ell(E)$ also has rank 2. If $\mathcal{S}_\ell(E)$ has rank 1, which implies $E[\ell](\mathbb{F}_q)$ has rank 1, then there is no need for a cokernel pairing, as we get a trivial pairing. To find a generator of $\mathcal{S}_\ell(E)$ in this case, we may simply use the Tate pairing. In higher dimensions, partially-rational cokernels are more interesting to study, in particular through the isomorphism with the partially-rational kernel.

3.4 The Generalized Cokernel Pairing

Similar to the generalized Weil and Tate pairing described in Sections 2.2 and 2.3, there seems to be no obstruction to generalizing the cokernel pairing to any separable isogeny $f : A \to B$ between abelian varieties, with m the exponent of $(\ker f)(\mathbb{F}_q)$. By restricting the map Φ_m, which we denote Φ_f, we get an isomorphism $(\operatorname{coker} f)\,(\mathbb{F}_q) \xrightarrow{\sim} (\ker f)\,(\mathbb{F}_q)$, and similarly $(\operatorname{coker} \widehat{f})\,(\mathbb{F}_q) \xrightarrow{\sim} (\ker \widehat{f})\,(\mathbb{F}_q)$. Thus, we may define the following generalization.

Definition 4. Let $f : A \to B$ be a separable isogeny between abelian varieties A and B over a finite field $\mathbb{F}_q$. Let m be the exponent of $(\ker f)\,(\mathbb{F}_q)$. Then, the *generalized f-cokernel pairing* is a pairing

$$\langle \quad \rangle_f : (\operatorname{coker} f)\,(\mathbb{F}_q) \times (\operatorname{coker} \widehat{f})\,(\mathbb{F}_q) \to \mu_m.$$

Given $P \in A(\mathbb{F}_q)$ and $Q \in B(\mathbb{F}_q)$, we define

$$\langle P, Q\rangle_f := e_f\left(\Phi_f(P), \Phi_{\widehat{f}}(Q)\right),$$

where e_f is the generalized Weil pairing $\ker f \times \ker \widehat{f} \to \mu_m$ with respect to f.

4 Computation of the Cokernel Pairing

We describe two methods to compute the cokernel pairing over $\mathbb{F}_q$ using a concrete instantiation of the map Φ_m, assuming that we know a basis T_1, T_2 of $E[m]$. We then give two concrete examples of a cokernel pairing computation.

Remark 3. The most straightforward computation uses the points R_P and R_Q with $[m]R_P = P$ and $[m]R_Q = Q$ in $E(\mathbb{F}_{q^m})$. Writing $\psi_m(x)$ for the m-th division polynomial, and ϕ_m and ω_m as in [Sil09, III, Ex. 3.7], we may write the map $[m] : E \to E$ as

$$[m](x, y) = \left(\frac{\phi_m(x)}{\psi_m^2(x)}, \frac{\omega_m(x, y)}{\psi_m^3(x)}\right). \tag{7}$$

Thus, we can find a preimage R of P by computing a non-zero root x_R of $\psi_m^2(x)\cdot x_P = \phi_m(x)$, which is the x-coordinate of R, and we find an associated y-coordinate y_R by solving the curve equation. Given R_P and R_Q, we may then compute $P_m = \pi(R_P) - R_P$ and $Q_m = \pi(R_Q) - R_Q$ explicitly in $E(\mathbb{F}_{q^m})$. We compute the Weil pairing $e_m(P_m, Q_m)$ over $\mathbb{F}_q$ to get $\langle P, Q\rangle_m$. This approach is usually rather expensive, as it requires us to go to the extension field $\mathbb{F}_{q^m}$, which may be prohibitive for large m.

4.1 Using Weil and Tate pairings

Recall that Φ_m is the endomorphism $\frac{\pi-1}{m} \in \operatorname{End}(E)$. In [DEFM+25, Appendix D], the authors describe an algorithm that computes endomorphisms of the form $\frac{a+b\alpha}{m}$ over $\mathbb{F}_q$, assuming a basis for the m-torsion. For completeness, we repeat their algorithm for our situation $a = -1$, $b = 1$, $\alpha = \pi$ in Algorithm 1. We assume a basis T_1, T_2 for $E[m]$, and set $\zeta = e_m(T_1, T_2)$ as a fixed m-th root of unity.

This algorithm costs two Tate pairings of degree m and two discrete logarithms in μ_m. We may thus apply Algorithm 1 twice to obtain $\Phi_m(P)$ and $\Phi_m(Q)$, and then compute $\langle P, Q\rangle_m$ by the Weil pairing of $\Phi_m(P)$ and $\Phi_m(Q)$, which takes two more Tate pairings of degree m and an inversion. This gives a total cost of six Tate pairings of degree m, two discrete logarithms in μ_m, and an inversion.

Algorithm 1 Rational computation of Φ_m

Input: A point $P \in E(\mathbb{F}_q)$, a basis T_1, T_2 of $E[m]$, and $\zeta = e_m(T_1, T_2) \in \mu_m$.
Output: The point $\Phi_m(P) \in E[m]$

$(\zeta_1, \zeta_2) \leftarrow (t_m(T_1, P), t_m(T_2, -P))$
$(r, s) \leftarrow (\log_\zeta(\zeta_2), \log_\zeta(\zeta_1))$
return $rT_1 + sT_2$

We can improve on this by noting that Algorithm 1 already describes $\Phi(P)$ and $\Phi(Q)$ as linear combinations $aT_1 + bT_2$ with $a, b \in \mathbb{Z}/m\mathbb{Z}$. This representation significantly simplifies the computation of the Weil pairing between $\Phi(P)$ and $\Phi(Q)$, and so we get

$$\langle P, Q\rangle_m = e_m\left(aT_1 + bT_2, cT_1 + dT_2\right) = \zeta^{ad-bc},$$

where $\zeta = e_m\left(T_1, T_2\right)$, for a total cost of four Tate pairings and four discrete logarithms in μ_m. This is summarized in Algorithm 2.

Algorithm 2 Cokernel Pairing Computation using Weil Pairing

Input: Points $P, Q \in E(\mathbb{F}_q)$, a basis T_1, T_2 of $E[m]$, and $\zeta = e_m(T_1, T_2) \in \mu_m$.
Output: The cokernel pairing $\langle P, Q\rangle_m \in \mu_m$

$(\zeta_1, \zeta_2) \leftarrow (t_m(T_1, P), t_m(T_2, -P))$
$(\zeta_3, \zeta_4) \leftarrow (t_m(T_1, Q), t_m(T_2, -Q))$
$(a, b) \leftarrow \big(\log_\zeta(\zeta_2), \log_{\zeta_0}(\zeta_1)\big)$
$(c, d) \leftarrow \big(\log_\zeta(\zeta_4), \log_{\zeta_0}(\zeta_3)\big)$
return ζ^{ad-bc}

Remark 4. We stress that, at its core, the above computation of $\langle P, Q\rangle_m$ requires us to first compute the positions of P and Q in $\mathcal{S}_m(E)/[m]\mathcal{S}_m(E)$. This happens in Algorithm 1 by computing the Tate profile $(t_m(T_1, P), t_m(T_2, P))$ with respect to a basis of $E[m]$. The resulting Weil pairing essentially verifies the independence of these Tate profiles. Thus, if we are only interested in non-triviality of the cokernel pairing, we may forgo the final Weil pairing and the discrete logarithm computations, and verify the independence of the Tate profiles themselves in μ_m^2.

Inverse of Φ_m. Given Algorithm 1, we may similarly wonder if we can compute the inverse $\Phi_m^{-1}(T)$ for $T \in E[m]$ as a map $E[m] \to E(\mathbb{F}_q)/[m]E(\mathbb{F}_q)$, given a basis (P, Q) of $E(\mathbb{F}_q)/[m]E(\mathbb{F}_q)$. This can be done with an algorithm very similar to Algorithm 1: given $\zeta = \langle P, Q\rangle_m$, we compute $\zeta_1 = t_m(T, -P)$ and $\zeta_2 = t_m(T, Q)$. We then find $a = \log_\zeta(\zeta_2)$ and similarly $b = \log_\zeta(\zeta_1)$ to get $\Phi_m^{-1}(T) = aP + bQ$.

Remark 5. Given the above description of an algorithm to invert the map Φ_m, we may complete the duality between the Weil pairing and the cokernel pairing. That is, given rational points $P, Q \in E[m]$, we may also compute $e_m(P, Q)$ as $\langle \Phi_m^{-1}(P), \Phi_m^{-1}(Q)\rangle_m$. This serves only for completeness, as it does not seem to give any benefit in computing $e_m(P, Q)$.

4.2 Using only Tate pairings

We may improve on the previous approach by the observation that we defined the (reduced) Tate pairing $t_m(P, Q)$ of degree m by $e_m\left(P, \pi(R) - R\right)$, where $[m]R = Q$. Thus, to compute $\langle P, Q\rangle_m$, we do not require both $\Phi_m(P)$ and $\Phi_m(Q)$: it is enough to compute $\Phi_m(P)$ and use $\langle P, Q\rangle_m = t_m(\Phi_m(P), Q)$. This gives Algorithm 3, with a total cost of three Tate pairings of degree m and two discrete logarithms in μ_m.

Algorithm 3 Cokernel Pairing Computation using Tate Pairings

Input: Points $P, Q \in E(\mathbb{F}_q)$, a basis T_1, T_2 of $E[m]$, and $\zeta_0 = e_m(T_1, T_2) \in \mu_m$.
Output: The cokernel pairing $\zeta = \langle P, Q\rangle_m \in \mu_m$

$(\zeta_1, \zeta_2) \leftarrow (t_m(T_1, P), t_m(T_2, -P))$
$(a, b) \leftarrow \big(\log_{\zeta_0}(\zeta_2), \log_{\zeta_0}(\zeta_1)\big)$
$P_m \leftarrow aT_1 + bT_2$
$\zeta \leftarrow t_m(P_m, Q)$
return ζ

4.3 Two concrete examples of cokernel pairings

We describe two concrete examples of cokernel pairings, one for degree $m = 2$ and one for degree $m = 5$, using the above methods to compute the pairing. We first discuss a supersingular example with symmetric Sylow m-torsion, for $m = 5$.

Example 1. Let $p = 4 \cdot 5^3 - 1$, and let $\mathbb{F}_q = \mathbb{F}_p(i)$ with $i^2 = -1$. Let $A = 439 + 245 \cdot i$ and let $E_A : y^2 = x^3 + Ax^2 + x$. The curve E_A is supersingular, and $E_A(\mathbb{F}_q) \cong \mathbb{Z}/(p+1)\mathbb{Z} \times \mathbb{Z}/(p+1)\mathbb{Z}$. Thus, for $m = 5$, we find that the Sylow m-torsion is symmetric:

$$\mathcal{S}_5(E_A) \cong \mathbb{Z}/(5^3)\mathbb{Z} \times \mathbb{Z}/(5^3)\mathbb{Z}.$$

A basis T_1, T_2 for $E_A[5]$ is given by $T_1 = (269 + 210 \cdot i, 319 + 35 \cdot i)$ and $T_2 = (498 + 486 \cdot i, 271 + 66 \cdot i)$, with $\zeta_0 = e_5(T_1, T_2) = 137 + 72 \cdot i$. We will compute the cokernel pairing for $P = (72 + 448 \cdot i, 433 + 172 \cdot i)$ and $Q = (467 + 169 \cdot i, 438 + 298 \cdot i)$. We first describe the naive approach: Solving Equation (7) over $\mathbb{F}_q(\alpha)$, where $\alpha^5 + i + 2 = 0$ gives the point $R = (x_R, y_R)$ such that $[5]R = P$, where

$$x_R = (439 + 185i)\alpha^4 + (321 + 112i)\alpha^3 + (461 + 412i)\alpha^2 + (178 + 222i)\alpha + 357 + 67i,$$
$$y_R = (295 + 234i)\alpha^4 + (335 + 159i)\alpha^3 + (141 + 409i)\alpha^2 + (317 + 20i)\alpha + 37 + 322i.$$

Then, we compute $\Phi_5(P) = \pi(R) - R = (492 + 177i, 399 + 442i) \in E[5]$. A similar computation gives $\Phi_5(Q) = (269 + 210i, 180 + 464i) \in E[5]$. The Weil pairing gives us

$$\langle P, Q\rangle_5 = e_5\left(\Phi_5(P), \Phi_5(Q)\right) = 137 + 427i.$$

By Theorem 3.6 for $h = 4$, we get that $[4]P$ and $[4]Q$ generate $\mathcal{S}_5(E)$, and, by its symmetry, both $[4]P$ and $[4]Q$ have order 5^3. For the approach using Algorithm 3, we first compute $\Phi_5(P) = [4]T_1 + [4]T_2$, and use $t_5(\Phi_5(P), Q)$ as another way to compute $\zeta = 137 + 427i$.

We get a different behavior in the following example of an ordinary curve with asymmetric Sylow m-torsion for $m = 2$.

Example 2. Let $p = 62723$, and let $\mathbb{F}_q = \mathbb{F}_p(i)$ with $i^2 = -1$. Let $a = 29939 + 47523 \cdot i$ and $b = 10859 + 6507 \cdot i$, and take $E : y^2 = x^3 + ax + b$. The curve E is ordinary, and $E_A(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$, where $n_1 = 2^6 \cdot 3 \cdot 7 \cdot 365903$ and $n_2 = 2^3$. Thus, for $m = 2$, the Sylow m-torsion is asymmetric, with structure

$$\mathcal{S}_2(E) \cong \mathbb{Z}/(2^6)\mathbb{Z} \times \mathbb{Z}/(2^3)\mathbb{Z}.$$

We use the basis $T_1 = (54664 + 59102 \cdot i, 0)$ and $T_2 = (18942 + 2030 \cdot i, 0)$ for $E[2]$, with $\zeta_0 = e_2(T_1, T_2) = -1$. We compute the cokernel pairing for $P = (29237 + 15619 \cdot i, 1514 + 12755 \cdot i)$ and $Q = (51627 + 57123 \cdot i, 17021 + 6724 \cdot i)$ using Algorithm 3. From $t_2(T_1, P) = 1$ and $t_2(T_2, -P) = -1$, we get $r = 1$ and $s = 0$, so $\Phi_2(P) = T_1$. Then, by $t_2(\Phi_2(P), Q) = t_2(T_1, Q) = -1$ we find that $\langle P, Q\rangle_2 = -1$, hence P and Q generate $E(\mathbb{F}_q)/[2]E(\mathbb{F}_q)$. Thus, some multiple of P and Q must generate $\mathcal{S}_2(E)$, and this multiple is given by the cofactor $h = 3 \cdot 7 \cdot 365903$, so that we get the Sylow-2 basis $P' = [h]P$ and $Q' = [h]Q$. In this case, both P' and Q' are of order 2^6. For elegance, we may take $R' = [5]P' - Q'$ instead, which has order 2^3, and use the basis (P', R') for $\mathcal{S}_2(E)$.

5 Connections to the Weil and Tate Pairing

We derive results that connect the cokernel pairing to the Weil pairing and Tate profiles. Let $m = \ell$ be prime. When the Sylow ℓ-torsion is symmetric, say $\mathcal{S}_\ell(E) \cong \left(\mathbb{Z}/\ell^f\mathbb{Z}\right)^2$, we find an easy connection to the Weil pairing of degree ℓ^f. Namely, we get $\mathcal{S}_\ell(E) = E[\ell^f]$, and both the Weil pairing of degree ℓ^f as well as the cokernel pairing of degree ℓ describe conditions for a basis P, Q of this object: the Weil pairing $e_{\ell^f}(P, Q)$ has order ℓ^k for $P, Q \in E[\ell^f]$ if and only if P and Q are a basis for $E[\ell^f]$.

Lemma 2. *Let E be an elliptic curve over $\mathbb{F}_q$ with symmetric Sylow ℓ-torsion of order ℓ^f. Let $P, Q \in E(\mathbb{F}_q)$, and let h denote the cofactor with respect to ℓ. Then*

$$\langle P, Q\rangle_\ell \neq 1 \quad \Rightarrow \quad e_{\ell^f}([h]P, [h]Q) \textit{ is a primitive } \ell^f\textit{-th root of unity.}$$

Furthermore, if $P, Q \in E[\ell^f]$, then we get the other direction

$$e_{\ell^f}(P, Q) \textit{ is a primitive } \ell^f\textit{-th root of unity} \quad \Rightarrow \quad \langle P, Q\rangle_\ell \neq 1.$$

Proof. When $\langle P, Q\rangle_\ell \neq 1$, we get that $[h]P$ and $[h]Q$ generate $\mathcal{S}_\ell(E) = E[\ell^f]$, and so the Weil pairing $e_{\ell^f}([h]P, [h]Q)$ is a primitive ℓ^f-th root of unity. Conversely, if $e_{\ell^f}(P, Q)$ is a primitive ℓ^f-th root of unity, then P and Q generate $E[\ell^f] = \mathcal{S}_\ell(E)$, and so $\langle P, Q\rangle_\ell \neq 1$. □

In the above case, we get that both the cokernel pairing and the Weil pairing can be seen as pairings on $E[\ell^f] \times E[\ell^f]$, however, the cokernel pairing maps to μ_ℓ, whereas the Weil pairing maps to μ_{ℓ^f}. When Frobenius acts as a scalar, we can make this connection more explicit, as we see in Section 5.1.

5.1 The cokernel pairing on maximal supersingular curves

For supersingular elliptic curves E over $\mathbb{F}_{p^2}$ with trace $t = \pm 2p$, Frobenius acts as a scalar. We take $t = -2p$ for this example, i.e., E is a maximal supersingular curve of order $(p+1)^2$, although the same reasoning holds for $t = 2p$ for E of order $(p-1)^2$. In this case, the characteristic polynomial of π factors as $(x+p)^2$, hence π acts as $[-p]$, and $E(\mathbb{F}_{p^2}) = E[\pi - 1] = E[p+1]$. We therefore must have symmetric Sylow ℓ-torsion, given by $\ell^f \parallel p+1$. The endomorphism $\frac{\pi-1}{\ell} : E(\mathbb{F}_q) \to E[\ell]$ simplifies to the scalar multiplication by $-\left[\frac{p+1}{\ell}\right]$, that is, we clear everything except the ℓ-torsion.

In this situation, we do not need a basis for $E[\ell]$ to compute the cokernel pairing, as we can replace Algorithm 1 by the scalar multiplication $P_\ell := \Phi_\ell(P) = -\left[\frac{p+1}{\ell}\right]P$. To compute $\langle P, Q\rangle_\ell$, we then compute the Tate pairing $t_\ell(P_\ell, Q)$. This essentially gives a new interpretation of the basis computation approach described in [CJLN+17] using descent:

Corollary 2. *Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$ with trace $t = -2p$ and $\ell^f \parallel p+1$. Let $P, Q \in E(\mathbb{F}_q)$ and let $h = \frac{p+1}{\ell^f}$. Then, if $t_\ell([h \cdot \ell^{f-1}]P, Q) \neq 1$, the points $([h]P, [h]Q)$ form a basis for $E[\ell^f]$.*

Furthermore, this allows us to express the cokernel pairing of degree ℓ in terms of the Weil pairing of degree ℓ^f on such supersingular curves.

Lemma 3. *Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$ with trace $t = -2p$ and with symmetric Sylow ℓ-torsion of order ℓ^f. Let $P, Q \in E[\ell^f]$. Let $\alpha \in \mathbb{Z}/\ell\mathbb{Z}$ such that $[\alpha] = -\left[\frac{p+1}{\ell^f}\right]$ on $E[\ell]$, so that $\Phi_\ell(P) = -\left[\frac{p+1}{\ell}\right]P = [\alpha \cdot \ell^{f-1}]P$. Then*

$$\langle P, Q\rangle_\ell = e_{\ell^f}(P, Q)^{\alpha^2 \cdot \ell^{f-1}}.$$

Proof. Using $e_{nm}(P, Q) = e_n([m]P, Q)$ when $P \in E[nm]$ and $Q \in E[n]$, we get

$$e_{\ell^f}(P, Q)^{\ell^{f-1}} = e_{\ell^f}(P, [\ell^{f-1}]Q) = e_\ell([\ell^{f-1}]P, [\ell^{f-1}]Q).$$

Then, as $\Phi_\ell(P) = [\alpha \cdot \ell^{f-1}]P$, we get

$$\begin{aligned}
\langle P, Q\rangle_\ell &= e_\ell(\Phi_\ell(P), \Phi_\ell(Q)) \\
&= e_\ell([\alpha \cdot \ell^{f-1}]P, [\alpha \cdot \ell^{f-1}]Q) \\
&= e_\ell([\ell^{f-1}]P, [\ell^{f-1}]Q)^{\alpha^2} \\
&= e_{\ell^f}(P, Q)^{\alpha^2 \cdot \ell^{f-1}}.
\end{aligned}$$

□

Remark 6. Although this section describes an alternative way to compute the cokernel pairing on minimal/maximal supersingular curves which does not require a basis for $E[\ell]$, this approach requires either a scalar multiplication by $[\ell^{f-1}]$, using Theorem 5.2 or a Weil pairing of degree ℓ^f, using Theorem 5.3. Both computations are expensive when f is large, and will quickly exceed the cost of Algorithm 3 if $E[\ell]$ is known.

5.2 When Frobenius is not a scalar

The simplified computation from Section 5.1 relies crucially on the fact that we can rewrite the action of $\frac{\pi-1}{\ell}$ as a scalar multiplication. For other curves, even if the Sylow ℓ-torsion is symmetric, which implies that a scalar multiplication $E(\mathbb{F}_q) \to E[\ell]$ exists, the action of $\frac{\pi-1}{\ell}$ is different. For example, let $E/\mathbb{F}_q$ be an ordinary curve with $\mathcal{S}_\ell(E) = E[\ell^f]$. Write $E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ with $n_2 \mid n_1$, so that we may write $n_1 = e \cdot r \cdot \ell^f$ and $n_2 = r \cdot \ell^f$ for some integers e and r. Let $\langle P, Q\rangle$ generate $E(\mathbb{F}_q)$ with P of order n_1 and Q of order n_2. Then one can similarly define a map $E(\mathbb{F}_q) \to E[\ell]$ by $P \mapsto [e \cdot r \cdot \ell^{f-1}]P$ and $Q \mapsto [r \cdot \ell^{f-1}]Q$, that is, we are clearing the cofactor. However, this map is crucially different from $\Phi_\ell = \frac{\pi-1}{\ell}$.

Example 3. We take $p = 535303$, $\ell = 3$ and $f = 3$. Then the curve

$$E/\mathbb{F}_p : y^2 = x^3 + 262034x^2 + x,$$

satisfies $\mathcal{S}_\ell(E) = E[\ell^f]$. As a basis take $P = (533658, 176488)$ and $Q = (402889, 457605)$. By going to $\mathbb{F}_{p^3}$, we are able to compute $\Phi_\ell(P) = (503161, 476634)$ and $\Phi_\ell(Q) = (525015, 190104)$, whereas clearing the cofactor gives us points $P' = (434272, 111323)$ and $Q' = (525015, 345199)$. These are connected by $\Phi_\ell(P) = [2](P' - Q')$ and $\Phi_\ell(Q) = [2]Q'$.

In general, with no assumption on the Sylow ℓ-torsion or the trace of Frobenius, the more natural connection of the cokernel pairing is to Tate profiles, as the following result shows.

Lemma 4. *The cokernel pairing $\langle P, Q\rangle_\ell$ is non-trivial if and only if the Tate profiles $t_{[\ell]}(P)$ and $t_{[\ell]}(Q)$ are non-trivial and independent.*

Proof. This is straightforward from Theorem 3.6 and the fact that non-trivial and independent Tate profiles imply a basis for the Sylow ℓ-torsion $\mathcal{S}_\ell(E)$ [Reij25]. □

We stress the difference between these two objects: the Tate profile explicitly requires a basis for $E[\ell]$ to give coordinates to $\mathcal{S}_\ell(E)/[\ell]\mathcal{S}_\ell(E)$, from which we derive that two independent profiles generate the Sylow ℓ-torsion, after computing the position of these points with respect to the given basis. The cokernel pairing, however, is formulated independently of a basis, and does not give us the position of these points. On the one hand, this implies that we have less information, however, we still have enough information to obtain a basis for the Sylow ℓ-torsion. On the other hand, this implies that we may hope to compute $\langle P, Q\rangle_\ell$ without a basis for $E[\ell]$, which is impossible for the Tate profile.

6 Applications of the Cokernel Pairing

We derive the main application of the cokernel pairing directly from Theorem 3.6, namely, finding a basis for the Sylow ℓ-torsion of an elliptic curve E over a finite field $\mathbb{F}_q$. As isogeny-based cryptography often works with supersingular curves over $\mathbb{F}_{p^2}$, we are specifically interested in finding a basis of $E[\ell^f]$. From a practical point of view, the cokernel allows us to compute an *implicit basis* for $E[\ell^f]$, which improves the efficiency of computing kernel points of order ℓ^f in practice.

6.1 Computing a Sylow torsion basis

Computing a basis for $E[\ell^f]$ is highly optimized for $\ell = 2$ on Montgomery curves using entangled basis generation [ZSPD+18], and can be generalized to other curve models when $E[2]$ is known [Reij25]. Nevertheless, these version of entangled basis generation are unenlightening for $\ell > 2$, and in this case, basis generation algorithms are more ad-hoc, especially when the Sylow torsion is asymmetric.

Using the cokernel pairing, we find an intuitive and straightforward approach, given a basis for the kernel $E[m]$, even for composite m. If we do not care for efficiency and simply want an easy method to find such a basis, we may sample random points in $E(\mathbb{F}_q)$, until we find a pair (P, Q) where $\langle P, Q\rangle_m$ is a primitive m-th root of unity.

A more efficient approach uses a combination of Tate pairings and cokernel pairings. Let T_1, T_2 be a basis for $E[m]$. First, we use the Tate pairings of degree m with kernel points T_1 and T_2 with random cokernel points $P \in E(\mathbb{F}_q)/[m]E(\mathbb{F}_q)$ until we get a non-trivial pair $\zeta_1 = t_m(T_1, P)$ and $\zeta_2 = t_m(T_2, -P)$, i.e., they generate an order-m subgroup of μ_m^2. Given ζ_1 and ζ_2, we compute $\Phi_m(P)$, and sample $Q \in E(\mathbb{F}_q)$ until $\langle P, Q\rangle_m$ is an m-th root of unity, which requires the $\Phi_m(P)$ computed before. After multiplication by $[h]$, we then have a basis for $\mathcal{S}_m(E)$. This is summarized in Algorithm 4

Algorithm 4 Sylow Torsion Basis generation

Input: A basis T_1, T_2 of $E[m]$, and $\zeta_0 = e_m(T_1, T_2) \in \mu_m$.
Output: A basis (P, Q) for $\mathcal{S}_m(E)$

1: Repeat $P \xleftarrow{\$} E(\mathbb{F}_q)$ until $\zeta_1 = t_m(T_1, P)$ and $\zeta_2 \leftarrow t_m(T_2, -P)$ have order m
2: $(a, b) \leftarrow \left(\log_{\zeta_0}(\zeta_2), \log_{\zeta_0}(\zeta_1)\right)$
3: $P_m \leftarrow aT_1 + bT_2$
4: Repeat $Q \xleftarrow{\$} E(\mathbb{F}_q)$ until $\zeta = \langle P, Q\rangle_m = t_m(P_m, Q)$ has order m
5: **return** $([h]P, [h]Q)$

Cost analysis. To compare against the performance of the approach using Tate profiles, we compute the probability of success of both approaches, and the expected number of degree-ℓ Tate pairings we need to compute.

First, both approaches sample a point P at random until the Tate pairings $\zeta_1 = t_\ell(T_1, P)$ and $\zeta_2 = t_\ell(T_2, -P)$ together are non-trivial.[3] The probability of failure is $\frac{1}{\ell^2}$, as this only happens when we sample $P \in [\ell]E(\mathbb{F}_q)$. Hence, on average, this requires $2 \cdot \frac{\ell^2}{\ell^2-1}$ Tate pairings for both approaches.

Both approaches then need to sample a random Q that completes the basis (P, Q). As P generates a subgroup of order ℓ in $E(\mathbb{F}_q)/[\ell]E(\mathbb{F}_q)$, which itself has order ℓ^2, we have a success probability $1 - \frac{\ell}{\ell^2} = \frac{\ell-1}{\ell}$, and so, we expect to require $\ell/(\ell - 1)$ samples of Q on average. Per Q, the approach using the cokernel pairing needs a single Tate pairing

[3] One may also consider the approach of randomly sampling P until ζ_1 is non-trivial, and then computing ζ_2. The expected value is slightly worse for this approach.

to confirm Q is correct. The approach using Tate profiles requires two Tate pairings to confirm Q is independent of P, except when one of ζ_1 or ζ_2 is trivial, in which case it only requires one. Such trivial ζ_i happen with probability $\frac{2\ell-1}{\ell^2-1}$, and so on average, we need $\frac{2\cdot(\ell^2-2\ell)+1\cdot(2\ell-1)}{\ell^2-1} \approx 2 - \frac{2}{\ell+1}$ Tate pairings for Q.

Additionally, the cokernel approaches requires discrete logarithms to compute the coefficients of P_ℓ, whereas the Tate profile approach requires discrete logarithms to verify the correctness of Q. The cost of these is equal for both approaches. Overall, we find that the cokernel approach requires an expected $2 \cdot \frac{\ell^2}{\ell^2-1} + \frac{\ell}{\ell-1} \approx 3 + \frac{1}{\ell+1}$ Tate pairings, and saves roughly a Tate pairing, by directly computing the 'correct' Tate pairing $t_\ell(P_\ell, Q)$, in comparison to the approach using Tate profiles.

6.2 Describing a kernel point of an ℓ^f-isogeny

Most isogeny-based schemes require us to compress a point $K \in E[\ell^k]$ using a deterministic basis (P', Q') of $E[\ell^f]$ as $K = [a]P' + [b]Q'$ with $a, b \in \mathbb{Z}/(\ell^f)\mathbb{Z}$, so that we may communicate K, and therefore the isogeny $E \to E/\langle K \rangle$, using only the values[4] a and b, instead of, e.g., the x-coordinate of K. This is a common technique in many isogeny-based schemes [JACC+17; DKLP+20; BDFL+24; AAAB+25].

We have seen already that we may generalize the requirement on P and Q to a basis of $\mathcal{S}_m(E)$ instead, and even more generally to a basis of $E(\mathbb{F}_q)/[m]E(\mathbb{F}_q)$. The definition of an *implicit basis* [CEMR24] captures the difference between a basis for $E(\mathbb{F}_q)/[m]E(\mathbb{F}_q)$ and $\mathcal{S}_m(E)/[m]\mathcal{S}_m(E)$.

Definition 5. Let $P, Q \in E(\mathbb{F}_q)$. We say that (P, Q) is an *implicit basis* for $\mathcal{S}_m(E)$ if there is an $h \in \mathbb{Z}_{>0}$, co-prime to m, such that $([h]P, [h]Q)$ is a basis for $\mathcal{S}_m(E)$.

Given a deterministically-sampled implicit basis (P, Q), we can similarly write $K = [a]([h]P) + [b]([h]Q)$. The gain is that we may now compute K as $K = [h]([a]P + [b]Q)$, which saves one application of the map $[h]$. For large cofactors, saving such a scalar multiplication can be significant [CEMR24]. That is, we may consider the implicit basis (P, Q) as an actual basis for compression, but the points themselves are not in $\mathcal{S}_m(E)$, only after applying the map $[h] : E(\mathbb{F}_q) \to \mathcal{S}_m(E)$.

The cokernel pairing allows us to generate a basis (P, Q) for $E(\mathbb{F}_q)/[m]E(\mathbb{F}_q)$, which is by definition an implicit basis for $\mathcal{S}_m(E)$. For example, in Algorithm 4, we may simply ignore the last multiplication by $[h]$ and return the implicit basis P, Q. Thus, the cokernel pairing gives us a very simple and natural tool to compute implicit bases (P, Q), summarized in the following result.

Corollary 3. *Let $P, Q \in E(\mathbb{F}_q)$. When $\langle P, Q \rangle_m$ is a primitive m-th root of unity, the pair (P, Q) is an implicit basis of $\mathcal{S}_m(E)$. The cofactor $h \in \mathbb{Z}_{>0}$ maps the implicit basis (P, Q) to an explicit basis $([h]P, [h]Q)$ of $\mathcal{S}_m(E)$.*

We conclude that we only need an implicit basis (P, Q) of $\mathcal{S}_m(E)$ to describe an isogeny effectively, and the cokernel pairing gives us the exact criterion for when P and Q are an implicit basis. Although torsion basis generation and point compression are elementary building blocks of isogeny-based cryptography, they are a significant part of the computational cost of isogeny-based primitives. Hence, the simplified approach using the cokernel pairing may improve several isogeny-based schemes.

[4] Often we only need one of these two: as we need K of order ℓ^f, either a or b is invertible, and we may choose P and Q in such a way that we can always express a generator of the same kernel by $P + a^{-1}bQ$.

7 Future Work

We have introduced the cokernel pairing and explored initial computations, applications, and connections to the Weil and Tate pairing. This opens up many questions for future work.

The main question is on an improved computation of the cokernel pairing. Both Algorithm 2 and Algorithm 3 require knowledge of a basis of $E[m]$ and explicitly computes one or both of $\Phi_m(P)$ and $\Phi_m(Q)$. Remarkably, the Tate pairing $e_m(P, \Phi_m(Q))$ may be computed without explicitly computing $\Phi_m(Q)$. We may hope that we can compute $\langle P, Q \rangle_m$ similarly, without a direct computation of Φ_m, or knowledge of the $E[m]$, although this seems like an extraordinary result. On the other hand, we were unable to show that a cokernel pairing compuation *needs* to compute Φ_m or $E[m]$, and it seems difficult to show that such a computation is required. In fact, in the peculiar case of maximal supersingular elliptic curves, we are able to compute the cokernel pairing without knowledge of $E[m]$, but the computation of Φ_m in such situations is rather expensive. Future work may explore the usage of cubical arithmetic [Rob24] for efficient computations of cokernel pairings.

Another direction is in generalizations of the cokernel pairing. We may similarly explore the cokernel pairing defined on more general abelian varieties, or hope to give a 'geometric interpretation' of the cokernel pairing in terms of cohomology. Another direction for generalization is inspired by [CHMM+23], which explores Tate pairings $T_f^{\alpha}(P, Q)$ defined as $e_f(P, \alpha(R))$ for α a suitable endomorphism and $f(R) = Q$, which coincides with the f-Tate pairing for $\alpha = \pi - 1$. For the cokernel pairing, we could similarly replace the role of $\pi - 1$ either in one argument, or in both arguments, given suitable endomorphisms α, β.

A more concrete direction of research is related to entangled basis generation [ZSPD+18], which results in a basis (P, Q) for $E[2^f]$ on specific supersingular elliptic curves $E/\mathbb{F}_{p^2}$ by a rather arbitrary choice of x_P and x_Q. Understanding why this choice of x_P and x_Q ensures $\langle P, Q \rangle_2 \neq 1$ may help in generalizing entangled basis generation to primes $\ell > 2$ or genus $g > 1$.

References

[AAAB+25] Marius A. Aardal et al. SQIsign 2.0: Algorithm specifications and supporting documentation. Technical report, 2025.

[BDFL+24] Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski. Sqisign2d-west - the fast, the small, and the safer. In Kai-Min Chung and Yu Sasaki, editors, *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part III*, volume 15486 of *Lecture Notes in Computer Science*, pages 339–370. Springer, 2024. ISBN: 978-981-96-0890-4. DOI: 10.1007/978-981-96-0891-1_11.

[BDLS20] Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. Faster computation of isogenies of large prime degree. In *ANTS-XIV-14th Algorithmic Number Theory Symposium*, volume 4, pages 39–55. Mathematical Sciences Publishers, 2020.

[BF01] Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In *Annual international cryptology conference*, pages 213–229. Springer, 2001.

[BGLS03] Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In *Advances in Cryptology—EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4–8, 2003 Proceedings 22*, pages 416–432. Springer, 2003.

[BKLS02] Paulo S. L. M. Barreto, Hae Y. Kim, Ben Lynn, and Michael Scott. Efficient algorithms for pairing-based cryptosystems. In *Advances in Cryptology—CRYPTO 2002: 22nd Annual International Cryptology Conference Santa Barbara, California, USA, August 18–22, 2002 Proceedings 22*, pages 354–369. Springer, 2002.

[BLS01] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. In *International conference on the theory and application of cryptology and information security*, pages 514–532. Springer, 2001.

[BLS04] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. Efficient implementation of pairing-based cryptosystems. *Journal of Cryptology*, 17:321–334, 2004.

[Bru11] Peter Bruin. The tate pairing for abelian varieties over finite fields. *Journal de theorie des nombres de Bordeaux*, 23(2):323–328, 2011.

[CEMR24] Maria Corte-Real Santos, Jonathan Komada Eriksen, Michael Meyer, and Krijn Reijnders. Aprèssqi: extra fast verification for sqisign using extension-field signing. In *Advances in Cryptology - EUROCRYPT 2024 - 43nd Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2024.

[CHMM+23] 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 *Annual International Cryptology Conference*, pages 762–792. Springer, 2023.

[CJLN+17] Craig Costello, David Jao, Patrick Longa, Michael Naehrig, Joost Renes, and David Urbanik. Efficient compression of sidh public keys. In *Advances in Cryptology–EUROCRYPT 2017: 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30–May 4, 2017, Proceedings, Part I 36*, pages 679–706. Springer, 2017.

[CR25] Maria Corte-Real Santos and Krijn Reijnders. Return of the kummer: a toolbox for genus-2 cryptography. *IACR Communications in Cryptology*, 2(3), 2025.

[DEFM+25] Pierrick Dartois, Jonathan Komada Eriksen, Tako Boris Fouotsa, Arthur Herlédan Le Merdy, Riccardo Invernizzi, Damien Robert, Ryan Rueger, Frederik Vercauteren, and Benjamin Wesolowski. PEGASIS: practical effective class group action using 4-dimensional isogenies. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology - CRYPTO 2025 - 45th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2025, Proceedings, Part I*, volume 16000 of *Lecture Notes in Computer Science*, pages 67–99. Springer, 2025. ISBN: 978-3-032-01854-0. DOI: 10.1007/978-3-032-01855-7_3.

[DKLP+20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 64–93, Cham. Springer International Publishing, 2020. ISBN: 978-3-030-64837-4.

[EVM12] Bas Edixhoven, Gerard Van der Geer, and Ben Moonen. Abelian varieties. *preprint*, 331, 2012.

[FR94] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of computation*, 62(206):865–874, 1994.

[Gal05] SD Galbraith. Pairings. london mathematics society lecture note series, vol. 317, 2005.

[GHS02] Steven D Galbraith, Keith Harrison, and David Soldera. Implementing the tate pairing. In *International Algorithmic Number Theory Symposium*, pages 324–337. Springer, 2002.

[HSSI99] Ryuichi Harasawa, Junji Shikata, Joe Suzuki, and Hideki Imai. Comparing the mov and fr reductions in elliptic curve cryptography. In *Advances in Cryptology—EUROCRYPT'99: International Conference on the Theory and Application of Cryptographic Techniques Prague, Czech Republic, May 2–6, 1999 Proceedings 18*, pages 190–205. Springer, 1999.

[HSV06] F. Hess, N.P. Smart, and F. Vercauteren. The eta pairing revisited. *IEEE Transactions on Information Theory*, 52(10):4595–4602, 2006. DOI: 10.1109/TIT.2006.881709.

[JACC+17] David Jao, Reza Azarderakhsh, Matt Campagna, Craig Costello, Luca de Feo, Basil Hess, Amir Jalili, Brian Koziel, Brian Lamacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, and David Urbanik. SIKE: Supersingular Isogeny Key Encapsulation. Technical report, 2017.

[Jou02] Antoine Joux. The weil and tate pairings as building blocks for public key cryptosystems: survey. In *International Algorithmic Number Theory Symposium*, pages 20–32. Springer, 2002.

[Jou04] Antoine Joux. A one round protocol for tripartite diffie–hellman. *Journal of cryptology*, 17(4):263–276, 2004.

[KT18] Takeshi Koshiba and Katsuyuki Takashima. New assumptions on isogenous pairing groups with applications to attribute-based encryption. In *International Conference on Information Security and Cryptology*, pages 3–19. Springer, 2018.

[Lic69] Stephen Lichtenbaum. Duality theorems for curves over p-adic fields. *Inventiones mathematicae*, 7(2):120–136, 1969.

[LR16] David Lubicz and Damien Robert. Arithmetic on abelian and Kummer varieties. *Finite Fields and Their Applications*, 39:130–158, May 2016. DOI: 10.1016/j.ffa.2016.01.009. eprint: 2014/493, HAL: hal-01057467.

[LWXZ24] Kaizhan Lin, Weize Wang, Zheng Xu, and Chang-An Zhao. A faster software implementation of sqisign. *IEEE Transactions on Information Theory*, 2024.

[Mil04] Victor S Miller. The Weil pairing, and its efficient calculation. *Journal of cryptology*, 17(4):235–261, 2004.

[MOV91] Alfred Menezes, Tatsuaki Okamoto, and Scott Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. In *Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing*, STOC '91, pages 80–89, New Orleans, Louisiana, USA. Association for Computing Machinery, 1991. ISBN: 0897913973. DOI: 10.1145/103418.103434.

[MS24] 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.

[Reij23] Krijn Reijnders. Effective Pairings in Isogeny-based Cryptography. In *International Conference on Cryptology and Information Security in Latin America*, pages 109–128. Springer, 2023.

[Reij25] Krijn Reijnders. The Tate Profile. In *Progress in Cryptology - LATINCRYPT 2025 - 9th International Conference on Cryptology and Information Security in Latin America, LATINCRYPT 2025, Medellin, Colombia, October 1-3, 2025, Proceedings*. Springer, 2025.

[Rob23] Damien Robert. The geometric interpretation of the tate pairing and its applications. Cryptology ePrint Archive, Paper 2023/177, 2023. URL: `https://eprint.iacr.org/2023/177`.

[Rob24] Damien Robert. Fast pairings via biextensions and cubical arithmetic. April 2024. eprint: 2024/517, HAL: hal-04848028.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[Sil10] Joseph H Silverman. A survey of local and global pairings on elliptic curves and abelian varieties. In *Pairing-Based Cryptography-Pairing 2010: 4th International Conference, Yamanaka Hot Spring, Japan, December 2010. Proceedings 4*, pages 377–396. Springer, 2010.

[Sta08] Katherine Stange. *Elliptic nets and elliptic curves*. PhD thesis, Brown University, 2008. URL: `https://repository.library.brown.edu/studio/item/bdr:309/PDF/`.

[Sta11] Katherine Stange. Elliptic nets and elliptic curves. *Algebra & Number Theory*, 5(2):197–229, 2011.

[Tat57] John Tate. Wc-groups over p-adic fields. *Séminaire Bourbaki*, 4:265–277, 1957.

[Tat62] John Tate. Duality theorems in Galois cohomology over number fields. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, pages 288–295, 1962.

[Vél71] Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes-Rendus de l'Académie des Sciences*, 273:238–241, 1971. URL: `https://gallica.bnf.fr/ark:/12148/cb34416987n/date`. `https://gallica.bnf.fr/ark:/12148/cb34416987n/date`.

[Ver09] Frederik Vercauteren. Optimal pairings. *IEEE transactions on information theory*, 56(1):455–461, 2009.

[Wei40] André Weil. Sur les fonctions algébriquesa corps de constantes fini. *CR Acad. Sci. Paris*, 210(1940):592–594, 1940.

[ZSPD+18] Gustavo HM Zanon, Marcos A Simplicio, Geovandro CCF Pereira, Javad Doliskani, and Paulo SLM Barreto. Faster key compression for isogeny-based cryptosystems. *IEEE Transactions on Computers*, 68(5):688–701, 2018.

A Galois Cohomology and the Cokernel Pairing

Silverman [Sil10] gives us an interpretation of the Weil and Tate pairing on abelian varieties in terms of (Galois) cohomology. A rich treatment of this subject for the Tate pairing is given by Robert [Rob23]. Here, we repeat the main ingredients from [Sil10] to describe the Weil and Tate pairing in terms of Galois cohomology, and then sketch approaches towards a cohomological description of the (unreduced) cokernel pairing.[5] We describe this section for abelian varieties A over a finite field k, as it is more enlightening than the case of elliptic curves.

A.1 The First Cohomology Groups

The cohomological interpretation of pairings requires some knowledge of the first cohomology groups, H^0, H^1 and H^2 for groups M on which $G_k = \mathrm{Gal}(\overline{k}/k)$ acts, so that $\pi(m)$ is well-defined for any $m \in M$. We explore these cohomology groups for $M = \overline{k}$, $M = \mu_m$, $M = A$ and $M = A[m]$, where A is an abelian variety over a field k. This is enough for a cohomological interpretation of the Tate pairing, and for a first approach towards a cohomological interpretation of the cokernel pairing. For the cokernel pairing, we will assume k is finite, as this has a significant impact on our deriviation. Hence, in this case, G_k is generated by π, and a map $G_k \to M$ may be defined by the image of π. We will use multiplicative notation, as we often find ourselves working in μ_m.

The zero-th group. To start, $H^0(G_k, M)$ is easy to understand: it contains the elements in M fixed by G_k, or in other words, the k-rational elements $M(k)$.

The higher groups. We define the higher groups $H^1(G_k, M)$ and $H^2(G_k, M)$ as equivalence classes of *cocycles* and *coboundaries*. Concretely, a 1-cocycle is a function $f : G_k \to M$ satisfying

$$f(\sigma \cdot \tau) = \sigma(f(\tau)) \cdot f(\sigma), \quad \text{for all } \sigma, \tau \in G_k,$$

and a 1-coboundary is a function $g : G_k \to M$ such that

$$g(\tau) = \tau(m)/m, \quad \text{for some } m \in M.$$

We can then define $H^1(G_k, M)$ as the group of 1-cocycles modulo the group of 1-coboundaries. Similarly, for $H^2(G_k, M)$, we define a 2-cocycle as a function $f : G_k \times G_k \to M$ satisfying

$$\sigma(f(\tau, \mu)) = f(\sigma \cdot \tau, \mu) \cdot f(\sigma, \tau)/f(\sigma, \tau \cdot \mu), \quad \text{for all } \sigma, \tau, \mu \in G_k,$$

and a 2-coboundary is a function $g : G_k \times G_k \to M$ satisfying

$$g(\sigma, \tau) = \sigma(h(\tau)) \cdot h(\tau)/h(\sigma \cdot \tau),$$

for some map $h : G_k \to M$. We can then define $H^2(G_k, M)$ as the group of 2-cocycles modulo the group of 2-coboundaries. The usefulness of these groups comes from the fact that we may associate a long exact sequence in the groups H^i to a short exact sequence. For our purposes, we are interested in the short exact sequence

$$0 \to A[m] \to A \xrightarrow{[m]} A \to 0,$$

associated to $[m] : A \to A$, from which we derive a long exact sequence

[5] Readers that are only interested in concrete computation and application of the cokernel pairing may skip this section. Readers interested in more details of the cohomological construction are advised to explore [Sil10] and then [Rob23].

$$\begin{tikzcd}
0 \arrow[r] & H^0(G_k, A[m]) \arrow[r] & H^0(G_k, A) \arrow[r] & H^0(G_k, A) \arrow[dll, rounded corners, "\delta"] \\
& H^1(G_k, A[m]) \arrow[r] & H^1(G_k, A) \arrow[r] & H^1(G_k, A) \arrow[dll, rounded corners, "\delta"] \\
& H^2(G_k, A[m]) \arrow[r] & H^2(G_k, A) \arrow[r] & H^2(G_k, A)
\end{tikzcd}$$

which gives us a connecting homomorphism $\delta : H^0(G_k, A) \to H^1(G_k, A[m])$. When we quotient out the image of $[m]$ on $H^0(G_k, A)$, and use the identity $H^0(G_k, M) = M(k)$, this gives us a map

$$A(k)/[m]A(k) \to H^1(G_k, A[m]), \quad [P] \mapsto \delta_P$$

where $\delta_P : G_k \to A[m]$ is some 1-cocycle. This map will be fundamental to construct the Tate pairing, and to study the cokernel pairing from a cohomological point of view. Furthermore, we need a few key facts, which we can derive from the long exact sequence

$$1 \to \mu_m \to \overline{k}^* \to \overline{k}^* \to 1,$$

associated to the exponentiation-by-m map $\overline{k}^* \to \overline{k}^*$.

Lemma 5. *The following holds:*

1. $H^1(G_k, \overline{k}^*) = 0$,
2. $H^1(G_k, \mu_m) \cong k^*/k^{*,m}$,
3. $H^2(G_k, \mu_m) \cong H^2(G_k, \overline{k}^*)[m]$,
4. *When k is finite,* $H^2(G_k, \overline{k}^*) = 0$.

The first two statements are commonly known as Hilbert's Theorem 90. The third statement follows from the first two by the derived long exact sequence. The fourth statement is related to Brauer groups, but for our purposes, we only need to know that this group is trivial.

The isomorphism in the second statement can be made more explicit: given $a \in k^*$, take an m-th root $\alpha \in \overline{k}^*$ so that $\alpha^m = a$. This identifies $a \in k^*$ with a 1-cocycle $\delta_a \in H^1(G_k, \mu_m)$ defined by $\delta_a(\sigma) = \frac{\sigma(\alpha)}{\alpha}$. Note that for elements $a \in k^{*,m}$, we find $\alpha \in k^*$, and so $\sigma(\alpha) = \alpha$ for all $\sigma \in G_k$.

A.2 The Tate Pairing

Given the map $\delta : A(k)/[m]A(k) \to H^1(G_k, A[m])$ derived from the long exact sequence, we may apply the Weil pairing with a point $Q \in \widehat{A}[m](k)$ to define a 1-cocycle in $H^1(G_k, \mu_m)$ as follows.

$$A(k)/[m]A(k) \times \widehat{A}[m](k) \to H^1(G_k, \mu_m), \quad (P, Q) \mapsto (\delta_{P,Q} : \sigma \mapsto e_m(Q, \delta_P(\sigma)))\,.$$

Using the isomorphism $H^1(G_k, \mu_m) \cong k^*/k^{*,m}$, we find the unreduced Tate pairing

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

When we compute this pairing in practice, we may forget this cohomological origin of the Tate pairing. However, we need to use several of the above concepts to define an unreduced cokernel pairing via a similar cohomologic construction. In particular, we should be slightly more precise about the exact construction above. In strictly cohomological terms, using $A(k) = H^0(G_k, A)$ and $\widehat{A}[m](k) = H^0(G_k, \widehat{A}[m])$, we can rewrite the first step as a map

$$H^0(G_k, \widehat{A}[m]) \times H^0(G_k, A) \xrightarrow{(1,\delta)} H^0(\widehat{A}[m]) \times H^1(G_k, A[m]).$$

Now, the second step, applying the Weil pairing, is in fact a map $H^1(G_k, A[m] \otimes \widehat{A}[m]) \to H^1(G_k, \mu_m)$. Luckily, the required map that connects these steps is a well-known map called the *cup product*

$$\cup : H^0(G_k, \widehat{A}[m]) \times H^1(G_k, A[m]) \to H^1(G_k, A[m] \otimes \widehat{A}[m]).$$

The cup products exists more generally as a map $H^i \times H^j \to H^{i+j}$, which we apply for $i = 0$ and $j = 1$ here. Altogether, we may compose $(1, \delta)$, $\cup$, and e_m to get a map

$$\begin{aligned} H^0(G_k, \widehat{A}[m]) \times H^0(G_k, A) \to \quad & H^1(G_k, \mu_m), \\ (Q, P) \quad \mapsto & \left(\delta_{P,Q} : \sigma \mapsto e_m(Q, \delta_P(\sigma))\right). \end{aligned}$$

The unreduced Tate pairing that we use in practice then identifies the former groups with explicit points on $A(k)$ and $\widehat{A}(k)$, and the latter group with $k^*/k^{*,m}$.

A.3 The Cokernel Pairing

We now sketch some approaches towards a cohomological interpretation of an (unreduced) cokernel pairing. As before, we get the map δ from the long exact sequence

$$\ldots \to H^0(G_k, A) \xrightarrow{[m]} H^0(G_k, A) \xrightarrow{\delta} H^1(G_k, A[m]) \to \ldots$$

and a similar map for the dual as $\widehat{\delta} : H^0(G_k, \widehat{A}) \to H^1(G_k, \widehat{A}[m])$. Thus, we may diagonalize these maps to get

$$H^0(G_k, A) \times H^0(G_k, \widehat{A}) \xrightarrow{(\delta,\widehat{\delta})} H^1(G_k, A[m]) \times H^1(G_k, \widehat{A}[m]). \tag{8}$$

First try. We might have hoped that, using δ, $\widehat{\delta}$, and again e_m, we may associate to (P, Q) the 1-cochain $g_{P,Q} : G_k \to \mu_m$ defined by

$$g_{P,Q} : \ \sigma \mapsto e_m(\delta_P(\sigma), \widehat{\delta}_Q(\sigma)).$$

However, $g_{P,Q}$ is not a 1-cocycle, as we can readily compute from the required conditions.

Second try. Repeating the logic from before, we may use the cup product $\cup$ for $i = 1$ and $j = 1$ to get a map

$$H^1(G_k, A[m]) \times H^1(G_k, \widehat{A}[m]) \xrightarrow{\cup} H^2(G_k, A[m] \otimes \widehat{A}[m]). \tag{9}$$

Again, this allows us to apply the Weil pairing $e_m : A[m] \times \widehat{A}[m] \to \mu_m$ to any 2-cocycle to get

$$H^2(G_k, A[m] \otimes \widehat{A}[m]) \xrightarrow{e_m} H^2(G_k, \mu_m). \tag{10}$$

With $H^0(G_k, A) = A(k)$, the composition of $(\delta, \widehat{\delta})$, $\cup$, and e_m then gives a map

$$\begin{aligned} A(k) \times \widehat{A}(k) &\to H^2(G_k, \mu_m) \\ (P, Q) &\mapsto X_{P,Q}. \end{aligned}$$

and we can explicitly describe $X_{P,Q} : G_k \times G_k \to \mu_m$ as the 2-cochain

$$X_{P,Q} : (\sigma, \tau) \mapsto e_m(\delta_P(\sigma), \sigma(\delta_Q(\tau))).$$

Tate [Tat57] shows that for p-adic fields $K/\mathbb{Q}_p$, the pairing

$$H^1(G_K, A[m]) \times H^1(G_K, \widehat{A}[m]) \to H^2(G_K, \mu_m)$$

is a non-degenerate pairing,[6] and for such fields K, we have $H^2(G_K, \mu_m) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$. However, in our case, where k is a finite field, Theorem A.1 tells us $H^2(G_k, \mu_m) = 0$ and so we find a most degenerate pairing.

Third try. From intuition, we know that the reduced cokernel pairing $\langle P, Q\rangle_m$ should equal the reduced Tate pairing $t_\ell(\pi(R) - R, Q)$ for $[\ell]R = P$, and symmetrically also $t_m(\pi(R') - R', P)$ for $[m]R' = Q$. This inspires us to fix an argument in $g_{P,Q}$ or $X_{P,Q}$. Dropping subscripts, we define

$$X_{\sigma,-} \ : \tau \mapsto e_m(\delta_P(\sigma), \sigma(\delta_Q(\tau))), \quad X_{-,\tau} \ : \sigma \mapsto e_m(\delta_P(\sigma), \sigma(\delta_Q(\tau))).$$

Lemma 6. *$X_{\sigma,-}$ and $X_{-,\tau}$ are 1-cocycles for all $\sigma, \tau \in G_k$.*

Proof. We show that $X_{\sigma,-}$ satisfies the 1-cocycle condition for any σ and $X_{-,\tau}$ follows naturally. First, recall that δ_P is a 1-cocycle, e.g., $\delta_P(\tau \cdot \mu) = (\tau \cdot \mu)(R) - R = \tau(\mu(R) - R) + \tau(R) - R = \tau(\delta_P(\mu)) + \delta_P(\tau)$ for any $\tau, \mu \in G_k$. Using that G_k is abelian, we find

$$\begin{aligned} X_{\sigma,-}(\tau \cdot \mu) &= e_m(\delta_P(\sigma), \sigma(\delta_Q(\tau \cdot \mu))) \\ &= e_m(\delta_P(\sigma), (\sigma \cdot \tau)(\delta_Q(\mu))) \cdot e_m(\delta_P(\sigma), \sigma(\delta_Q(\tau))) \\ &= \tau(X_{\sigma,-}(\mu)) \cdot X_{\sigma,-}(\tau) \end{aligned}$$

where the last line uses $\tau(\delta_P(\sigma)) = \delta_P(\sigma)$ as $\delta_P(\sigma)$ is now a fixed point in $A[m] \subseteq A(\mathbb{F}_q)$. □

We get a map to $H^1(G_k, H^1(G_k, \mu_m))$ given a pair of points (P, Q), by

$$\begin{aligned} A(k) \times \widehat{A}(k) &\to H^1(G_k, H^1(G_k, \mu_m)) \\ (P, Q) &\mapsto \ (\ X : \sigma \mapsto X_{\sigma,-}\ ), \end{aligned}$$

where $X_{\sigma,-} \ : \tau \mapsto e_m(\ \delta_P(\sigma),\ \sigma\delta_Q(\tau)\ ) \in H^1(G_k, \mu_m)$, and symmetrically another map using $X_{-,\tau}$. In the case that we are interested in, e.g., k is finite and $A[m] \subseteq A(k)$, this definition seems to coincide with the unreduced pairing values we may expect to obtain using the interpretation as an unreduced Tate pairing with respect to $\Phi_m(P)$, resp. $\Phi_m(Q)$. Nevertheless, the approach feels somewhat unnatural and teleological.

[6] A specific example of local Tate duality.