Decomposition of the Ate Pairing and its Relation to Generalized Pairing Inversion

Takakazu Satoh

e-mail: satoh.df603@gmail.com

Abstract

In this note, we study decomposition of the Ate pairing on certain elliptic curves defined over finite fields. As an application, we reduce a generalized pairing inversion to root findings of an element of the affine coordinate ring appearing in the decomposition. For a supersingular curve $E/\mathbf{F}_q$ satisfying $E(\mathbf{F}_q)=q+1$, heuristic observation suggests that a number of calls to a root finding algorithm seems to $O(N)$ where N is the maximal power of 2 dividing $q+1$. It is remarkable that the resulting algorithm does not utilize fixed argument pairing inversions. An underlying key observation is that the Miller function forms a factor system.

Key words and phrases: Ate pairing, factor system, generalized pairing inversion, GPI

1. Introduction

Let G, G' and T be Abelian groups. For a bilinear pairing $e: G\times G' \to T$, Galbraith, Hess and Vercauteren[8] formulated the following three problems:

Fixed Argument Pairing Inversion 1 (FAPI-1): Given $z\in T$ and $g\in G$, find any $g'\in G'$ satisfying $e(g, g')=z$.

Fixed Argument Pairing Inversion 2 (FAPI-2): Given $z\in T$ and $g'\in G'$, find any $g\in G$ satisfying $e(g, g')=z$.

Generalized Pairing Inversion (GPI): Given $z\in T$, find $g\in G$ and $g\in G'$ satisfying $e(g, g')=z$.

FAPI-1 and FAPI-2 are collectively called FAPI. In cryptographic applications, the groups are often assumed to contain (or be isomorphic to) a cyclic group of a large prime order.

Hardness of pairing inversion is an important assumption to pairing based cryptography. It is obvious that a feasible algorithm for FAPI breaks the bilinear Diffie-Hellman assumption and hence t-strong Diffie-Hellman assumption for any $t\geq 1$. Verheul[22] showed that the Diffie-Hellman problem in the image of the pairing is solved using FAPI. Not only nullifying security assumptions, FAPI often gives direct break for some cryptosystem. See e.g. Galbraith, Hess and Vercauteren[8, end of Sect. III], Duc and Jetchev[6, Sect. 5.2]. We also note that FAPI immediately breaks the verify evaluate algorithm of the KZG polynomial commitment protocol by Kate Zaverucha and Goldberg[12]. On the other hand, implication of GPI to cryptographic protocols is not clear. Joux[11, Chap.4] pointed out that GPI with DLP on G (or G')

solves FAPI.

There are several works on hardness of FAPI which take account of an algorithm to compute a pairing. Those include, but are not limited to, Galbraith, Hess and Vercauteren[8], Satoh[18], Vercauteren[21], Chang et al.[4], Lashermes, Fournier and Goubin[14], Akagi and Nogami[2], Kim and Cheon[13], Satoh[19]. As far as the author knows, there is no work on GPI which utilizes some underlying mathematical structure in computation of the pairing in question.

Let us consider FAPI and GPI for the Ate pairing. The Ate pairing is originally devised to compute the reduced Tate pairing efficiently by Hess, Smart and Vercauteren[10]. Let $\mathbf{F}_q$ be a finite fields with q elements where q is a power of odd prime. Let $E/\mathbf{F}_q$ be an elliptic curve. For simplicity, we restrict ourselves to the case that E is supersingular curve satisfying ${}^{\#}E(\mathbf{F}_q)=q+1$ and $E[2]\subset E(\mathbf{F}_q)$ in this introduction. (See Sect. 5 for general cases.) Let $\mathrm{Tr}_2 : E(\mathbf{F}_{q^2})\to E(\mathbf{F}_q)$ be the trace map. Let l be a large prime divisor of $q+1$. Under these settings, the generalized Ate pairing due to Granger et al. [9] is explicitly given as

$$e(A, Q) := h_{q,A}(Q). \tag{1.1}$$

Here, $A\in(\mathrm{Ker}\,\mathrm{Tr}_2)[l]$, $Q\in E(\mathbf{F}_q)[l]$ and $h_{q,A}$ is the qth Miller function. It is bilinear on $(\mathrm{Ker}\,\mathrm{Tr}_2)[l]\times E(\mathbf{F}_q)[l]$ and thus $e(A, Q)\in\mu_l$, the group of the lth root of unity.

Apparently, GPI is not more difficult than FAPI. However, difficulty to study algorithms for pairing inversions has another story. Solving FAPI-1 is equivalent to finding a zero of the univariate function $h_{q,A}(\cdot)=z$ for given $z\in\mu_l$. On the other hand, solving GPI is not that simple. A naive method first one can think of is to solve the bivariate equation $h_{q,\cdot}(\cdot)=z$, which is more complicated than solving univariate equations. So far, whether one can solve GPI without using FAPI is not known for any specific pairing.

Our method to solve GPI is as follows. We construct a rational function φ (cf. (6.1) and (6.2)) defined over $\mathbf{F}_q$ satisfying

$$h_{q,-A}(Q) = \frac{c_{A,Q}}{\varphi(A+Q)} \text{ with } c_{A,Q} := \frac{(\partial\varphi)(A)\varphi(Q)}{\xi(Q)-\xi(A)} \tag{1.2}$$

for $A\in\mathrm{Ker}\,\mathrm{Tr}_2$ and $Q\in E(\mathbf{F}_q)-E[2]$. Here ∂ is a translation invariant derivation on $\mathbf{F}_q(E)$ (whose definition will be given in Definition 3.5) and ξ is the X-coordinate function. But the precise definition of $c_{A,Q}$ is irrelevant here. What is important here is that $c_{A,Q}\in\mathbf{F}_q^{\times}$ (Theorem 5.3) and that $c_{A,Q}$ seems to take $O(q)$ values when A and Q vary satisfying $h_{q,-A}(Q)=z$.

For a given $z\in\mu_{(q+1)/2}-\{\pm1\}$, we repeat taking a random $c\in\mathbf{F}_q^{\times}$ until $\varphi(2R)=\frac{c}{z}$ have a solution $R\in E(\mathbf{F}_{q^2})-\mathrm{Ker}\,\mathrm{Tr}_2$. Once we obtained such R, we put $A:=R-\mathrm{Fr}_qR$ and $Q:=R+\mathrm{Fr}_qR$. Then $A\in\mathrm{Ker}\,\mathrm{Tr}_2$ and $Q\in E(\mathbf{F}_q)$. Using the assumption $E[2]\subset E(\mathbf{F}_q)$, we can show that A, $Q\in E\left[\frac{q+1}{2}\right]$. Hence $h_{q,-A}(Q)\in\mu_{(q+1)/2}$ by bilinearity of the Ate pairing. Since $A+Q=2R$, we have

$$\frac{h_{q,-A}(Q)}{z} = \frac{h_{q,-A}(Q)}{c/\varphi(A+Q)} = \frac{c_{A,Q}}{c} \in \mu_{(q+1)/2}\cap\mathbf{F}_q^{\times} = \{\pm1\}.$$

We can adjust the sign by adding suitable elements of $E[2]$ to A and Q (Theorem 5.7). Thus we obtained a solution to GPI.

Actually, φ is a product of a polynomial of ξ and the Y-coordinate function. To the best of the author's knowledge, finding R involves a polynomial factorization of degree $\Omega(q)$ over $\mathbf{F}_{q^2}$. Needless to say, unless we have a feasible method to find R, a brute force search seems to be much efficient than our method. Hence our result is only of theoretical interest. We notice that our method does not use FAPI.

The rest of the paper is organized as follows. Sect. 2 describes some group theoretic background why we can expect decomposition (1.2) (and the reason for the minus sign in the left hand side of $-A$ in (1.2)). Sect. 3 summarizes basic properties of derivations on elliptic curves. In Sect. 4, we modify the definition of the Ate pairing so that it is bilinear on whole $\mathrm{Ker}\mathrm{Tr}_2 \times E(\mathbf{F}_q)$. The modification is inevitable since for a non trivial point P of $\mathrm{Ker}\mathrm{Tr}_2 \cap E(\mathbf{F}_q)$, the original definition (1.1) yields $e(P, P) = 0$. We prove our main results on the decomposition of the Ate pairing in Sect. 5. We present our algorithm to solve GPI in Sect. 6 with implementational remarks. In Sect. 7, we discuss a formula used in Sect.4, whose background has an independent interest.

Notation.

Throughout this paper, p denotes a (fixed) odd prime. For a positive integer l prime to p, we denote the group of lth roots of the unity by μ_l. When the characteristic of the field of definition is not 2, we assume that an elliptic curve E is given by the Weierstrass form

$$Y^2 = X^3 + a_2X^2 + a_4X + a_6.$$

The X and Y coordinate functions are denoted by ξ and η, respectively. We use $\tau := -\xi/\eta$ as a local parameter at the point $\mathcal{O}$ at the infinity of E. For $P \in E$, we denote the translation by P map by t_P. That is $t_P(A) = A+P$ for all $A \in E$. Put $\tau_P := \tau \circ t_{-P}$, which is a local parameter at P. For a rational function f on E, we denote by $\mathrm{ord}_P f$ the order of zero of f at P (negative if f has a pole at P). We also denote by $\mathrm{lc}_P(f)$ the leading coefficient of Laurent series expansion of a non-zero rational function f at P w.r.t. τ_P, i.e.,

$$f = \mathrm{lc}_P(f)\tau_P^m + O(\tau_P^{m+1})$$

where $m = \mathrm{ord}_P f$. A non-zero rational function f is said to be normalized if $\mathrm{lc}_{\mathcal{O}}(f) = 1$. Finally, for $P \in E$ and $n \in \mathbf{N}$, we denote by $h_{n,P}$ the normalized n-th Miller function for P, i.e., the normalized rational function satisfying $\mathrm{div} h_{n,P} = n[P] - [nP] - (n-1)[\mathcal{O}]$. We will frequently use the formula $h_{n,P} = (\xi - \xi(P))^{\lfloor n/2 \rfloor}$ for $P \in E[2] - \{\mathcal{O}\}$.

2. The Miller Function as a Factor System

In this section, we observe some group theoretic background for Section 5. Impatient readers can safely skip this section because it is only meant for informative.

Let E be an elliptic curve defined over a perfect field k. Let l be a positive integer prime to $\mathrm{char}(k)$. Put $K := k(E[l])$ for simplicity. Note $\mu_l \subset K$ by Silverman[20,

Cor. III.8.1.1]. The lth Miller function $h_{l,A}$ for $A \in E$ is a unique normalized function satisfying

$$\mathrm{div} h_{l,A} = l[A] - [lA] - (l-1)[\mathcal{O}].$$

For P, $Q \in E[l]$, we have $\mathrm{div} h_{l,P} = l([P] - [\mathcal{O}])$ and thus

$$\mathrm{div} h_{l,-P} \circ t_Q = l([-P-Q] - [-Q]) = l([-P-Q] - [\mathcal{O}]) - l([-Q] - [\mathcal{O}]).$$

So, there exists a constant $c_{P,Q}$ satisfying

$$h_{l,-P} \circ t_Q = c_{P,Q} \frac{h_{l,-P-Q}}{h_{l,-Q}}.$$

Looking at the Laurent expansion at $\mathcal{O}$, we see that $c_{P,Q} = \mathrm{lc}_{\mathcal{O}}(h_{l,-P} \circ t_Q) = \mathrm{lc}_Q(h_{l,-P})$ and that

$$h_{l,-P} \circ t_Q = \mathrm{lc}_Q(h_{l,-P}) \frac{h_{l,-P-Q}}{h_{l,-Q}}.$$

Therefore, for *any* $R \in E$,

$$\mathrm{lc}_R(h_{l,-P} \circ t_Q) = \mathrm{lc}_Q(h_{l,-P}) \frac{\mathrm{lc}_R(h_{l,-P-Q})}{\mathrm{lc}_R(h_{l,-Q})}$$

$$\mathrm{lc}_{Q+R}(h_{l,-P}) \mathrm{lc}_R(h_{l,-Q}) = \mathrm{lc}_Q(h_{l,-P}) \mathrm{lc}_R(h_{l,-P-Q}).$$

In particular, letting $\gamma_l(P, Q) := \mathrm{lc}_Q(h_{l,-P})$, we have

$$\gamma_l(P, Q+R) \gamma_l(Q, R) = \gamma_l(P, Q) \gamma_l(P+Q, R), \tag{2.1}$$

which implies that γ_l is a factor system on $E[l]$ to $K^\times$.

Remark 2.1. We can obtain numerical value of $\gamma(P, Q)$ by a similar method to obtain $h_{l,-P}(Q)$. For A, $B \in E$, let V_A and $L_{A,B}$ be normalized rational functions on E satisfying

$$\mathrm{div} V_A = [A] + [-A] - 2[\mathcal{O}],$$

$$\mathrm{div} L_{A,B} = [A] + [B] + [-A-B] - 3[\mathcal{O}].$$

As is well known, for m, $n \in \mathbf{N}$, it holds that

$$h_{m+n,A} = \frac{L_{nA,mA}}{V_{(m+n)A}} h_{m,A} h_{n,A}.$$

Therefore

$$\mathrm{lc}_Q(h_{m+n,-P}) = \frac{\mathrm{lc}_Q(L_{-mP,-nP})}{\mathrm{lc}_Q(V_{-(m+n)P})} \mathrm{lc}_Q(h_{m,-P}) \mathrm{lc}_Q(h_{n,-P}).$$

Suppose E is given by the Weierstrass form

$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6.$$

Using the addition formula on E, we obtain

$$\xi = \xi(A) + \mathfrak{X}\tau_A + (a_1 \mathfrak{X} - \mathfrak{Y})\tau_A^2 + ((2\xi(A) + a_1^2 + a_2)\mathfrak{X} - a_1 \mathfrak{Y})\tau_A^3 + O(\tau_A^4) \tag{2.2}$$

where $A \in E - \{\mathcal{O}\}$ and

$$\mathfrak{X} := 2\eta(A) + a_1 \xi(A) + a_3,$$

$$\mathfrak{Y} := a_1 \eta(A) - (3\xi(A)^2 + 2a_2 \xi(A) + a_4).$$

Explicitly,

$$V_B = \begin{cases} 1 & (B = \mathcal{O}), \\ \xi - \xi(B) & (B \neq \mathcal{O}). \end{cases}$$

Therefore,

$$\mathrm{lc}_A(V_B) = \begin{cases} 1 & (A = \mathcal{O} \text{ or } B = \mathcal{O}) \\ \xi(A) - \xi(B) & (A \neq \mathcal{O},\ B \neq \mathcal{O},\ A \neq \pm B) \\ \mathfrak{X} & (A \neq \mathcal{O},\ B \neq \mathcal{O},\ A = \pm B,\ A \notin E[2]) \\ -\mathfrak{Y} & (B \neq \mathcal{O},\ A = B \in E[2]). \end{cases}$$

Using (2.2) and the expansion

$$\eta = \eta(A) - \mathfrak{Y}\tau_A + (a_2 + 3\xi(A))\mathfrak{X}\tau_A^2 + ((\mathfrak{X} + 3a_1\xi(A) + a_1a_2)\mathfrak{X} - (2\xi(A) + a_2)\mathfrak{Y})\tau_A^3 + O(\tau_A^4),$$

we also obtain a formula for $\mathrm{lc}_A(L_{B,C})$ which needs $O(1)$ arithmetic operations in K. Thus, we can evaluate $\gamma_l(P,Q)$ with $O(\log l)$ arithmetic operations in K by the standard add-and-double algorithm. Note that the method is applicable to compute $h_{m,P}(Q)$ even in case that Q is a multiple of P.

Let $\bar{\gamma}_l$ be the class of γ_l in the second cohomology group $H^2(E[l], K^\times)$. The class $\bar{\gamma}_l$ is non-trivial, since otherwise γ_l is symmetric, which contradicts to the non-degeneracy of the Weil pairing. Since $E[l]$ is finite, the order of $\bar{\gamma}_l$ is finite. This means that there exists $n \in \mathbf{N}$ and a map $f : E[l] \to K^\times$ satisfying

$$\gamma_l(P, Q)^n = \frac{f(P)f(Q)}{f(P+Q)}. \tag{2.3}$$

Once we observe that such decomposition exists, it is not that difficult to obtain an instance of such n and f (recall that f is only unique up to $\mathrm{Hom}_{(\mathrm{Ab})}(E[l], K^\times)$):

$$n := l, \qquad f(P) := \frac{\mathrm{lc}_P(\psi_l)}{\mathrm{lc}_{\mathcal{O}}(\psi_l)}.$$

Here, ψ_l is the usual lth division function on E, i.e., the unique rational function on E determined by $\mathrm{div}\,\psi_l = \sum_{P \in E[l]} [P] - l^2[\mathcal{O}]$ with normalization $\mathrm{lc}_{\mathcal{O}}(\psi_l) = (-1)^{l-1}l$.

The Tate pairing $\langle P, \bar{Q} \rangle_l$ of $P \in E[l]$ and $\bar{Q} \in E(K)/lE(K)$ is defined to be

$$\langle P, \bar{Q} \rangle_l := \text{equivalence class of } h_{l,A}(Q) \text{ in } K^\times/K^{\times l}.$$

(We note $E(K)[l] = E[l]$ since $K = k(E[l])$.) Since $\gamma_l(P, Q)^l \in K^{\times l}$, decomposition like (2.3) is useless to study Tate pairing inversion if $l \mid n$. To overcome this problem, we work with a subgroup G of $E[l]$ such that the restriction $\gamma_l|_{G \times G}$ defines a trivial class in $H^2(G, K^\times)$, i.e.

$$\gamma_l(P, Q) = \frac{f(P)f(Q)}{f(P+Q)} \tag{2.4}$$

for P, $Q \in G$ with some $f : G \to K^\times$. Since R in (2.1) is arbitrary, there is a good chance that (2.4) holds for $P \in G$ and $Q \in E$. If so, (2.4) gives some information on $h_{l,-P}(Q)$. In Section 5, we take the trace zero subgroup of $E[l]$ for G and observe its implication to the Ate pairing inversion.

3. Derivations on Elliptic Curves

We summarize some basic properties of derivations on elliptic curves. For basic properties on derivations, see e.g. Nakai[16, Chap.1], Cartier[3].

Let R be a unitary commutative ring. Let A be a unitary R-algebra and M a unitary left A-module. Note the action of R on A introduces R module structure to M.

Definition 3.1. A map $\delta: A \to M$ is called an R-derivation from A to M if δ satisfies the following three conditions:

(i) $\delta c = 0$ for $c \in R$.

(ii) $\delta(a+b) = \delta(a) + \delta(b)$ for $a,\ b \in A$.

(iii) $\delta(ab) = a\delta(b) + b\delta(a)$ for $a,\ b \in A$.

The set of such δ is denoted by $\mathrm{Der}_R(A, M)$.

By the definition, $\mathrm{Der}_R(A, M) \subset \mathrm{Hom}_{R\text{-Mod}}(A, M)$, which is a left A-module.

Example 3.2. Let X and Y be indeterminates and consider the case $A = R[X, Y]$. The definition implies that $\delta \in \mathrm{Der}_R(A, M)$ is uniquely determined by $\delta(X)$ and $\delta(Y)$. On the other hand, for any α and $\beta \in M$, the map $\delta_{\alpha,\beta}: A \to M$ defined by

$$\delta_{\alpha,\beta}\left(\sum a_{m,n} X^m Y^n\right) := \sum a_{m,n}(mX^{m-1}Y^n\alpha + nX^mY^{n-1}\beta) \qquad (a_{m,n} \in R)$$

belongs to $\mathrm{Der}_R(A, M)$. Moreover $\delta_{\alpha,\beta}(X) = \alpha$ and $\delta_{\alpha,\beta}(Y) = \beta$. From this, we see $\mathrm{Der}_R(A, M) \cong M \oplus M$ as a left A-module.

Example 3.3. Take $F \in A = R[X, Y]$ and put $\bar{A} := A/\langle F \rangle$ where $\langle F \rangle$ is a principal ideal of A generated by F. Let $\pi: A \to \bar{A}$ be the canonical map. The ring $\bar{A}$ has a natural A-module structure by π. Suppose $\delta \in \mathrm{Der}_R(A, \bar{A})$ satisfies $\delta(F) = 0$. Then δ induces the unique $\bar{\delta} \in \mathrm{Der}_R(\bar{A}, \bar{A})$ characterized by

$$\bar{\delta}(\pi(a)) := \delta(a).$$

This is well-defined because $\delta(F) = 0$.

Example 3.4. Assume that A is an integral domain and denote its quotient field by K. Suppose M is a K vector space. Then, $\delta \in \mathrm{Der}_R(A, M)$ uniquely extends to $\tilde{\delta} \in \mathrm{Der}_R(K, M)$ by

$$\tilde{\delta}\left(\frac{x}{y}\right) = \frac{1}{y^2}(y\delta(x) - x\delta(y)).$$

This is well-defined. In particular, $\tilde{\delta}(x/1) = \delta(x)$. Hence there is no confusion if we identify $\tilde{\delta}$ with δ.

Now we define a derivation from a rational function on an elliptic curve. Let k be a perfect field. Let

$$F(X, Y) := Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6) \in k[X, Y]$$

such that $F(X, Y) = 0$ defines an elliptic curve E/k. We denote the coordinate function for X and Y by ξ and η respectively.

Definition 3.5. Define $\partial_0 \in \mathrm{Der}_k(k[X, Y], k(E))$ by

$$\partial_0(X) := F_Y(\xi, \eta) \ (= 2\eta + a_1\xi + a_3),$$

$$\partial_0(Y) := -F_X(\xi, \eta) \ (= -a_1\eta + 3\xi^2 + 2a_2\xi + a_4).$$

Here, F_X and F_Y are formal partial derivatives of F by X and Y, respectively. Then,

$$\partial_0(F) = F_X(\xi, \eta) \cdot \partial_0(X) + F_Y(\xi, \eta) \cdot \partial_0(Y) = 0.$$

Thus ∂_0 induces $\partial \in \mathrm{Der}_k(k[E], k(E))$. Then ∂ extends to $\mathrm{Der}_k(k(E), k(E))$ which is also written as ∂. When there is no fear of confusion, we write $\partial(f)$ as ∂f.

Proposition 3.6. *The derivation ∂ is translation invariant, i.e.,*

$$\partial(f \circ t_A) = \partial(f) \circ t_A \tag{3.1}$$

for $f \in k(E)$ and $A \in E$.

Proof. Let $\omega := \dfrac{1}{2\eta + a_1\xi + a_3} d\xi \in \Omega^1(E)$ be the invariant differential. Note that

$$df = (\partial f)\omega \tag{3.2}$$

for $f \in k(E)$. Since $d \in \mathrm{Der}_k(k(E), \Omega^1(E))$ and $\partial \in \mathrm{Der}_k(k(E), k(E))$, it is enough to show (3.2) for generators ξ, η of $k(E)/k$. For these cases, (3.2) is an immediate consequence of the definition of ∂. Therefore,

$$(\partial(f \circ t_A))\omega = d(f \circ t_A) = t_A^*(df) = t_A^*((\partial f)\omega) = t_A^*(\partial f) t_A^* \omega = ((\partial f) \circ t_A)\omega$$

by the translation invariant property of ω (Silverman[20, Prop. III.5.1]). Since $\Omega^1(E)$ is a one dimensional $k(E)$ vector space and $\omega \neq 0$, we have (3.1). □

Recall that $\tau = -\xi/\eta$. Using $\mathrm{ord}_{\mathcal{O}} \partial\xi \geq -3$ and $\mathrm{ord}_{\mathcal{O}} \partial\eta \geq -4$, we see $\mathrm{ord}_{\mathcal{O}} \partial f \geq \mathrm{ord}_{\mathcal{O}} f - 1$ for any $f \in k[E] - \{0\}$ and thus for any $f \in k(E)^\times$. This implies that ∂ is uniformly continuous with respect to τ adic valuation on $k(E)$. Hence ∂ extends to $\mathrm{Der}_k(k((\tau)), k((\tau)))$ which satisfies

$$\partial\left(\sum_{n=N}^{\infty} c_n \tau^n\right) = \left(\sum_{n=N}^{\infty} n c_n \tau^{n-1}\right) \partial\tau \tag{3.3}$$

and $\mathrm{ord}_{\mathcal{O}} \partial(f) \geq \mathrm{ord}_{\mathcal{O}} f - 1$ for any $f \in k((\tau))^\times$. Moreover, if f is regular at $\mathcal{O}$, then ∂f is also regular at $\mathcal{O}$. Observe that

$$\begin{aligned} \partial\tau &= \partial\left(-\frac{\xi}{\eta}\right) = -\frac{\eta\partial\xi - \xi\partial\eta}{\eta^2} \\ &= -\frac{-a_3\eta - \xi^3 + a_4\xi + 2a_6}{\eta^2} = 1 + \frac{a_1\xi\eta - a_2\xi^2 + 2a_3\eta - 2a_4\xi - 3a_6}{\eta^2}. \end{aligned}$$

Since

$$-5 = \mathrm{ord}_{\mathcal{O}}(\xi\eta) < \mathrm{ord}_{\mathcal{O}}(\xi^2) < \mathrm{ord}_{\mathcal{O}}\eta < \mathrm{ord}_{\mathcal{O}}\xi < \mathrm{ord}_{\mathcal{O}}1 = 0,$$

we see $\partial\tau \neq 1$ in case of $\mathrm{char}(k) \neq 2$. (In case of $\mathrm{char}(k) = 3$, the curve $Y^2 = X^3 + a_6$ is singular because k is perfect.) However, we have

$$\partial\tau = 1 - a_1\tau - a_2\tau^2 - 2a_3\tau^2 - 2(a_1a_3 + a_4)\tau^4 + O(\tau^5)$$

and in particular $\partial\tau = 1 + O(\tau)$. By the translation invariance (3.1) of ∂, we have $\partial\tau_A = 1 + O(\tau_A)$ for any $A \in E$. Similarly, we see that $\mathrm{ord}_A \partial f \geq \mathrm{ord}_A f - 1$ for $f \in k((\tau_A))^\times$ and that ∂f is regular at A if f is regular at A.

Let $f \in k(E)$ and suppose f is regular at $A \in E$. Let $\sum_{n=0}^{\infty} \alpha_n \tau_A^n$ be the expansion of f at A by τ_A. Note that $\alpha_0 = f(A)$. Since

$$\partial f = \alpha_1 \partial\tau_A + 2\alpha_2 \tau_A \partial\tau_A + O(\tau_A^2) = \alpha_1 + O(\tau_A)$$

we have

$$\alpha_1 = (\partial f)(A) \tag{3.4}$$

and thus

$$f = f(A) + (\partial f)(A)\tau_A + O(\tau_A^2).$$

In particular

$$\mathrm{lc}_A(f) = (\partial f)(A) \text{ if } \mathrm{ord}_A f = 1. \tag{3.5}$$

Perhaps, the most significant different property between derivations and usual differential is lack of a chain rule. In the first place, in Definition 3.1, M is just a left A-module and it is unclear what does the "chain" mean. However, we have a chain rule like formula for ∂.

Theorem 3.7. *Let Φ be an endomorphism on E whose field of definition is K. Define $c \in K$ by*

$$\tau \circ \Phi = c\tau + O(\tau^2).$$

(Note c is independent of choice of a local parameter at $\mathcal{O}$.) For $f \in K(E)$, we have

$$\partial(f \circ \Phi) = c\,\partial(f) \circ \Phi. \tag{3.6}$$

Proof. The assertion is clear for the case $\Phi = \mathcal{O}$ (a constant map). Suppose $\Phi \neq \mathcal{O}$. Then Φ is surjective. Let $N := \{A \in E : f$ is regular at A and $\Phi(A)\}$, which is an open dense subset of E. Let $A \in N$. Let

$$f = \sum_{n=0}^{\infty} \alpha_n \tau_{\Phi(A)}^n$$

be the Taylor expansion of f at $\Phi(A)$. Then, by (3.4),

$$\alpha_1 = (\partial f)(\Phi(A)) = ((\partial f) \circ \Phi)(A). \tag{3.7}$$

Since $\Phi = t_{\Phi(A)} \circ \Phi \circ t_{-A}$, we have

$$\begin{aligned} f \circ \Phi &= \sum_{n=0}^{\infty} \alpha_n (\tau \circ \Phi \circ t_{-A})^n \\ &= \sum_{n=0}^{\infty} \alpha_n ((c\tau + O(\tau^2)) \circ t_{-A})^n \\ &= \sum_{n=0}^{\infty} \alpha_n (c\tau_A + O(\tau_A^2))^n \\ &= \alpha_0 + c\alpha_1 \tau_A + O(\tau_A^2). \end{aligned}$$

Noting (3.4), we have $\partial(f \circ \Phi)(A) = c\alpha_1$. By (3.7), we have

$$(\partial(f \circ \Phi))(A) = (c(\partial f) \circ \Phi)(A)$$

for all $A \in N$. Since N is open dense, we have (3.6). □

Corollary 3.8. *Let $f \in k(E)$. Then ∂f is odd (resp. even) if f is even (resp. odd).*

Proof. Let $[-1]$ be the multiplication by -1 map on E. Then, $\tau \circ [-1] = -\tau + O(\tau^2)$. By (3.7),

$$\partial(f \circ [-1]) = -(\partial f) \circ [-1]. \tag{3.8}$$

In case that f is even, it holds that $f \circ [-1] = f$ and (3.8) reduces to

$$\partial f = -(\partial f) \circ [-1].$$

This shows that ∂f is odd. Similarly, in case that f is odd, $f \circ [-1] = -f$ and thus

$$-(\partial f) = -(\partial f)\circ[-1],$$

which shows that ∂f is even. □

4. The Ate Pairing on Supersingular Curves

Let $E/\mathbf{F}_q$ be an supersingular elliptic curves satisfying $^{\#}E(\mathbf{F}_q)=q+1$. For such a curve, not only a specific cyclic subgroup of $E(\mathbf{F}_q)$ but also the entire $E(\mathbf{F}_q)$ has embedding degree two. In our application to the generalized pairing inversion, it is desirable to have a bilinear pairing on the whole group $E(\mathbf{F}_q)$ and the trace zero subgroup of $E(\mathbf{F}_{q^2})$. However these two groups have a nontrivial intersection. Let P be a such point. Evaluation of the self pairing of P by the usual definition of the Ate paring results in zero, which is unacceptable. In this section, we modify the definition of the Ate pairing Granger et al.[9, Theorem2] so that the resulting pairing is bilinear on entire $E(\mathbf{F}_q)$ and the trace zero subgroup. We show its image contains at least $\mu_{(q+1)/2}$ in Theorem 4.8 and Theorem 4.9.

Let q be a power of an odd prime p and let $E/\mathbf{F}_q$ be an elliptic curve. In this section, we assume that E is defined by the Weierstrass equation satisfying $a_1=a_3=0$. Let $K/\mathbf{F}_q$ be a finite algebraic extension of degree n We denote by Fr_q the Frobenius automorphism of $\mathrm{Gal}(K/\mathbf{F}_q)$. Thus $\mathrm{Fr}_q(c)=c^q$ for $c\in K$. The action extends to $K(E)$ where Fr_q acts trivially on ξ and η. On the other hand, the q power Frobenius endomorphism of E is also denoted by Fr_q:

$$\mathrm{Fr}_q(P) = (\xi(P)^q, \eta(P)^q)$$

for $P\in E(K)-\{\mathcal{O}\}$. This overloaded notation does not give rise to ambiguity. Note, for $f\in K(E)$ and $P\in E(K)$ satisfying $\mathrm{ord}_P f\ge 0$, it holds that

$$\mathrm{Fr}_q(f(P)) = (\mathrm{Fr}_q(f))(\mathrm{Fr}_q(P)).$$

We define $\mathrm{Tr}_n\in\mathrm{End}(E)$ by $\mathrm{Tr}_n(P):=\sum_{i=0}^{n-1}\mathrm{Fr}_q^{\,i}(P)$ where $P\in E$. Note $\mathrm{Tr}_n(P)\in E(\mathbf{F}_q)$ for $P\in E(\mathbf{F}_{q^n})$.

Lemma 4.1. *Let $K/\mathbf{F}_q$ be an algebraic extension. For $f\in K(E)$ and $P\in E(K)$, we have*

$$\mathrm{lc}_P(f^q) = \mathrm{lc}_{\mathrm{Fr}_q(P)}(\mathrm{Fr}_q(f)). \tag{4.1}$$

Proof. Put $n:=\mathrm{ord}_P f$ and $a:=\mathrm{lc}_P(f)$ for simplicity. Then, there exists $g\in K(E)$ satisfying $\mathrm{ord}_P g\ge 1$ and

$$f = \tau_P^n\cdot(a+g).$$

Since $\mathrm{Fr}_q(\tau_P)=\tau_{\mathrm{Fr}_q(P)}$, we have

$$\mathrm{Fr}_q(f) = \tau_{\mathrm{Fr}_q(P)}^n(\mathrm{Fr}_q(a)+\mathrm{Fr}_q(g)).$$

This implies

$$\mathrm{lc}_{\mathrm{Fr}_q(P)}\mathrm{Fr}_q(f) = \mathrm{Fr}_q(a) = a^q. \tag{4.2}$$

On the other hand, $f^q=\tau_P^{nq}(a^q+g^q)$ which implies

$$\mathrm{lc}_P(f^q) = a^q. \tag{4.3}$$

Combining (4.2) and (4.3), we obtain (4.1). □

In the rest of this section, we assume that E is a supersingular curve satisfying $\#E(\mathbf{F}_q)=q+1$. This implies $\widehat{\mathrm{Fr}_q}=-\mathrm{Fr}_q$ where $\widehat{\ }$ denotes the dual isogeny. Note that $\widehat{\mathrm{Tr}_2}=1-\mathrm{Fr}_q$ and that $\mathrm{Ker}\widehat{\mathrm{Tr}_2}=E(\mathbf{F}_q)$. By the non-degeneracy of the generalized Weil pairing on $\mathrm{Ker}\mathrm{Tr}_2\times\mathrm{Ker}\widehat{\mathrm{Tr}_2}$ (see e.g. Silverman[20, Exercise 3.15]), we see

$$\mathrm{Ker}\mathrm{Tr}_2 \cong \mathrm{Ker}\widehat{\mathrm{Tr}_2} = E(\mathbf{F}_q) \tag{4.4}$$

as an Abelian group. For simplicity we put $r:=q^2$. By Menezes, Okamoto and Vanstone[15, Table 1],

$$E(\mathbf{F}_q) \cong \begin{cases} \mathbf{Z}/\dfrac{q+1}{2}\mathbf{Z}\oplus\mathbf{Z}/2\mathbf{Z}, & (E[2]\subset E(\mathbf{F}_q)) \\ \mathbf{Z}/(q+1)\mathbf{Z} & (E[2]\not\subset E(\mathbf{F}_q)), \end{cases} \tag{4.5}$$

$$E(\mathbf{F}_r) = E[q+1] \cong \mathbf{Z}/(q+1)\mathbf{Z}\oplus\mathbf{Z}/(q+1)\mathbf{Z}. \tag{4.6}$$

Definition 4.2. Let $A,\ B\in E$. We define two rational functions V_A and $L_{A,B}$ as the unique normalized functions satisfying

$$\mathrm{div}(V_A) = [A]+[-A]-2[\mathcal{O}],$$
$$\mathrm{div}(L_{A,B}) = [A]+[B]+[-A-B]-3[\mathcal{O}],$$

respectively. Explicitly,

$$V_A = \begin{cases} \xi-\xi(A) & (A\neq\mathcal{O}), \\ 1 & (A=\mathcal{O}). \end{cases} \tag{4.7}$$

Note $L_{A,\mathcal{O}}=L_{\mathcal{O},A}=L_{A,-A}=V_A$. In case of $A\neq\mathcal{O},\ B\neq\mathcal{O},\ A+B\neq\mathcal{O}$,

$$L_{A,B} = \lambda(\xi-\xi(A))-\eta+\eta(A) \tag{4.8}$$

where

$$\lambda := \begin{cases} \dfrac{\eta(B)-\eta(A)}{\xi(B)-\xi(A)} & (A\neq\pm B), \\ \dfrac{3\xi(A)^2+2a_2\xi(A)+a_4}{2\eta(A)} & (A=B\notin E[2]). \end{cases}$$

Definition 4.3. The Ate pairing on $E/\mathbf{F}_q$ is a map $e:\mathrm{Ker}\mathrm{Tr}_2\times E(\mathbf{F}_q)\to\mathbf{F}_r^\times$ defined by

$$e(A,Q) := \mathrm{lc}_Q(h_{q,A}) \quad (A\in\mathrm{Ker}\mathrm{Tr}_2,\ Q\in E(\mathbf{F}_q)).$$

Remark 4.4. In case of $Q\notin\mathrm{supp}(\mathrm{div}h_{q,A})=\{\mathcal{O},\pm A\}$, the definition is nothing but $e(A,Q):=h_{q,A}(Q)$, which essentially coincides with the definition by Granger et al.[9, Theorem 2]. In case of $Q=\mathcal{O}$, by the normalization of the Miller function, $e(A,\mathcal{O})=1$ regardless of A. In case of $Q\neq\mathcal{O}$ but $Q=\pm A$, we see $Q\in\mathrm{Ker}\mathrm{Tr}_2\cap E(\mathbf{F}_q)\subset E[2]$, which implies $Q=A\in E[2]$.

Theorem 4.5. *The Ate pairing is bilinear on* $\mathrm{Ker}\mathrm{Tr}_2\times E(\mathbf{F}_q)$.

Proof. First we show the linearity with respect to $\mathrm{Ker}\mathrm{Tr}_2$. Let $A,\ B\in\mathrm{Ker}\mathrm{Tr}_2$. Then

$$\mathrm{div}\left(\frac{h_{q,A}h_{q,B}}{h_{q,A+B}}\right) = q([A]+[B]-[A+B]-[\mathcal{O}])-([-A]+[-B]-[A+B]-[\mathcal{O}]) = \mathrm{div}\left(\frac{(L_{A,B}/V_{A+B})^q}{L_{-A,-B}/V_{A+B}}\right)$$

Therefore

$$\frac{h_{q,A}h_{q,B}}{h_{q,A+B}} = \frac{(L_{A,B}/V_{A+B})^q}{L_{-A,-B}/V_{-A-B}}$$

since both hands sides are normalized. Taking the leading coefficients at $Q \in E(\mathbf{F}_q)$, we have

$$\frac{e(A, Q)e(B, Q)}{e(A+B, Q)} = \frac{\mathrm{lc}_Q((L_{A,B}/V_{A+B})^q)}{\mathrm{lc}_Q(L_{-A,-B}/V_{-A-B})} = \frac{\mathrm{lc}_{\mathrm{Fr}_q(Q)}(\mathrm{Fr}_q(L_{A,B})/\mathrm{Fr}_q(V_{A+B}))}{\mathrm{lc}_Q(L_{-A,-B}/V_{-A-B})}.$$

by Lemma 4.1 Since $Q \in E(\mathbf{F}_q)$, it holds that $\mathrm{Fr}_q(Q) = Q$. By (4.7) and (4.8), we see $\mathrm{Fr}_q(V_A) = V_{\mathrm{Fr}_q(A)}$ and $\mathrm{Fr}_q(L_{A,B}) = L_{\mathrm{Fr}_q(A),\,\mathrm{Fr}_q(B)}$. By the assumption $A,\ B \in \mathrm{Ker}\,\mathrm{Tr}_2$, we have

$$\frac{e(A, Q)e(B, Q)}{e(A+B, Q)} = \frac{\mathrm{lc}_Q(L_{-A,-B}/V_{-A-B})}{\mathrm{lc}_Q(L_{-A,-B}/V_{-A-B})} = 1.$$

The linearity with respect to $E(\mathbf{F}_q)$. Let $A \in \mathrm{Ker}\,\mathrm{Tr}_2$ and $P, Q \in E(\mathbf{F}_q)$. We have to show

$$\mathrm{lc}_P(h_{q,A})\mathrm{lc}_Q(h_{q,A}) = \mathrm{lc}_{P+Q}(h_{q,A}). \tag{4.9}$$

First, we prove some simple cases. In case of $A = \mathcal{O}$, this is trivial since $h_{q,\mathcal{O}} = 1$ (a constant function). Since $h_{q,A}$ is normalized, (4.9) holds for either $P = \mathcal{O}$ or $Q = \mathcal{O}$. Since q is odd, $h_{q,A} \circ [-1] = h_{q,-A}$. Noting that in fact V_A is defined over $\mathbf{F}_q$ for any $A \in \mathrm{Ker}\,\mathrm{Tr}_2$, we have

$$\mathrm{lc}_Q(h_{q,A})\mathrm{lc}_{-Q}(h_{q,A}) = \mathrm{lc}_Q(h_{q,A})\mathrm{lc}_Q(h_{q,-A}) = \mathrm{lc}_Q(V_A^{q-1}) = (\mathrm{lc}_Q(V_A))^{q-1} = 1 = \mathrm{lc}_{\mathcal{O}}(h_{q,A}) \tag{4.10}$$

for all $Q \in E(\mathbf{F}_q)$. Hence (4.9) is valid for the case $P + Q = \mathcal{O}$. In case of $A = \pm P$, it holds that $A = P \in E[2] \cap E(\mathbf{F}_q)$. Thus, $h_{q,A} = V_A^{(q-1)/2}$. Since $A \in E[2]$, we see

$$\mathrm{div}(V_A \cdot (V_A \circ t_A)) = 2([A] - [\mathcal{O}]) + 2([\mathcal{O}] - [A]) = 0$$

Hence, there exists a constant $c \in \mathbf{F}_q^\times$ satisfying $V_A \cdot (V_A \circ t_A) = c$. Looking at the expansion at $\mathcal{O}$, we obtain $c = \mathrm{lc}_A(V_A)$. Taking $(q-1)/2$ power, we obtain

$$\mathrm{lc}_Q(h_{q,A} \cdot h_{q,A} \circ t_A) = c^{(q-1)/2} = \mathrm{lc}_A(h_{q,A}).$$

Thus

$$\mathrm{lc}_Q(h_{q,A})\mathrm{lc}_{Q+A}(h_{q,A}) = \mathrm{lc}_A(h_{q,A}).$$

Noting $\mathrm{lc}_Q(h_{q,A}) = \mathrm{lc}_Q(V_A)^{(q-1)/2} = \pm 1$, we have

$$\mathrm{lc}_{Q+A}(h_{q,A}) = \mathrm{lc}_A(h_{q,A})\mathrm{lc}_Q(h_{q,A}).$$

Since $A = P$, we obtain (4.9). The case $A = \pm Q$ is proved in the same way. Suppose $A = \pm(P+Q)$. Again, $A = P+Q \in E[2]$. We have already showed that (4.9) holds in case of $A = P \in E[2]$. Substituting (P, Q) in (4.9) with $(P+Q, -Q)$, we obtain

$$\mathrm{lc}_{P+Q}(h_{q,A})\mathrm{lc}_{-Q}(h_{q,A}) = \mathrm{lc}_P(h_{q,A}).$$

By (4.10), we obtain (4.9).

Now we assume

$$\begin{aligned} &A \neq \mathcal{O},\ P \neq \mathcal{O},\ Q \neq \mathcal{O}\ , P+Q \neq \mathcal{O} \\ &A \neq \pm P,\ A \neq \pm Q \text{ and } A \neq \pm(P+Q), \end{aligned} \tag{4.11}$$

in what follows. By a similar computation as above, we have

$$\mathrm{lc}_A\left(\frac{h_{q,P}h_{q,Q}}{h_{q,P+Q}}\right) = \frac{\mathrm{lc}_A((L_{P,Q}/V_{P+Q})^q)}{\mathrm{lc}_A(L_{-P,-Q}/V_{-P-Q})} = \frac{\mathrm{lc}_{\mathrm{Fr}_q(A)}(L_{P,Q}/V_{P+Q})}{\mathrm{lc}_A(L_{-P,-Q}/V_{-P-Q})}$$

by Lemma 4.1. Since $A \in \mathrm{Ker}\mathrm{Tr}_2$, it holds that $\mathrm{Fr}_q(A) = -A$. Put $g_{P,Q} := L_{P,Q}/V_{P+Q}$ for simplicity. By (4.7) and (4.8), we have $g_{P,Q}{}^{\circ}[-1] = -g_{-P,-Q}$. Thus $\mathrm{lc}_{-A}(g_{P,Q}) = -(-1)^{\mathrm{ord}_A(g_{P,Q})}\mathrm{lc}_A(g_{-P,-Q})$. Therefore,

$$\mathrm{lc}_A\left(\frac{h_{q,P}h_{q,Q}}{h_{q,P+Q}}\right) = -(-1)^{\mathrm{ord}_A(g_{P,Q})}. \tag{4.12}$$

Under the condition (4.11), $\mathrm{ord}_A g_{P,Q} = \mathrm{ord}_A h_{q,P} = \mathrm{ord}_A h_{q,Q} = \mathrm{ord}_A h_{q,P+Q} = 0$. Then (4.12) yields

$$\frac{h_{q,P}(A)h_{q,Q}(A)}{h_{q,P+Q}(A)} = -1.$$

Let W_{q+1} be the $(q+1)$st Weil pairing on E, defined as in Silverman[20, Sect. III.8]. It holds that

$$W_{q+1}(R, S) = \frac{h_{q+1,S}(R)}{h_{q+1,R}(S)} = -\frac{h_{q,S}(R)}{h_{q,R}(S)}$$

for R, $S \in E[q+1] - \{\mathcal{O}\}$, $R \neq \pm S$. See Enge[7, (8)]. Therefore,

$$\frac{W_{q+1}(A, P)h_{q,A}(P)W_{q+1}(A, Q)h_{q,A}(Q)}{W_{q+1}(A, P+Q)h_{q,A}(P+Q)} = 1.$$

By the bilinearity of the Weil pairing, we have (4.9). This completes the proof. □

Lemma 4.6. *It holds that*

$$E[2] \cap E(\mathbf{F}_q) = E[2] \cap \mathrm{Ker}\mathrm{Tr}_2 = E(\mathbf{F}_q) \cap \mathrm{Ker}\mathrm{Tr}_2. \tag{4.13}$$

Proof. Put $I := E[2] \cap E(\mathbf{F}_q) \cap \mathrm{Ker}\mathrm{Tr}_2$. We prove that the three sets in (4.13) is, in fact, equal to I.

Let $Q \in E[2] \cap E(\mathbf{F}_q)$. Then $\mathrm{Fr}_q Q = Q$. Since $Q \in E[2]$, it holds that $Q = -Q$, Hence $\mathrm{Fr}_q Q = -Q$, which implies $Q \in \mathrm{Ker}\mathrm{Tr}_2$. Thus, $E[2] \cap E(\mathbf{F}_q) \subset I$.

Let $A \in E[2] \cap \mathrm{Ker}\mathrm{Tr}_2$. Then $\mathrm{Fr}_q A = -A$. Since $A \in E[2]$, it holds that $-A = A$. Hence $\mathrm{Fr}_q A = A$, which implies $A \in E(\mathbf{F}_q)$. Thus $E[2] \cap \mathrm{Ker}\mathrm{Tr}_2 \subset I$.

Finally, let $R \in E(\mathbf{F}_q) \cap \mathrm{Ker}\mathrm{Tr}_2$. We have $\mathrm{Fr}_q R = R$ and $\mathrm{Fr}_q R = -R$. Thus $R = -R \in E[2]$, which implies $E(\mathbf{F}_q) \cap \mathrm{Ker}\mathrm{Tr}_2 \subset I$.

The converse inclusions are obvious. □

Theorem 4.7. *Let q be a power of p. Let $E/\mathbf{F}_q$ be a supersingular elliptic curve satisfying $\#E(\mathbf{F}_q) = q+1$. Denote the $(q+1)$st Weil pairing on E by W_{q+1}. For $A \in E(\mathbf{F}_{q^2}) - \{\mathcal{O}\}$ satisfying $\mathrm{Fr}_q(A) = -A$ and $Q \in E(\mathbf{F}_q) - \langle A \rangle$, it holds that*

$$W_{q+1}(A, Q) = h_{q,A}(Q)^{-2}. \tag{4.14}$$

Proof. Note $h_{q,A}(Q) \neq 0$ by $Q \notin \langle A \rangle$. As is well known (see e.g. Enge[7, (8)]),

$$W_{q+1}(A, Q) = \frac{h_{q+1,Q}(A)}{h_{q+1,A}(Q)} = -\frac{h_{q,Q}(A)}{h_{q,A}(Q)}. \tag{4.15}$$

We need an another relation

$$h_{q,Q}(A) = -h_{q,-A}(Q)^{-q}, \tag{4.16}$$

which follows from (7.4) and (7.6) . Applying (4.16) to the numerator of (4.14), we

obtain

$$W_{q+1}(A, Q) = -\frac{h_{q,Q}(A)}{h_{q,A}(Q)} = \frac{h_{q,-A}(Q)^{-q}}{h_{q,A}(Q)}.$$

Since E is defined over $\mathbf{F}_q$,

$$h_{q,-A}(Q)^q = \mathrm{Fr}_q(h_{q,-A}(Q)) = h_{q,\mathrm{Fr}_q(-A)}(\mathrm{Fr}_q(Q)) = h_{q,A}(Q),$$

which completes the proof of (4.14). □

Theorem 4.8. *Suppose* $E[2] \subset E(\mathbf{F}_q)$. *Put* $l := \frac{q+1}{2}$. *There exist* $A \in \mathrm{Ker}\,\mathrm{Tr}_2$ *and* $Q \in E(\mathbf{F}_q)$ *such that* $e(A, Q)$ *is a primitive* l *th root of the unity.*

Proof. Write $l = 2^m n$ where n is odd. The assumption $E[2] \subset E(\mathbf{F}_q)$ implies that $q \equiv 3 \bmod 4$ and that $m \geq 1$.

The case $m = 1$. We first prove that for any $P \in E[2] - \{\mathcal{O}\}$, there exists $A \in \mathrm{Ker}\,\mathrm{Tr}_2$ of order l satisfying $\frac{l}{2}A = P$. Let A_0 be any element in $\mathrm{Ker}\,\mathrm{Tr}_2$ whose order is l. Put $A := A_0 + (P - nA_0)$. Since the order of $P - nA_0$ is two,

$$nA = nA_0 + (P - nA_0) = P.$$

This also shows $A \neq \mathcal{O}$. Let s be the order of A. By the definition of A, we have

$$sP = s(n-1)A_0. \tag{4.17}$$

Hence $2s(n-1)A_0 = \mathcal{O}$. Thus $2n \mid 2s(n-1)$, which yields $n \mid s$. Suppose $s = n$, which is odd. Then (4.17) yields

$$P = \frac{n-1}{2} \cdot (2n)A_0 = \mathcal{O}.$$

This contradicts to $P \neq \mathcal{O}$. It is clear that $2nA = \mathcal{O}$. Thus, $s = 2n = l$.

Similarly, for any $P \in E[2] - \{\mathcal{O}\}$, there exists $Q \in E(\mathbf{F}_q)$ of order l satisfying $\frac{l}{2}Q = P$.

Choose P_0, $P_1 \in E[2]$ satisfying $P_0 \neq P_1$ and $e(P_0, P_1) = -1$. This is possible since $e(P_0, P_1) = -e(P_1, P_0)$ for $P_0 \neq P_1$ in case of $q \equiv 3 \bmod 4$. Let $A \in \mathrm{Ker}\,\mathrm{Tr}_2$ be of order l satisfying $\frac{l}{2}A = P_0$ and let $Q \in E(\mathbf{F}_q)$ be of order l satisfying $\frac{l}{2}Q = P_1$. We show $\langle A \rangle \cap \langle Q \rangle = \{\mathcal{O}\}$, where $\langle g \rangle$ stands for the cyclic group generated by g. Observe that $\langle A \rangle \cap \langle Q \rangle \subset \mathrm{Ker}\,\mathrm{Tr}_2 \cap E(\mathbf{F}_q) = E[2]$ by (4.13). However $\langle A \rangle \cap E[2] = \{P_0, \mathcal{O}\}$ and $\langle Q \rangle \cap E[2] = \{P_1, \mathcal{O}\}$. Since $P_0 \neq P_1$, we have $\langle A \rangle \cap \langle Q \rangle = \{\mathcal{O}\}$. Thus $\langle A \rangle \oplus \langle Q \rangle = E[l]$. Put $z := W_l(A, Q)$ where W_l is the Weil l pairing. Since $W_l : E[l] \times E[l] \to \mu_l$ is surjective, z is a primitive lth root of the unity. By the compatibility property of the Weil pairing (see e.g. Silverman[20, Prop. III.8.1(e)]), $W_{q+1}(A, Q) = z^2$. Note $l \geq 2$ and $z \neq 1$, hence $Q \neq \pm A$. By Theorem 4.7, we see $e(A, Q) = h_{q,A}(Q) = \pm z^{-1}$. Suppose $e(A, Q) = -z$. Then $e(P_0, Q) = (-1)^n \cdot z^{-l/2} = 1$, a fortiori, $e(P_0, P_1) = 1$, which contradicts to the choice of P_0 and P_1. Hence $e(A, Q) = z^{-1}$, which completes the proof for the case $m = 1$.

The case $m \geq 2$. Take $A \in \mathrm{Ker}\,\mathrm{Tr}_2$ and $Q \in E(\mathbf{F}_q)$ of order l. Put $P_0 := \frac{l}{2}A$ and $P_1 := \frac{l}{2}Q$. We assert $P_0 \neq P_1$. Assume contrarily $P_0 = P_1$. Put $R := \frac{l}{4}(A - Q)$. (Note that $m \geq 2$ implies $4 \mid l$.) Then $R \in E[2] \subset E(\mathbf{F}_q)$. This yields $\frac{l}{4}A = \frac{l}{4}Q + R \in E(\mathbf{F}_q)$. Since $A \in \mathrm{Ker}\,\mathrm{Tr}_2$, $\frac{l}{4}A \in E(\mathbf{F}_q) \cap \mathrm{Ker}\,\mathrm{Tr}_2 = E[2]$. This contradicts to the choice of A since the order of $\frac{l}{4}A$ is 4. As above, we see that $\langle A \rangle \cap \langle Q \rangle = \{\mathcal{O}\}$ and that $\langle A \rangle \oplus \langle Q \rangle = E[l]$. Thus

$e(A, Q) = \pm W_l(A, Q)$. Since $4 \mid l$, the order of $e(A, Q)$ is equal to the order of $W_l(A, Q)$ which is l. □

Theorem 4.9. *Suppose* $E[2] \not\subset E(\mathbf{F}_q)$. *In case of* $q \equiv 3 \bmod 4$, *there exist* $A \in \mathrm{Ker}\,\mathrm{Tr}_2$ *and* $Q \in E(\mathbf{F}_q)$ *such that* $e(A, Q)$ *is a primitive* $(q+1)$*st root of the unity. In case of* $q \equiv 1 \bmod 4$, *There exist* $A \in \mathrm{Ker}\,\mathrm{Tr}_2$ *and* $Q \in E(\mathbf{F}_q)$ *such that* $e(A, Q)$ *is ether a primitive* $(q+1)$*st root of the unity or a primitive* $\dfrac{q+1}{2}$ *th root of the unity.*

Proof. Take $Q \in E(\mathbf{F}_q)$ of order $q+1$. Since $E(\mathbf{F}_r) = E[q+1]$ is a free $\mathbf{Z}/(q+1)\mathbf{Z}$ module of rank 2, there exist $B \in E(\mathbf{F}_r)$ such that $\langle Q, B \rangle = E[q+1]$. Put $z := W_{q+1}(B, Q)$, which is a primitive $(q+1)$st root of the unity. Put $A := B - \mathrm{Fr}_q B$. Clearly, $A \in \mathrm{Ker}\,\mathrm{Tr}_2$. By the Galois compatibility and bilinearity of the Weil pairing, $W_{q+1}(A, Q) = z^{1-q} = z^{2-(q+1)} = z^2$. Thus, $e(A, Q) = \pm z^{-1}$ by Theorem 4.7. In case of $q \equiv 3 \bmod 4$, that is, $4 \mid q+1$, the order of $-z^{-1}$ is equal to the order of z^{-1}. In ether way, $e(A, Q)$ is a primitive $(q+1)$st root of the unity. In case of $q \equiv 1 \bmod 4$, that is, $2 \mid q+1$ but $4 \nmid q+1$, the order of $-z^{-1}$ is $\dfrac{q+1}{2}$. This completes the proof. □

5. Decomposition of the Ate Pairing

The aim of this section is to prove the decomposition formula (Theorem 5.3) of the Ate pairing. As an application, we observe how it is related to generalized pairing inversion (Theorem 5.5).

Let q be a power of an odd prime p. Let $E/\mathbf{F}_q$ be an elliptic curve defined by $F(X, Y) = 0$ where

$$F(X, Y) = Y^2 - (X^3 + a_2 X^2 + a_4 X + a_6)$$

as in Sect. 4. In particular, in case that E is supersingular, $\#E(\mathbf{F}_q) = q+1$. We now define two subgroups of E and some integers depending on whether E is ordinary or supersingular. Once they are defined, we can state our results regardless of supersingularity of E.

In case that E is ordinary: Let l be an odd prime dividing $\#E(\mathbf{F}_q)$. We denote the embedding degree for l by k. We assume that $2 \mid k$ and $l \nmid k$. Put

$$G_0 := \{P \in E[l] \,:\, \mathrm{Fr}_q P = qP\},$$
$$G_1 := E(\mathbf{F}_q) \cap E[l].$$

Since $k > 1$, it holds that $l \nmid q-1$. Therefore,

$$G_0 \cong G_1 \cong \mathbf{Z}/l\mathbf{Z},$$
$$G_0 \cap G_1 = \{\mathcal{O}\}.$$

We further put $r := q^k$ and $s := q^{k/2}$. Since $l \mid \sum_{i=0}^{k-1} q^i$ but $l \nmid k$ we see

$$G_0 = \mathrm{Ker}\,\mathrm{Tr} \cap E[l].$$

Moreover, $l \mid s+1$ implies $\mathrm{Fr}_q{}^{k/2} P = -P$ for $P \in G_0$.

In case that E is supersingular: We assume $\#E(\mathbf{F}_q) = q+1$. We put $k := 2$, $r := q^2$ and $s := q$. Under the condition, recall that $\widehat{\mathrm{Fr}_q} = -\mathrm{Fr}_q$ and that $E(\mathbf{F}_q) = \mathrm{Ker}(1 - \mathrm{Fr}_q) = \mathrm{Ker}\,\widehat{\mathrm{Tr}}$. Put

$$l := \begin{cases} (q+1)/2 & (E[2] \subset E(\mathbf{F}_q)) \\ \text{the largest odd divisor of } q+1 & (E[2] \not\subset E(\mathbf{F}_q)), \end{cases}$$

Since p is odd, $E[2] \subset E(\mathbf{F}_q)$ implies $4 \mid {}^{\#}E(\mathbf{F}_q) = q+1$, and thus $q \equiv 3 \bmod 4$. Hence l is even in this case. On the other hand, by definition, l is odd in case of $E[2] \not\subset E(\mathbf{F}_q)$. Define two groups G_0 and G_1 by

$$\begin{aligned} G_0 &:= \begin{cases} \mathrm{Ker}\,\mathrm{Tr}_2 & (E[2] \subset E(\mathbf{F}_q)) \\ \dfrac{q+1}{l}\mathrm{Ker}\,\mathrm{Tr}_2 & (E[2] \not\subset E(\mathbf{F}_q)), \end{cases} \\ G_1 &:= \begin{cases} E(\mathbf{F}_q) & (E[2] \subset E(\mathbf{F}_q)) \\ \dfrac{q+1}{l}E(\mathbf{F}_q) & (E[2] \not\subset E(\mathbf{F}_q)). \end{cases} \end{aligned} \tag{5.1}$$

Then, $G_0 \cong G_1$ by (4.4). By (4.5), we have

$$G_0 \cong G_1 \cong \begin{cases} \mathbf{Z}/l\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} & (E[2] \subset E(\mathbf{F}_q)), \\ \mathbf{Z}/l\mathbf{Z} & (E[2] \not\subset E(\mathbf{F}_q)). \end{cases} \tag{5.2}$$

and

$$G_0 = \mathrm{Ker}\,\mathrm{Tr}_2 \cap E[l], \qquad G_1 = E(\mathbf{F}_q) \cap E[l].$$

By Lemma 4.6,

$$G_0 \cap G_1 = \begin{cases} E[2] & (E[2] \subset E(\mathbf{F}_q)), \\ \{\mathcal{O}\} & (E[2] \not\subset E(\mathbf{F}_q)). \end{cases}$$

In what follows, E is of one of the types described in above. Note that we choose l in case of ordinary E whereas l is uniquely determined by E in case of supersingular E. Denote ${}^{\#}G_0$ by N for simplicity. Note $\sum_{P \in G_0} P = \mathcal{O}$ (cf. [17, Lem. 2.2]). By Silverman[20, Cor. III.3.5], there exists a unique normalized rational function φ satisfying

$$\mathrm{div}\,\varphi = \sum_{P \in G_0} [P] - N[\mathcal{O}]. \tag{5.3}$$

Since G_0 is stable under Fr_q, the function φ is defined over $\mathbf{F}_q$. Moreover, $[-1]^*\mathrm{div}\,\varphi = \mathrm{div}\,\varphi$ where $[n]$ stands for the multiplication map by n on E for $n \in \mathbf{Z}$. Since $\mathrm{ord}_{\mathcal{O}}\varphi = N-1$, we see that φ is an odd (resp. even) function if N is even (resp. odd). Finally, we note $\varphi \in \mathbf{F}_q[\xi, \eta]$ because φ is regular outside of $\{\mathcal{O}\}$.

Lemma 5.1. *Under the above setting,* $G_0 + G_1 = E[l]$.

Proof. The inclusion $G_0 + G_1 \subset E[l]$ is clear. We prove $E[l] \subset G_0 + G_1$. Let $P \in E[l]$. In case of an odd l (note that l may not be a prime), there exists an integer m satisfying $m(q-1) \equiv 1 \bmod l$. Put

$$\begin{aligned} A &:= m(\mathrm{Fr}_q P - P), \\ Q &:= P - A. \end{aligned}$$

Then $A \in \mathrm{Ker}\,\mathrm{Tr} \cap E[l] = G_0$. We show $Q \in G_1 = E(\mathbf{F}_q) \cap E[l]$ by using $\mathrm{Fr}_q A = qA$. Indeed,

$$\begin{aligned} \mathrm{Fr}_q Q - Q &= \mathrm{Fr}_q P - \mathrm{Fr}_q A - (P - A) = \mathrm{Fr}_q P - P - (q-1)A \\ &= \mathrm{Fr}_q P - P - (q-1)m(\mathrm{Fr}_q P - P) = \mathcal{O} \end{aligned}$$

since $\mathrm{Fr}_q P - P \in E[l]$. Thus $Q \in E(\mathbf{F}_q) \cap E[l] = G_1$.

In case of an even l, it holds that E is supersingular and that $E[2] \subset E(\mathbf{F}_q)$. Since $l = \frac{q+1}{2}$, there exists $R \in E[q+1] = E(\mathbf{F}_r)$ satisfying $P = 2R$. Put $A := R - \mathrm{Fr}_q R$ and $Q := R + \mathrm{Fr}_q R$. Apparently, $A \in \mathrm{Ker}\,\mathrm{Tr} = G_0$, $Q \in E(\mathbf{F}_q) = G_1$ and $A + Q = 2R = P$. □

Lemma 5.2. *Let $f \in \mathbf{F}_q(E)$ be an even function. Then, $f(P) \in \mathbf{F}_s$ for $P \in G_0$. In particular, $\xi(P) \in \mathbf{F}_s$ for $P \in G_0$.*

Proof. Observe that

$$\mathrm{Fr}_q{}^{k/2} f(P) \;=\; f(\mathrm{Fr}_q{}^{k/2} P) \;=\; f(-P) \;=\; f(P).$$

Hence $f(P) \in \mathbf{F}_s$. The latter assertion is clear since ξ is an even function. □

Theorem 5.3. *Let ∂ be the derivation defined in Definition 3.5. Let $A \in G_0 - \{\mathcal{O}\}$ and $P \in E - G_0$. We have the followings:*

(i) $h_{N,-A}(P) = \dfrac{(\partial\varphi)(A)\varphi(P)}{\varphi(A+P)}$.

(ii) $h_{s,-A}(P) = \dfrac{1}{V_A(P)} \left(\dfrac{(\partial\varphi)(A)\varphi(P)}{\varphi(A+P)} \right)^{\nu}$ where $\nu := \dfrac{s+1}{N}$.

(iii) $\dfrac{((\partial\varphi)(A)\varphi(Q))^{\nu}}{V_A(Q)} \in \mathbf{F}_s^{\times}$ for $Q \in E(\mathbf{F}_q) - G_0$.

Proof. (i): Since $A \in G_0$,

$$\mathrm{div}\left(\frac{\varphi}{\varphi \circ t_A}\right) \;=\; N([-A] - [\mathcal{O}]) \;=\; \mathrm{div} h_{N,-A}.$$

Hence there exists a constant c_A satisfying

$$h_{N,-A} \;=\; c_A \frac{\varphi}{\varphi \circ t_A}.$$

Looking at the leading terms at $\mathcal{O}$, we have

$$1 \;=\; c_A \frac{1}{\mathrm{lc}_A(\varphi)}.$$

Therefore,

$$\mathrm{lc}_P(h_{N,-A}) \;=\; \frac{\mathrm{lc}_A(\varphi)\mathrm{lc}_P(\varphi)}{\mathrm{lc}_{A+P}(\varphi)}.$$

Since $\mathrm{ord}_A \varphi = 1$, we have $\mathrm{lc}_A(\varphi) = (\partial\varphi)(A)$ by (3.5). On the other hand, by $P \notin G_0$ and $A + P \notin G_0$, we have $\mathrm{lc}_P(\varphi) = \varphi(P)$ and $\mathrm{lc}_{A+P}(\varphi) = \varphi(A+P)$. Thus (i) holds.

(ii) Note $\nu N = s+1$. Since $A \in E[N]$, we have

$$h_{N,-A}^{\nu} \;=\; h_{s+1,-A} \;=\; V_A h_{s,-A} \tag{5.4}$$

Assume $V_A(P) = 0$. Since $A \neq \mathcal{O}$, we have $V_A(P) = \xi(P) - \xi(A)$ and $P = \pm A$. This contradicts to $P \notin G_0$. Hence $V_A(P) \neq 0$. Applying (i) on the left hand side of (5.4), we obtain (ii).

(iii) Since $A \in G_0 - \{\mathcal{O}\}$ and $Q \in E(\mathbf{F}_q) - G_0$, we have $V_A(Q) = \xi(Q) - \xi(A) \in \mathbf{F}_s$. We already proved that $V_A(Q) \neq 0$ in (ii). The assumption $Q \in E(\mathbf{F}_q) - G_0$ implies $\mathrm{ord}_Q \varphi = 0$. Since φ is defined over $\mathbf{F}_q$ and $Q \in E(\mathbf{F}_q)$, it holds that $\varphi(Q) \in \mathbf{F}_q$. In case of even l, it holds that $2 \mid N$ and that φ is an odd function. By Corollary 3.8, $\partial\varphi$ is even (and $\nu = 1$ in this case). Similarly, in case of odd l, it holds that $\partial\varphi$ is an odd function and that $2 \mid \nu$. Thus $(\partial\varphi)^{\nu}$ is even. Therefore $(\partial\varphi)(A)^{\nu} \in \mathbf{F}_s$ by Lemma 5.2. This completes the proof of (iii). □

Remark 5.4. Using Theorem 5.3(ii), we can solve FAPI for the Ate paring. However, the rational function $\varphi \circ t_A$ is not a polynomial of ξ and η. It is questionable whether it results in a faster FAPI algorithm than direct application of a root finding algorithm to $h_{s,-A}$.

Theorem 5.5. *Let ν be as in Theorem 5.3(ii). Let $z \in \mu_l - \{\pm 1\}$. Suppose that $c \in \mathbf{F}_s^\times$ and that the equation $\varphi(kR)^\nu = c/z$ has a solution $R \in E(\mathbf{F}_r) \cap E[kl]$ satisfying $k\mathrm{Tr}_k R \neq \mathcal{O}$. In case of odd l, let m be an integer satisfying $ml \equiv 1 \bmod k$. In case of even l, we define $m := 0$. Put $A := kR - (1-ml)\mathrm{Tr}_k R$ and $Q := (1-ml)\mathrm{Tr}_k R$. Then the followings hold:*

(i) $A \in G_0 - \{\mathcal{O}\}$.

(ii) $Q \in G_1 - G_0$.

(iii) $h_{s,-A}(Q) = \pm z$. Moreover in case of odd l, we always have $h_{s,-A}(Q) = z$.

Proof. (i) Note $\mathrm{Tr}_k P = kP$ For $P \in E(\mathbf{F}_q)$. Since Tr_k is additive, we have

$$\mathrm{Tr}_k A \;=\; k\mathrm{Tr}_k R - k\mathrm{Tr}_k R + mlk\mathrm{Tr}_k R \;=\; m\mathrm{Tr}_k \mathcal{O} \;=\; \mathcal{O}.$$

Thus $A \in \mathrm{Ker}\mathrm{Tr}_k$. Now we show $A \in G_0$. In case of odd l, the definition of A implies

$$lA \;=\; klR - \mathrm{Tr}_k lR + ml\mathrm{Tr}_k lR.$$

Since $lR \in E[k]$, we see that $\mathrm{Tr}_k lR \in E[k]$ and thus $ml\mathrm{Tr}_k lR = \mathrm{Tr}_k lR$. Thus $lA = \mathcal{O}$. Therefore $A \in \mathrm{Ker}\mathrm{Tr}_k \cap E[l] = G_0$. In case of even l, the curve E is supersingular satisfying $E[2] \subset E(\mathbf{F}_q)$. Hence $A \in \mathrm{Ker}\mathrm{Tr}_2$ implies $A \in G_0$ by the definition (5.1) of G_0.

Finally, we show $A \neq \mathcal{O}$. Assume contrary. This implies $kR = (1-ml)\mathrm{Tr}_k R \in E(\mathbf{F}_q)$. Since φ is defined over $\mathbf{F}_q$, we have

$$\frac{1}{z} \;=\; \frac{\varphi(kR)^\nu}{c} \;\in\; \mathbf{F}_s^\times$$

while $\frac{1}{z} \in \mu_l \subset \mu_{s+1}$ by the assumption. Thus $z \in \mathbf{F}_s \cap \mu_{s+1} = \{\pm 1\}$, which is a contradiction.

(ii) It trivially holds that $Q \in E(\mathbf{F}_q)$. Hence $Q \in G_1$ in case of even l. In case of odd l, observe that $Q = kR - A$, which implies $Q \in E[l]$, Therefore $Q \in G_1$. Assume that $Q \in G_0$. Since $A \in G_0$, we have $kR = A + Q \in G_0$, a contradiction to $k\mathrm{Tr}_k R \neq \mathcal{O}$.

(iii) By Theorem 5.3(ii),

$$h_{s,-A}(Q) \;=\; \left(\frac{(\partial\varphi)(-A)\varphi(P)}{V_A(Q)}\right)^\nu \cdot \frac{1}{\varphi(kR)^\nu}.$$

Eliminating $\varphi(kR)$, we obtain

$$\frac{h_{s,-A}(Q)}{z} \;=\; \left(\frac{(\partial\varphi)(-A)\varphi(P)}{V_A(Q)}\right)^\nu \frac{1}{c}. \tag{5.5}$$

Since $A \in G_0$ and $Q \in G_1$, the bilinearity of the Ate pairing implies $h_{s,-A}(Q) \in \mu_l$. Thus the left hand side of (5.5) belongs to μ_l. The right hand side of (5.5) belongs to $\mathbf{F}_s^\times$ by Theorem 5.3(iii) and the choice of c. Therefore the value belongs to $\mu_l \cap \mathbf{F}_s^\times \subset \mu_{s+1} \cap \mathbf{F}_s^\times = \{\pm 1\}$. In case of odd l, it is clear that $-1 \notin \mu_l$. Hence $\mu_l \cap \mathbf{F}_s^\times = \{1\}$. □

Remark 5.6. In case that E is supersingular, $kl \mid q+1$. In this case, the condition $q \equiv 1 \bmod 4$ or $E[2] \subset E(\mathbf{F}_q)$ implies $kl = q+1$, hence $E[kl] \cap E(\mathbf{F}_r) = E(\mathbf{F}_r)$.

Theorem 5.7. *Suppose l is even. Let $A \in G_0$ and $Q \in G_1$. There exist B, $P \in E[2]$ satisfying $h_{s,-(A+B)}(Q+P) = -h_{s,-A}(Q)$.*

Proof. In this case, E is supersingular satisfying $E[2] \subset E(\mathbf{F}_q)$, hence $s=q$. Take two different C and R from $E[2]-\{\mathcal{O}\}$. Note $^{\#}E[2]=4$ since p is odd. The assumption $E[2] \subset E(\mathbf{F}_q)$ implies $q \equiv 3 \bmod 4$, thus -1 is a non-square element in $\mathbf{F}_q$. Hence either $V_C(R)=\zeta(R)-\zeta(C)$ or $V_R(C)$ is a non-square element in $\mathbf{F}_q$. Without loss of generality, we can assume that $V_C(R)$ is non-square element of $\mathbf{F}_q$. Since $h_{q,C}=V_C^{(q-1)/2}$, we have $h_{q,C}(R)=-1$. Note $h_{q,-A}(R)=\pm 1$ and $h_{q,-C}(Q)=\pm 1$ because $C,\ R \in E[2]$.

Now, in case of $h_{q,C}(Q)=-1$, we have $h_{q,-(A+C)}(Q)=h_{q,-A}(Q)h_{q,-C}(Q)=-h_{q,-A}(Q)$. Thus we can take $B:=C$ and $P:=\mathcal{O}$. Similarly, in case of $h_{q,A}(R)=-1$, we can take $B:=\mathcal{O}$ and $P:=R$. Otherwise $h_{q,B}(Q)=h_{q,A}(R)=1$. Then

$$h_{q,-(A+C)}(Q+R) = h_{q,-A}(Q)h_{-q,C}(Q)h_{-q,A}(R)h_{-q,C}(R) = h_{q,-A}(Q)\cdot 1\cdot 1\cdot(-1).$$

Hence we can take $B:=C$ and $P:=R$. □

Remark 5.8. In reality, evaluating $h_{q,-A}(R)$ by the Miller algorithm may fail since R may belong to $\langle A \rangle$. In practice, we simply compute $h_{q,-A}(Q+R)$, $h_{q,-(A+C)}(Q)$, and $h_{q,-(A+C)}(Q+R)$ by the Miller algorithm which will always success. Theorem 5.7 guarantees that at least one of them is z.

6. Relation to Generalized Pairing Inversion

We present a pseudo code derived from Theorem 5.5 and Remark 5.8. For supersingular curves, it gives a solution to GPI. For ordinary curves, we need some wrapper procedure (Algorithm 6.6) to obtain a solution to GPI. However, for ordinary curves, the algorithm is too inefficient even for numerical experiments for small values of q (cf. Remark 6.5).

Algorithm 6.1.
Input: q, E, l, N, k, φ: as in Theorem 5.5,
$z \in \mu_l - \{\pm 1\}$.
Output: $(A, Q) \in G_0 \times G_1$ satisfying $h_{q^{k/2},-A}(Q)=z$.
Procedure:

```
 1: r := q^k ; s := q^{k/2} ;
 2: v := (s+1)/N ;
 3: if (l is even)
 4:   m := 0 ;
 5: else
 6:   compute m ∈ N satisfying ml ≡ 1 mod k ;
 7: γ := γ_0 := any vth power root of 1/z ;
 8: ω := a primitive ((s-1)v)th root of the unity ;
 9: do {
10:   foreach (R_0 ∈ E(F_r) satisfying φ(R_0) = γ) {
11:     foreach (R ∈ E(F_r) satisfying kR_0 = R) {
12:       T := Tr_k R ;
13:       if (kT ≠ O and klR = O) {
14:         Q := (1-ml)T ; A := kR - Q ;
15:         if (l is even and h_{q,-A}(Q) = -z) {
16:           // Here, k=2, s=q, E[2] ⊂ E(F_p). Apply Remark 5.8 to change the sign.
17:           Let x_0 and x_1 be two solutions of X^3+a_2X^2+a_4X+a_6=0 ;
```

18: **if** $((x_1-x_0)^{(q-1)/2}=1)$
19: swap x_0 and x_1 ;
20: $B:=(x_0, 0)$; $P:=(x_1, 0)$;
21: **if** $(h_{q,-(A+B)}(Q)=z)$
22: $A:=A+B$;
23: **else if** $(h_{q,-A}(Q+P)=z)$
24: $Q:=Q+P$;
25: **else** {
26: $A:=A+B$; $Q:=Q+P$;
27: }
28: }
29: **return** (A, Q) ;
30: }
31: } // end loop on R
32: } // end loop on R_0
33: $\gamma:=\omega\gamma$;
34: } **while** $(\gamma\neq\gamma_0)$;
35: // should not reach here

Remark 6.2. Step 9: We know $\varphi\circ[k]$ is defined over $\mathbf{F}_q$ and we search for $\mathbf{F}_r$ rational points R satisfying $\varphi(kR)^v=z/c$ for a given $z\in\mu_l$ and all $c\in\mathbf{F}_s^\times=\mu_{s-1}$. Since $\varphi(kR)\in\mathbf{F}_r$, we see that $\varphi(kR)=w$ for some $w\in\mathbf{F}_r^\times$ satisfying $w^v=c/z$. Recall $v=\frac{s+1}{N}$ and $l\mid N$. Thus z has vth power root in $\mathbf{F}_r^\times$ $(=\mu_{r-1})$. We also note

$$\{\ \alpha\ :\ \alpha^v\in\mu_{s-1}\ \}\ =\ \mu_{v(s-1)}\ \subset\ \mu_{r-1}.$$

This is much faster than solving $(\varphi\circ[k])^v(R)=c/z$ directly.

Remark 6.3. The algorithm calls probabilistic algorithms, e.g. the vth power root algorithm, solving $\varphi(\cdot)=\gamma$ which would use polynomial factorizations over finite fields. However, the control sequence in Algorithm 6.1 is deterministic. Changing Step 9 to random choice might make implementation simpler. Though, the change does not seem to affect average number of loop count on γ before the algorithm terminates.

Remark 6.4. In Algorithm 6.1, φ is of an opaque input datum. If we can accept $O(l)$ space complexity, we may use naive representation for rational functions on E. Then, we precompute φ as follows. In case of odd l, the group G_0 is cyclic of order l. Let A_0 be a generator of G_0. Then $\varphi=g(\xi)$ where

$$g(T)\ :=\ \prod_{i=1}^{(l-1)/2}(T-\xi(iA_0)).$$

One should use an asymptotic fast algorithm (e.g. Aho, Hopcroft and Ullmann[1, Theorem 8.14]) to compute the above product. In case of even l, we see

$$\varphi\ =\ -\,g(\xi)\eta \tag{6.1}$$

(note $\mathrm{lc}_{\mathcal{O}}\eta=-1$) where

$$g(T)\ :=\ \prod_{A\in(G_0-E[2])/\{\pm1\}}(T-\xi(A)).$$

A handy (but a bit slow) method to compute g is to use

$$g(T)\ =\ \gcd(T^q-T,\ (T^3+a_2T^2+a_4T+a_6)^{(q-1)/2}+1) \tag{6.2}$$

with a fast gcd algorithm. In ether case, we can use a root finding algorithm for rational functions on E in Step 10.

Remark 6.5. For $z \in \mu_l$, put

$$C_z := \{ (A, Q) \in G_0 \times G_1 : A \neq \mathcal{O},\ Q \notin E[2] \text{ and } h_{s,-A}(Q) = z \},$$

$$S_z := \{ \tilde{\varphi}(A+Q) : (A, Q) \in C_z \}.$$

Let ϱ_z be the probability that R in Step 10 exists when we choose ω uniformly randomly from $z^{-1/v}\mu_{(s-1)v}$. Suppose l is an odd prime. Then, $\#C_z = l-1 = N-1$ for $z \neq 1$. Therefore

$$\varrho_z = \frac{\#S_z}{\#\mu_{(s-1)v}} \leq \frac{\#C_z}{(s-1)v} < \frac{N}{(s-1)v} \leq \frac{s+1}{s-1}\cdot\frac{1}{v^2} \leq \frac{2}{v^2}$$

for $q \geq 3$. Since $\frac{1}{v} \leq \frac{(q+1)/2}{q^{k/2}}$, we see ϱ_z is exponentially small with respect to $\log q$ if E is ordinary. Suppose E is supersingular. In case of odd l, numerical experiments for small q suggests that $\varrho_z \approx \frac{\#((\mathbf{Z}/l\mathbf{Z})^\times)}{2lv^2}$ on average for $z \in \mu_l - \{1\}$. In case of even l, the main term of ϱ_z seems to $\frac{1}{2}$ and the exponent of 2 in l seems to lower ϱ_z. However, the tested range of q is too small and therefore the conjecture on estimate of ϱ_z is an open problem.

For ordinary curves, Algorithm 6.1 does not give a solution to GPI for the Ate pairing. The following algorithm fixes the problem.

Algorithm 6.6.

Input: q, E: ordinary, l: odd prime, k, φ: as in Theorem 5.5
$z \in \mu_l - \{1\}$

Output: $(A, Q) \in G_0 \times G_1$ satisfying $h_{q,-A}(Q) = z$.

Procedure:

1: Let (B, Q) be the output of Algorithm 6.1 with input $(q, E, l, l, k, \varphi, z^{k/2})$.
2: **return** $(q^{k/2-1}B, Q)$;

Theorem 6.7. *Algorithm 6.6 returns a correct value.*

Proof. In case of ordinary E, it is assumed that l is an odd prime not dividing k. Hence

$$\mu_l \cap \mu_{k/2} = \{1\}. \tag{6.3}$$

In particular, $z^{k/2} \neq \pm 1$ for $z \in \mu_l - \{1\}$. Algorithm 6.1 in Step 1 returns (B, Q) satisfying $h_{q^{k/2},-B}(Q) = z^{k/2}$. On the other hand, By a similar computation to Granger et al.[9, Eq. (5)], we see

$$h_{q^{k/2},-B}(Q) = h_{q,-q^{(k/2)-1}B}(Q)^{k/2}.$$

Therefore,

$$h_{q,-q^{(k/2)-1}B}(Q)^{k/2} = z^{k/2}.$$

Using (6.3) again, we obtain $h_{q,-q^{(k/2)-1}B}(Q) = z$ as desired. □

7. Appendix: the Miller Function at a Generic Point

In the proof of Theorem 4.7, we used Corollary 7.4, the relation between $h_{q,Q}(A)$ and $h_{q,A}(Q)$ where orders of Q and A are not necessarily prime. This naturally follows from a property of the Miller function $h_{n,A}(Q)$ viewed as a function of A while Q is fixed. This kind of idea, which has independent interest of pairings, is not new and is probably a folklore. Even if we limit ourselves to a context of pairing inversion, we find the use in Cherepniov[5, p.738]. However, "viewing as a function of A" is not so obvious than it looks. Consider (4.7) in Definition 4.2. It seems to be natural to define $\xi(Q)-\xi$ as a $V_A(Q)$ viewed as a rational function of A. However, this breaks a recurrence relation

$$h_{n,A} = \frac{L_{(n-1)A,A}}{V_{nA}} h_{n-1,A}$$

when n is an order of A. The value of V_{nA} should be always 1 in this case. A similar problem occurs in $L_{(n-1)A,A}$. One possible way is to change definitions of V_{nA} and $L_{(n-1)A,A}$ as a rational functions of A when n is a multiple of the order of A. Our method is different and can be interpreted as considering the Miller function at a generic point of E.

In this section, k denotes an arbitrary perfect field. Let E/k be an elliptic curve defined by the long Weierstrass model. We put $p := \mathrm{char}(k)$ (so, p may be zero). For an integer n, we denote the multiplication by n map by $[n]$. This is unambiguously distinguished from a divisor $[P]$ for a point P on E. We write the inseparable degree of $[n]$ as $\varepsilon(n)$. Thus, $\varepsilon(n)=1$ for $p=0$, In case of $p>0$, writing $n=n'p^e$ with $e\geq 0$, $\gcd(n', p)=1$, we have

$$\varepsilon(n) = \begin{cases} p^e & (E:\text{ordinary}), \\ p^{2e} & (E:\text{supersingular}). \end{cases}$$

Finally, for a non-zero $\Phi \in \mathrm{End}(E)$, we define $\mathrm{lc}(\Phi)$ by

$$\tau^{\circ}\Phi = \mathrm{lc}(\Phi)\tau^{\deg_i \Phi} + O(\tau^{1+\deg_i \Phi}). \tag{7.1}$$

Definition 7.1. For $Q \in E(k)-\{\mathcal{O}\}$ and positive integers m and n, we define rational functions $\lambda_{m,n}$, $L^{\vee}_{n,m,Q}$, $V^{\vee}_{n,Q} \in k(E)$ as follows:

$$\lambda_{n,m} := \begin{cases} \left(\dfrac{3\xi^2+2a_2\xi+a_4-a_1\eta}{2\eta+a_1\xi+a_3}\right)^{\circ}[n] & (n = m) \\ \dfrac{\eta^{\circ}[n]-\eta^{\circ}[m]}{\xi^{\circ}[n]-\xi^{\circ}[m]} & (n \neq m) \end{cases}$$

$$L^{\vee}_{n,m,Q} := -\eta(Q) + \lambda_{n,m}\cdot(\xi(Q)-\xi) + \eta$$

$$V^{\vee}_{n,Q} := \xi(Q) - \xi^{\circ}[n].$$

We further define a rational function $h^{\vee}_{n,Q}$ inductively by

$$h^{\vee}_{n,Q} := \begin{cases} 1 & (n = 1), \\ \dfrac{L^{\vee}_{n-1,1,Q}}{V^{\vee}_{n,Q}} h^{\vee}_{n-1,Q} & (n > 1). \end{cases}$$

For $A \notin E[n]$, the condition $\xi(nA)=\xi(A)$ is equivalent to $A \in E[n-1] \cup E[n+1]$. Put

$$U_n := \bigcap_{i=1}^{n} E[i]^c,$$

$$U_{n,Q} := \{A \in U_n : Q \neq \pm iA \text{ for all } 1 \leq i \leq n\}.$$

Note both U_n and $U_{n,Q}$ are open dense subsets of E. For $A \in U_n$, we see

$$L^{\vee}_{n-1,\,1,\,Q}(A) = L_{(n-1)A,A}(Q),$$

$$V^{\vee}_{n,\,Q}(A) = V_{nA}(Q).$$

Therefore

$$h^{\vee}_{n,\,Q}(A) = h_{n,A}(Q) \tag{7.2}$$

for $A \in U_{n,Q}$. So, $h^{\vee}_{n,\,Q}$ is almost $h_{n,A}(Q)$ viewed as a function of A. However, in Theorem 7.3, we will see that there exist A, $Q \in E$ such that the both hand sides of (7.2) are defined and that (7.2) does *not* hold. (However, we can retrieve $h_{n,A}(Q)$ from $\mathrm{lc}_A(h^{\vee}_{n,\,Q})$.) The next two theorems are fundamental results on $h^{\vee}_{n,\,Q}$, which yield Corollary 7.4

Theorem 7.2. *For a positive integer n and $Q \in E-\{\mathcal{O}\}$, we have*

$$\mathrm{div} h^{\vee}_{n,\,Q} = n([Q]-[\mathcal{O}]) - [n]^*([Q]-[\mathcal{O}]), \tag{7.3}$$

$$\mathrm{lc}(h^{\vee}_{n,\,Q}) = (-1)^{n-1}\mathrm{lc}([n]).$$

In particular $\mathrm{ord}_{\mathcal{O}} h^{\vee}_{n,\,Q} = \varepsilon(n) - n$.

Theorem 7.3. *Let $n \in \mathbf{N}$ and $A \in E-\{\mathcal{O}\}$. For $Q \in E-\{\mathcal{O}\}$ satisfying $Q \neq \pm A$, $\pm 2A$, …, $\pm nA$, the expansion of $h^{\vee}_{n,\,Q}$ at A is*

$$h^{\vee}_{n,\,Q} = \begin{cases} h_{n,A}(Q) + O(\tau_A) & (nA \neq \mathcal{O}), \\ -\mathrm{lc}([n]) h_{n,A}(Q) \tau_A^{\varepsilon(n)} + O(\tau_A^{\varepsilon(n)+1}) & (nA = \mathcal{O}). \end{cases} \tag{7.4}$$

Before describing proofs of Theorem 7.2 and Theorem 7.3, we state their corollary which is used in Sect. 4.

Corollary 7.4. *Let E be supersingular. Suppose that n is a power of p. For $Q \in E-\{\mathcal{O}\}$, define $R \in E$ by $Q = nR$. (Note that such R is unique because E is supersingular.) Then,*

$$h^{\vee}_{n,\,Q} = \mathrm{lc}([n]) h^{-n}_{n,R}. \tag{7.5}$$

Moreover, in case that E is defined over $\mathbf{F}_q$ and that $^{\#}E(\mathbf{F}_q) = q+1$,

$$h^{\vee}_{q,\,Q} = -h^{-q}_{q,-Q} \tag{7.6}$$

for $Q \in E[q+1]-\{\mathcal{O}\}$.

Proof. Note that $[n]$ is purely inseparable. By (7.3), we obtain

$$\begin{aligned} \mathrm{div} h^{\vee}_{n,\,Q} &= n([nR]-[\mathcal{O}]) - n^2([R]-[\mathcal{O}]) \\ &= -n(n[R]-[nR]-(n-1)[\mathcal{O}]) = \mathrm{div} h^{-n}_{n,R}. \end{aligned}$$

For a prime power n, we have $(-1)^{n-1}=1$ in k. Since $h_{n,R}$ is normalized, (7.5) holds. Now we prove (7.6). The condition $^{\#}E(\mathbf{F}_q) = q+1$ implies that $\mathrm{Fr}_q^{\,2} = -[q]$ in $\mathrm{End}(E)$. Thus $\mathrm{lc}([q]) = -1$. Since $Q = q(-Q)$, we see $R = -Q$ by the uniqueness of R. Substituting $\mathrm{lc}([n])$ and R in (7.5) with them, we obtain (7.6). □

Note that (7.5) and (7.6) are equalities between rational functions.

At the moment of writing this, the only proofs of Theorem 7.2 and Theorem 7.3 the author has is to apply induction on n to explicit forms of divisors and leading coefficients of $L^{\vee}_{1,n,Q}$ (Lemma 7.8) and $V^{\vee}_{n,Q}$ (Lemma 7.9). The proof of Lemma 7.8 use the expansion of $\lambda_{1,1}$ (Lemma 7.6) and $\lambda_{n,1}$ (Lemma 7.7). The proofs of these lemmas are omitted because they consist of very long straightforward (but fairly elementary) computations. The author believes that there must be fancy conceptual proofs with help of high powered algebraic geometry. We note that (7.3) is an equality of divisors, not of some equivalence classes and that Theorem 7.2 uniquely characterize $h^{\vee}_{n,Q}$. We also note that over the complex numbers, Theorem 7.2, Lemma 7.8 and Lemma 7.9 are special cases of the following Theorem. However, we should have an algebraic proof, since in our main application, $[n]$ is purely inseparable.

Theorem 7.5. *Let Λ be a lattice in $\mathbf{C}$ and put $\mathscr{E} := \mathbf{C}/\Lambda$. Let $N \geq 2$ be an integer, and let $n_1, n_2, \ldots, n_N, m_1, \ldots, m_N$ be non-zero integers satisfying*

$$\sum_{i=1}^{N} n_i m_i = 0. \tag{7.7}$$

Put $\Omega := \mathbf{C} - \bigcup_{i=1}^{N} \frac{1}{n_i}\Lambda$. Let Θ be a continuous function $\Theta : \mathbf{C} \times \mathbf{C} \to \mathbf{P}(\mathbf{C}^1)$ where we identify $\mathbf{P}^1(\mathbf{C})$ with $\mathbf{C} \cup \{\infty\}$. Define $\Theta_{1,w}$ and $\Theta_{2,z}$ by $\Theta_{1,w}(z) := \Theta(z, w)$ and $\Theta_{2,z}(w) := \Theta(z, w)$, respectively. For all $w \in \Omega$, assume that $\Theta_{1,w}$ is an elliptic function with respect to Λ satisfying

$$\operatorname{div}(\Theta_{1,w}) = \sum_{j=1}^{N} m_j([n_j w] - [0]), \tag{7.8}$$

as a rational function of $\mathscr{E}$ and

$$\operatorname{lc}_0(\Theta_{1,w}) = 1. \tag{7.9}$$

Then, for all $z \in \mathbf{C} - \Lambda$, the function $\Theta_{2,z}$ is an elliptic function with respect to Λ satisfying

$$\operatorname{div}(\Theta_{2,z}) = \sum_{j=1}^{N} m_j [n_j]^*([z] - [0]) \tag{7.10}$$

and

$$\operatorname{lc}_0(\Theta_{2,z}) = \prod_{i=1}^{N} (-n_i)^{-m_i}. \tag{7.11}$$

Proof. Let σ be the σ-function with respect to Λ normalized as $\sigma'(0) = 1$. Recall that σ has simple zeros at Λ and that σ is non zero outside of Λ. Note that (7.8) and (7.9) uniquely determines Θ. Explicitly,

$$\Theta(z, w) = \prod_{i=1}^{N} \left(\frac{\sigma(z - n_i w)}{\sigma(z)\sigma(-n_i w)} \right)^{m_i} \tag{7.12}$$

by Silverman[20, Prop. VI.3.4] or Whittaker and Watson[23, Sect. 20-53]. Since σ is an entire function, $\Theta_{2,z}$ is meromorphic over $\mathbf{C}$ for $z \in \mathbf{C} - \Lambda$. In order to show that $\Theta_{2,z}$ is an elliptic function, we recall that, for $\lambda \in \Lambda$, there exist constants α and β (depending on λ) satisfying

$$\sigma(w + \lambda) = \exp(\alpha w + \beta\lambda)\sigma(w)$$

for all $w \in \mathbf{C}$ (cf. Silverman[20, Lemma VI.3.3(c)] or Whittaker and Watson[23, Sect. 20-422]). We obtain

$$\sigma(w+n\lambda) = \exp\left(n\alpha w + \frac{n(n-1)}{2}\alpha\lambda + n\beta\lambda\right)\sigma(w) \tag{7.13}$$

for all $n \in \mathbf{N}$ by induction on n. It is obvious that (7.13) holds for $n=0$. Substituting w with $w-n\lambda$ in (7.13), we obtain

$$\sigma((w-n\lambda)+n\lambda) = \exp\left(n\alpha(w-n\lambda) + \frac{n(n-1)}{2}\alpha\lambda + n\beta\lambda\right)\sigma(w-n\lambda)$$

$$\sigma(w) = \exp\left(n\alpha w - \frac{(-n)((-n)-1)}{2}\alpha\lambda + n\beta\lambda\right)\sigma(w+(-n)\lambda).$$

Hence (7.13) also holds in case that n is a negative integer. Therefore,

$$\begin{aligned}
\Theta_{2,z}(w+\lambda) &= \prod_{i=1}^{N}\left(\frac{\sigma(z-n_i w-n_i\lambda)}{\sigma(z)\sigma(-n_i w-n_i\lambda)}\right)^{m_i} \\
&= \prod_{i=1}^{N}\left(\frac{\exp\left(n_i\alpha(z-n_i w)+\frac{n_i(n_i-1)}{2}\alpha\lambda+n_i\beta\lambda\right)\sigma(z-n_i w)}{\sigma(z)\exp\left(n_i\alpha(-n_i w)+\frac{n_i(n_i-1)}{2}\alpha\lambda+n_i\beta\lambda\right)\sigma(-n_i w)}\right)^{m_i} \\
&= \prod_{i=1}^{N}\left(\exp(n_i\alpha z)\frac{\sigma(z-n_i w)}{\sigma(z)\sigma(-n_i w)}\right)^{m_i} = \exp\left(\alpha z\sum_{i=1}^{N} m_i n_i\right)\prod_{i=1}^{N}\left(\frac{\sigma(z-n_i w)}{\sigma(z)\sigma(-n_i w)}\right)^{m_i} = \Theta_{2,z}(w)
\end{aligned}$$

by the assumption (7.7). This proves that $\Theta_{2,z}$ is an elliptic function for all $z \in \mathbf{C}-\Lambda$. Then, (7.10) and (7.11) are obvious from (7.12). □

Lemma 7.6. *Let $A \in E$. The expansion of $\lambda_{1,1}$ at A is as follows:*

$$\lambda_{1,1}(A) + 2\delta\tau_A + (3(\partial\xi)(A) - (4\lambda_{1,1}(A)+a_1)\delta)\tau_A^2 + O(\tau_A^3) \quad (A \notin E[2],\ \delta := \xi(A)-\xi(2A)) \tag{7.14}$$

$$\frac{1}{a_1}\tau_A^{-2} + O(\tau_A^{-1}) \quad (A \in E[2]-\{\mathcal{O}\},\ p=2) \tag{7.15}$$

$$\frac{1}{2}\tau_A^{-1} - \frac{3}{4}a_1 + O(\tau_A) \quad (A \in E[2]-\{\mathcal{O}\},\ p \geq 3) \tag{7.16}$$

$$\frac{1}{a_1}\tau^{-2} + \frac{a_1a_2+a_3}{a_1^2} + O(\tau^2) \quad (A=\mathcal{O},\ p=2,\ a_1 \neq 0)$$

$$\frac{1}{a_3}\tau^{-4} + \frac{a_2^2+a_4}{a_3} + a_3\tau^2 + O(\tau^4) \quad (A=\mathcal{O},\ p=2,\ a_1=0)$$

$$a_1 + O(\tau) \quad (A=\mathcal{O},\ p=3)$$

$$-\frac{3}{2}\tau^{-1} + \frac{1}{4}a_1 + \left(\frac{1}{8}a_1^2 + \frac{1}{2}a_2\right)\tau + O(\tau^2) \quad (A=\mathcal{O},\ p \geq 5)$$

Lemma 7.7. *Let $n \geq 2$ be an integer. For $A \in E$, put $\tau_{n,A} := \tau^{\circ}[n]^{\circ}t_{-A}$. Put $D_n := E[n]^c \cap E[n+1] \cap E[n-1]$ for simplicity. (Note $D_n = \emptyset$ if $2 \mid n$.) The expansion of $\lambda_{n,1}$ at A is as follows:*

$$\lambda_{n,1}(A)-((n+1)\xi((n+1)A)-n\xi(nA)-\xi(A))\tau_A+O(\tau_A^2) \quad (A\in E[n]^c\cap E[n+1]^c) \tag{7.17}$$

$$\tau_{n+1,A}^{-1}-a_1+O(\tau_A^{\varepsilon(n+1)}) \quad (A\in E[n]^c\cap E[n+1]\cap E[n-1]^c) \tag{7.18}$$

$$\tau_{n+1,A}^{-1}-a_1+O(\tau_A^{\varepsilon(n+1)}) \quad (A\in D_n,\ p\geq 3) \tag{7.19}$$

$$\tau_{n+1,A}^{-1}-a_1+O(\tau_A^{\varepsilon(n+1)}) \quad (A\in D_n,\ n\equiv 3 \bmod 4,\ p=2) \tag{7.20}$$

$$\tau_{n+1,A}^{-1}+O(1) \quad (A\in D_n,\ n\equiv 1 \bmod 4,\ p=2) \tag{7.21}$$

$$-\tau_{n,A}^{-1}+O(\tau_{n,A}) \quad (A\in E[n]-\{\mathcal{O}\}) \tag{7.22}$$

$$-\tau_{n,A}^{-1}+O(1) \quad (A=\mathcal{O},\ n\equiv 0 \bmod p)$$

$$-\frac{3}{2}\tau^{-1}+\frac{a_1}{4}+\frac{a_1^2+4a_2}{8}\tau+O(\tau^2) \quad (A=\mathcal{O},\ n\equiv 1 \bmod p,\ p\geq 5)$$

$$a_1-(a_1^2+a_2)\tau+O(\tau^2) \quad (A=\mathcal{O},\ n\equiv 1 \bmod p,\ p=3)$$

$$\tau_{n+1,A}^{-1}(1+O(\tau^2)) \quad (A=\mathcal{O},\ n\equiv 1 \bmod p,\ p=2,\ a_1\neq 0)$$

$$a_3^{-(\varepsilon(n+1)-1)/3}\tau^{-\varepsilon(n+1)}(1+O(\tau^2)) \quad (A=\mathcal{O},\ n\equiv 1 \bmod p,\ p=2,\ a_1=0)$$

$$\tau_{n+1,A}^{-1}-a_1+O(\tau^{\varepsilon(n+1)-2}) \quad (A=\mathcal{O},\ n\equiv -1 \bmod p,\ p\neq 2)$$

$$-\frac{n^2+n+1}{n(n+1)}\tau^{-1}+\frac{1}{2n(n+1)}a_1+O(\tau) \quad (A=\mathcal{O},\ n\not\equiv 0,\pm 1 \bmod p)$$

In the last case, $\lambda_{n,1}$ is regular at $\mathcal{O}$ if $n \bmod p$ is a primitive third root of unity in k.

Lemma 7.8. *Let n be a positive integer. For $Q\neq\mathcal{O}$, it holds that*

$$\begin{aligned}\operatorname{div}L_{n,1,Q}^{\vee} &= [Q]-[\mathcal{O}]+[n]^*([Q]-[\mathcal{O}])+[n+1]^*([-Q]-[\mathcal{O}])\\ L_{n,1,Q}^{\vee} &= \frac{\tau^{-\varepsilon(n)-\varepsilon(n+1)-1}}{\mathrm{lc}([n])\mathrm{lc}([n+1])}\left(1-\frac{\varepsilon(n)+\varepsilon(n+1)+1}{2}a_1\tau+O(\tau^2)\right).\end{aligned} \tag{7.23}$$

Here, in case of $p=2$, we note that $\varepsilon(n)+\varepsilon(n+1)+1$ is always an even integer. We first evaluate $\dfrac{\varepsilon(n)+\varepsilon(n+1)+1}{2}$, which is always an integer, and then embed the value in k.

Lemma 7.9. *Let n be a positive integer. For $Q\neq\mathcal{O}$, it holds that*

$$\operatorname{div}V_{n,Q}^{\vee} = [n]^*([Q]+[-Q]-2[\mathcal{O}]), \tag{7.24}$$

$$\mathrm{lc}(V_{n,Q}^{\vee}) = -\mathrm{lc}([n])^{-2}. \tag{7.25}$$

Proof. Note $V_{n,Q}^{\vee}=-V_Q\circ[n]$, which proves (7.24). The assertion on the leading coefficient follows from the definition (7.1) of a leading coefficient and the expansion

$$\xi = \tau^{-2}+O(\tau^{-1})$$

(cf. Silverman[20, formulae after the proof of Lemma IV.1.2]). □

Proof of Theorem 7.2. The assertion is trivial in case of $n=1$. For the case $n\geq 2$, the assertion follows from Lemma 7.8 and Lemma 7.9 by easy induction on n. □

Proof of Theorem 7.3. We use induction on n. The assertion trivially holds for $n=1$.

Assume $n=2$. First, we prove the case $A\in E[2]-\{\mathcal{O}\}$. In this case, it holds that

$$\lambda_{1,1} = \mathrm{lc}([2])\tau_A^{-\varepsilon(2)}+O(\tau_A^{-\varepsilon(2)+1}). \tag{7.26}$$

Indeed, in case of $p=2$, the curve E is ordinary, since $A\neq\mathcal{O}$, Therefore, we have $a_1\neq 0$, $\mathrm{lc}[2]=a_1$ and $\varepsilon(2)=2$. Hence (7.26) follows from (7.15). In case of $p\geq 3$, we have $\mathrm{lc}([2])=2$ and $\varepsilon(2)=1$. Then (7.26) follows from (7.16). Therefore, regardless of the parity of p, it holds that

$$L^{\vee}_{1,1,Q} = (\mathrm{lc}([2])^{-1}\tau_A^{-\varepsilon(2)} + O(\tau_A^{-\varepsilon(2)+1}))(\xi(Q) - (\xi(A) + O(\tau_A))) + \eta(A) + O(\tau_A) - \eta(Q)$$
$$= \mathrm{lc}([2])^{-1}V_A(Q)\tau_A^{-\varepsilon(2)} + O(\tau_A^{-\varepsilon(2)+1}).$$

Using $Q \neq \pm A$, we see that the coefficient of $\tau_A^{-\varepsilon(2)}$ is non-zero. On the other hand, $2A = \mathcal{O}$ implies

$$V^{\vee}_{2,Q} = \xi(Q) - \xi\circ[2]\circ t_A \circ t_{-A} = -(\tau^{-2} - a_1\tau^{-1} + O(1))\circ[2]\circ t_{-A} + O(1).$$

Since $\tau\circ[2] = \mathrm{lc}([2])\tau^{\varepsilon(2)} - a_1\varepsilon(2)\tau^{\varepsilon(2)+1} + O(\tau^{\varepsilon(2)+2})$,

$$V^{\vee}_{2,Q} = -\mathrm{lc}([2])^{-2}\tau_A^{-2\varepsilon(2)}(1 - \varepsilon(2)a_1\tau_A + O(\tau_A^2)).$$

Therefore,

$$h^{\vee}_{2,Q} = \frac{L^{\vee}_{1,1,Q}}{V^{\vee}_{2,Q}} = \frac{\mathrm{lc}([2])^{-1}V_A(Q)\tau_A^{-\varepsilon(2)} + O(\tau_A^{-\varepsilon(2)+1})}{-\mathrm{lc}([2])^{-2}\tau_A^{-2\varepsilon(2)} + O(\tau_A^{-2\varepsilon(2)+1})} = -\mathrm{lc}([2])V_A(Q)\tau_A^{\varepsilon(2)} + O(\tau_A^{\varepsilon(2)+1}). \quad (7.27)$$

On the other hand, the assumption $2A = \mathcal{O}$ implies that $h_{2,A} = L_{A,A}/V_{2A} = V_A/1 = V_A$ and thus $V_A(Q) = h_{2,A}(Q)$. Replacing $V_A(Q)$ in (7.27) with $h_{2,A}(Q)$, we obtain (7.26).

Next, assume $2A \neq \mathcal{O}$. In this case $\lambda_{1,1}$ and $L^{\vee}_{1,1,Q}$ are regular at A. By definition, $L^{\vee}_{1,1,Q}(A) = L_{A,A}(Q)$, which is non-zero by $Q \neq A, -2A$. On the other hand, the conditions $2A \neq \mathcal{O}$ and $Q \neq \pm 2A$ implies that $V^{\vee}_{2,Q}(A) = \xi(Q) - \xi(2A) = V_{2A}(Q) \neq 0$. Therefore,

$$h^{\vee}_{2,Q} = \frac{L^{\vee}_{1,1,Q}}{V^{\vee}_{2,Q}} = \frac{L^{\vee}_{1,1,Q}(A) + O(\tau_A)}{V^{\vee}_{2,Q}(A) + O(\tau_A)} = \frac{L_{A,A}(Q) + O(\tau_A)}{V_{2A}(Q) + O(\tau_A)} = \frac{L_{A,A}(Q)}{V_{2A}(Q)} + O(\tau_A)$$
$$= h_{2,A}(Q) + O(\tau_A).$$

This completes that proof of (7.4) for the case $n = 2$.

In case of $n \geq 3$: Assume

$$h^{\vee}_{n-1,Q} = \begin{cases} h_{n-1,A}(Q) + O(\tau_A) & ((n-1)A \neq \mathcal{O}), \\ -\mathrm{lc}([n-1])h_{n-1,A}(Q)\tau_A^{\varepsilon(n-1)} + O(\tau_A^{\varepsilon(n-1)+1}) & ((n-1)A = \mathcal{O}). \end{cases} \quad (7.28)$$

In case of $(n-1)A \neq \mathcal{O}$ and $nA \neq \mathcal{O}$: Since $n-1 \geq 2$, we have

$$L^{\vee}_{n-1,1,Q} = (\lambda_{n-1}(A) + O(\tau_A))(\xi(Q) - \xi) + \eta - \eta(Q) = L_{A,(n-1)A}(Q) + O(\tau_A)$$

by (7.17). Hence $L^{\vee}_{n-1,1,Q}$ is regular at A. The assumption $Q \neq A, (n-1)A, -nA$ implies $L^{\vee}_{n-1,1,Q}(A) = L_{(n-1)A,A}(Q) \neq 0$. On the other hand, since $nA \neq \mathcal{O}$ and $Q \neq \pm A$ the function $V^{\vee}_{n,Q}$ is non-zero regular at A because

$$V^{\vee}_{n,Q} = \xi(Q) - (\xi(nA) + O(\tau_A)) = V_{nA}(Q) + O(\tau_A). \quad (7.29)$$

Therefore, by the induction hypothesis,

$$h^{\vee}_{n,Q} = h^{\vee}_{n-1,Q}\frac{L^{\vee}_{n-1,1,Q}}{V^{\vee}_{n,Q}} = (h_{(n-1),A}(Q) + O(\tau_A))\frac{L_{(n-1)A,A}(Q) + O(\tau_A)}{V_{nA}(Q) + O(\tau_A)} = h_{n,A}(Q) + O(\tau_A)$$

and (7.4) is correct in case of $(n-1)A \neq \mathcal{O}$ and $nA \neq \mathcal{O}$.

In case of $(n-1)A \neq \mathcal{O}$ and $nA = \mathcal{O}$: In this case, it holds that $h^{\vee}_{n-1,Q} = h_{n-1,A}(Q) + O(\tau_A)$ by (7.28). By (7.18)–(7.21),

$$\lambda_{n-1} = (\tau\circ[n]\circ t_{-A})^{-1} + O(1) = ((\mathrm{lc}([n])\tau^{\varepsilon(n)} + O(\tau^{\varepsilon(n)+1}))\circ t_{-A})^{-1} + O(1)$$
$$= \mathrm{lc}([n])^{-1}\tau_A^{-\varepsilon(n)} + O(t_A^{-\varepsilon(n)+1})$$

which yields

$$L^{\vee}_{n-1,\,1,\,Q} = (\mathrm{lc}([n])^{-1}\tau_A^{-\varepsilon(n)}+O(t_A^{-\varepsilon(n)+1}))(\xi(Q)-\xi(A)+O(\tau_A)+O(1)) = \mathrm{lc}([n])V_A(Q)\tau_A^{-\varepsilon(n)}+O(\tau_A^{-\varepsilon(n)+1}).$$

(Note $V_A(Q)\neq 0$.) Using $nA=\mathcal{O}$, we obtain

$$\begin{aligned} V^{\vee}_{n,\,Q} &= \xi(Q)-\xi\circ[n]\circ t_A\circ t_{-A} = \xi(Q)-\xi\circ[n]\circ t_{-A} = -(\tau^{-2}+O(\tau^{-1}))\circ[n]\circ t_{-A}+O(1)\\ &= -\mathrm{lc}([n])^{-2}\tau_A^{-2\varepsilon(n)}+O(\tau_A^{-\varepsilon(n)}). \end{aligned}$$

On the other hand, $nA=\mathcal{O}$ implies that $L_{(n-1)A,A}=V_A$ and that $V_{nA}=1$ (a constant function). Therefore,

$$\begin{aligned} h^{\vee}_{n,\,Q} &= h^{\vee}_{n-1,\,Q}\frac{L^{\vee}_{n-1,\,1,\,Q}}{V^{\vee}_{n,\,Q}} = (h_{(n-1),A}(Q)+O(\tau_A))\frac{\mathrm{lc}([n])^{-1}V_A(Q)\tau_A^{-\varepsilon(n)}+O(\tau_A^{-\varepsilon(n)+1})}{-\mathrm{lc}([n])^{-2}\tau_A^{-2\varepsilon(n)}+O(\tau_A^{-\varepsilon(n)})}\\ &= -\mathrm{lc}([n])h_{(n-1),A}(Q)\frac{L_{(n-1)A,A}(Q)}{V_{nA}(Q)}\tau_A^{\varepsilon(n)}+O(\tau_A^{\varepsilon(n)+1})\\ &= -\mathrm{lc}([n])h_{n,A}(Q)\tau_A^{\varepsilon(n)}+O(\tau_A^{\varepsilon(n)+1}). \end{aligned}$$

Thus, (7.4) is correct in this case.

In case of $(n-1)A=\mathcal{O}$ and $nA\neq\mathcal{O}$: By the induction hypothesis (7.28), we have

$$h^{\vee}_{n-1,\,Q} = -\mathrm{lc}([n-1])h_{n-1,A}(Q)\tau_A^{\varepsilon(n-1)}+O(\tau_A^{\varepsilon(n-1)+1}).$$

By (7.22), we have

$$\begin{aligned} \lambda_{1,n-1} &= -(\tau\circ[n-1]\circ t_{-A})^{-1}+O(\tau_A)\\ &= -\mathrm{lc}([n-1])^{-1}\tau_A^{-\varepsilon(n-1)}+O(\tau_A^{-\varepsilon(n-1)+1}) \end{aligned}$$

and

$$\begin{aligned} L^{\vee}_{1,\,n,\,Q} &= (-\mathrm{lc}([n-1])^{-1}\tau_A^{-\varepsilon(n-1)}+O(\tau_A^{-\varepsilon(n-1)+1}))(\xi(Q)-(\xi(A)+O(\tau_A)))+\eta(A)+O(\tau_A)-\eta(Q)\\ &= -\mathrm{lc}([n-1])^{-1}V_A(Q)\tau_A^{-\varepsilon(n-1)}+O(\tau_A^{-\varepsilon(n-1)+1}). \end{aligned}$$

Using (7.29) again, we obtain

$$\begin{aligned} h^{\vee}_{n,\,Q} &= (-\mathrm{lc}([n-1])h_{n-1,A}(Q)\tau_A^{\varepsilon(n-1)}+O(\tau_A^{\varepsilon(n-1)+1}))\frac{-\mathrm{lc}([n-1])^{-1}V_A(Q)\tau_A^{-\varepsilon(n-1)}+O(\tau_A^{-\varepsilon(n-1)+1})}{V_{nA}(Q)+O(\tau_A)}\\ &= h_{n-1,A}(Q)\frac{V_A(Q)}{V_{nA}(Q)}+O(\tau_A). \end{aligned}$$

On the other hand, $L_{(n-1)A,A}=V_A$ by the assumption$(n-1)A=\mathcal{O}$. Since $Q\neq\pm A$, it holds that $V_A(Q)\neq 0$. Therefore,

$$h^{\vee}_{n,\,Q} = h_{n,A}(Q)+O(\tau_A)$$

which proves (7.4) for the case $(n-1)A=\mathcal{O}$ and $nA\neq\mathcal{O}$. Thus (7.4) holds for any $A\neq\mathcal{O}$, which completes the proof of the theorem. □

Acknowledgment. The author would link to thank Prof. Katsuyuki Takashima for comments on a draft of this paper.

References

1. Aho, A. V., Hopcroft, J. E. and Ullman, J. D.: The design and analysis of computer algorithms. Reading, Mass.: Addison-Wesley pub. 1974.
2. Akagi, S. and Nogami, Y.: Exponentiation inversion problem reduced from fixed argument pairing inversion on twistable Ate pairing and its difficulty, Advances in Information and Computer Security. IWSEC 2014, Lect. Notes in Comput. Sci., **8639**, 240-249, ed. Yoshida, M. and Mouri, K., Springer, 2014. doi: 10.1007/978-3-319-09843-2_18
3. Cartier, P.: Dérivations dans les corps, Séminaire Henri Cartan, **8(exp. 13)**, 1956.

4. Chang, S., Hong, H., Lee, E. and Lee, H.S.: Pairing inversion via non-degenerate auxiliary pairings, Pairing based cryptography – Pairing 2013, Lect. Notes in Comput. Sci., **8365**, 77-96, ed. Cao, Z. and Zhang, F., Springer, 2014. doi: 10.1007/978-3-319-04873-4_5
5. Cherepniov, M.A.: Pairing inversion for finding discrete logarithms. J. Math. Sciences, **206**, 734-741 (2015). doi: 10.1007/s10958-015-2349-x
6. Duc, A. and Jetchev, D.: Hardness of computing individual bits for one-way functions on elliptic curves, Crypto 2012, Lect. Notes in Comput. Sci., **7417**, 832-849, ed. Safavi-Naini, R. and Canetti, R., Berlin, Heidelberg: Springer, 2012. doi: 10.1007/978-3-642-32009-5_48
7. Enge, A.: Bilinear pairings on elliptic curves. Enseign. Math., **61**, 211-243. doi: 10.4171/LEM/61-1/2-9
8. Galbraith, S., Hess, F. and Vercauteren, F.: Aspects of Pairing inversion. IEEE Trans. Info. Theory, **54**, 5719-5728 (2008). doi: 10.1109/TIT.2008.2006431
9. Granger, R., Hess, F., Oyono, R., Thériault, N. and Vercauteren, F.: Ate pairing on hyperelliptic curves, Advances in Cryptology - EUROCRYPT 2007, Lect. Notes in Comput. Sci., **4515**, 430-447, ed. Naor, M., Springer, 2007. doi: 10.1007/978-3-540-72540-4_25
10. Hess, F., Smart, N.P. and Vercauteren, F.: The eta pairing revisited. IEEE trans. on IT, **52**, 4995-4602 (2006). doi: 10.1109/TIT.2006.881709
11. Joux, A.: The Weil and Tate pairings as building blocks for public key cryptosystems (survey), Algorithmic number theory (Sydney, Australia, July 2002), Lect. Notes in Comput. Sci., **2369**, 20-32, ed. Fieker, C. and Kohel, D., Berlin: Springer, 2002.
12. Kate, A., Zaverucha, G.M. and Goldberg, I.: Constant-size commitments to polynomials and their applications, Advances in cryptology - ASIACRYPT 2010, Lect Notes in Comput. Sci., **6477**, 177-194, ed. Abe, M., Springer Verlag, 2010. doi: 10.1007/978-3-642-17373-8_11
13. Kim, S. and Cheon, J.H.: Fixed argument pairing inversion on elliptic curves. Des. Codes Crypto., **77**, 143-152 (2015) (IACR e-print 2012/657). doi: 10.1007/s10623-014-9993-x
14. Lashermes, R., Fournier, J. and Goubin, L.: Inverting the final exponentiation of Tate pairings on ordinary elliptic curves using faults., CHES 2013, Lect. Notes in Comput. Sci., **8086**, 365-382, ed. Bertoni, G. and Coron, J.-S., Springer, 2013. doi: 10.1007/978-3-642-40349-1_21
15. Menezes, A. J., Okamoto, T. and Vanstone, S. A.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Info. Theory, **39**, 1639-1646 (1993). doi: 10.1109/18.259647
16. Nakai, Y.: Kakankan to bibun (Commutative rings and differential). Kyouritsu Pub. 1973 (in Japanese).
17. Satoh, T.: Generalized division polynomials. Math. Scand., **94**, 161-184 (2004).
18. Satoh, T.: Closed formulae for the Weil pairing inversion. Finite fields and their appl., **14**, 743-765 (2008). doi: 10.1016/j.ffa.2007.12.003
19. Satoh, T.: Miller inversion is easy for the reduced Tate pairing of embedding degree greater than one, (revised 2025) preprint, IACR e-print 2019/385.
20. Silverman, J. H.: The arithmetic of elliptic curves. GTM, 106. Berlin-Heidelberg-New York: Springer 1986.
21. Vercauteren, F.: The hidden root problem, Paring-based cryptography 2008, Lect. Notes in Comput. Sci., **5209**, 89-99, Berlin, Heidelberg: Springer, 2008. doi: 10.1007/978-3-540-85538-5
22. Verheul, E.R.: Evidence that XTR is more secure than supersingular elliptic curve cryptosystem, Advances in cryptology - EUROCRYPT 2001, **2045**, 195-210, Berlin Heidelberg: Springer-Verlag, 2001.
23. Whittaker, E.T. and Watson, G.N.: A course of modern analysis (4th ed.), Cambridge Univ. Press, 1927 (reprint 1984).