A Note on the Tate Pairing of Curves over Finite Fields

F. Hess

Computer Science Department,
Woodland Road,
University of Bristol, BS8 1UB, UK.
florian@cs.bris.ac.uk

Abstract. A short and elementary proof for the non-degeneracy of the Tate pairing of curves over finite fields is given.

1 Introduction

The Tate pairing provides a non-degenerate pairing from a subgroup and a quotient group of the divisor class group of a curve over a finite field onto a quotient group of the multiplicative group of the finite field. In [4] it has been used to map a discrete logarithm problem in the divisor class group to the multiplicative group of a finite field, where it can be solved more easily if certain conditions are met. This is of particular interest in regard to discrete logarithm based cryptosystems and is known as Frey-Rück attack. More recently the Tate pairing has proven useful, if not essential, in identity based cryptography as for example in [2, 9].

The non-degeneracy of the Tate pairing is an essential property in these applications. The proof given in [4] is fairly long and involves cohomological methods. The purpose of this expositional note is to provide a short and rather elementary or direct proof 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 [11, Remark 1.6]). We are primarily interested in the case k a finite field where the Brauer group is trivial. For a divisor D its class is denoted by $[D]$.

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 $\mathrm{div}(a)$ and $\mathrm{div}(b)$ have disjoint support. Then*

$$a\big(\mathrm{div}(b)\big) = b\big(\mathrm{div}(a)\big).$$

Proof. 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 [13, Ex. 2.11] and [10, p. 243–245]. □

The proof shows that $a\big(\mathrm{div}(b)\big) = \mathrm{N}_{k(C)/k(b)}(a)\big(\mathrm{div}_{k(b)}(b)\big)$ can be computed without having to compute or factorize $\mathrm{div}(b)$ since $\mathrm{div}_{k(b)}(b)$ is just the zero of b minus the pole of b in the rational function field $k(b)$. Thus $\mathrm{N}_{k(C)/k(b)}(a)$ is of the form $(c_1 b^r + \cdots + c_2)/(c_3 b^r + \cdots + c_4)$ with $c_i \in k^\times$ and $a\big(\mathrm{div}(b)\big) = (c_2 c_3)/(c_1 c_4)$.

4 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 $m \mid \#\mathcal{C}l^0(k(C))$. 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 2 *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 and Z is non-degenerate if the associated homomorphisms $A \to \mathrm{Hom}(B, Z)$ and $B \to \mathrm{Hom}(A, Z)$ are injective.

Theorem 3 *The Tate pairing t_m is non-degenerate if the base field k is finite and contains the m-th roots of unity.*

This theorem was proved in [4]. We now give an alternative, shorter and more elementary proof.

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 $s \mid m$. We have that the polynomial $x^s - f$ is irreducible in $k(C)[x]$ and defines a Kummer extension of $k(C)$, see [14, A.13]. From the Chebotarev density theorem and the van der Waerden criterion ([5, 5.16] and [15, Chap. 1] or [12, p. 128 (9.40)]) we conclude that for any $d \mid s$ 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 $t_m(x, y) \notin (k^\times)^m$. 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 hence injective. The non-degeneracy now follows from Lemma 4 since $\mathcal{C}l^0(k(C))[m] \cong \mathcal{C}l^0(k(C))/m\mathcal{C}l^0(k(C))$ and $k^\times/(k^\times)^m \cong \mathbb{Z}/m\mathbb{Z}$. □

Lemma 4 *Let A, B be finite abelian groups of exponent m with $\#A = \#B$. 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.*

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.

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 4. 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 3 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 $c_i \mid c_{i+1}$. 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.

Assume m prime, $m \mid \#\mathcal{C}l^0(k(C))$, but that k does not contain the m-th roots of unity. If we perform a finite constant field extension to k_1 which contains the m-th roots of unity then the $\mathbb{Z}/m\mathbb{Z}$-rank of the groups $\mathcal{C}l^0(k(C))[m]$ and $\mathcal{C}l^0(k(C))/m\mathcal{C}l^0(k(C))$ has to double at least, since the Tate pairing t_m will be non-degenerate over k_1. This observation can for example be used to determine the minimal field extension over which an elliptic curve obtains its second prime factor.

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 possibly large exponents, an implementation for general curves based on [8] can be found in Magma [3]. There are more efficient algorithms for the elliptic curve case, given in [1, 6].

We finally remark that the Chebotarev density theorem for number fields can be used in a similar way to verify the multiplicative independence of algebraic numbers modulo prime powers [7, 16].

Acknowledgement

I would like to thank S. Galbraith for helpful comments on Weil reciprocity.

References

1. P. Barreto, H. Kim, B. Lynn, and M. Scott, *Efficient algorithms for pairing-based cryptosystems*, Advances in Cryptology - CRYPTO 2002 (M. Yung, ed.), LNCS 2442, Springer-Verlag, Berlin-Heidelberg-New York, 2002, pp. 354–369.
2. D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, Advances in Cryptology - CRYPTO 2001 (J. Kilian, ed.), LNCS 2139, Springer-Verlag, Berlin-Heidelberg-New York, 2001, pp. 213–229.

3. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comp. **24, 3/4** (1997), 235–265.
4. 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** (1994), 865–874.
5. M. Fried and M. Jarden, *Field arithmetic*, Springer-Verlag, Berlin-Heidelberg-New York, 1986.
6. S. Galbraith, K. Harrison, and D. Soldera, *Implementing the Tate-pairing*, Proceedings of the Fifth Symposium on Algorithmic Number Theory, ANTS-V (Sydney, Australia) (C. Fieker and D. R. Kohel, eds.), LNCS 2369, Springer-Verlag, Berlin-Heidelberg-New York, 2002, pp. 324–337.
7. F. Hess, *Zur Klassengruppenberechnung in algebraischen Zahlkörpern*, MSc Thesis, Technische Universität Berlin, 1996.
8. F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comp. **33** (2002), no. 4, 425–445.
9. F. Hess, *Efficient identity based signature schemes based on pairings*, Proceedings of SAC 2002 (St. Johns, Newfoundland) (K. Nyberg and H. Heys, eds.), LNCS 2595, Springer-Verlag, Berlin-Heidelberg-New York, 2003, pp. 310–324.
10. S. Lang, *Elliptic functions*, Addison-Wesley Publishing Company, Reading, Massachusetts, 1973.
11. J. S. Milne, *Jacobian varieties*, Arithmetic Geometry (Storrs, Connecticut) (G. Cornell & J. H. Silverman, ed.), Springer-Verlag, Berlin-Heidelberg-New York, 1986, pp. 167–212.
12. M. E. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, 1st paperback ed., Cambridge University Press, Cambridge, 1997.
13. J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin-Heidelberg-New York, 1986.
14. H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, Berlin-Heidelberg-New York, 1993.
15. B. van der Waerden, *Algebra I*, Springer-Verlag, Berlin-Heidelberg-New York, 1971.
16. K. Wildanger, *Über Grundeinheitenberechnung in algebraischen Zahlkörpern*, MSc Thesis, Heinrich-Heine-Universität Düsseldorf, 1993.