Pairing Lattices

Florian Hess

Technische Universität Berlin, Germany
hess@math.tu-berlin.de

Abstract. We provide a convenient mathematical framework that essentially encompasses all known pairing functions based on the Tate pairing. We prove non-degeneracy and bounds on the lowest possible degree of these pairing functions and show how efficient endomorphisms can be used to achieve a further degree reduction.

1 Introduction

The cryptographic importance of efficiently computable, bilinear and non-degenerate pairings that are hard to invert in various ways has been amply demonstrated. The currently only known instantiations of pairings suitable for cryptography are the Weil and Tate pairings on elliptic curves or on Jacobians of more general algebraic curves. In view of the applications, efficient algorithms for computing these pairings are of great importance.

Let E be an elliptic curve over $\mathbb{F}_q$ and let G_1, G_2 be two subgroups of $E(\mathbb{F}_q)$ of prime order r satisfying $r \,|\, (q-1)$. Let μ_r be the subgroup of r-th roots of unity of $\mathbb{F}_q^\times$. Then we can in principle define a pairing $e : G_1 \times G_2 \to \mu_r$ by taking any generator of μ_r as the pairing value of a generator of G_1 and a generator of G_2 and by extending via linearity. Since the computation of pairing values would then require taking discrete logarithms, this is not a practical approach.

A different approach avoiding the problem with the discrete logarithms would be to use an algebraic representation of e such that pairing values are obtained by substituting the coordinates of the input points with respect to a short Weierstrass form of E into an algebraic expression. This can in principle generally be achieved by using polynomial interpolation and would for example lead to a representation $e(P,Q) = f(x_P, y_P, x_Q, y_Q)$ where $P = (x_P, y_P) \in G_1$, $Q = (x_Q, y_Q) \in G_2$ and $f \in \mathbb{F}_{q^k}[x_1, y_1, x_2, y_2]$ is a fixed polynomial of total degree about r^2 (or r if viewed in x_1, y_1 and x_2, y_2 separately). However, this approach will also be impractical unless some efficient, i.e. at least polynomial time in $\log(r)$, way of storing and evaluating f is found.

The approach currently employed is to use rational functions f_P on E depending on P instead of interpolation polynomials such that the pairing values are obtained by a function evaluation $e(P,Q) = f_P(Q)^{(q-1)/r}$. The functions f_P are given by means of principal divisors with large coefficients but small support. One then essentially applies the Riemann-Roch theorem in form of Miller's algorithm to find a polynomial-in-$\log(r)$-sized representation of f, consisting of a short product of quotients of linear polynomials in x and y with large exponents, which enables the efficient evaluation of $f_P(Q)$.

The Tate and ate pairings are two special forms of functions f_P. Recently, some more variants have been given in [4, 8]. Products of the Tate and the ate pairing with the goal of reducing the degree of the resulting pairing function have been considered in [3]. This idea has been much extended in [7] and is also the objective of this paper. In addition to the construction from [7] we provide a convenient mathematical framework that allows to formulate a much clearer non-degeneracy condition and relation with the Tate pairing. The key idea here is to use a degenerate ate pairing instead of the non-degenerate ate pairing. We prove the non-degeneracy of the pairings given by certain functions of lowest degree, prove some optimal lower and upper bounds in every admissible dimension and extend the construction to allow the use of efficiently computable automorphisms and endomorphisms.

2 Preliminaries

2.1 Notation

In this paper we will consider ordinary elliptic curves only, although the general logic behind the construction generalises to supersingular elliptic or hyperelliptic curves. Let us first briefly define the standard notation and setting for pairings on such elliptic curves.

Let E be an ordinary elliptic curve over a finite field $\mathbb{F}_q$. Let r be a prime factor of $\#E(\mathbb{F}_q)$ with embedding degree $k \geq 2$ such that $k \mid (r-1)$. Then $E(\mathbb{F}_{q^k})[r] \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ and there exists a basis P, Q of $E(\mathbb{F}_{q^k})[r]$ satisfying $\pi(P) = P$ and $\pi(Q) = qQ$, where π is the q-power Frobenius endomorphism on E. We define $G_1 = \langle P \rangle$ and $G_2 = \langle Q \rangle$. Note that $G_1 \cap G_2 = \{\mathcal{O}\}$.

Let $\mathcal{O}$ be the point at infinity and $z \in \mathbb{F}_q(E)$ a fixed local uniformiser at $\mathcal{O}$. We say that $f \in \mathbb{F}_{q^k}(E)$ is monic if $(fz^{-v})(\mathcal{O}) = 1$ where v is the order of f at $\mathcal{O}$. In other words this says that the Laurent series expansion

of f in terms of z is of the form $f = z^v + O(z^{v+1})$. We will consider monic functions f throughout the paper.

For $s \in \mathbb{Z}$ and $R \in E(\mathbb{F}_{q^k})$ we let $f_{s,R} \in \mathbb{F}_{q^k}(E)$ be the uniquely determined monic function with divisor $(f_{s,R}) = s((R) - (\mathcal{O})) - ((sR) - (\mathcal{O}))$ where (R) is the prime divisor corresponding to the point R. Miller's algorithm expresses $f_{s,R}$ as a product about $\log_2(|s|)$ powers of quotients of monic linear functions. Note that for $R \in E(\mathbb{F}_q)$ we have $f_{s,R} \in \mathbb{F}_q(E)$.

The r-th roots of unity in $\mathbb{F}_{q^k}$ are denoted by μ_r. The n-th cyclotomic polynomial is denoted by Φ_n, and its degree by $\varphi(n)$.

2.2 Tate and Ate Pairings

Recall that the reduced Tate pairing and ate pairings are bilinear pairings $G_2 \times G_1 \to \mu_r$ and are given as follows. The reduced Tate pairing is

$$t : G_2 \times G_1 \to \mu_r, \quad (Q, P) \mapsto f_{r,Q}(P)^{(q^k-1)/r}.$$

It is in fact defined on all $E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})[r]$ and is always non-degenerate.

Let s be an arbitrary integer such that $s \equiv q \bmod r$. Let $N = \gcd(s^k - 1, q^k - 1)$, $L = (s^k - 1)/N$ and $c = \sum_{j=0}^{k-1} s^{k-1-j} q^j \bmod N$. The ate pairing with respect to s is given by

$$a_s : G_2 \times G_1 \to \mu_r, \quad (Q, P) \mapsto f_{s,Q}(P)^{c(q^k-1)/N}.$$

The relation with the Tate pairing is $a_s(Q, P) = t(Q, P)^L$. It is thus non-degenerate if and only if $r \nmid L$.

It is possible to have the same final exponent in the ate pairing as in the Tate pairing. Consider the modified ate pairing

$$a_s : G_2 \times G_1 \to \mu_r, \quad (Q, P) \mapsto f_{s,Q}(P)^{(q^k-1)/r}.$$

Since $r \mid N$ and $r \nmid c$ this is always bilinear, and using the relation with the Tate pairing it is not difficult to show that it is non-degenerate if and only if $s^k \not\equiv 1 \bmod r^2$ (see also Corollary 13).

It is in general not true that the ate pairing can be extended to a bilinear pairing on proper overgroups of G_2 or G_1.

3 Pairing Functions of Lowest Degree

Let s be an integer. For $h = \sum_{i=0}^{d} h_i x^i \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod r$ let $f_{s,h,R} \in \mathbb{F}_{q^k}(E)$ for $R \in E(\mathbb{F}_{q^k})[r]$ be the uniquely defined monic function

satisfying

$$(f_{s,h,R}) = \sum_{i=0}^{d} h_i((s^i R) - (\mathcal{O})).$$

Furthermore, define

$$\|h\|_1 = \sum_{i=0}^{d} |h_i|.$$

If d is less than the order of s modulo r then $\|h\|_1/2 \leq \deg(f_{s,h,Q}) \leq \|h\|_1$.

Theorem 1 *Assume that s has order k modulo r. Then there is $h \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod r$, $\deg(h) \leq \varphi(k) - 1$ and $\|h\|_1 = O(r^{1/\varphi(k)})$ such that*

$$a_{s,h} : G_2 \times G_1 \to \mu_r, \quad (Q, P) \mapsto f_{s,h,Q}(P)^{(q^k-1)/r}$$

is a non-degenerate bilinear pairing. The polynomial h can be efficiently computed. The relation with the Tate pairing is

$$a_{s,h}(Q, P) = t(Q, P)^{h(s)/r}.$$

Any $h \in \mathbb{Z}[x]$ with $\deg(h) \leq k - 1$ such that $a_{s,h}$ is a non-degenerate bilinear pairing satisfies $\|h\|_1 \geq r^{1/\varphi(k)}$.

The O-constant depends only on k.

Proof. We may replace s by $s + ir$ without affecting the statement of the theorem. Since k is coprime to r we can find i such that $(s + ir)^k \equiv 1 \bmod r^2$. In the following we thus assume that s has order k modulo r and $s^k \equiv 1 \bmod r^2$.

It is convenient to describe the situation in terms of the ring $A = \mathbb{Z}[x]/(x^k - 1)\mathbb{Z}[x]$ and its ideals $I^{(i)} = \{h + (x^k - 1)\mathbb{Z}[x] \mid h(s) \equiv 1 \bmod r^i\}$ for $i \in \{1, 2\}$ (thus we use the notation from the beginning of section 4 in the case $R = \mathbb{Z}$). In addition, let W be the multiplicative group of functions $G_2 \times G_2 \to \mu_r$ and W_{bilin} the subgroup of bilinear functions. We want to define a map $a_s : I^{(1)} \to W$.

Since $f_{s,h(x)(x^k-1)+g(x),R} = f_{s,g(x),R}$ we can consider $f_{s,h,R}$ also for $h \in I^{(1)}$ in a natural way. Note that $f_{s,x-s,R}$ is equal to $f_{s,R}$ using the previous notation.

We now define $a_s : I^{(1)} \to W$ where h is mapped to $a_{s,h}$ with $a_{s,h}(T, S) = f_{s,h,T}(S)^{(q^k-1)/r}$ and $a_{s,h}(\mathcal{O}, S) = a_{s,h}(T, \mathcal{O}) = 1$ for $T \in G_2$ and $S \in G_1$. Note $a_{s,h+g} = a_{s,h}a_{s,g}$ for all $h, g \in I^{(1)}$, so a_s is a homomorphism.

We wish to show $\mathrm{im}(a_s) = W_{\mathrm{bilin}}$ and $\ker(a_s) = I^{(2)}$. By Lemma 2 we have $I^{(i)} = r^i A + (x-s)A$ for $i \in \{1,2\}$. Now $a_{s,r}$ is the Tate pairing and $a_{s,x-s}$ is the degenerate ate pairing with respect to s. Hence $a_{s,r}, a_{s,x-s} \in W_{\mathrm{bilin}}$. Since s has order k modulo r there is i such that $s \equiv q^i \bmod r$. Then $a_{s,xh} = (a_{s,h})^{q^i} \in W_{\mathrm{bilin}}$ for all $h \in I^{(1)}$. This together with the additivity of a_s shows that if $a_{s,h} \in W_{\mathrm{bilin}}$, then $a_{s,gh} \in W_{\mathrm{bilin}}$ for all $g \in \mathbb{Z}[x]$ and all $g \in A$. Hence $\mathrm{im}(a_s) \subseteq W_{\mathrm{bilin}}$ because $I^{(1)} = rA + (x-s)A$. Finally, since $a_{s,r} \neq 1$ and r is prime, we have $\mathrm{im}(a_s) = W_{\mathrm{bilin}}$.

The above argument also shows that $\ker(a_s)$ is an ideal of A. Since a_s is surjective, the index satisfies $(I^{(1)} : \ker(a_s)) = \#W_{\mathrm{bilin}} = r$. But $r^2, x-s \in \ker(a_s)$ so $I^{(2)} \subseteq \ker(a_s)$. By Lemma 2 we have $(I^{(1)} : I^{(2)}) = r$ so $\ker(a_s) = I^{(2)}$ follows.

Having set up the link to the ring A and the ideals $I^{(i)}$ the theorem follows from the lattice arguments of Lemma 4, the isomorphism of Lemma 2 and the lower bound of Lemma 3. □

We remark that the the construction of the proof is complete in the following sense: Let $w, h_i \in \mathbb{Z}$ such that $\sum_{i=0}^{k-1} h_i(\pi^i(Q)) - w(\mathcal{O})$ is a principal divisor. Then $\sum_{i=0}^{k-1} h_i(\pi^i(T)) - w(\mathcal{O})$ is a principal divisor for every $T \in G_2$ since necessarily $\sum_{i=0}^{k-1} h_i q^i \equiv 0 \bmod r$. Let $f_T \in \mathbb{F}_{q^k}(E)$ be monic such that $(f_T) = \sum_{i=0}^{k-1} h_i(\pi^i(T)) - w(\mathcal{O})$. Then $(T,S) \mapsto f_T(S)^{(q^k-1)/r}$ defines a bilinear pairing that is equal to $a_{q,h}$ for $h = \sum_{i=0}^{k-1} h_i x^i \in I^{(1)}$, as is directly seen. As a consequence, there are no additional functions left in $\mathbb{F}_{q^k}(E)$ that are supported on $Z = \{\pi^i(Q) \,|\, 0 \leq i \leq k-1\}$ and could possibly define a bilinear pairing.

4 Some Lemmas

This section contains some technical lemmas dealing with the ring A and its ideals $I^{(i)}$ that occured in the proof of Theorem 1.

In the following we will work with $R = \mathbb{Z}$, $R = \mathbb{Z}[t]$ and $R = \mathbb{Q}[t]$. It is hence convenient to deal with these cases simultaneously for a moment.

Let R be a domain and let $r, s \in R$ such that $r \neq 0$ is not a unit and s has order $n \geq 2$ in $(R/rR)^\times$. Define the R-algebra and its ideals

$$A = R[x]/(x^n - 1)R[x],$$
$$I^{(i)} = \{h + (x^n - 1)R[x] \,|\, h(s) \equiv 0 \bmod r^i\},$$

for $i \geq 0$ such that $s^n \equiv 1 \bmod r^i R$. In the following we will identify elements of A with their representing polynomials of degree $\leq n-1$. We

also define the R-modules

$$I^{(i),m} = \{h \in I^{(i)} \mid \deg(h) \leq m-1\}.$$

Note $I^{(i),m} \subseteq I^{(j),w}$ for $m \leq w$ and $i \leq j$. Also $I^{(i),n} = I^{(i)}$.

Lemma 2 *The $I^{(i)}$ and $I^{(i),m}$ have the following properties:*

1. $I^{(i)} = r^i A + (x-s)A$.
2. $I^{(i),m}$ *is free of rank* m *and a basis is* $r^i, x-s, x^2-s^2, \ldots, x^{m-1}-s^{m-1}$.
3. $I^{(i)}/I^{(i+1)} \cong R/rR$ *under* $h \mapsto h(s)/r^i$ *with inverse* $g \mapsto r^i g$.
4. *If* $m \geq \varphi(n)$ *then* $I^{(i),m} = M \oplus I^{(i),\varphi(n)}$ *with* $M = \{h \in I^{(i),m} \mid h \equiv 0 \bmod \Phi_n\}$.

Proof. From the definition of $I^{(i)}$ it is clear that $r^i A + (x-s)A \subseteq I^{(i)}$. Conversely, let $h \in I^{(i)}$. Polynomial division by $x-s$ with remainder shows $h = g \cdot (x-s) + h(s)$ with $g \in A$ and $h(s) \in R$. By definition of $I^{(i)}$ we have $h(s) \in r^i R$. Thus $h = h(s) + g \cdot (x-s) \in r^i A + (x-s)A$. This proves the first assertion.

The second assertion follows easily from the first assertion and a short Hermite normal form calculation. Another basis of $I^{(i),m}$ is given by $r^i, x-s, x(x-s), \ldots, x^{m-2}(x-s)$.

The third assertion follows from the form of the bases in the second assertion. Or, polynomial division by $x-s$ with remainder shows that $h \mapsto h(s)/r^i$ splits $g \mapsto r^i g$ and has zero kernel by the first assertion.

The last assertion follows using polynomial division by Φ_n with remainder: The inclusion $I^{(i),\varphi(n)} \to I^{(i),m}$ is split by the projection $I^{(i),m} \to I^{(i),\varphi(n)}$, $h \mapsto h \bmod \Phi_n$. Here $h \bmod \Phi_n \in I^{(i),\varphi(n)}$ since $\Phi_n(s) \equiv 0 \bmod r^i$. Note that M is a free R-module with basis $\Phi_n, \ldots, x^{m-\varphi(n)-1}\Phi_n$. □

We remark that in addition to Lemma 2 one can show $I^{(i)} = (I^{(1)})^i$ if $R = nR + rR$ (for example $R = \mathbb{Z}$ and r a prime). Since the ideals $I^{(i)}$ are closed under multiplication by x we see that they are closed under rotation of the coefficients of $h \in I^{(i)}$.

4.1 The case $R = \mathbb{Z}$

We keep the above notation and assume $r \geq 2$. For $h = \sum_{i=0}^{d} h_i x^i \in \mathbb{Z}[x]$ define

$$\|h\|_1 = \sum_{i=0}^{d} |h_i| \quad \text{and} \quad \|h\|_2 = \sum_{i=0}^{d} |h_i|^2.$$

Extend this definition to A by using class representatives of degree $\leq n-1$. This makes $I^{(i)}$ into a lattice. We have $\|\cdot\|_1 = \Theta(\|\cdot\|_2)$ on $I^{(i)}$ where the constants depend only on n.

Lemma 3 *Assume $s^n \equiv 1 \bmod r^i$ and let $h \in \mathbb{Z}[x]$ such that $h(s) \equiv 0 \bmod r^i$. If $h \not\equiv 0 \bmod \Phi_n$ then*

$$\|h\|_1 \geq r^{i/\varphi(n)}.$$

Proof. Let ζ be a primitive n-th root of unity in $\bar{\mathbb{Q}}$ and $B = \mathbb{Z}[\zeta]$ the ring of integers of the n-cyclotomic number field $K/\mathbb{Q}$. Let $\mathfrak{a} = r^i B + (\zeta - s)B$. Then $\mathfrak{a}$ is an ideal of B of norm $N_{K/\mathbb{Q}}(\mathfrak{a}) = r^i$, by assumption on s. We have $\zeta \equiv s \bmod \mathfrak{a}$. Thus $h(\zeta) \in \mathfrak{a}$ by assumption on h and

$$|N_{K/\mathbb{Q}}(h(\zeta))| \geq N_{K/\mathbb{Q}}(\mathfrak{a}) = r^i.$$

On the other hand, the $\varphi(n)$ complex conjugates $\zeta^{(j)}$ of ζ satisfy $|\zeta^{(j)}| = 1$. Hence $|h(\zeta^{(j)})| \leq \|h\|_1$ and

$$|N_{K/\mathbb{Q}}(h(\zeta))| = \Big|\prod_{j=1}^{\varphi(n)} h(\zeta^{(j)})\Big| \leq \|h\|_1^{\varphi(n)}.$$

Combining the two inequalities proves the first assertion. □

Lemma 4 *Assume $s^n \equiv 1 \bmod r^2$. Let $m \geq \varphi(n)$ and $w = m - \varphi(n)$. Any length ordered LLL-reduced basis $v_1, \ldots, v_m$ of $I^{(1),m}$ satisfies*

$$\|v_i\|_1 = O(1) \text{ and } v_i \in I^{(2)} \text{ for } 1 \leq i \leq w,$$
$$\|v_i\|_1 = \Theta(r^{1/\varphi(n)}) \text{ and } v_i \neq I^{(2)} \text{ for } w < i \leq m.$$

The O- and Θ-constants depend only on n and the element relations hold for r sufficiently large in comparison to n.

Proof. By Lemma 2 the determinant of $I^{(1),m}$ is r and its dimension is m. We also have $I^{(1),m} = M \oplus I^{(1),\varphi(n)}$ with $M = \{h \in I^{(1),m} \mid h \equiv 0 \bmod \Phi_n\}$. Thus there are at least $\varphi(n)$ basis vectors v_i whose projection onto $I^{(1),\varphi(n)}$ is not zero. By Lemma 3 these v_i satisfy $\|v_i\|_2 = \Omega(r^{1/\varphi(n)})$. On the other hand, the LLL-property shows $\prod_{i=1}^{m} \|v_i\|_2 = O(r)$. Thus there are precisely $\varphi(n)$ basis vectors v_i of size $\Theta(r^{1/\varphi(n)})$ whose projection onto $I^{(1),\varphi(n)}$ is not zero. The other basis vectors v_i are in M and satisfy $\|v_i\|_2 = O(1)$. Since the v_i are assumed to be ordered by length the assertion on the norms follows observing $\|\cdot\|_1 = \Theta(\|\cdot\|_2)$.

Now $\Phi_n(s) \equiv 0 \bmod r^2$ by assumption on s. Hence $v \in I^{(2)}$ for every $v \in M$. This shows $v_i \in I^{(2)}$ for $1 \le i \le w$. On the other hand, if $v \in I^{(1),m} \backslash M$ and $v \in I^{(2)}$, then $v \not\equiv 0 \bmod \Phi_n$ and $v(s) \equiv 0 \bmod r^2$. Then $\|v\|_2 = \Omega(r^{2/\varphi(n)})$ by Lemma 3. This finally shows $v_i \notin I^{(2)}$ for $w < i \le m$. □

The true constants of the O-terms and Θ-terms cannot easily be given, only worst case bounds are available that are usually much too large. Since r will in practice be much larger than n the contribution of these terms is small and can essentially be neglected. Then the element relations will hold as well. Note that, unconditionally, any (LLL-reduced) basis of $I^{(1),m}$ must contain at least one basis element that is not in $I^{(2)}$.

4.2 The case $R = \mathbb{Z}[t]$

We keep the above notation and assume $\deg(r) \ge 1$. For $h = \sum_{i=0}^{d} h_i x^i \in \mathbb{Q}[t,x]$ with $h_i \in \mathbb{Q}[t]$ define

$$\deg_t h = \max_{0 \le i \le d} \deg(h_i).$$

Extend this definition to A by using class representatives of degree $\le n-1$. This makes $I^{(i)}$ into a 'lattice' with respect to deg.

Lemma 5 *Assume $s^n \equiv 1 \bmod r^i\mathbb{Q}[t]$ and let $h \in \mathbb{Q}[t,x]$ such that $h(s) \equiv 0 \bmod r^i\mathbb{Q}[t]$. If $h \not\equiv 0 \bmod \Phi_n(x)\mathbb{Q}[t,x]$ then*

$$\deg_t(h) \ge i/\varphi(n) \deg(r).$$

Proof. Let ζ be a primitive n-th root of unity in $\bar{\mathbb{Q}}$ and $B = \mathbb{Q}[t,\zeta]$ the integral closure of $\mathbb{Q}[t]$ in the function field $K = \mathbb{Q}(t,\zeta)/\mathbb{Q}$. Let $\mathfrak{a} = r^i B + (\zeta - s)B$. Then $\mathfrak{a}$ is an ideal of B of norm $N_{K/\mathbb{Q}(t)}(\mathfrak{a}) = r^i$, by assumption on s. We have $\zeta \equiv s \bmod \mathfrak{a}$. Thus $h(\zeta) \in \mathfrak{a}$ by assumption on h and

$$\deg(N_{K/\mathbb{Q}(t)}(h(\zeta))) \ge \deg(N_{K/\mathbb{Q}(t)}(\mathfrak{a})) = i \deg(r).$$

On the other hand, the $\varphi(n)$ Puiseux series expansions of ζ with respect to the degree valuation of $\mathbb{Q}(t)$ are just the constant complex conjugates $\zeta^{(j)}$ of ζ and thus satisfy $\deg(\zeta^{(j)}) = 0$. Hence $\deg(h(\zeta^{(j)})) \le \deg_t(h)$ and

$$\begin{aligned} \deg(N_{K/\mathbb{Q}(t)}(h(\zeta))) &= \deg\left(\prod_{j=1}^{\varphi(n)} h(\zeta^{(j)})\right) \\ &= \sum_{j=1}^{\varphi(n)} \deg(h(\zeta^{(j)})) \le \varphi(n) \deg_t(h). \end{aligned}$$

Combining the two inequalities proves the assertion. □

The following lemma uses the function field LLL (e.g. [5]). On input of $M \in \mathbb{Q}[t]^{n\times n}$ with $\det(M) \neq 0$ the function field LLL outputs $N, T \in \mathbb{Q}[t]^{n\times n}$ such that $N = MT$, $\det(T) = 1$ and the sum of the maximal degrees occuring in each column equals the degree of $\det(M)$. The columns of N are then by definition independent LLL-reduced elements of $\mathbb{Q}[t]^n$.

Lemma 6 *Assume $s^n \equiv 1 \bmod r^2\mathbb{Q}[t]$. Let $m \geq \varphi(n)$ and $w = m-\varphi(n)$. Any length ordered LLL-reduced independent elements $v_1, \ldots, v_m$ of $I^{(1),m}$ generating a submodule of finite index satisfy*

$$\deg_t v_i = 0 \text{ and } v_i \in I^{(2)} \text{ for } 1 \leq i \leq w,$$
$$\deg_t(v_i) = 1/\varphi(n)\deg(r) \text{ and } v_i \neq I^{(2)} \text{ for } w < i \leq m.$$

Proof. The assertion and proof are exactly analogous to Lemma 4, if we replace $I^{(1),m}$ by $\mathbb{Q}I^{(1),m}$ (i.e. allowing rational coefficients or using $R = \mathbb{Q}[t]$), require that the v_i be a length ordered LLL-reduced basis of $\mathbb{Q}I^{(1),m}$ and observe the analogy $\deg_t = \log(\|\cdot\|_2)$). The lemma then follows because any LLL-reduced independent elements of $I^{(1),m}$ generating a submodule of finite index are an LLL-reduced basis of $\mathbb{Q}I^{(1),m}$. □

The $v_i \in I^{(1),m}$ of Lemma 6 can be obtained from any LLL-reduced basis of $\mathbb{Q}I^{(1),m}$ by multiplying each v_i by a suitable integer, for example such that the transformation matrix of the input basis of $I^{(1),m}$ from Lemma 2 and the LLL-reduced basis will be defined over $\mathbb{Z}[t]$.

5 Extended Ate Pairings

The next theorem extends the ate pairing with respect to s to a possibly slightly larger set of admissible values of s. We will then apply this to extend Theorem 1 in order to make use of automorphisms of E.

Theorem 7 *Let $n = \operatorname{lcm}(k, \#\mathrm{Aut}(E))$. Then the n-th roots of unity modulo r are defined in integers. Let s be any n-th root of unity modulo r. Write $s = uq^d \bmod r$ with u an $\#\mathrm{Aut}(E)$-th root of unity modulo r and let e be the order of u modulo r. Define*

$$N = \gcd(s^n - 1, q^k - 1), \quad L = (s^n - 1)/N,$$
$$c = \sum_{i=0}^{k-1} (s^e)^{k-1-i}(q^{de})^i \bmod N.$$

Then there is $\gamma \in \mathrm{Aut}(E)$ *of order* e *such that* $(\gamma\pi^d)(Q) = sQ$ *and*

$$a_s : G_2 \times G_1 \to \mu_r,$$
$$(Q, P) \mapsto \left(\prod_{j=0}^{e-1} f_{s,Q}(\gamma^{-j}(P))^{q^{jd} s^{e-1-j}} \right)^{c(q^k-1)/N}$$

defines a bilinear pairing. If $k \mid \#\mathrm{Aut}(E)$ *then there is* $\gamma \in \mathrm{Aut}(E)$ *such that* $\gamma(P) = sP$ *and*

$$a_s^{\mathrm{twist}} : G_1 \times G_2 \to \mu_r,$$
$$(P, Q) \mapsto \left(\prod_{j=0}^{e-1} f_{s,P}(\gamma^{-j}(Q))^{s^{e-1-j}} \right)^{c(q^k-1)/N}$$

also defines a bilinear pairing. Both pairings a_s *and* a_s^{twist} *are non-degenerate if and only if* $r \nmid L$.

The relation with the reduced Tate pairing is

$$a_s(Q, P) = t(Q, P)^L \quad \textit{and} \quad a_s^{\mathrm{twist}}(P, Q) = t(P, Q)^L.$$

We remark that if $P = \mathcal{O}$ or $Q = \mathcal{O}$ then the pairing values are defined to be equal to 1.

Proof (of Theorem 7). Since automorphisms of cyclic groups operate by integer multiplication we get isomorphisms $\mathrm{Aut}(G_1) \cong \mathrm{Aut}(G_2) \cong \mathbb{F}_r^\times$. Now, since E is ordinary, $\mathrm{Aut}(E)$ is a cyclic group (of order 2, 4 or 6) and operates faithfully on G_2 and G_1. The Frobenius endomorphism π operates faithfully on G_2 with order k. Since $\mathrm{Aut}(G_2)$ is cyclic, $\mathrm{Aut}(E)$ and π generate a cyclic subgroup H of $\mathrm{Aut}(G_2)$ of order $n = \mathrm{lcm}(k, \#\mathrm{Aut}(E))$. The image of H in $\mathbb{F}_r^\times$ is the group of n-th roots of unity, which shows that the n-roots of unity modulo r are defined in integers and that s can be written as $s \equiv uq^d \bmod r$ with u of order e modulo r and $e \mid \#\mathrm{Aut}(E)$.

In the ate pairing case, since $u^e \equiv 1 \bmod r$ and $e \mid \#\mathrm{Aut}(E)$, there is $\gamma \in \mathrm{Aut}(E)$ corresponding to the multiplication-by-u automorphism of G_2 such that $sQ = (uq^d)Q = (\gamma\pi^d)(Q)$. In the twisted ate pairing case, since $s^{\#\mathrm{Aut}(E)} \equiv 1 \bmod r$, there is $\gamma \in \mathrm{Aut}(E)$ corresponding to the multiplication-by-s automorphism of G_2 such that $sP = \gamma(P)$. Define $\psi = \gamma\pi^d$ for the ate pairing case. Define $\psi = \gamma\pi^d$ and interchange P, Q for the twisted ate pairing case. In either case we have a purely inseparable

isogeny ψ of degree q^d with $\psi(Q) = sQ$ and $\psi(P) = (s^{-1}q^d)P = u^{-1}P$. It now suffices to show that

$$t(Q,P)^L = \left(\prod_{j=0}^{e-1} f_{s,Q}(\psi^{-j}(P))^{q^{jd}s^{e-1-j}}\right)^{c(q^k-1)/N}, \tag{8}$$

since $f_{s,P}(\pi(Q)) = f_{s,P}(Q)^q$ and equation (8) implies that the ate and twisted ate pairing are bilinear, and non-degenerate if and only if $r \nmid L$.

The proof now is essentially the same as in [2], with some small modifications. From Lemma 1 of [2] we obtain

$$t(Q,P) = f_{r,Q}(P)^{(q^k-1)/r} = f_{N,Q}(P)^{(q^k-1)/N}$$

and

$$\begin{aligned} t(Q,P)^L &= f_{N,Q}(P)^{L(q^k-1)/N} = f_{LN,Q}(P)^{(q^k-1)/N} \\ &= f_{s^n-1,Q}(P)^{(q^k-1)/N} \\ &= f_{s^n,Q}(P)^{(q^k-1)/N}. \end{aligned} \tag{9}$$

Lemma 2 of [1] yields

$$f_{s^n,Q} = f_{s,Q}^{s^{n-1}} f_{s,sQ}^{s^{n-2}} \cdots f_{s,s^{n-1}Q}. \tag{10}$$

Since ψ is purely inseparable of degree q^d, we obtain from Lemma 4 in [2]

$$f_{s,\psi^i(Q)} \circ \psi^i = f_{s,Q}^{q^{id}}. \tag{11}$$

We have $\psi^i(Q) = s^iQ$ and $\psi^{ie}(P) = P$. Combining this with (10) and (11) and a short calculation collecting functions that are evaluated at the same points gives

$$f_{s^n,Q}(P) = \left(\prod_{j=0}^{e-1} f_{s,Q}(\psi^{-j}(P))^{q^{jd}s^{e-1-j}}\right)^{\sum_{i=0}^{k-1}(s^e)^{k-1-i}(q^{de})^i}. \tag{12}$$

Substituting (12) into (9) yields (8). □

Corollary 13 *With the notation and assumptions of Theorem 7, define* $v = u^{-1} \bmod r$. *Then*

$$a_s : G_2 \times G_1 \to \mu_r, \quad (Q,P) \mapsto \left(\prod_{j=0}^{e-1} f_{s,Q}(\gamma^{-j}(P))^{v^j}\right)^{(q^k-1)/r}$$

is a bilinear pairing that is non-degenerated if and only if $s^n \not\equiv 1 \bmod r^2$.

Proof. Raising the ate pairing to the power N/r shows that the exponent $(q^k-1)/N$ can be replaced by the exponent $(q^k-1)/r$ and the resulting pairing will still be bilinear. It will be non-degenerate if and only if $r \nmid L$ and $r \nmid (N/r)$, and this condition is equivalent to $s^n \not\equiv 1 \bmod r^2$, since $s^n - 1 = LN$. After raising to the power of $(q^k-1)/r$ every other exponent may be reduced modulo r. Observing $s^{-1}q^d \equiv u^{-1} \bmod r$ and hence $s^{-e}q^{de} \equiv 1 \bmod r$ we have $c \equiv \sum_{i=0}^{k-1}(s^e)^{k-1-i}(q^{de})^i \equiv k(q^{de})^{k-1} \not\equiv 0 \bmod r$. Hence c can be omitted without affecting bilinearity or non-degeneracy. Finally, $q^{jd}s^{e-1-j} \equiv s^{e-1}v^j \bmod r$. By omitting s^{e-1} for the same reason we arrive at the pairing of the assertion. □

Since the automorphism group of an ordinary elliptic curve can only be cyclic of order 2, 4 or 6 there are only few cases in which Theorem 7 can be applied.

6 Extended Pairing Functions of Lowest Degree

Using the extended ate pairing we obtain an extended version of Theorem 1.

Theorem 14 *Let $n = \operatorname{lcm}(k, \#\mathrm{Aut}(E))$. Then the n-th roots of unity modulo r are defined in integers. Let s be any n-th root of unity modulo r. Write $s = uq^d \bmod r$ with u an $\#\mathrm{Aut}(E)$-th root of unity modulo r and let e be the order of u modulo r. Define $v = u^{-1} \bmod r$. Let $\gamma \in \mathrm{Aut}(E)$ of order e such that $(\gamma\pi^d)(Q) = sQ$.*

Then there is $h \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod r$, $\deg(h) \leq \varphi(n) - 1$ and $\|h\|_1 = O(r^{1/\varphi(n)})$ such that

$$a_{s,h} : G_2 \times G_1 \to \mu_r, \quad (Q,P) \mapsto \left(\prod_{j=0}^{e-1} f_{s,h,Q}(\gamma^{-j}(P))^{v^j} \right)^{(q^k-1)/r}$$

is a non-degenerate bilinear pairing. The polynomial h can be efficiently computed. The relation with the Tate pairing is

$$a_{s,h}(Q,P) = t(Q,P)^{h(s)/r}.$$

Any $h \in \mathbb{Z}[x]$ with $\deg(h) \leq n-1$ such that $a_{s,h}$ is a bilinear non-degenerate pairing satisfies $\|h\|_1 \geq r^{1/\varphi(n)}$.

The O-constant depends only on n.

Proof. Using Corollary 13, the proof is essentially that of Theorem 1. The only point to note is that if $a_{s,h} \in W_{\text{bilin}}$, then also $a_{s,xh} \in W_{\text{bilin}}$. This is clear since $T \mapsto sT$ is an automorphism of G_2. Then there is in fact a t of order n modulo r such that $a_{s,xh} = a_{s,h}^t$, but this is not needed for the proof. The rest of the proof of Theorem 1 applies as is and can be left to the reader.

Note that Corollary 13 and Theorem 14 can also be formulated for the extended twisted ate pairing from Theorem 7. Since the automorphism group of ordinary elliptic curves is rather small the best improvement we can get is $\phi(n) = 2\phi(k)$. This happens precisely when

1. k is odd and $\#\mathrm{Aut}(E) = 4$ (equivalently $D = -1$)
2. k is not divisible by 3 and $\#\mathrm{Aut}(E) = 6$ (equivalently $D = -3$).

In all other cases, $\phi(n) = \phi(k)$.

It is interesting to look for further extensions. The key point with the ate pairing reduction is equation (11). But every purely inseparable function of degree q^i is of the form $\gamma\pi^i$ with $\gamma \in \mathrm{Aut}(E)$. Thus we cannot do better than Theorem 14.

On the other hand, we could choose to not use (11). Based on solely (10) it is indeed possible to define non-degenerate bilinear pairing of the following form.

Theorem 15 *Let n be any divisor of $r-1$ and s an integer of order n modulo r such that $s^n \not\equiv 1 \bmod r^2$. Then there is $h \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod r$, $\deg(h) \leq \varphi(n) - 1$ and $\|h\|_1 = O(r^{1/\varphi(n)})$ such that*

$$a_{s,h} : G_2 \times G_1 \to \mu_r, \quad (Q, P) \mapsto \left(\prod_{j=0}^{n-1} f_{s,h,s^jQ}(P)^{s^{n-1-j}} \right)^{(q^k-1)/r}$$

is a non-degenerate bilinear pairing. The polynomial h can be efficiently computed. The relation with the Tate pairing is

$$a_{s,h}(Q, P) = t(Q, P)^{h(s)/r}.$$

Any $h \in \mathbb{Z}[x]$ with $\deg(h) \leq n-1$ such that $a_{s,h}$ is a bilinear non-degenerate pairing satisfies $\|h\|_1 \geq r^{1/\varphi(n)}$.

The O-constant depends only on n.

Proof. Using equation (10) and the argument in the proof of Corollary 13, the proof is the same as that of Theorem 1 and can be left to the reader.

Note that the product in the definition of $a_{s,h}$ runs over n function evaluations, as opposed to e function evaluations in Theorem 14. This is precisely the effect of the missing ate pairing reduction. While the product over n function evaluations is a big disadvantage it might be outweighed by using h with very small norm and efficient endomorphisms α such that $\alpha(Q) = sQ$. An example for a similar construction, which does give a fast pairing, are the NSS curves from [6]. See also [7], where these pairings are called superoptimal pairings.

Of course it would be nice to have $n > k$ and still use a pairing as in Theorem 1, that is only one function evaluation instead of more function evaluations. We have tried some examples of elliptic curves and n with $k \mid n$ and determined all functions in $\mathbb{F}_{q^k}(E)$ supported in $Z_s = \{s^i Q \mid 0 \leq i \leq n-1\}$ that would define a bilinear (non-degenerate) pairing. Except for the already known functions supported on $Z = \{q^i Q \mid 0 \leq i \leq k-1\}$ we did not find any new functions. This suggests that at least generically all functions defining pairings are in fact of the form like in Theorem 1.

7 Parametric Families

For parametric families of pairing friendly elliptic curves we get the following theorem.

Theorem 16 *Assume that q, s, r are given as polynomials in $\mathbb{Z}[t]$ such that for $t_0 \in \mathbb{Z}$ large enough there is an elliptic curve E over $\mathbb{F}_{q(t_0)}$ with parameters $n, r(t_0), s(t_0)$ as in Theorem 1 (here $n = k$), Theorem 14 or Theorem 15.*

Then there is $h \in \mathbb{Z}[t][x]$ with $\deg(h) \leq \varphi(n) - 1$ and $\deg_t(h) = 1/\varphi(n)\deg(r)$ such that

$$a_{s,h(t_0,x)} : G_2 \times G_1 \to \mu_r$$

from said theorem is a non-degenerate bilinear pairing for all t_0 sufficiently large. The polynomial h can be efficiently computed.

Any $h \in \mathbb{Z}[t][x]$ with $\deg(h) \leq n - 1$ such that $a_{s,h(t_0,x)}$ is non-degenerate for all t_0 sufficiently large satisfies $\deg_t(h) \geq 1/\varphi(n)\deg(r)$.

Proof. We define $A, I^{(1)}, I^{(2)}$ for $R = \mathbb{Z}[t]$ and r, s as at the beginning of section 4. From Lemma 6 we see that there are $\mathbb{Z}[t]$-linearly independent $v_i \in I^{(1)}$ with $\deg_t(v_i) = 0$ for the first and $\deg_t(v_i) = 1/\varphi(n)\deg(r)$ for the last elements. Looking at the determinant we see that there are only finitely many t_0 such that the specialised elements $v_i(t_0)$ will not be

$\mathbb{Z}$-linearly independent. Since t_0 is to be chosen sufficiently large we can assume that the $v_i(t_0)$ are $\mathbb{Z}$-linearly independent. Then $\|v_i(t_0)\|_1 = O(1)$ for the first and $\|v_i(t_0)\|_1 = \Theta(r(t_0)^{1/\varphi(n)})$ for the last elements, where the constants only depend on n.

We now use $A, I^{(1)}, I^{(2)}$ for $R = \mathbb{Z}$. From Lemma 2 we have $I^{(1),m} = M \oplus I^{(1),\varphi(n)}$ with $M = \{h \in I^{(1),m} \mid h \equiv 0 \bmod \Phi_n\}$ using polynomial division by Φ_n with remainder. Any vector having non zero projection onto $I^{(1),\varphi(n)}$ has norm in $\Omega(r(t_0)^{1/\varphi(n)})$ because of Lemma 3. Thus $v_i(t_0) \in M$ for the first elements. Since the $v_i(t_0)$ are linearly independent the last $v_i(t_0)$ must have non-zero projection onto $I^{(1),\varphi(n)}$. Lemma 3 together with $\|v_i(t_o)\|_1 = \Theta(r(t_0)^{1/\varphi(n)})$ implies $v_i(t_0) \notin I^{(2)}$. Thus the last $v_i(t_0)$ define a non-degenerqate bilinear pairing and we can choose h as one of the $v_i(t_0)$. Since the v_i are computed by means of the function field LLL, the polynomial h can be efficiently computed.

The last statement follows since $\|h(t_0, x)\|_1 \geq r(t_0)^{1/\varphi(n)}$ for t_0 tending to infinity. □

A consequence of the Theorem is that in parametric families $\deg(r)$ must be divisible by $\phi(n)$.

For examples of this construction we refer to [7].

References

1. P.S.L.M. Barreto, S. Galbraith, C. O'hEigeartaigh, and M. Scott, "Efficient pairing computation on supersingular abelian varieties," Designs, Codes and Cryptography, Vol. 42, No. 3, (2007) pp. 239–271.
2. F. Hess, N.P. Smart and F. Vercauteren. "The Eta Pairing Revisited", *IEEE Transaction on Information Theory*, Vol. 52, No. 10 (2006) pp. 4595–4602.
3. E. Lee, H.-S. Lee, C.-M. Park "Efficient and Generalized Pairing Computation on Abelian Varieties", *Cryptology ePrint Archive*, Report 2008/040, 2008. `http://eprint.iacr.org/2008/0040`
4. S. Matsuda, N. Kanayama, F. Hess, E. Okamoto. "Optimised Versions of the Ate and Twisted Ate Pairings" *Eleventh IMA International Conference on Cryptography and Coding*, Lecture Notes in Computer Science 4887, Springer-Verlag (2007) pp. 302–312.
5. S. Paulus. "Lattice basis reduction in function fields", *ANTS-III*, Lecture Notes in Computer Science 1423, Springer-Verlag (1998), pp. 567–575.
6. M. Scott. "Faster Pairings Using an Elliptic Curve with an Efficient Endomorphism", *INDOCRYPT 2005*, Lecture Notes in Computer Science 3797, Springer-Verlag (2005), pp. 258-269.
7. F. Vercauteren. "Optimal Pairings", *Cryptology ePrint Archive*, Report 2008/096, 2008. `http://eprint.iacr.org/2008/096`
8. C.-A. Zhao, F. Zhang and J. Huang. "A Note on the Ate Pairing", *Cryptology ePrint Archive*, Report 2007/247, 2007. `http://eprint.iacr.org/2007/247`