Some Remarks on the Weil and Tate Pairings of Curves over Finite Fields

F. Hess

Computer Science Department,
Woodland Road, University of Bristol, BS8 1UB, UK

Abstract. This manuscript is of expositional purpose. We provide elementary proofs for the equivalence of two common definitions of the Weil pairing and for the non-degeneracy of the Tate pairing.

1 Introduction

The Weil and Tate pairings provide non-degenerate pairings from subgroups and quotient groups of the divisor class group of a curve over a finite field onto subgroups and quotient groups of the multiplicative group of the finite field. In addition to numerous other applications these pairings have recently proved useful, if not essential, in identity based cryptography.

In [10, 11] a method for computing the Weil pairing on an elliptic curve is described. However, the definition used for the computation of the Weil pairing does not coincide with the definition in [14], and the connection is left as an exercise in [14] but is not immediately obvious. As for the Tate pairing, a fairly long proof for its non-degeneracy is given in [5], using cohomological methods.

The objective of this manuscript is to provide rather elementary proofs for the equivalence of the two definitions of the Weil pairing and for the non-degeneracy of the Tate pairing.

2 Preliminaries

Let C be an absolutely irreducible projective curve defined over the field k. The function field of C is denoted by $k(C)$.

The divisor class group of degree zero divisors is denoted by $\mathcal{C}l^0(k(C))$, where we consider divisors as finite sums of places of $k(C)$. If C is non-singular and the Brauer group of k is trivial then $\mathcal{C}l^0(k(C))$ is isomorphic to the group of k-rational points of the Jacobian of C (see [12, Remark 1.6]). The class of a divisor D is denoted by $[D]$, and the principal divisor of an element $a \in k(C)^\times$ by $\mathrm{div}((a))$.

Let $D = \sum_i \lambda_i P_i$ be a divisor of $k(C)$ where the P_i are places. The evaluation $f(P)$ of a function $f \in k(C)$ with no pole at the place P is an element of the

residue class field $k(P) = \mathcal{O}_P/P$. Using the norm map of the extension $k(P_i)/k$ of degree $\deg(P_i)$ we can further define an evaluation at divisors via

$$f(D) := \prod_i \mathrm{N}_{k(P_i)/k}(f(P_i))^{\lambda_i},$$

provided f has no zero at P_i when $\lambda_i < 0$ and no pole when $\lambda_i > 0$. The evaluation map enjoys homomorphic properties in f and D. Furthermore, it commutes with base extension or, in other words, if $\mathrm{con}_{k_1(C)/k(C)}$ is the conorm map for an extension $k_1(C)/k(C)$ we have

$$\mathrm{con}_{k_1(C)/k(C)}(f)\big(\mathrm{con}_{k_1(C)/k(C)}(D)\big) = f(D).$$

Consider a cover $C \to C'$ of absolutely irreducible curves defined over k. The associated norm $\mathrm{N}_{k(C)/k(C')}$ and conorm $\mathrm{con}_{k(C)/k(C')}$ maps are adjoint with respect to the evaluation at divisors. For $f \in k(C)$ and D a divisor of $k(C')$ we have

$$f\big(\mathrm{con}_{k(C)/k(C')}(D)\big) = \mathrm{N}_{k(C)/k(C')}(f)(D),$$

and for $f \in k(C')$ and D a divisor of $k(C)$

$$f\big(\mathrm{N}_{k(C)/k(C')}(D)\big) = \mathrm{con}_{k(C)/k(C')}(f)(D),$$

provided the values are defined.

3 Weil Reciprocity

Weil reciprocity is well known and a very useful tool in studying the Weil and Tate pairings.

Theorem 1 *Let $a, b \in k(C)^\times$ such that (a) and (b) have disjoint support. Then*

$$a\big((b)\big) = b\big((a)\big).$$

Proof (Standard version). The standard proof goes as follows. It is not difficult to prove the theorem for $C = \mathbb{P}^1$ or when $a \in k$ or $b \in k$. Otherwise, consider the extension $k(C)/k(b)$ of the rational function field $k(b) \cong k(\mathbb{P}^1)$. We indicate by the subscript $k(b)$ if a principal divisor is to be taken in $k(b)$ rather than $k(C)$. Then

$$\begin{aligned} a\big(\mathrm{div}(b)\big) &= a\big(\mathrm{div}(\mathrm{con}_{k(C)/k(b)}(b))\big) = a\big(\mathrm{con}_{k(C)/k(b)}(\mathrm{div}_{k(b)}(b))\big) \\ &= \mathrm{N}_{k(C)/k(b)}(a)\big(\mathrm{div}_{k(b)}(b)\big) = b\big(\mathrm{div}_{k(b)}(\mathrm{N}_{k(C)/k(b)}(a))\big) \\ &= b\big(\mathrm{N}_{k(C)/k(b)}(\mathrm{div}(a))\big) = \mathrm{con}_{k(C)/k(b)}(b)\big(\mathrm{div}(a)\big) = b\big(\mathrm{div}(a)\big). \end{aligned}$$

See also [14, Ex. 2.11] and [9, p. 243–245] (thanks to S. Galbraith).

Proof (More explicit version). This essentially spells out the details of the first proof in a combined form. It suffices to prove the theorem under the additional assumption that k is algebraically closed, since the evaluation of functions at divisors commutes with base extension. If $a \in k$ or $b \in k$ then $a(\operatorname{div}(b)) = b(\operatorname{div}(a)) = 1$. Indeed, if $a \in k$ then $b(\operatorname{div}(a)) = 1$ because it is an empty product. On the other hand, $a(P) = a$ for any place P and $\deg(\operatorname{div}(b)) = 0$, thus $a(\operatorname{div}(b)) = a^{\deg(\operatorname{div}(b))} = 1$.

Assume now that $a \notin k$ and $b \notin k$. We have $a\big([k(C) : k(a,b)]\operatorname{div}_{k(a,b)}(b)\big) = \operatorname{con}_{k(C)/k(a,b)}(a)\big(\operatorname{con}_{k(C)/k(a,b)}(\operatorname{div}_{k(a,b)}(b))\big) = a\big(\operatorname{div}(b)\big)$ where $\operatorname{div}_{k(b)}(b)$ is taken in $k(a,b)$. This means that we can restrict to the case $k(C) = k(a,b)$.

Let $f(x,y) \in k[x,y]$ be an irreducible polynomial such that $f(a,b) = 0$. This polynomial is defined uniquely up to multiples in $k^\times$. Write

$$f(x,y) = (c_1x^r + \cdots + c_2)y^n + \cdots + (c_3x^s + \cdots + c_4)$$

with $n \geq 1$ and $c_1 \neq 0$. Since a and b do not have a common zero we have $c_4 \neq 0$ and hence by definition $c_3 \neq 0$. Now

$$f(x,1/y)y^n = (c_3x^s + \cdots + c_4)y^n + \cdots + (c_1x^r + \cdots + c_2)$$

is an irreducible polynomial which evaluated at a and $1/b$ is zero. Since a and $1/b$ do not have a common zero we have $c_2 \neq 0$. We see that a highest power of y in $f(x,y)$ occurs in the form c_2y^n without a cofactor of the form x^j. Reversing the role of a and b or x and y respectively and looking at $f(x,y)$ and $f(x,1/y)y^n$ this remark implies that $\deg_x f(x,y) = s$ and $\deg_x f(x,1/y)y^n = r$. We thus have $s = \deg_x f(x,y) = \deg_x f(x,1/y)y^n = r$.

Let

$$f(x,y) \equiv c_2 \prod_j (y - b_j)^{e_j} \bmod x\, k[x,y]$$

be the factorization of $f(x,y)$ modulo x. This means that the zero divisor of a can be written in the form $\operatorname{div}(a)_0 = \sum_j \sum_\nu P_{j,\nu}^{e_{j,\nu}}$ where $b(P_{j,\nu}) = b_j$ and $\sum_\nu e_{j,\nu} = e_j$ (compare [15, III.3.7] and its proof). Consequently we have $b(\operatorname{div}(a)_0) = \prod_j b_j^{e_j} = (-1)^n c_4/c_2$. For the pole divisor of a we have $\operatorname{div}(a)_\infty = \operatorname{div}(1/a)_0$ hence $b(\operatorname{div}(a)_\infty) = b(\operatorname{div}(1/a)_0)$. By symmetry we obtain that $b(\operatorname{div}(a)_\infty) = (-1)^n c_3/c_1$, $a(\operatorname{div}(b)_0) = (-1)^s c_4/c_3$ and $a(\operatorname{div}(b)_\infty) = (-1)^r c_2/c_1$. Thus

$$\begin{aligned} a\big(\operatorname{div}(b)\big) &= a\big(\operatorname{div}(b)_0\big)/a\big(\operatorname{div}(b)_\infty\big) \\ &= (c_1c_4)/(c_2c_3) \\ &= b\big(\operatorname{div}(a)_0\big)/b\big(\operatorname{div}(a)_\infty\big) \\ &= b\big(\operatorname{div}(a)\big). \end{aligned}$$

We remark that the proofs also yield an algorithm to determine $a\big(\operatorname{div}(b)\big)$ which does not require the computation or factorization of $\operatorname{div}(b)$.

4 The Weil Pairing

Let E be an elliptic curve defined over the algebraically closed field k and fix $m \in \mathbb{Z}^{\geq 2}$, coprime to $\mathrm{char}(k)$ if $\mathrm{char}(k) > 0$. Let $T, S \in E[m]$ and $X \in E$ such that $\{O, T, X, X+S\} = 4$. There are functions $f, h \in k(E)$ with $\mathrm{div}(f) = m(T) - m(O)$ and $\mathrm{div}(h) = m(X+S) - m(X)$. The m-th roots of unity of k are denoted by $\mu_m(k)$. The computational definition of the Weil pairing in [10] is as follows.

Definition 2 *The Weil pairing $e_m : E[m] \times E[m] \to \mu_m(k)$ is defined by*

$$e_m(S,T) = f((X+S) - (X)) \,/\, h((T) - (O)).$$

Following [14, pp. 95] let $T' \in E$ with $[m]T' = T$. There is a function $g \in k(E)$ such that $\mathrm{div}(g) = [m]^*((T) - (O)) = \sum_{R \in E[m]} (T' + R) - (R)$ and $f \circ [m] = g^m$. The definition of the Weil pairing in [14] is as follows.

Definition 3 *The Weil pairing $e_m : E[m] \times E[m] \to \mu_m(k)$ is defined by*

$$e_m(S,T) = g(X+S) \,/\, g(X).$$

Using the first definition together with Weil reciprocity it is easy to prove that the Weil pairing is well defined, bilinear, antisymmetric, that it commutes with the action of Galois and is compatible for different m. The non-degeneracy appears to be easiest proven as in [14], using the second definition. We now verify that both definitions coincide, see also [14, Ex. 3.16].

Theorem 4 *We have $f((X+S) - (X)) \,/\, h((T) - (O)) = g(X+S) \,/\, g(X)$.*

Proof. Let $S', X' \in E$ with $mS' = S$ and $mX' = X$. For $Z \in E$ the divisor $m(Z) - m(O)$ is linearly equivalent to $(mZ) - (O)$. Applying this for $Z = X'$ and $Z = X' + S'$ and subtracting shows that there is an $u \in k(E)$ such that $\mathrm{div}(u) = m(X'+S') - m(X') - (X+S) + (X)$. Using this in turn and $f \circ [m] = g^m$ we obtain

$$\begin{aligned} f((X+S) - (X)) &= f((mX' + mS') - (mX')) \\ &= g^m((X'+S') - (X')) \\ &= g(m(X'+S') - m(X')) \\ &= g((X+S) - (X)) \cdot g(\mathrm{div}(u)). \end{aligned}$$

By Weil reciprocity we have $g(\mathrm{div}(u)) = u(\mathrm{div}(g))$ and it suffices to show that $u(\mathrm{div}(g)) = h((T) - (O))$. Using the translation map $\tau_R : Z \mapsto Z + R$ we define $u_1 = \prod_{R \in E[m]} u \circ \tau_R$. Then $u(\mathrm{div}(g)) = u(\sum_{R \in E[m]} (T' + R) - (R)) = u_1((T') - (O))$. Clearly $u_1 \circ \tau_R = u_1$ for every $R \in E[m]$ and hence $u_1 = u_2 \circ [m]$ for some $u_2 \in k(E)$, see [14, III.4.10]. From $\mathrm{div}(u) = m(X'+S') - m(X') - (X+S) + (X)$ we obtain $\mathrm{div}(u_2) = m(X+S) - m(X) - (mX) + (mX) = \mathrm{div}(h)$. Hence

$$\begin{aligned} u(\mathrm{div}(g)) &= u_1((T') - (O)) \\ &= u_2((T) - (O)) \\ &= h((T) - (O)). \end{aligned}$$

5 The Tate Pairing

Let C be defined over $\mathbb{F}_q$ and let k be an algebraic extension of $\mathbb{F}_q$. Let $m \in \mathbb{Z}^{\geq 1}$ be coprime to q with $m \,|\, \#\mathcal{C}l^0(k(C))$. Using the approximation theorem we see that for divisor classes $x \in \mathcal{C}l^0(k(C))[m]$ and $y \in \mathcal{C}l^0(k(C))/m\mathcal{C}l^0(k(C))$ there are coprime divisors D and E such that $x = [D]$ and $y = [E] + m\mathcal{C}l^0(k(C))$. Furthermore, there is an $f \in k(C)$ such that $\mathrm{div}(f) = mD$.

Definition 5 *The Tate pairing* $t_m : \mathcal{C}l^0(k(C))[m] \times \mathcal{C}l^0(k(C))/m\mathcal{C}l^0(k(C)) \to k^\times/(k^\times)^m$ *is defined by*

$$t_m(x, y) = f(E).$$

Using Weil reciprocity we have $f(\mathrm{div}(g)) = g(\mathrm{div}(f)) = g(mD) \in (k^\times)^m$ for $g \in k(C)^\times$. It is now easily seen that the Tate pairing is well-defined and bilinear. Furthermore it commutes with the action of Galois.

A pairing $t : A \times B \to Z$ of abelian groups A, B, Z is non-degenerate if the associated homomorphisms $A \to \mathrm{Hom}(B, Z)$ and $B \to \mathrm{Hom}(A, Z)$ are injective.

Theorem 6 *The Tate pairing* t_m *is non-degenerate if the base field* k *is finite and contains the* m*-th roots of unity.*

Proof. Let $x = [D]$ be arbitrary in $\mathcal{C}l^0(k(C))[m]$ of precise order s and $f \in k(C)$ with $\mathrm{div}((f)) = sD$ where $s \,|\, m$. We have that the polynomial $x^s - f$ is irreducible in $k(C)[x]$ and defines a Kummer extension of $k(C)$, see [15, A.13]. From the Chebotarev density theorem and the van der Waerden criterion ([6, 5.16] and [16, Chap. 1] or [13, p. 128 (9.40)]) we conclude that for any $d \,|\, s$ and $l \geq$ some constant there is a place P of degree l such that $x^s - f(P)$ splits into irreducible factors of degree s/d in $k(P)[x]$. This means that $f(P)$ is a generator of $(k(P)^\times)^d/(k(P)^\times)^s$. The norm $\mathrm{N}_{k(P)/k}$ is surjective and induces an isomorphism $k(P)^\times/(k(P)^\times)^s \to k^\times/(k^\times)^s$. It follows that $\mathrm{N}_{k(P)/k}(f(P))$ is a generator of $(k^\times)^d/(k^\times)^s$.

By the previous paragraph applied with $d = 1$ and $d = s$ there exist places P and Q of the same degree and not in the support of D such that $\mathrm{N}_{k(P)/k}(f(P)) \notin (k^\times)^s$ and $\mathrm{N}_{k(Q)/k}(f(Q)) \in (k^\times)^s$. With $E := P - Q$ and $y := [E] + m\mathcal{C}l^0(k(C))$ we then have $t_m(x, y) \notin (k^\times)^m$. This means that the associated homomorphism $\mathcal{C}l^0(k(C))[m] \to \mathrm{Hom}(\mathcal{C}l^0(k(C))/m\mathcal{C}l^0(k(C)), k^\times/(k^\times)^m)$ is injective. The non-degeneracy now follows from Lemma 7 because $\mathcal{C}l^0(k(C))[m] \cong \mathcal{C}l^0(k(C))/m\mathcal{C}l^0(k(C))$ and $k^\times/(k^\times)^m \cong \mathbb{Z}/m\mathbb{Z}$.

Lemma 7 *Let* A, B *be finite abelian groups of exponent* m*. A pairing* $t : A \times B \to \mathbb{Z}/m\mathbb{Z}$ *is non-degenerate if and only if the associated homomorphism* $A \to \mathrm{Hom}(B, \mathbb{Z}/m\mathbb{Z})$ *is injective and* $\#A = \#B$*.*

Proof. The pairing t is non-degenerate by definition if the corresponding homomorphisms $A \to \mathrm{Hom}(B, \mathbb{Z}/m\mathbb{Z})$ and $B \to \mathrm{Hom}(A, \mathbb{Z}/m\mathbb{Z})$ are injective. Then $\#A = \#B$ since $\mathrm{Hom}(A, \mathbb{Z}/m\mathbb{Z}) \cong A$, $\mathrm{Hom}(B, \mathbb{Z}/m\mathbb{Z}) \cong B$ and because of the injectivity of the homomorphisms.

If $A \to \mathrm{Hom}(B, \mathbb{Z}/m\mathbb{Z})$ is injective then it is also surjective because $\#A = \#B = \#\mathrm{Hom}(B, \mathbb{Z}/m\mathbb{Z})$. Given $b \in B$ and $c \in \mathbb{Z}/m\mathbb{Z}$ of the same order as b there is an $h \in \mathrm{Hom}(B, \mathbb{Z}/m\mathbb{Z})$ such that $h(b) = c$. Because of the surjectivity there is an $a \in A$ such that $h = t(a, \cdot)$ and $t(a, b) = c$. This means $t(\cdot, b)$ is at least of the order of b and hence $B \to \mathrm{Hom}(A, \mathbb{Z}/m\mathbb{Z})$ is injective. □

Consider the general pairing t of Lemma 7. If t is non-degenerate we necessarily have $A \cong \mathrm{Hom}(B, \mathbb{Z}/m\mathbb{Z}) \cong B$. Also, if m is the minimal exponent of A or B respectively then a non-degenerate t is surjective. This means that the condition on the m-th roots of unity in Theorem 6 will often be not only sufficient but also necessary. Furthermore we have the following. Let $A \cong B \cong \mathbb{Z}/c_1\mathbb{Z} \times \cdots \times \mathbb{Z}/c_r\mathbb{Z}$ with $c_i \in \mathbb{Z}^{>1}$ and $c_i \,|\, c_{i+1}$. A Gaussian elimination technique shows that t is non-degenerate if and only if there are generators a_i of A and b_i of B for $1 \leq i \leq r$ such that $t(a_i, b_j) = 0$ for $i \neq j$ and $t(a_i, b_i) = m/c_i$, in which case the a_i and b_i have the precise orders c_i.

Let k_1/k be a finite extension of the finite field k and let m be prime. Assume that $m \,|\, \#\mathcal{C}l^0(k(C))$ and that k_1 contains the m-th roots of unity while k does not contain the m-th roots of unity. Since t_m is non-degenerate over k_1 the $\mathbb{Z}/m\mathbb{Z}$-rank of $\mathcal{C}l^0(k_1(C))[m]$ is at least twice the $\mathbb{Z}/m\mathbb{Z}$-rank of $\mathcal{C}l^0(k(C))[m]$. This observation can for example be used to determine the minimal field extension over which an elliptic curve of order m over its base field obtains its "second" subgroup of order m, without considering the eigenvalues of Frobenius as in [1].

The Tate pairing can be efficiently computed from its definition if f is represented in compact form as a power product of small degree functions but with possibly large exponents, an implementation for general curves based on [8] can be found in Magma [3, 4]. More efficient algorithms for the elliptic curve case are given in [2, 7].

References

1. R. Balasubramanian and N. Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes - Okamoto - Vanstone algorithm. *J. Cryptology*, 11(2):141–145, 1998.
2. P. Barreto, H. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing-based cryptosystems. In M. Yung, editor, *Advances in Cryptology - CRYPTO 2002*, LNCS 2442, pages 354–369. Springer-Verlag, Berlin-Heidelberg-New York, 2002.
3. W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symbolic Comp.*, 24, 3/4:235–265, 1997.
4. Comp. algebra group. Magma. `http://www.maths.usyd.edu.au:8000/u/magma/`, 2004.
5. G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62:865–874, 1994.
6. M. Fried and M. Jarden. *Field Arithmetic*. Springer-Verlag, Berlin-Heidelberg-New York, 1986.
7. S. Galbraith, K. Harrison, and D. Soldera. Implementing the Tate-pairing. In C. Fieker and D. R. Kohel, editors, *Proceedings of the Fifth Symposium on Algorithmic Number Theory, ANTS-V*, LNCS 2369, pages 324–337, Sydney, Australia, 2002. Springer-Verlag, Berlin-Heidelberg-New York.

8. F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comp.*, 33(4):425–445, 2002.
9. S. Lang. *Elliptic Functions*. Addison-Wesley Publishing Company, Reading, Massachusetts, 1973.
10. A. Menezes. *Elliptic curve public key cryptosystems*. Kluwer Academic Publishers, Boston, 1993.
11. V. Miller. Short programs for functions on curves. Unpublished manuscript, 1986.
12. J. S. Milne. Jacobian varieties. In G. Cornell & J. H. Silverman, editor, *Arithmetic Geometry*, pages 167–212, Storrs, Connecticut, 1986. Springer-Verlag, Berlin-Heidelberg-New York.
13. M. E. Pohst and H. Zassenhaus. *Algorithmic Algebraic Number Theory*. Cambridge University Press, Cambridge, 1st paperback edition, 1997.
14. J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, Berlin-Heidelberg-New York, 1986.
15. H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer-Verlag, Berlin-Heidelberg-New York, 1993.
16. B. van der Waerden. *Algebra I*. Springer-Verlag, Berlin-Heidelberg-New York, 1971.