The arithmetic of theta groups and biextensions of abelian varieties

DAMIEN ROBERT

Abstract. We investigate the use of biextensions and the theta groups to understand isogenies. Namely we show that every isogeny of odd degree between elliptic curves lift canonically to theta groups and we give an algorithm to compute this lfit. We discuss some consequences of this for the DLP.

1. Introduction

In this article, we study various consequences of the following result, with follows from the algebraic theory of the theta group as constructed by Mumford [Mum66; Mum67a; Mum67b].

Theorem 1.1. *Let $f : (A, \mathscr{L}) \to (B, \mathscr{M})$ be an N-isogeny between ppavs, with N odd. Assume that $\mathscr{L}$ and $\mathscr{M}$ are symmetric. Let m be an odd integer prime to N. Then $f : A[m] \to B[m]$ lifts canonically to a map of theta groups $\tilde{f} : G(\mathscr{L}^m) \to G(\mathscr{M}^m)$, sending symmetric elements to symmetric elements.*

Proof. Since f is an N-isogeny, we have an isomorphism $f^*\mathscr{M} \simeq \mathscr{L}^N$. The descent of $\mathscr{L}^N$ to $\mathscr{M}$ is encoded by a symmetric lift $\widetilde{K}$ of $K = \operatorname{Ker} f$ in the theta group $G(\mathscr{L}^N)$. Since $\mathscr{M}$ is symmetric, $\widetilde{K}$ is composed of symmetric elements. Since N is odd, if $P \in K$ is of order $N' \mid N$, there is a unique symmetric element $g_P \in G(\mathscr{L}^N)$ of the same order N'. Hence $\widetilde{K}$ is uniquely determined. We have a canonical isomorphism $F : Z(\widetilde{K})/\widetilde{K} \simeq G(\mathscr{M})$, which commutes with δ_{-1} since $\widetilde{K}$ is symmetric, so sends symmetric element to symmetric elements

There is also a map $\varepsilon_m : G(\mathscr{L}^N) \to G(\mathscr{L}^{mN})$, which commutes with δ_{-1}, so $\varepsilon_m(\widetilde{K}) \subset G(\mathscr{L}^{mN})$ is also a symmetric lift of K in $G(\mathscr{L}^{mN})$. It encodes the descent of $\mathscr{L}^{Nm}$ into $\mathscr{M}^m$. We obtain a canonical isomorphism $F_m : Z(\varepsilon_m(\widetilde{K}))/\varepsilon_m(\widetilde{K}) \simeq G(\mathscr{M}^m)$, commuting with δ_{-1}.

Finally, there is also a map $\varepsilon_N : G(\mathscr{L}^m) \to G(\mathscr{L}^{mN})$. It lends inside $Z(\varepsilon_m(\widetilde{K}))$ because the orthogonal $K^\perp$ of K with respect to the Weil pairing $e_{W,\mathscr{L}}$ on $A[mN]$ contains $A[m]$.

Our map is $\tilde{f} = F_m \circ \varepsilon_N : G(\mathscr{L}^m) \to G(\mathscr{M}^m)$. If $\alpha \in \overline{k}^*$, $\tilde{f}(\alpha) = \alpha^N$, so its kernel is $\{\alpha \in \overline{k}^* \mid \alpha^N = 1.\}$. □

We will give an explicit version of Theorem 1.1 for elliptic curves in Section 2 and we give some applications in Appendix A.1.

2. The theta group of a divisor on an elliptic curve

Let E/k be an elliptic curve and D a divisor. Its algebraic equivalence class is determined by its degree $\deg D \in \mathbb{Z}$. We have a morphism $\Phi_D : E \to \hat{E}, P \in E \mapsto t_{P,*}D - D$. This map is an isogeny iff $\deg D \neq 0$, in which case $K(D) := \operatorname{Ker} \Phi_D = E[\deg D]$ (provided

Date: August 11, 2023.

the degree is prime to the characteristic). If $\deg D = 0$, then $\operatorname{Ker} \Phi_D = E$. The divisor D is ample iff $\deg D > 0$.

2.1. The theta group.

Definition 2.1. Assume that D is ample. The theta group $G(D)$ is given by tuples $(P, f_{D,P})$ with $P \in \operatorname{Ker} \Phi_D = E[\deg D]$, and $f_{D,P}$ any function with divisor $t_{P,*}D - D$. The composition law is given by $(P, f_{D,P}).(Q, f_{D,Q}) = (P + Q, f_{D,P}(x) f_{D,Q}(x - P))$. In particular, $(P, f_{D,P})^{-1} = (-P, f_{D,P}^{-1}(x + P))$.

The theta group acts on $\Gamma(D)$ via $(P, f_{D,P}) \cdot s = f_{D,P}(x) s(x-P)$. The action is irreducible (Mumford).

We remark that for any divisor D, we can build up a function of the type $f_{D,P}$ by combining functions $\mu_{P,Q}$ with divisor $(P) + (Q) - (P+Q) - (0_E)$, as is done for pairing computations.

Let $g_P = (P, f_{D,P})$ and $g_Q = (Q, f_{D,Q})$ in $G(D)$. Then $g_P.g_Q = (P+Q, f_{D,P}(x) f_{D,Q}(x-P))$ while $g_Q.g_P = (P+Q, f_{D,Q}(x) f_{D,P}(x-Q))$. So $g_Q.g_P = \alpha g_P.g_Q$ with $\alpha = f_{D,Q}(x)/f_{D,Q}(x-P) \cdot f_{D,P}(x-Q)/f_{D,P}(x) = e_{W,D}(P,Q)$. The commutator pairing $[g_P, g_Q]$ is the Weil pairing $e_{W,D}(P,Q)$.

We also check that if $g_P = (P, f_{D,P})$, then $g_P^m = (mP, f_{D,P}(x) f_{D,P}(x-P) \dots f_{D,P}(x - (m-1)P))$. Thus g_P is of order n iff $f_{D,P}(x) f_{D,P}(x-P) \dots f_{D,P}(x-(n-1)P) = 1$.

2.2. 2-cocycle.

Pick any section $s : K(D) \to G(D)$. Say take for $f_{D,P}$ be a function appropriately normalised at 0_E. Another solution is to take a symmetric lift (see Section 2.4). Then we can work with $G(D)$ by representing an element $g \in G(D)$ by a tuple (P, γ), where γ represents the function $\gamma s(P)$. The group law is then given by $(P, \gamma_P).(Q, \gamma_Q) = (P + Q, \gamma_P \gamma_Q S(P,Q))$ where S is the 2-cocycle associated to s: $s(P)s(Q) = S(P,Q)s(P+Q)$. In practice, this all boils down to elementary computation with Miller functions of the form $\mu_{P,Q}$.

Notice that this 2-cocycle is normalized $S(T,0) = S(0,T) = 1$, and that since the commutator pairing is the Weil pairing, we have

$$S(T_1, T_2) = e_{W,\ell}(T_1, T_2) S(T_2, T_1). \tag{1}$$

Hence the 2-cocycles describing the theta group may be seen as a generalisation of the Weil pairing.

Example 2.2. Take $D = d(0_E)$, $s(P) = (P, f_{d,P})$ where $f_{d,P}$ is the usual Miller function normalised at (0_E), we compute $S(P,Q) = f_{d,Q}(-P)$. So the corresponding 2-cocycle is the usual non reduced Tate pairing (up to a sign)!

2.3. Isomorphisms of theta groups.

The isomorphism class of the theta group depends only on the line bundle $\mathcal{L}(D)$ associated to D. If $D' = D + \operatorname{div}(g)$, an explicit isomorphism is given by

$$(P, f_{D,P}) \mapsto (P, f_{D,P}(x) g(x-P)/g(x)). \tag{2}$$

This isomorphism commutes with the action on sections via $\Gamma(D) \simeq \Gamma(D'), s \mapsto s/g$.

If $D = t_{c,*}D$, we also have an isomorphism of $G(D)$ with $G(D')$ via

$$(P, f_{D,P}) \mapsto (P, t_{c,*}f_{D,P}(x) = f_{D,P}(x-c)), \tag{3}$$

with is compatible with the action via $\Gamma(D) \simeq \Gamma(D'), s(x) \mapsto t_{c,*}(s)(x) = s(x-c)$.

Any divisor D of degree d is linearly equivalent to a divisor of the form $D' = (P) + (d-1)(0_E)$, and if $P = dP_0$, then $t_{P_0,*}D'$ is linearly equivalent to $d(0_E)$. Hence by Equations (2) and (3), $G(D)$ is isomorphic (over the field where P_0 is defined) to $G(d(0_E))$.

If $Q \in K(D)$, $t_{Q,*}D$ is linearly equivalent to D by definition. Write $t_{Q,*}D = D + \mathrm{div}(f_{D,Q})$, $g_Q = (Q, f_{D,Q})$, combining Equations (2) and (3), we obtain an automorphism of $G(D)$ given by

$$g_P = (P, f_{D,P}) \mapsto (P, f_{D,P}(x-Q) f_{D,Q}(x)/f_{D,Q}(x-P)) = g_Q g_P g_Q^{-1} = (P, e_{W,D}(P,Q) f_{D,P}). \tag{4}$$

2.4. **Symmetric divisors.** If $\mathcal{L}(D)$ is symmetric, then $[-1]^*D$ is linearly equivalent to D. Write $D = -D + \mathrm{div}(g)$. We have an isomorphism $G(D) \simeq G(-D)$,

$$(P, f_{D,P}) \mapsto (-P, [-1]^* f_{D,P}(x) = f_{D,P}(-x)). \tag{5}$$

Combining with the isomorphism form Equation (2), we obtain an involution

$$\delta_{-1} : G(D) \to G(D), (P, f_{D,P}) \mapsto (-P, f_{D,P}(-x) g(x-P)/g(x)). \tag{6}$$

Note that this does not depends on the choice of g.

If D is symmetric, we can take $g = 1$, so $\delta_{-1}(P, f_{D,P}) = (-P, f_{D,P}(-x))$. An element $g_P = (P, f_{D,P})$ is said to be symmetric if $\delta_{-1}(g_P) = g_P^{-1}$. This is the case iff $f_{D,P}^{-1}(x+P) = f_{D,P}(-x) g(x-P)/g(x)$, ie $f_{D,P}(x) f_{D,P}(P-x) = g(-x)/g(-P-x)$. If $P = P_0$, this equation becomes $f_{D,P}(P_0)^2 = g(-P_0)/g(-3P_0)$. If $g = 1$, these simplify to $f_{D,P}(x) f_{D,P}(P-x) = 1$ and $f_{D,P}(P_0)^2 = 1$.

Thus for any $P \in K(D)$, there are two symmetric elements $\pm g_P \in G(D)$ above P. If g_P and g_Q are symmetric above P and Q respectively, and g_P commutes with g_Q (ie $e_{W,D}(P,Q) = 1$), then $g_P g_Q$ is symmetric. In particular, if g_P is symmetric above P, g_P^n is symmetric above nP.

If P is of order n, then since the two symmetric elements above 0_E are $(0_E, 1)$ and $(0_E, -1)$, we see that $g_P^n = \pm 1$. So if P is of odd order n, one of the two symmetric lift is of order n and the other is of order $2n$. We will call the symmetric lift of order n the canonical symmetric lift g_P of P. But if P is of even order $n = 2n_0$, then both symmetric lifts are of order either $2n$ or n. Let $T = n_0 P$, it is a point of 2-torsion. Then for both symmetric lifts $\pm g_P$, we have $g_P^n = e_{D,*}(T)$. So the symmetric lifts are of order n iff $e_{D,*}(T) = 1$.

If D is symmetric, Mumford shows in [Mum66, Proposition 2 p.307] that $e_{D,*}(T) = (-1)^{\mathrm{mult}_D(T) - \mathrm{mult}_D(0)}$. A divisor is said to be totally symmetric if $e_{D,*}(T) = 1$ for all $T \in E[2]$, this is the case iff D is linearly equivalent to $2D_0$ with D_0 a symmetric divisor.

The symmetric divisors of degree d are given by $(d-1)(0_E) + T$ for each $T \in E[2]$. If d is even, only $d(0_E)$ is totally symmetric among these four symmetric divisors in the corresponding algebraic equivalence class.

If $d := \deg D$ is odd, we thus have a canonical (set) section $s : K(D) \to G(D)$, which maps P to the canonical symmetric element g_P above it, hence a canonical 2-cocycle $S : K(D) \times K(D) \to \mathbb{G}_m$, $S(P,Q) = s(P).s(Q).s(P+Q)^{-1}$. An elementary, if somewhat tedious (see below), computation shows that $S(P,Q) = e_{W,D}(P,Q)^{1/2} \in \mu_d$.

When d is odd, we will define $h_{D,P}$ to be the canonical function such that $g_P = (P, h_{D,P})$ is the unique symmetric element of order d.

2.5. **Heisenberg group.** Let D be a divisor of degree d, and $E[d] = E_1[d] \oplus E_2[d]$ a symplectic decomposition for the Weil pairing. Let $\widetilde{E}_i[d]$ be any lift of $E_i[d]$ into the theta group $G(D)$, $s : E_i[d] \to \widetilde{E}_i[d]$ the corresponding isomorphism..

Since $E_1[d]$ and $E_2[d]$ are orthogonal, we can extend s into a set section for any $P = P_1 + P_2 \in E[d]$ by $s(P) = s(P_1)s(P_2) = s(P_2)s(P_1)$.

The corresponding cocycle is then given by $S(P,Q) = e_{W,D}(P_1, Q_2) e_{W,D}(P_2, Q_1)$. We represent an element of $G(D)$ by a tuple (α, P) which encodes the element $\alpha s(P)$.

The group law is then given for all $n \in \mathbb{Z}$ by $(\alpha, P)^n = (\alpha^n S(P,P)^{n(n-1)/2}, nP)$, in particular $-(\alpha, P) = (S(P,P)/\alpha, -P)$.

If the level subgroups $\widetilde{E_i}$ are symmetric (if d is even these exists only if D is totally symmetric), then they commute with δ_{-1} hence we have $\delta_{-1}(\alpha, -P) = (\alpha, -P)$. It follows that the symmetric elements above P are given by $(\pm S(P,P)^{1/2}, P)$, and if d is odd the unique symmetric lift of order d is given by $(S(P,P)^{1/2}, P)$.

So the cocycle S_0 associated to the symmetric section s_0 is given by $S_0(P,Q) = e_{W,D}(P,Q)^{1/2}$.

Anticipating Section 2.8 and reusing Mumford's notations, the map $\varepsilon_N : G(D) \to G(ND)$ is described by $(\alpha, P) \mapsto (\alpha^N, P)$ provided that the subgroups $\widetilde{E}_i[Nd]$ are compatible with $\widetilde{E}_i[d]$. The isogeny descent map $\tilde{f} : G(D_1) \to G(D_2)$ is given by $(\alpha, P) \mapsto (\alpha, f(P))$ provided that the level subgroups of D_2 are compatible via $\tilde{f}$ with the ones on D_1. So the map $\eta_n = \widetilde{[n]} \circ \epsilon_n$ is given by $(\alpha, P) \mapsto (\alpha^n, nP)$. And the map $\delta_n : (\alpha, P) \mapsto (\alpha^{n^2}, nP)$.

Finally, if $P \in K(D)$ and $P = 2P_0$, P_0 determines a unique symmetric lift of P. (Assume $e_*(P) = 1$). Indeed, we let $g_{P_0} \in G(2D)$ one of the two symmetric lifts, we use ε_2 to get an element in $G(4D)$ and we descend via $[2]$ to get back an element of $G(D)$ which does not depend on the sign. Since $P_0 \in 2K(4D)$, the descent does not depend on the choice of $\widetilde{E[2]}$.

2.6. The case of a divisor of degree 0.

It is also instructive to look at the theta group $G(D)$ of a divisor D of degree 0.

Such a divisor is always linearly equivalent to $D_Q = (Q) - (0)$ so we will restrict to this case. We have $K(D_Q) = E$ and $\Phi_{D_Q} = 0$. The Weil pairing e_{D_Q} is trivial so $G(D_Q)$ is commutative. An element $g_{P,Q} = (P, f_{P,D_Q}) \in G(D_Q)$ has divisor $(P+Q)+(0)-(P)-(Q)$ so corresponds to a multiple of the usual Miller function $\mu_{P,Q}$. In particular, we also have $g_{P,Q} \in G(D_P)$.

There are thus two interpretations of the addition law $g_{P_1,Q} g_{P_2,Q}$. The first one is given by working in $G(D_Q)$. But we can also interpret $g_{P_1,Q}$ as being above Q in $G(D_{P_1})$, $g_{P_2,Q}$ as being above Q in $G(D_{P_2})$, so the product of the two functions $f_1 f_2$ is above Q in $G(D_{P_1} + D_{P_2})$. But $D_{P_1} + D_{P_2}$ is linearly equivalent to $D_{P_1+P_2}$, so using our isomorphisms of theta group we get an element of $G(D_{P_1+P_2})$ above Q which we reinterpret as an element of $G(Q)$ above $P_1 + P_2$. Both interpretation give the same addition law.

We check: $\mu_{P_1,Q} \star \mu_{P_2,Q} = \mu_{P_1,P_2}(-Q)\mu_{P_1+P_2,Q}$.

We could thus define a partial group law G above $(E \times E)$ which is defined above $(P_1, Q), (P_2, Q)$ and above $(P, Q_1), (P, Q_2)$. This group law encodes the arithmetic operations done when computing pairings.

For instance, if $g_P = (P, \mu_{P,Q})$, then g_P^n is given by est donné par $1/f_{n,P}(-Q)\mu_{nP,Q}$. So if P is of order n, we get that the equivalence class of $g_P^n \in \mathbb{G}_m$ is represented by the Tate pairing $e_{T,n}(Q,P)$.

Note the link with the torsor interpretation of the Tate pairing (see [Rob23b]). Let $K = \langle P \rangle$. The divisor D_Q descends on $E_2 = E/K$ iff we can find a lift of K in $G(D_Q)$, iff there exists g_P such that $g_P^n = 1$, iff for an arbitrary g_P, $g_P^n \in \mathbb{G}_m$ is a n-th power.

But descents $D_{Q'}$ of D_Q via $f : E \to E_2$ corresponds exactly to preimages of Q via $\tilde{f} : E_2 \to E$, so the above conditions mean that $\tilde{f}^{-1}(Q)$ has a rational preimage.

2.7. Theta group and isogenies.

Let K be a finite subgroup, and $f : E \to E_2 = E/K$ the corresponding isogeny. A natural question is whether D is linearly equivalent to $D' := f^* D_2$, for some divisor D_2 on E_2, in which case we say that D descends to D_2.

If that is the case, since f^*D_2 is invariant by translation by $T \in K$, then for all $T \in K$, $t_{T,*}D$ should be linearly equivalent to D, so a first condition is that $K \subset K(D)$.

Let $D' = f^*D_2$ and α_f any rational function with divisor $D' - D$. Since D' is invariant by translation by K, we have that for all $T \in K$, $\alpha_f(x)/\alpha_f(x-T) = f_{D,T}$.

Conversely, for each $T \in K$, pick a $g_T = (T, f_{D,T})$ so that $t_{T,*}D = D + \mathrm{div} f_{D,T}$.

Then these g_T glue together to form a function α_f such that $\alpha_f(x)/\alpha_f(x-T) = f_{D,T}$ if and only if they form a group $\widetilde{K}$ (the cocycle condition for α_f to exists translate into the group law of the theta group). We say that $\widetilde{K}$ is a lift of K to $G(D)$; such a lift exists (possibly over an extension) iff K is isotropic for the Weil pairing $e_{W,D}$.

In this case, $D' = D + \mathrm{div}(\alpha_f)$ is a divisor invariant by translation by $T \in K$, hence is of the form $D' = f^*D_2$.

Note that α_f is not unique, if g is any function on E_2, then $\alpha'_f = \alpha_f \cdot g \circ f$ satisfy the cocycle condition, and via α'_f, D descends to $D_2 + \mathrm{div}(g)$. In other words, $\widetilde{K}$ determines D_2 only up to its linear equivalence class.

Note also that D may have different (non linearly equivalent) descent to E_2, indeed if $\widetilde{K}$ is a lift, the other ones are given by the conjugation action Equation (4) of $P \in K(D)/K^{\perp}$, which gives a descent of D to $t_{P,*}D_2$ (which is algebraically equivalent to D_2 however).

If $g \in \Gamma(D')$, g descends to E_2, ie is of the form $g_2 \circ f$, iff g is invariant by translation by $T \in K$. By Equation (2), we have an isomorphism $G(D) \simeq G(D')$, $(P, f_{D,P}) \mapsto \alpha_f(x - P)/\alpha_f(x) f_{D,P}$. In particular, by definition of α_f, it sends $g_T \in \widetilde{K}$ to $(T, 1)$, and the action of $(T, 1)$ on $\Gamma(D')$ is the action by translation. Hence a section $s \in \Gamma(D)$ corresponds to a section $s' \in \Gamma(D')$ which descends to E_2 iff s is invariant by $\widetilde{K}$.

Proposition 2.3. *We have an isomorphism $Z(\widetilde{K})/\widetilde{K} \simeq G(D_2)$ which sends $f_{D,P}$ for $P \in K^{\perp}$ into the element $f_{D_2,f(P)}$ such that $f_{D_2,f(P)} \circ f = f_{D,P}\alpha_f(x-P)/\alpha_f(x)$.*

We thus obtain a partial morphism $\tilde{f} : G(D) \to G(D_2)$.

Proof. The element $g_P \in G(D)$ descends to $G(D_2)$ iff it commutes with $\widetilde{K}$, and by construction of D_2, the descent of elements in $\widetilde{K}$ is trivial. The resulting map is an isomorphism by [Mum66]. The explicit formula follows by the isomorphisms above. □

Proposition 2.4 (Mumford). *The divisor D descends to a symmetric divisor D_2 (more precisely to a divisor linearly equivalent to a symmetric divisor) iff $\widetilde{K}$ is symmetric. In this case, the (partial) morphism $\tilde{f}$ commutes with δ_{-1}.*

We remark that if K is rational and $d = \#K$ is odd, there is a unique symmetric lift $\widetilde{K}$ above K by Section 2.4, hence $\widetilde{K}$ is rational. However if d is even, there may be an obstruction to the existence of a symmetric $\widetilde{K}$ (which can always be solved by changing the algebraic equivalence class of D), and if K is cyclic and the obstruction vanishes, there are two possibilities for symmetric $\widetilde{K}$; if the first one descends to D_2, the second one descends to $t_{f(T),*}D_2$, where $T \in E[2]/K[2]$.

We now detail the most important case where $D = N(0_E)$. For this divisor, if $P \in E[N]$, we abbreviate $f_{N,P}$ for $f_{D,P}$. Let $K \subset E[d]$ be a maximal isotropic cyclic subgroup, with $N = md$. Assume that d is odd. Take $D_2 = m(0_{E_2})$ on E_2, then $f^*D_2 = \sum_{T \in K} m(T)$ is linearly equivalent to $N(0_E)$. (Note that if d is even, f^*D_2 is linearly equivalent to $N(0_E)$ iff m is even.) Since D_2 is symmetric, it corresponds, by the general theory above, to the unique symmetric lift $\widetilde{K}$ above K.

There exists a (unique up to a constant) function $\alpha_{f,m}$ with divisor $\sum_{T \in K} m(T) - N(0_E)$; this is the function which gives the linear equivalence between $D = N(0_E)$ and $D' = f^*D_2$.

We check that if $T \in K$, $\alpha_{f,m}(x)/\alpha_{f,m}(x-T)$ has for divisor $N(T)-N(0_E)$, and in fact by the theory above we know it has to satisfy $\alpha_{f,m}(x)/\alpha_{f,m}(x-T) = f_{N,T}$ for all $(T, f_{N,T}) \in \widetilde{K}$.

Note that since $\operatorname{div} \alpha_{f,m}$ is symmetric, we have $[-1]^* \alpha_{f,m} = \pm \alpha_{f,m}$. But the $(T, f_{N,T}) \in \widetilde{K}$ above is symmetric, this force $\alpha_{f,m}(-x) = \alpha_{f,m}(x)$. And indeed, an explicit version of $\alpha_{f,m}$ is given by $\alpha_{f,m} = \alpha_f^m = \prod_{T \in K'} (x - x(T))^m$ for any K' where $K = K' \bigcup -K' \bigcup \{0_E\}$. This explicit form is clearly invariant by $[-1]$.

If $(P, f_{N,P}) \in G(N(0_E))$, then $F_{N,P} := \frac{\alpha_{f,m}(x-P)}{\alpha_{f,m}(x)} f_{N,P}$ has for divisor $\sum_{T \in \operatorname{Ker} f} (m(P+T) - m(T))$. This divisor is invariant by translation by $\operatorname{Ker} f$ hence descends to E_2. However $F_{N,P}$ needs not be invariant by translation.

Indeed, if $\mathcal{E} = \operatorname{div} f_{\mathcal{E}}$ is a principal divisor invariant by translation by K, it does not mean that $f_{\mathcal{E}}$ itself is invariant, we only have that $f_{\mathcal{E}}(x+T) = \gamma_T f_{\mathcal{E}}$ for some constant γ_T. Unraveling the definitions, this γ_T is given by a Weil-Cartier pairing:

Lemma 2.5. *Let $\mathcal{E} = \sum_i a_i \sum_{T \in K} (P_i + T) = \operatorname{div} f_{\mathcal{E}}$ a principal divisor and $P_0 := \sum a_i P_i$. Then $f_{\mathcal{E}}$ is invariant by translation iff $P_0 \in K$.*

Proof. If $T \in K$, $f_{\mathcal{E}}(x+T)/f_{\mathcal{E}}(x) = e_f(T, f(P_0)) = e_{\deg f}(T, P_0)$. So $f_{\mathcal{E}}$ is invariant by $K \Leftrightarrow P_0 \in E[\ell]$ is orthogonal to $K \Leftrightarrow P_0 \in K \Leftrightarrow f(P_0) = 0$.

Another equivalent proof is to remark that $f_{\mathcal{E}}$ is invariant by translation iff $\mathcal{E}$ descends to a divisor on E_2 which is linearly equivalent to (0), which is the case iff $P_0 \in K$. □

Example 2.6. Take $Q_1, Q_2 \in E(k)$, $\mathcal{E} = \sum_{T \in K} ((Q_1+T) + (-Q_1+T) - (Q_2+T) - (-Q_2+T))$, $f_{\mathcal{E}} = \prod_{T \in K} \frac{x - x(Q_1+T)}{x - x(Q_2+T)}$ (convention: $x - 0_E := 1$). Then $f_{\mathcal{E}}$ is invariant by translation and descends to $\frac{X - f(Q_1)}{X - f(Q_2)}$ on E/K, X a Weierstrass coordinate. When $Q_2 = 0_E$, we recover a formula from [CH17; Ren18]; the denominator is then equal to α_f^2.

Going back to our $F_{N,P}$ above, by Lemma 2.5, it descends to a function on E_2 iff $mP \in \operatorname{Ker} f$, ie iff $P \in \operatorname{Ker} f^{\perp}$, as expected. So $F_{N,P} = h \circ f$, and we define $\tilde{f}(P, f_{N,P}) = (f(P), h)$. This map is defined for elements $g \in G(N(0_E))$ above $P \in \operatorname{Ker} f^{\perp}$. Furthermore if $T \in \operatorname{Ker} f$, then our $F_{N,T}$ above has trivial divisor, hence is constant. In fact, if $(T, f_{N,T}) \in \widetilde{\operatorname{Ker} f}$, then $F_{N,T} = 1$.

So we get a morphism $Z(\widetilde{\operatorname{Ker} f})/\widetilde{\operatorname{Ker} f} \to G(E_2[m])$. We check via the formula that it sends a symmetric element into a symmetric element, and that $\tilde{f}(0_{E_1}, \gamma) = (0_{E_2}, \gamma)$.

2.8. **The canonical lift of an isogeny to the theta groups.** If D is an ample divisor on E, there is also a map $\varepsilon_N : G(D) \to G(ND)$ defined by $\varepsilon_N(P, f_{D,P}) = (P, f_{D,P}^N)$. Likewise, it commutes with δ_{-1}, so sends symmetric elements to symmetric elements.

Let $f : E \to E_2$ be a cyclic N-isogeny, with N odd. The unique symmetric lift $\widetilde{K}$ of $K = \operatorname{Ker} f$ in $G(N(0_E))$ induces a descent of $N(0_E)$ into (0_{E_2}). For any m, we have that $\varepsilon_m(\widetilde{K})$ is the unique symmetric lift of $\widetilde{K}$ in $G(Nm(0_E))$, which induces a descent of $Nm(0_E)$ to $m(0_{E_2})$. We have a map $\tilde{f} : Z(\varepsilon_m(\widetilde{K})) \to G(m(0_{E_2}))$. In $E[mN]$, given a symplectic decomposition $E[mN] = K_1 \oplus K_2$ with $K = K_1[N]$, then $K^{\perp} = K_1 \oplus K_2[m]$.

We also have a map $\varepsilon_N : G(m(0_E)) \to G(mN(0_E))$. The image of ε_N lends into $Z(\widetilde{\operatorname{Ker} f})$, so composing with $\tilde{f}$ we obtain our canonical morphism from Theorem 1.1

$$\tilde{f} : G(E_1[m]) \to G(E_2[m])$$

which sends symmetric elements to symmetric elements. If m is odd, it sends the canonical symmetric lift above P to the canonical symmetric lift above $f(P)$.

Since $\varepsilon_N(0_{E_1}, \gamma) = (0_{E_1}, \gamma^N)$, we have that $\tilde{f}(0_{E_1}, \gamma) = (0_{E_2}, \gamma^N)$. So if m is prime to N, since $\mathrm{Ker} f \cap E_1[N] = 0$, then $\tilde{f}$ is almost an isomorphism, the kernel is given by $\{(0, \gamma) \mid \gamma^N = 1\}$.

The map $\tilde{f}$ is thus a lift of the map $f : E_1[m] \to E_2[m]$ to the theta groups; sometime I may call it f too by abuse of notations when the context is clear.

Example 2.7 (Mumford). $\delta_n := \widetilde{[n]} : G(E[m]) \to G(E[m])$ is given by $g_P \mapsto g_P^{(n^2+n)/2}(\delta_{-1} g_P)^{(n^2-n)/2}$.

In this context, Theorem 1.1 becomes:

Theorem 2.8. *Let $f : E = E_1 \to E_2$ be a cyclic N-isogeny with N odd and kernel K. Let m be an odd integer prime to N. Let α_f be any function with divisor $\sum_{T \in K}(T) - N(0_E)$. Let $P \in E[m]$ and $g_P = (P, h_{m,P})$ the canonical symmetric lift of P to $G(m(0_E))$. Let $Q = f(P)$ and $g_Q = (Q, h_{m,Q})$ the canonical symmetric lift of Q to $G(m(0_{E_2})$. Then*

$$h_{m,Q}(f(x)) = \frac{\alpha_f^m(x-P)}{\alpha_f^m(x)} h_{m,P}^N(x) \tag{7}$$

Proof. The Theorem follows from unravelling the formula from Section 2.7. We can also check it directly by checking that both functions $g_1 = f^* h_{m,Q}$ and $g_2 = \frac{\alpha_f^m(x-P)}{\alpha_f^m(x)} h_{m,P}^N(x)$ have the same divisor $\sum_{T \in K} m(Q+T) - m(T)$, satisfy the symmetry condition $g_i(P-x)g_i(x) = 1$ and the order condition $g_i(x)g_i(x-P) \cdots g_i(x-(m-1)P) = 1$. The first condition shows that $g_2 = cg_1$, the second one that $c = \pm 1$, and the third one that $c^m = 1$ which forces $c = 1$ since m is odd. □

Note that $\tilde{f}((0_E, \alpha)) = (0_{E_2}, \alpha^N)$, so since the Weil pairing is the commutator pairing, we recover that $e_{W,m}(f(P), f(Q)) = e_{W,m}(P, Q)^N$.

3. Bi-extensions

(1) For abelian schemes, a birigidified line bundle has a natural structure of biextension (I always consider biextensions by $\mathbb{G}_m$), so we have isomorphisms

$$\mathrm{BiExt}(A, B; \mathbb{G}_m) = \mathrm{Corresp}(A, B) = \mathrm{Hom}(A, \hat{B}) = \mathrm{Hom}(\hat{B}, A)$$

[Gro72, p. 7.VII.2.9.6]

In particular the identity map $A \to A$ gives the Poincaré bundle seen either as a bundle or a biextension of $A \times \widehat{A}$

(2) To a biextension, Grothendieck associate a 'Weil pairing' in [Gro72, p. 7.VIII], and Stange associate a 'Tate pairing' in her thesis, [Sta08, Chapter 17].

(3) Grothendieck shows that his Weil pairing is the standard Weil pairing (up to a sign), and Stange proves that the Tate pairing associated to the Poincaré bi-extension is the standard Tate pairing (in the case of an elliptic curve, but the general case is the same).

I guess that the Tate pairing associated to the biextension of $A \times \hat{B}$ associated to an isogeny $f : A \to B$ is the usual Tate-Cartier pairing?

(4) For the Poincaré biextension, if I unravel the definitions, we can describe it in terms of theta group as follow: if $(P, Q) \in A \times \widehat{A}$, then Q corresponds to a divisor D_Q in A, algebraically equivalent to 0.

The theta group $G(D_Q)$ associated to D_Q then gives an extension $1 \to \mathbb{G}_m \to G(D_Q) \to A \to 1$, hence an element $g_{P,Q} \in G(D_Q)$ above P corresponds to an element in the Poincaré biextension above (P, Q). $g_{P,Q}$ corresponds to an isomorphism $t_P^* D_Q \simeq D_Q$.

The biextension group laws can then be given by: - $g_{P,Q} *_1 g_{P',Q} = g_{P,Q} g_{P',Q}$ (multiplication in the theta group) - $g_{P,Q} *_2 g_{P,Q'} = g_{P,Q} g_{P,Q'}$ (via the tensor product $G(D_Q) \otimes G(D_{Q'}) \to G(D_{Q+Q'})$)

And I guess the biextension on $A \times \hat{B}$ associated to $f : A \to B$ should be given by associating an element $g_{P,Q}$ above P in A, Q in $\hat{B}$ which gives an isomorphism $t_P^* f^* D_Q \simeq D_Q$.

(5) If I have an ample line bundle L, I can consider the polarisation $\varphi_L : A \to \widehat{A}$ hence a biextension of $A \times A$.

I think we can describe it this way: if (P, Q) in $A \times A$, then to Q we can associte $t_Q^* L \otimes L^{-1}$ which is a divisor algebraically equivalent to 0. Then we take an element $g_{P,Q} in G(t_Q^* L \otimes L^{-1})$. Rearranging things, this element $g_{P,Q}$ corresponds to an isomorphism $t_{P+Q}^* L \otimes L \simeq t_P^* L \otimes t_Q^* L$, ie an explicit isomorphism from the theorem of the square!

(6) I like to think of an explicit isomorphism from the theorem of the square as the following information: fix trivialisations of L on some point x, as well as $x + P$ and $x + Q$. Then $g_{P,Q}$ determines (and is determined) by a trivialisation of L on $x + P + Q$.

This gives a way to represent $g_{P,Q}$; and compute in practice the group laws associated to the biextension; hence compute pairings. For an elliptic curve, if we fix $L = (0_E)$, $g_{P,Q}$ corresponds to a function with divisor $(P + Q) + (0) - (P) - (Q)$ hence we are essentially reformulating Miller's algorithm.

(7) The reason I am mentionning trivialisations is that we have a weak form of algebraic Riemann relations:

Theorem 3.1. *Assume that L is symmetric. Let $P, Q, R, S \in A$ such that $P + Q + R + S = 2T$ and let $P' = T - P, Q' = T - Q, R' = T - R, S' = T - S$. Then we have a canonical isomorphism $t_P^* L \otimes t_Q^* L \otimes t_R^* L \otimes t_S^* L \simeq {t'_P}^* L \otimes {t'_Q}^* L \otimes {t'_R}^* L \otimes {t'_S}^* L$*

In particular if we have chosen a trivialisation for 7 out of the 8 points in Riemann relation, it fixes the last one canonically.

Proof. We have $R' = T - R$, $S' = T - S$ so $R' + S' = P + Q$. Fix any isomorphism $\alpha : t_P * L \otimes t_Q * L = t'_R * L \otimes t'_S * L$.

Fix an isomorphism $\psi : L \to L^{-1}$. We remark that $[-1]^* \Psi$ gives an isomorphism $L^{-1} \to L$ and we could normalize Ψ (up to a sign) by requiring that the composition $L \to L$ is the identity (eg equal to 1 on $L \mid 0$), but we won't require this.

Via ψ we get an isomorphism $t_{-P}^* L \otimes t_{-Q}^* L \simeq t_{-R'}^* L \otimes t_{-S'}^* L$ which we translate by T to get an isomorphism $\beta : t_{P'}^* L \otimes t_{Q'}^* L \simeq t_R^* L \otimes t_S^* L$.

Hence $\alpha \otimes \beta^{-1}$ gives an isomorphism $t_P^* L \otimes t_Q^* L \otimes t_R^* L \otimes t_S^* L \simeq t_{P'}^* L \otimes t_{Q'}^* L \otimes t_{R'}^* L \otimes t_{S'}^* L$.

But remark that if we fix another isomorphism $\alpha' = \lambda \alpha$, then $\beta' = \lambda \beta$, hence $\alpha \otimes \beta^{-1} = \alpha' \otimes' \beta^{-1}$. The isomorphism we have computed is canonical!

(This could probably be proved by the theorem of the cube also.) □

We can see this argument as a special case of Riemann relations for theta functions (analytic Riemann or the algebraic ones proved by Mumford), which describe the canonical isomorphism defined above explicitly in terms of basis of sections given by theta functions.

Now we can specialize: the following points are in Riemann relations:

-

- $(P+Q)(P-Q)00; Q-QPP$
- $(P+Q+R)PQR; 0(Q+R)(P+Q)(P+Q)$

In particular from a trivialisation of L at 0 and P we can recover a canonical polarisation of L at $n.P$. And from a trivialisation of L at $0, P, Q$ and $P+Q$ we can recover a canonical polarisation at $n.P+m.Q$

And the second case gives a way to compute in the biextension: let $g_{P_1,Q}$ be an isomorphism $t^*_{P_1+Q}L \otimes t^*_0 L \simeq t^*_{P_1}L \otimes t^*_Q L$ and let $g_{P_2,Q}$ be an isomorphism $t^*_{P_2+Q}L \otimes t^*_0 L \simeq t^*_{P_1}L \otimes t^*_Q L$

So fix any trivialisation of L at $0, P_1, P_2, Q, P_1+P_2$. Use $g_{P_i,Q}$ to get the corresponding trivialisation at P_i+Q. The above case of Riemann relations fixes a canonical trivialisation of L at P_1+P_2+Q, from which we deduce an explicit isomorphism $t^*_{P_1+P_2+Q}L \otimes t^*_0 L \simeq t^*_{P_1+P_2}L \otimes t^*_Q L$. Thus we obtain an element $g_{P_1+P_2,Q}$, and we can check that it does not depend on our starting choices of trivialisation.

(8) Unraveling the formula, this gives us the following interpretation of the Tate pairing with respect to L:

- if P is a point of n-torsion, we fix a trivialisation of L at $0, P, Q, P+Q$ (or $R, R+P, R+Q, R+P+Q$)
- from these trivialisation, we determine a canonical trivialisation of L at nP which we compare with the one at 0, and of L at $nP+Q$ which we compare with the one at Q.
- The quotient gives us the Tate pairing $e_{T,L}(P,Q)$

(9) If we apply this approach to L of level n with a symmetric theta structure, fixing a trivialisation of L at P amount to choosing affine coordinates for $\theta_i(P)$ above the projective coordinates.

We then use the theta Riemann relations to keep track of our trivialisations, ie to work with 'affine theta coordinates'. So we compute $nP+Q$ and nP in affine coordinates and we compare with the affine coordinates of Q and 0; they differ by some projective factors whose quotient is the Tate pairing.

We recover the algorithms we had with David Lubicz for computing the Tate pairing in theta coordinates.

(10) I think we can also recover elliptic nets this way: this time we start with a principal line bundle $L=(0_E)$

Let's start with rank 1 nets: we fix a trivialisation of L at 0_E and P. This determines by the above a trivialisation of L at every n.P.

Now on L we have the section $'Z'$ (if we think of projective Weierstrass coordinates; or the Weierstrass σ function if we think analytically, aka the theta function which has a zero exactly at the points of the lattice), which is 0 on 0_E.

The trivialisations of L at each $n.P$ defines a value $Z(n.P)$ at every point, with $Z(n.P)=0$ iff $n.P=0_E$.

A slight annoyance is that $Z(0)=0$ so we cannot use the value of Z at 0 to specify the trivialisation of L on 0, but we can specify the trivialisation of L on P by requiring $Z(P)=1$; and the value $Z(2P)$ can be seen as implicitly fixing a trivialisation of L on 0 (equivalently of L on $2P$).

Likewise, we can define rank 2 (or more) nets; but to compute the Tate pairing we need to shift the offset by one so that we get a non zero value.

(11) The above strategy works for any ppav: but this is a different approach than the standard construction of elliptic nets. What I am saying is that for any model (A,L) where we have an explicit version of the theorem of the square for a line bundle L_0, so that we can compute the canonical Riemann isomorphisms for L_0; then if we fix a basis of sections $g_1, \dots, g_m$ of L_0 we can define generalised elliptic nets as the value of g_i on trivialisations of $L_0 \mid nP + mQ$, which are entirely defined from a trivialisation of L_0 on $0, P, Q, P+Q$.

Here I am allowed to represents point on A by sections of L to compute the isomorphism given by the theorem of the square on L_0; this is like using the x, y Weierstrass coordinates (ie sections of L_0^3) to compute the Miller functions.

The theta function approach from 9) is the case $L = L_0$ of level n, using the theta Riemann relations.

Standard elliptic nets works differently: the key is a recurrence relation that allows to compute the value of the net on any point given some value on some points; this allows to take L_0 principal without needing any other intermediate line bundle L for the actual computations.

This recurrence approach extends to higher dimension by using the theta Riemann relations, this is done in the thesis of Christophe Tran [Tra14]. at least for Jacobians of hyperelliptic curves.

(12) In summary, there is a canonical way ("algebraic Riemann relations") from fixing a trivialisation of a line bundle on L on some points P_i (and some sums) to compute a canonical trivialisation of L on any $\Sigma n_i \widetilde{P}_i$ (where $\widetilde{P}$ means that I am implicitely working on the biextension, not on the abelian variety).

If we evaluate a basis of theta functions on these trivialiation we recover the theta pairing algorithm; and if we use instead the section $'Z'$ of the divisor (0_E) on an elliptic curve we recover an elliptic net.

So I guess this is an alternate way of seeing the Tate pairing as being the Tate pairing associated to some biextension: it simply means that we keep track of trivialisations.

I guess this gives an alternative way of computing elliptic nets: we work with "affine Weierstrass coordinates" (X, Y, Z) and we compute differential additions from the algebraic Riemann relations; the value of Z is the value of the net.

(Or more precisely we get the value of the original elliptic net to the cube because X, Y, Z are sections of L^3, $L = (0_E)$. Say Z_0 is the section of L, then X_0, Z_0^2 are the sections of L^2 and $X = X_0 Z_0, Y, Z = Z_0^3$ are the sections of L^3.)

4. Biextensions and theta groups

Let P be a point of n-torsion, and fix a trivialisation of L at 0 and P, then we get a trivialisation of L^n at 0 and P But $t_P^* L^n \simeq L^n$, and these trivialisation defines an explicit isomorphism between the two, ie an element $g_P \in G(L^n)$. (And changing our trivialisation of L by ζ does not change g_P). In particular, since g_P is global, we can use g_P to associate a trivialisation of L^n at $x + P$ from a trivialisation of L^n at x.

Thus we can use the arithmetic of biextensions to work at level (say) m on L to recover the action of the theta group at level nm on L^n. In particular, we can check that g_P is symmetric iff our trivialisations satisfy the same symmetry relation we use to normalizing our theta functions.

We can thus reformulate [Rob21, §2.9] as follow: an explicit version of the theorem of the square at level m allows to work with the biextension laws (via the algebraic Riemann relations) and via this to recover the action of the theta group at level nm. This can be used to compute the Weil and Tate pairings, isogenies (given generators of the kernel) and theta (say given a basis of the nm-torsion).

At the time I wrote my hdr, I was not aware that the computations I was doing with trivialisation and algebraic Riemann relations were related to biextensions. This concept was brought to my attention by Prof. Stange who pointed out to me following [Rob23b] [Sta08, Chapter 17] giving the interpreation of the Tate pairing from biextensions.

Question: can every Riemann relation be expressed in term of the biextensions laws?

Another relation between theta group and trivialisations is as follow: fix an isogeny: $f : A \to B = A/K$. A lift $\widetilde{K}$ of K to $G(L)$ gives a descent M of L and an isomorphism $f^*M \to L$. We can fix this isomorphism by specifying a trivialisation of M and L at 0. From this, we can use this isomorphism to relate a trivialisation of L on x to a trivialisation of M on $f(x)$ and conversely.

This gives an alternative proof that the biextension law is related to pairing: fixing trivialisations of L on P of n-torsion induce a trivialisation of L^{n^2} on P' (such that $nP' = P$). But P' is in the theta group of L^{n^2} and we can use the fact that the Weil pairing is the commutator pairing on the theta group, and then use the compatibility of pairings with scalar multiplication.

This also gives an alternative proof of Riemann relations: the isogeny $F : (P, Q) \mapsto (P + Q, P - Q)$ is an isogeny $(A \times A, L^2 \star L^2) \to (A \times A, L \star L)$. The kernel is $A[2]$ (embedded canonically), which lift canonically to the theta group: above every $T \in A[2]$ there are two symmetric elements $\pm g_T$ which both give the same element $g_T \otimes g_T$ on $G(L^2 \star L^2)$.

In particular, fixing a trivialisation of $L^2 \star L^2$ on (x', y', z', t') gives a trivialisation of $L \star L$ on $(x'+y', x'-y', z'+t', z'-t')$, but also (by permutation) on $(x'+t', x'-t', z'+y', z'-y')$, which is another form of the Riemann relations.

5. Lifting the DLP

As a particular case of lifting isogenies, we can lift DLPs canonically to the theta group via the symmetric section. If Q, P are points of ℓ-torsion, with $Q = mP$, we have the lift

$$h_{\ell,Q}(mx) = \left(\frac{\alpha_m(x-P)}{\alpha_m(x)}\right)^{\ell} h_{\ell,P}(x)^{m^2}.$$

Here $g_P = (P, h_{\ell,P})$ and $g_Q = (Q, h_{\ell,Q})$ are the canonical symmetric lift.

We remark that in this case, α_m can be given by the division polynomial ψ_m.

Looking at the group law, since $g_Q = g_P^m$ (because the canonical symmetric lifts of $\langle P \rangle$ form a group), we also have $h_{\ell,Q}(x) = h_{\ell,P}(x) h_{\ell,P}(x-P) \cdots h_{\ell,P}(x-(m-1)P)$.

If we could find a x in which we knew both mx and $\frac{\alpha_m(x-P)}{\alpha_m(x)}^{\ell}$, then since we know $h_{\ell,Q}$ and $h_{\ell,P}$ we could recover m via a DLP over $\mathbb{F}_p^*$. The obvious choice of using P_0 does not work since in this case $h_{\ell,P}(P_0) = 1$ by definition of the symmetric lift.

If we could find another lift, say $g'_Q = {g'_P}^m$, then if $\gamma_P = g'_P / g_P$ and $\gamma_Q = g'_Q / g_Q$ we would have $\gamma_Q = \gamma_P^m$ and we would reduce to a DLP in $\mathbb{F}_q^*$.

More generally, we would like to exploit the arithmetic of the theta groups and biextensions to study the DLP. Say we are on an elliptic curve, P is of order L and $Q = m.P$ and we want to recover the DLP m. If $\mu_\ell \subset \mathbb{F}_q$ we can use the Tate pairing.

As explained in [Rob23b], we can understand the pairings $e_{T,\ell}(P, Q)$ and $e_{T,\ell}(P, P)$, and passing to the isomorphism classes we get an equation: $[e_T, l(P, Q)] = [e_T, l(P, P)]^m$.

If l is prime to $q - 1$, then the isomorphism class is trivial so we obtain the non useful equation $[1] = [1]^m$. So passing to the isomorphism class lose too much information. But we might still hope that an explicit isomorphism between the two torsors can give us some information about m. Notice that the equation on the canonical symmetric lifts above is essentially precisely such an isomorphism between $e_{T,\ell}(Q,Q)$ and $e_{T,\ell}(P,P)$.

Fix a trivialisation of L at 0. Now since ℓ is prime to $q-1$, there is a unique rational trivialisation of L at P which induces the symmetric element $h_{\ell,P}$ on L^{ℓ}: the others ones are given by multiplying by ζ which is not rational by assumption.

In terms of affine lift: P is of order ℓ, and if $\widetilde{P}$ is any lift, $\ell.\widetilde{P} = \lambda\widetilde{O}$, so $\widetilde{P}$ is of order dividing $\ell(q-1)$. The "canonical lift" $\widetilde{P}_0$ is the unique one of order ℓ. (So a way to compute it is to start with an arbitrary lift, recover λ as above, and correct by λ^{1/ℓ^2} which is well defined because ℓ is prime to $q-1$). (This "canonical lift" is the same as defined on level 1 via elliptic nets by Stange in [Sta08, Chapter 19].)

Now start with a lift $\widetilde{P}$ (say with $Z(\widetilde{P}) = 1$ as with elliptic nets). Take a lift $\widetilde{Q}$ of Q (say with the same normalisation); and assume that the lift is defined in such a way that $\widetilde{Q}$ is in the group generated by $\widetilde{P}$: $\widetilde{Q} = m'\widetilde{P}$, with $m' = m + a\ell$ for some unknown a. Multiplying by ℓ, we get an equation above 0: $\lambda'_Q = {\lambda'_P}^{m'^2}$ (and this gives a way to check that $\widetilde{Q}$ is indeed a multiple of $\widetilde{P}$). Solving a DLP over $\mathbb{F}_q^*$, we recover m'^2 modulo $q-1$. An alternative way is to compare $\widetilde{P}, \widetilde{Q}$ with their canonical lift: $\widetilde{P} = \lambda_P\widetilde{P}_0$, $\widetilde{Q} = \lambda_Q\widetilde{Q}_0$. Since $\widetilde{Q}_0 = m\widetilde{P}_0 = m'\widetilde{P}_0$, we get $\lambda_Q = \lambda_P^{m'^2}$ (and in fact $\lambda'_Q = \lambda_Q^{\ell^2}$ and the same for λ'_P).

However this information is not enough to recover anything about m: because ℓ is prime to $q-1$, knowing $m + a\ell$ modulo $q-1$ does not gives information about m modulo ℓ since a is unknown. This would change if we could force $a = 0$ (say).

One way to do that is via 'projective coordinate leak' [NSS04]. Say we do a Montgomery ladder on (X_P, Z_P), and we are given (X_Q, Z_Q) rather than $(X_Q : Z_Q)$. Then since the (affine) ladder is essentially computing on the biextension rather than on E, we recover m^2 modulo $q-1$ (here we know that $a = 0$!) This allows to recover m^2 (hence m unless $q-1$ has a lot of factors) from only one DLP in $\mathbb{F}_q^*$: so unlike [NSS04] only one projective coordinate leak is enough for an attack.

Of course, nobody sends $(X_Q : Z_Q)$ since sending $x_Q = X_Q/Z_Q$ saves bandwidth and everyone is aware about the above attack. But that idea could still be used in some sidechannel attacks I guess.

It would be nice if we could extend this approach to more general cases; or maybe use the biextension law in some index calculus attacks. Some failed experiments are in the appendix.

References

[CD23] W. Castryck and T. Decru. "An efficient key recovery attack on SIDH". In: Springer-Verlag (Eurocrypt 2023), Apr. 2023.

[CH17] C. Costello and H. Hisil. "A simple and compact algorithm for SIDH with arbitrary degree isogenies". In: *Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II 23*. Springer. 2017, pp. 303–329.

[Gro72] A. Grothendieck. *Groupes de Monodromie en Géométrie Algébrique: SGA 7*. Springer-Verlag, 1972.

[MMPPW23] L. Maino, C. Martindale, L. Panny, G. Pope, and B. Wesolowski. "A Direct Key Recovery Attack on SIDH". In: Springer-Verlag (Eurocrypt 2023), 2023.

[Mum66] D. Mumford. "On the equations defining abelian varieties. I". In: *Invent. Math.* 1 (1966), pp. 287–354.

[Mum67a] D. Mumford. “On the equations defining abelian varieties. II”. In: *Invent. Math.* 3 (1967), pp. 75–135.

[Mum67b] D. Mumford. “On the equations defining abelian varieties. III”. In: *Invent. Math.* 3 (1967), pp. 215–244.

[NSS04] D. Naccache, N. P. Smart, and J. Stern. “Projective coordinates leak”. In: *Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings 23*. Springer. 2004, pp. 257–267.

[Ren18] J. Renes. “Computing isogenies between Montgomery curves using the action of (0, 0)”. In: *Post-Quantum Cryptography: 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings*. Springer. 2018, pp. 229–247.

[Rob21] D. Robert. “Efficient algorithms for abelian varieties and their moduli spaces”. HDR thesis. Université Bordeaux, June 2021. URL: http://www.normalesup.org/~robert/pro/publications/academic/hdr.pdf. Slides: 2021-06-HDR-Bordeaux.pdf (1h, Bordeaux).

[Rob23a] D. Robert. “Breaking SIDH in polynomial time”. Apr. 2023. URL: http://www.normalesup.org/~robert/pro/publications/articles/breaking_sidh.pdf. eprint: 2022/1038, HAL: hal-03943959, Slides: 2023-04-Eurocrypt.pdf (15 min, Eurocrypt 2023, April 2023, Lyon, France).

[Rob23b] D. Robert. “The geometric interpretation of the Tate pairing and its applications”. Feb. 2023. URL: http://www.normalesup.org/~robert/pro/publications/articles/geometric_tate_pairing.pdf. eprint: 2023/177, HAL: hal-04295743v1.

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

[Tra14] C. Tran. “Formules d’addition sur les jacobiennes de courbes hyperelliptiques: application à la cryptographie”. PhD thesis. Rennes 1, 2014. URL: https://www.theses.fr/185903150.

Appendix A. Failed experiments

A.1. **Trying to reconstruct isogenies.** Let $f : E = E_1 \to E_2$ be a cyclic N-isogeny with N odd. We assume that E_1, E_2 and N are known and we want to try to reconstruct f.

By the SIDH attacks [CD23; MMPPW23; Rob23a], it suffices to recover the image of f on some basis of ℓ_i-torsion: $f : E_1[\ell_i] \to E_2[\ell_i]$ for enough ℓ_i such that $\prod \ell_i > N$. We can assume $\ell_i \wedge N = 1$, and we will restrict to ℓ_i odd.

We first guess the image of f on the ℓ_0 torsion. Then we use Theorem 2.8 to recover the action of f on the ℓ_i torsion. If our guess is wrong, we will detect it either on the intermediate steps because we won't have any solution, or at the end where our higher dimensional isogeny embedding f won't give an isogeny which projects back to E_2.

Since the action of $G(m(0_E))$ on $\Gamma(m(0_E))$ is irreducible, and the $f_{m,P}$ are given by the action of $(P, f_{m,P})$ on 1, we see that they generate $\Gamma(m(0_E))$. By Lefschetz theorem, they thus give a projective embedding of E whenever $m \geq 3$. So a point $x \in E$ is completely determined by the projective point $(f_{m,P}(x))_{P \in E[m]}$.

Since we can assume that we know the action of f on the ℓ_0 torsion, we know that, setting $m = \ell_0$, $f_{m,f(P)}(f(x)) = \frac{\alpha_f^m(x-P)}{\alpha_f^m(x)} f^N_{m,P}(x)$ for all $P \in E[m]$. If we knew how to evaluate α_f, we could then evaluate $f_{m,f(P)}(f(x))$ on any point, by the remark above this would completely determine $f(x)$.

But of course being able to evaluate α_f is closely related to evaluating f in the first place, see also Example 2.6. We need to tweak Equation (7) to not depend on α_f.

The first idea is to take a product $\prod f_{m,f(P)}(f(x-iP))$, but of course because of the order condition both members of Equation (7) become equal to 1.

Instead, we use that for $P \in E[m]$ and any Q,

$$\frac{f_{m,f(P)}(f(x+P+Q))}{f_{m,f(P)}(f(x+P))} = \left(\frac{\alpha_f(x+P)\alpha_f(x+Q)}{\alpha_f(x+P+Q)\alpha_f(x)}\right)^m \frac{f^N_{m,P}(x+P+Q)}{f^N_{m,P}(x+P)} \tag{8}$$

Note that when seen as μ_m-torsors, the element on the left is in the isomorphism class of the Tate pairing $e_{T,m}(f(P), f(Q))$ while the one on the right of $e_{T,m}(P,Q)^N$ (see [Rob23b]).

Now if $Q \in E[\ell_i]$, let $m_2 = \ell_i$. We make a guess for $Q' = f(Q)$. If our guess is correct, the following equation should hold:

$$\frac{f_{m_2,Q'}(f(x+P+Q))}{f_{m_2,Q'}(f(x+Q))} = \left(\frac{\alpha_f(x+P)\alpha_f(x+Q)}{\alpha_f(x+P+Q)\alpha_f(x)}\right)^{m_2} \frac{f^N_{m_2,Q}(x+P+Q)}{f^N_{m_2,Q}(x+Q)} \tag{9}$$

Fixing x a point which we know the image of (for instance another point of m-torsion), we let $C_1 = \frac{f_{m,f(P)}(f(x+P+Q))}{f_{m,f(P)}(f(x+P))}\frac{f^N_{m,P}(x+P)}{f^N_{m,P}(x+P+Q)}$, $C_2 = \frac{f_{m_2,Q'}(f(x+P+Q))}{f_{m_2,Q'}(f(x+P))}\frac{f^N_{m_2,P}(x+Q)}{f^N_{m_2,P}(x+P+Q)}$, and $C_0 = \frac{\alpha_f(x+P)\alpha_f(x+Q)}{\alpha_f(x+P+Q)\alpha_f(x)}$.

We can evaluate C_1 and C_2, not C_0 but we know (if our guess of Q' is correct) that $C_1 = C_0^m$ and $C_2 = C_0^{m_2}$. So we check if such a constant C_0 exists. If not, we know our choice of Q' is wrong, and we try with a new one.

Heuristic: only $Q' = f(Q)$ satisfy this condition.

Under this heuristic, we can uniquely recover $f(Q)$. We can thus hope to reconstruct f in polynomial time, given (E_1, E_2, N).

Some justification for this heuristic: if $f : E_1 \to E_2$ is a cyclic N-isogeny, f may not be uniquely determined from (E_1, E_2, N). However, if $f_2 : E_1 \to E_2$ is another cyclic N-isogeny, then $\tilde{f_2} \circ f : E_1 \to E_1$ is an endomorphism of degree N^2 different from $[N]$ (even up to automorphism).

So this imposes E_1 to have complex multiplication, and with a non integer endomorphism of norm N^2. If the image of f on the m-torsion is further prescribed, and f_2 has the same image, then $\tilde{f_2} \circ f$ and $[N]$ have the same image on $E_1[N]$, so $\tilde{f_2} \circ f - [N] = m\alpha$ for some endomorphism α. This imposes further constraints on E_1.

So, except for very few exceptions, f is completely determined by (E_1, E_2, N) and its image on $E_1[m]$. That's why we can hope to try to reconstruct f from this data.

Actual experiments: The heuristic is wrong. Essentially because of Weil's reciprocity theorem, this equality is always satisfied, so the condition is not "generic".

A.2. **Playing with cycocles.**

(13) We now focus on trying to reconstruct the isogeny from CSIDH. As above we want to recover how f acts on the ℓ-torsion: $E_1[\ell] \to E_2[\ell]$.

(14) Take ℓ which splits as $\ell = \ell_1\ell_2$ in $\mathbb{Z}[\alpha]$. This happens with probability $1/2$.

Then $E_1[\ell] = E_1[\ell_1] \oplus E_1[\ell_2]$ (and we know which is which), and since f commutes with α, $f(E_1[\ell_i]) = E_2[\ell_i])$.

Take (P_1, P_2) a symplectic basis of $E_1[\ell]$ with $P_i \in E_1[\ell_i]$ with respect to ζ (for the Weil pairing), (Q_1, Q_2) a similar symplectic basis of $E_2[\ell]$ but with respect to ζ^N. We know that f is diagonal with respect to these basis: $f = \operatorname{diag}(u, v)$.

Furthermore since $e_{W,\ell}(f(P_1), f(P_2)) = e_{W,\ell}(P_1, P_2)^N = e_{W,\ell}(uQ_1, vQ_2)$, we know that $uv = 1 \mod \ell$.

Thus it suffices to determine u for sufficiently many small ℓ.

(15) Since $\tilde{f}$ sends symmetric elements, and that $\tilde{f}(\gamma g_P) = \gamma^N \tilde{f}(g_P)$, $\tilde{f}$ is completely determined by the restriction of f to the ℓ-torsion.

So the fact that $\tilde{f}$ exists adds more constraints on the possible values of f on the ℓ-torsion. For instance the pairing condition above is one of the constraint induced by the existence of $\tilde{f}$.

(16) So fixing a basis (P_1, P_2) and (Q_1, Q_2) as above, we want to find the u, v with $v = u^{-1} \mod \ell$ such that $f(P_1) = uQ_1$ and $f(P_2) = vQ_2$.

We have a canonical set section $s_1 : E_1[\ell] \to G(E_1[\ell])$ which sends P to the unique symmetric lift g_P of order ℓ. This defines a canonical 2-cocycle $S_1(T_1, T_2) = s_1(T_1)s_1(T_2)s_1(T_1 + T_2)^{-1}$. Likewise we define s_2, S_2. Notice that these 2-cocycles are normalised: $S(T, 0) = S(0, T) = 1$, and that since the commutator pairing is the Weil pairing, we have

$$S(T_1, T_2) = e_{W,\ell}(T_1, T_2) S(T_2, T_1). \tag{10}$$

Furthermore, if g_1, g_2 are two symmetric and commuting elements, then $g_1 g_2$ is also symmetric, so $s(g^a) = s(g)^a$ and $S(aT, bT) = 1$, or equivalently $S(T_1, T_2) = 1$ if $e_{W,\ell}(T_1, T_2) = 1$.

Note that $G(E[\ell])$ is a central extension of $E[\ell]$ by $\mathbb{G}_m$ so it corresponds to an element in $H^2(E[\ell], \mathbb{G}_m)$, the 2-cocycle S above is a canonical representative of this element.

The cocycle condition is

$$S(T_1, T_2) S(T_1 + T_2, T_3) = S(T_1, T_2 + T_3) S(T_2, T_3). \tag{11}$$

(17) Now since $\tilde{f}$ sends symmetric elements to symmetric elements, we get that $s_2 = \tilde{f} \circ s_1$, hence

$$S_2(f(T_1), f(T_2)) = \tilde{f} \circ S_1(T_1, T_2) = S_1(T_1, T_2)^N. \tag{12}$$

In particular, u, v have to satisfy $S_2(auQ_1 + bvQ_2, cuQ_1 + dvQ_2) = S_1(aP_1 + bP_2, cP_1 + dP_2)^N$ for all $a, b, c, d \in \mathbb{Z}/\ell\mathbb{Z}$.

By Equation (10) above, Equation (12) implies that $e_{W,\ell}(f(T_1), f(T_2)) = e_{W,\ell}(T_1, T_2)^N$. A key difference is that unlike $e_{W,\ell}$, S_1 and S_2 are not bilinear. So Equation (12) induces some non trivial relations compared to just the ones coming from the Weil pairing.

(18) If α is an A-endomorphism on E, and $A \wedge \ell = 1$ for simplicity, it induces a morphism $\tilde{\alpha}$ of the theta group $G(E[\ell])$. So the cocycle S has to satisfy the compatibility conditions

$$S(\alpha(T_1), \alpha(T_2)) = \tilde{\alpha} \circ S(T_1, T_2) = S(T_1, T_2)^A. \tag{13}$$

When α is the Frobenius π_p, $A = p$, and it is easy to check that $\widetilde{\pi_p}(P, f_{m,P}) = (\pi(P), f_{m,P}^p)$ if $f_{m,P}$ is rational. More generally for a general P, write $\pi_p \circ f_{m,P} = g_{m,P} \circ \pi_p$, then $\widetilde{\pi_p}(P, f_{m,P}) = (\pi(P), g_{m,P})$.

Taking $\alpha = [n]$, we get that $S(nT_1, nT_2) = S(T_1, T_2)^{n^2}$. Taking $\alpha = [\ell]$, we get that $S(T_1, T_2)^{\ell^2} = 1$, and taking $\alpha = [1 + \ell]$, we see that $S(T_1, T_2)^{1+\ell^2+2\ell} = S(T_1, T_2)$, so since ℓ is odd, $S(T_1, T_2)^\ell = 1$.

(19) By taking $\alpha = [-1]$, we also get $S(-T_1, -T_2) = S(T_1, T_2)$. So if f satisfy Equation (12), then so does $-f$, or more generally γf for any $\gamma \in \mathbb{Z}$ such that $\gamma^2 = 1 \mod \ell$.

(20) Let us assume that ℓ is an odd prime (or a prime power), so that ± 1 are the only two square roots of 1. If u is a solution for Equation (12), then so is $-u$.

Heuristic: we expect that there are many ℓ for which there are only two possibilities $\pm u$ for u which satisfy the compatible cocycle conditions from Equation (12) above.

(21) So if we take v primes ℓ_i satisfying the heuristic, we have 2^v possibilities for the action, so we cannot take v too large. On the other hand we need $\prod_{i=1}^{v} \ell_i > N$ so if v is small, the primes ℓ_i will be large. And our complexity is polynomial in ℓ_i.

We can hope for a subexponential attack by taking $v = O(\sqrt{\log N})$, the primes ℓ_i of size $L(1/2)$ for an attack in $L(1/2)$. If we manage to find a prime power $\ell = \ell_0^e$ with ℓ_0 small and $E_i[\ell]$ living in a not too large extension it would be ideal.

It remains to justify our heuristic.

(22) Since we know that $\tilde{f}$ exists, we can always change Q_1, Q_2 so that $u = v = 1$. In particular, we then have $S_2(Q_1, Q_2) = S_1(P_1, P_2)^N$. Note that since $S_1(P_1, P_2) = S_1(P_2, P_1)e_\ell(P_1, P_2)$, at least one of $S_1(P_1, P_2), S_1(P_2, P_1)$ is of order ℓ.

The question is then whether there can exist another u (hence v), with $u \neq \pm 1$, such that the compatibility conditions of Equation (12) are satisfied. A first condition is then that $S_2(uQ_1, vQ_2) = S_2(Q_1, Q_2)$, or more generally that $S_2(auQ_1, bvQ_2) = S_2(aQ_1, bQ_2)$ for all a, b. In particular, we want $S_2(Q_1, u^{-2}cQ_2)^{u^2} = S_2(Q_1, cQ_2)$ for all c.

The points P_1, Q_1, P_2, Q_2 are eigenvectors for the orientation α, say of eigenvalue $\lambda_1 \neq \lambda_2$. We have $S_2(\lambda_1 Q_1, \lambda_2 Q_2) = S_2(Q_1, Q_2)^A$.

Using $\alpha = \pi_p, A = p$, we have $S_2(Q_1, \lambda Q_2)^{\lambda_1^2} = S_2(Q_1, Q_2)^p$ with $\lambda = \lambda_2/\lambda_1$, and we also have $\lambda_1\lambda_2 = p \mod \ell$. If λ is primitive modulo ℓ (argue that this happens often), we have that there exists a such that $\lambda^a = u^{-2}$. Hence $S_2(Q_1, u^{-2}Q_2)^{\lambda_1^a}) = S_2(Q_1, Q_2)^{p^a}$, ie $S_2(Q_1, u^{-2}Q_2)^{(\lambda_1/p)^a} = S_2(Q_1, Q_2)$. But $u^2 = (\lambda_1/\lambda_2)^a \neq (1/\lambda_2)^a$ unless $\lambda_1^a = 1$.

(23) **Actual experiments:** This fails, because a computation shows that the canonical cocycle S induced by the symmetric lift is given by the square root of the Weil pairing.

A.3. **Lifting the DLP.** What we can do is plug $x = -P$; we know $mx = -Q$ and obtain:

$$h_{\ell,Q}(-Q) = \left(\frac{\alpha_m(-2P)}{\alpha_m(-P)}\right)^\ell h_{\ell,P}(-P)^{m^2}.$$

Since $\alpha_m = \psi_m$ and $\psi_{ab}(x) = \psi_a(bx)\psi_b(x)^{a^2}$ (if appropriately normalised at infinity), and $m.P = (x - \psi_{m-1}\psi_{m+1}/\psi_m^2, \psi_{2m}/2\psi_m^4)$ we decuce that

$$h_{l,Q}(-Q) = \left(-2y_Q\psi_{m^3}(-P)/\psi_2(-P)^{n^2}\right)^l h_{l,P}(-P)^{m^2} = (-2y_Q)^l\psi_m(-P)^{3l}(h_{l,P}(-P)/\psi_2(-P)^l)^{n^2}.$$

The unknown are m and $\psi_m(-P)^{3l}$. We obtain an equation in μ_3: $U = V^{n^2}$, which provided that $V \neq 1$ gives us $n^2 \mod 3$, hence if $n = 0, n = \pm 1 \mod 3$.

Actual experiments: But this fails because $V = 1$.

INRIA Bordeaux–Sud-Ouest, 200 avenue de la Vieille Tour, 33405 Talence Cedex FRANCE
Email address: damien.robert@inria.fr
URL: http://www.normalesup.org/~robert/

Institut de Mathématiques de Bordeaux, 351 cours de la liberation, 33405 Talence cedex FRANCE