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 and also applies to the Weil pairing. We prove non-degeneracy and bounds on the lowest possible degree of these pairing functions and show how 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 us take a look at the problem of defining efficiently computable pairings on elliptic curves starting from a general point of view.

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 $r \mid (q-1)$. Let μ_r be the subgroup of r-th roots of unity of $\mathbb{F}_q^\times$. We are interested in bilinear pairings $e : G_1 \times G_2 \to \mu_r$. Such a pairing can in principle be defined 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 specific rational functions f_P and f_Q on E depending on P and Q instead of interpolation polynomials such that the pairing values are obtained by a function evaluation of the form

$$e(P, Q) = f_P(Q)^{(q-1)/r} \tag{1}$$

or

$$e(P, Q) = f_P(Q)/f_Q(P). \tag{2}$$

The functions f_P and f_Q are defined 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_P and f_Q, consisting of a short product of quotients of linear polynomials in x and y with large exponents, which enables the efficient evaluation of $f_P(Q)$ and $f_Q(P)$.

The Tate pairing is based on (1) and the Weil pairing is based on (2). The function $(P, Q) \mapsto f_P(Q)$ alone is in general not bilinear and does not take values in μ_r. The effect of raising $f_P(Q)$ to the power of $(q^k - 1)/r$ or of dividing $f_P(Q)$ by $f_Q(P)$ is to force the resulting functions to be bilinear and to take values in μ_r. We may refer to pairings of the form (1) as pairings defined by the Tate pairing methodology and to pairings of the form (2) as pairings defined by the Weil pairing methodology.

The Ate pairing of [2] and the pairings of [5, 10] are pairings defined by the Tate methodology whose pairing functions have reduced degree in comparison with the Tate pairing. Products of the Tate pairing and these pairings with the goal of a further degree reduction have been considered in [4]. This idea has been much extended in [9]. In the case of the Weil pairing methodology considerably less work has been done. In [11] the reduction idea of [2] is applied to the Weil pairing.

The objective of this paper is to present a unified and extended treatment of the idea to find new pairing functions of small degree by using products of existing pairing functions. We provide a convenient mathematical framework that allows to formulate a much clearer non-degeneracy condition and relation with the Tate pairing in comparison to [2, 5, 10, 4, 9]. We also show that our framework applies to the Weil pairing, based on an improvement and extension of [11], and prove (or give

heuristic arguments) for the optimality and exhaustiveness of our results for ordinary elliptic curves.

While we strive to find suitable pairing functions of smallest degree, the objective of the paper is not to give the most efficiently evaluated pairing functions. This is illustrated best with the following example. The polynomial $f(x) = (x-a)^n \in \mathbb{F}_q[t]$ can have very large degree but still has efficient representation and can be efficiently evaluated at elements of $\mathbb{F}_q$. On the other hand, $g(x) = \prod_{i=1}^{m}(x-a_i) \in \mathbb{F}_q[x]$ may have much smaller degree than f while the cost of representing and evaluating g can be much higher. On the other hand, if there are suitable relations between the a_i, the cost might also be smaller. In this paper we will go from pairing functions of a form analogous to f to pairing functions of a form analogous to g, but with rather small m. It is open whether our pairing functions will lead to more efficiently evaluated pairing functions. Some positive examples are given in [9]. Our intention is to provide a good overview over (all) possible pairing functions and we hope that this will prove useful for finding new efficiently evaluated pairing functions.

We give a brief guideline to the paper. The main results are Theorem 1, Theorem 2, Theorem 3 and Theorem 5. Theorem 1 is just a special, but arguably the most important case of Theorem 3. Theorem 3 is based on Theorem 2 , which provides a direct generalisation (and improvement) of [2, 5, 10, 11] that makes use of endomorphisms. Theorem 5 is an independent add on to the other theorems and shows how the pairings from these theorems can be used in parametric families of elliptic curves. The reader who wants to get a quick overview of the results of this paper is advised to read Section 2.1, Section 3 and Theorem 5, then continue with Theorem 3 and the rest of the paper.

2 Preliminaries

2.1 Notation

In this paper we will consider ordinary elliptic curves only, although the general logic behind the construction can be applied to supersingular curves and higher genus curves as well. 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 $r \geq 5$ be a prime factor of $\#E(\mathbb{F}_q)$ with embedding degree $k \geq 2$ such that $k \,|\, (r-1)$. 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 without further mentioning.

If $f \in E(\mathbb{F}_{q^k})^\times$ then the degree of f is defined as the sum of the positive coefficients of the divisor (f) of f, which is equal to sum of the negative coefficients.

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 $(f_{s,R}) = ((sR) - (\mathcal{O})) - s((R) - (\mathcal{O}))$ where (R) is the prime divisor corresponding to the point R (note that our definition is just the inverse of the standard definition $(f_{s,R}) = s((R)-(\mathcal{O}))-((sR)-(\mathcal{O}))$). Miller's algorithm expresses $f_{s,R}$ as a product of about $\log_2(|s|)$ quotients of monic linear functions with exponents of bitlength up to about $\log_2(|s|)$. 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, Ate and Weil 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 non-degenerate on $G_2 \times G_1$.

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 $r \nmid L$ (see [5]).

For $k \mid \#\mathrm{Aut}(E)$ the twisted ate pairing with respect to s is given by

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

The relation with the Tate pairing is $a_s^{\text{twist}}(P,Q) = t(P,Q)^L$. It is thus non-degenerate if and only if $r \nmid L$ (see [5]).

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

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

and the modified twisted ate pairing

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

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

The Weil pairing (see [6]) is

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

It is in fact defined on all $E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})[r]$ and is non-degenerate on $G_1 \times G_2$. Since r is an odd prime we always have $(-1)^r = -1$. For $k \mid \#\mathrm{Aut}(E)$ and $s \equiv q \bmod r$ the Weil pairing with ate reduction[1] with respect to s is given by

$$e_s : G_1 \times G_2 \to \mu_r, \quad (P,Q) \mapsto -w f_{s,P}(Q)/f_{s,Q}(P)$$

for some suitable k-th root of unity $w \in \mathbb{F}_q$. A variant of this pairing, but with final exponentiation, is considered in [11]. For our version see Theorem 2.

It is in general not true that the ate pairing, twisted ate pairing or Weil pairing with ate reduction can be extended to a bilinear pairing on the full r-torsion $E(\mathbb{F}_{q^k})[r]$. Moreover, the twisted ate pairing and the Weil pairing with ate reduction will in general not be bilinear for $k \nmid \#\mathrm{Aut}(E)$.

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

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

[1] Following the naming analogy of the Tate and ate pairing we might call this pairing also the eil pairing. Note that eil is the german word for hurry. For a suitable choice of s the eil pairing can indeed be computed faster than the Weil pairing.

Furthermore, define

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

A relation of $\|h\|_1$ with $\deg(f_{s,h,R})$ is given in Lemma 1 below.

Theorem 1 *Assume that s is a primitive k-th root of unity modulo r^2.*

Let $h \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod r$. Then

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

defines a bilinear pairing. If $k \,|\, \#\mathrm{Aut}(E)$ then

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

and

$$e_s : G_1 \times G_2 \to \mu_r,$$
$$(P, Q) \mapsto \left((-1)^{h(1)} f_{s,h,P}(Q)/f_{s,h,Q}(P)\right)^{\gcd(k,q-1)}$$

define bilinear pairings. The pairings $a_{s,h}$, $a_{s,h}^{\mathrm{twist}}$ and $e_{s,h}$ are non-degenerate if and only if $h(s) \not\equiv 0 \bmod r^2$ holds.

The relation with the Tate and Weil pairing is

$$a_{s,h}(Q, P) = t(Q, P)^{h(s)/r}, \quad a_{s,h}^{\mathrm{twist}}(P, Q) = t(P, Q)^{h(s)/r},$$
$$e_{s,h}(P, Q) = e(P, Q)^{h(s)/r}.$$

There exists an efficiently computable $h \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod r$, $\deg(h) \leq \varphi(k) - 1$ and $\|h\|_1 = O(r^{1/\varphi(k)})$ such that the above pairings are non-degenerate. The O-constant depends only on k.

Any $h \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod r$ such that the above pairings are non-degenerate satisfies $\|h\|_1 \geq r^{1/\varphi(k)}$.

Proof. Theorem 1 is a special case of Theorem 3 with s a primitive k-th root of unity modulo r and $d \geq 0$ such that $s = q^d \bmod r$, thus $e = 1$. □

Some remarks on the theorem are in order.

Choice of s. Suppose that s is an integer with $s^k \equiv 1 \bmod r$. Since k is coprime to r we can find i such that $(s + ir)^k \equiv 1 \bmod r^2$. Replacing s by $s + ir$ we can thus assume that $s^k \equiv 1 \bmod r^2$ without loss of generality.

The pairings a_s, a_s^{twist} and e_s depend only on the value of s modulo r^2, as is directly seen from the relations with the Tate and Weil pairing. Since there are no further congruence conditions on s, the value of s can be freely changed modulo r^2 without affecting a_s, a_s^{twist} and e_s.

Computation of h. The polynomial h of Theorem 1 can be determined as follows. Let m be an integer with $\phi(n) \leq m \leq n$ and consider the $m \times m$ integer matrix

$$M = \begin{pmatrix} r & 0 & & \dots & & 0 \\ -s & 1 & 0 & & \dots & 0 \\ -s^2 & 0 & 1 & 0 & \dots & 0 \\ & & \vdots & & & \\ -s^{m-1} & 0 & & \dots & 0 & 1 \end{pmatrix}.$$

Suppose $m = \phi(n)$ and $w = (w_0, w_1, \dots, w_{m-1})$ is a shortest $\mathbb{Z}$-linear combination of the rows of M, then we can take $h = \sum_{i=0}^{m-1} w_i x^i$. An (approximation of) w can be computed using the first LLL reduced basis element obtained by the LLL algorithm when applied to the rows of M.

As a variation, it is also possible to choose m such that $\phi(n) < m \leq n$. We apply the LLL algorithm in the same manner and take w as the smallest LLL reduced basis element satisfying $\|w\|_1 \geq r^{1/\varphi(n)}$.

Exponent. The final exponent satisfies $\gcd(k, q-1) \in \{1, 2, 3, 4, 6\}$. If it is one or even (or q is even) then the term $(-1)^{h(1)}$ can of course be discarded.

Completeness. The construction of pairings of the form $a_{s,h}$ and $a_{s,h}^{\text{twist}}$ of Theorem 1 is complete in the following sense: Consider the case of a_s and let $f_Q \in E(\mathbb{F}_{q^k})^\times$ be any function supported on $Z = \{\pi^i(Q) \,|\, 0 \leq i \leq k-1\}$ such that $S \mapsto f_Q(S)^{(q^k-1)/r}$ defines a homomorphism $G_1 \to \mu_r$. Then there are $w, h_i \in \mathbb{Z}$ such that $(f_Q) = \sum_{i=0}^{k-1} h_i(\pi^i(Q)) - w(\mathcal{O})$. Then $\sum_{i=0}^{k-1} h_i q^i \equiv 0 \bmod r$ and $\sum_{i=0}^{k-1} h_i(\pi^i(T)) - w(\mathcal{O})$ is a principal divisor for every $T \in G_2$. Let $f_T \in \mathbb{F}_{q^k}(E)^\times$ be monic such that $(f_T) = \sum_{i=0}^{k-1} h_i(\pi^i(T)) - w(\mathcal{O})$ for every $T \in G_2$. Then $(T, S) \mapsto f_T(S)^{(q^k-1)/r}$ defines a bilinear pairing equal to $a_{s,h}$ for $h = \sum_{i=0}^{k-1} h_i x^i \in I^{(1)}$ by Theorem 1. Hence the homomorphism defined by f_Q is obtained by a pairing $a_{s,h}$ from Theorem 1 with fixed first argument Q.

The promised relation of $\|h\|_1$ with $\deg(f_{s,h,R})$ is given by the following lemma.

Lemma 1 *Assume that $s \not\equiv 0 \bmod r$, d is less than the order of s modulo r and $R \neq \mathcal{O}$. We then have*

$$\|h\|_1/2 \leq \deg(f_{s,h,R}) \leq \|h\|_1.$$

Proof. Let $(f_{s,h,R}) = \sum_{j=-1}^{n} \lambda_j(P_j)$ with pairwise distinct P_j and $P_{-1} = \mathcal{O}$. We have $\sum_j \lambda_j = 0$ and hence $\deg(f_{s,h,R}) = \sum_{\lambda_i>0} |\lambda_i| = \sum_{\lambda_i<0} |\lambda_i|$. We may thus assume $\lambda_{-1} \leq 0$. This implies $\sum_{\lambda_j>0} |\lambda_j| \leq \sum_{j\geq 0} |\lambda_j|$. If $j \geq 0$, every λ_j is a sum of some h_i and every h_i occurs in at most one of the λ_j, hence $\sum_{j\geq 0} |\lambda_j| \leq \sum_{i=0}^{d} |h_i| = \|h\|_1$, which proves the upper degree bound without using the assumption on s, d, R.

For the proof of the lower degree bound observe that $\deg(f_{s,h,R}) = \sum_j |\lambda_j|/2$ since $\sum_{\lambda_j>0} |\lambda_j| = \sum_{\lambda_j<0} |\lambda_j|$, again using $\sum_j \lambda_j = 0$. Also note that the assumption on s, d, R implies that the $s^i R$ are pairwise distinct for $0 \leq i \leq d$, hence we can assume $P_j = s^j R$, $\lambda_j = h_j$ for $0 \leq j \leq n$ and $n = d$. Then $\sum_j |\lambda_j|/2 \geq \sum_{j\geq 0} |\lambda_j|/2 = \|h\|_1/2$, which proves the lower degree bound. □

4 Extended Pairings

The next theorem extends the ate pairing, twisted ate pairing and Weil pairing with ate reduction 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. We let $v_r(m)$ denote the maximal exponent of r in m.

Theorem 2 *Let s be any primitive n-th root of unity modulo r with $n \,|\, \mathrm{lcm}(k, \#\mathrm{Aut}(E))$. Let $u = sq^{-d} \bmod r$ be some primitive e-th root of unity modulo r with $e \,|\, \gcd(n, \#\mathrm{Aut}(E))$ and $d \geq 0$. Define $v = s^{-1}q^d = u^{-1} \bmod r$. Let $\alpha \in \mathrm{Aut}(E)$ of order e with $\alpha(Q) = uQ$.*

Then

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

defines a bilinear pairing. If $n \,|\, \#\mathrm{Aut}(E)$ then

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

defines a bilinear pairing. The pairings a_s and a_s^{twist} are non-degenerate if and only if $s^n \not\equiv 1 \bmod r^2$ holds.

Suppose $n \,|\, \#\mathrm{Aut}(E)$ and let $\nu = \min(2, v_r(q^k - 1)) \geq 1$. With e, d as above let $v = s^{-1}q^d \bmod r^\nu$. Then there is an n-th root of unity $w \in \mathbb{F}_q$

such that

$$e_s : G_1 \times G_2 \to \mu_r,$$
$$(P, Q) \mapsto \prod_{j=0}^{e-1} \left(-w f_{s,P}(\alpha^j(Q))/f_{s,\alpha^j(Q)}(P)\right)^{v^j}$$

defines a bilinear pairing. The pairing e_s is non-degenerate if and only if $s^n \not\equiv 1 \bmod r^2$ holds.

We refer to these pairings as extended ate, extended twisted ate pairing and extended Weil pairing with ate reduction (or simply extended eil pairing).

Some remarks on the theorem are in order.

Special inputs. If $P = \mathcal{O}$ or $Q = \mathcal{O}$ then the pairing values are defined to be equal to 1.

Existence of primitive n-th roots modulo r. Let $m = \operatorname{lcm}(k, \#\mathrm{Aut}(E))$. The proof of Theorem 2 will show that $m \,|\, (r-1)$ and that $\mathbb{F}_r$ contains all m-th roots of unity.

Choice of d, e and s. An easy calculation with cyclic groups shows that it is always possible to choose $d \geq 0$ such that $u = sq^{-d} \bmod r$ has order e modulo r for some $e \,|\, \#\mathrm{Aut}(E)$. The value of s can be changed modulo r^2 without changing the pairings a_s, a_s^{twist} and e_s.

Possible cases. Since the automorphism group of an ordinary elliptic curve can only be cyclic of order 2, 4 or 6 there are only few new cases in which Theorem 2 can be applied. On the other hand, there is some freedom of choice regarding the parameters e, d. If $s = q$ then $e = d = 1$ is possible and we recover the non-extended versions of the pairings.

Point multiples. The proof of Theorem 2 will show the existence of $\alpha, \beta \in \mathrm{Aut}(E)$ such that $sQ = (\alpha\pi^d)(Q)$ and $sP = \beta(P)$ (the latter only if $n \,|\, \#\mathrm{Aut}(E)$).

Computation of w. There is only very few possibilties for $w \in \mu_n \cap \mathbb{F}_q$, and it is probably easiest to try these cases in turn and check for which choice of w the condition $e_s(2P, Q) = e_s(P, Q)^2$ holds.

Another approach is as follows. Let e_s^{raw} denote the function obtained from the definition of e_s using $w = -1$. Then there is a $\operatorname{lcm}(2, n)$-th root

of unity $w_s \in \mathbb{F}_q$ such that $e_s(S,T) = w_s e_s^{\mathrm{raw}}(S,T)$ for all $S \in G_1$ and $T \in G_2$. The element w_s can be computed from the failing bilinearity of e_s^{raw}: We have $w_s = e_s^{\mathrm{raw}}(2P,Q)/e_s^{\mathrm{raw}}(P,Q)^2$.

Proof (of Theorem 2). We first show the general reduction equation (6). Suppose that $T, S \in E(\mathbb{F}_{q^k})[r]$ and ψ is a purely inseparable $\mathbb{F}_q$-rational isogeny of degree q^d with $\psi(T) = sT$ and $\psi(S) = s^{-1}q^d S = vS$, where the order of s modulo r is equal to n and the order of $s^{-1}q^d$ modulo r is equal to e. We compute

$$f_{r,T}^{(s^n-1)/r} = f_{s^n-1,T} = f_{s^n,T}, \tag{3}$$

where the second equality holds because $s^n \equiv 1 \bmod r$. Lemma 2 of [1] yields

$$f_{s^n,T} = f_{s,T}^{s^{n-1}} f_{s,sT}^{s^{n-2}} \cdots f_{s,s^{n-1}T}. \tag{4}$$

Since ψ is purely inseparable of degree q^d and $\mathbb{F}_q$-rational, we obtain from Lemma 4 in [2]

$$f_{s,\psi^i(T)} \circ \psi^i = w_{s,\psi} f_{s,T}^{q^{id}} \tag{5}$$

for some n-th root of unity $w_{s,\psi} \in \mathbb{F}_q$ (recall that all functions are assumed to be monic). We have $\psi^i(T) = s^i T$ and $\psi^{ie}(S) = S$. Let $k' = n/e$. Combining this with (3), (4), (5) and a short calculation collecting functions that are evaluated at the same points gives

$$\begin{aligned} f_{r,T}(S)^{(s^n-1)/r} &= w \prod_{m=0}^{n-1} f_{s,T}(\psi^{-m}(S))^{s^{n-1-m}q^{dm}} \\ &= w \left(\prod_{j=0}^{e-1} f_{s,T}(\psi^{-j}(S))^{s^{e-1-j}q^{dj}} \right)^{\sum_{i=0}^{k'-1}(s^e)^{k'-1-i}(q^{ed})^i} \end{aligned} \tag{6}$$

for some n-th root of unity $w \in \mathbb{F}_q$. Thus raising $f_{r,T}(S)$ to the power $(s^n-1)/r$ yields a reduced expression. In the following we will choose T, S as Q, P or P, Q. The choice of ψ requires a closer look at the automorphism group of E and its operation on G_1 and G_2.

Automorphisms of additive cyclic groups operate by non-zero integer multiplication. We thus get isomorphisms $\mathrm{Aut}(G_1) \cong \mathrm{Aut}(G_2) \cong \mathbb{F}_r^\times$. Because 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 s can be written as $s \equiv uq^d \bmod r$ with u of order e modulo r and $e \,|\, \#\mathrm{Aut}(E)$.

In the ate pairing case, since $u^e \equiv 1 \bmod r$ and $e \,|\, \#\mathrm{Aut}(E)$, there is $\alpha \in \mathrm{Aut}(E)$ corresponding to the multiplication-by-u automorphism of G_2 such that $(\alpha\pi^d)(Q) = uq^dQ = sQ$. Define $T = Q$, $S = P$ and $\psi_\alpha = \alpha\pi^d$. Then $\psi_\alpha(P) = \alpha(P) = (s^{-1}q^d)P = vP$ and (6) holds with these definitions, giving

$$f_{r,Q}(P)^{(s^n-1)/r} = w \left(\prod_{j=0}^{e-1} f_{s,Q}(\alpha^{-j}(P))^{s^{e-1-j}q^{dj}} \right)^{\sum_{i=0}^{k'-1}(s^e)^{k'-1-i}(q^{ed})^i} \tag{7}$$

for some n-th root of unity $w \in \mathbb{F}_q$.

In the twisted ate pairing case, since $s^{\#\mathrm{Aut}(E)} \equiv 1 \bmod r$, there is $\beta \in \mathrm{Aut}(E)$ corresponding to the multiplication-by-s automorphism of G_2 such that $\beta(P) = sP$. Define $T = P$, $S = Q$ and $\psi_\beta = \beta\pi^d$. Then $\psi_\beta(Q) = (s^{-1}q^d)Q = vQ$ and (6) holds with these definitions. Note that $\alpha(Q) = uQ$ and $\psi_\beta(Q) = vQ = \alpha^{-1}(Q)$, so we obtain

$$f_{r,P}(Q)^{(s^n-1)/r} = w \left(\prod_{j=0}^{e-1} f_{s,P}(\alpha^{j}(Q))^{s^{e-1-j}q^{dj}} \right)^{\sum_{i=0}^{k'-1}(s^e)^{k'-1-i}(q^{ed})^i} \tag{8}$$

for some n-th root of unity $w \in \mathbb{F}_q$.

In order to conclude the proof for the ate and twisted ate pairing we raise (7) and (8) to the power $(q^k-1)/r$, observing $w^{(q^k-1)/r} = 1$. The left hand sides then become $t(Q,P)^{(s^n-1)/r}$ and $t(P,Q)^{(s^n-1)/r}$ respectively, so the right hand sides define bilinear pairings that are non-degenerate if and only if $s^n \not\equiv 1 \bmod r^2$. We then consider the exponents occuring in (7) and (8) modulo r. We have $s^e \equiv (uq^d)^e \equiv q^{ed} \bmod r$, so $c = \sum_{i=0}^{k'-1}(s^e)^{k'-1-i}(q^{ed})^i \equiv k'q^{ed(k'-1)} \not\equiv 0 \bmod r$. Hence the outer exponent c can be omitted without affecting bilinearity or non-degeneracy. Finally, $s^{e-1-j}q^{dj} = s^{e-1}(q^ds^{-1})^j \equiv s^{e-1}v^j \bmod r$. By omitting s^{e-1} for the same reason we arrive at the pairings of the assertion.

For the Weil pairing we apply both cases simultaneously. By means of the chinese remainder theorem we make some additional assumptions on s without changing $s \bmod r^2$. We assume $\nu = v_r(q^k-1)$, $s \equiv 0 \bmod (q^k-1)/r^\nu$ and that s is even. Also also assume that $u = sq^{-d} \bmod r^\nu$ and

$v = u^{-1} \bmod r^\nu$ for this new ν. These new assumptions will be removed at the end of the proof. Dividing (8) and (7) gives

$$\begin{aligned} e(P,Q)^{(s^n-1)/r} &= (-1)^{s^n-1} f_{r,P}(Q)^{(s^n-1)/r} / f_{r,Q}(P)^{(s^n-1)/r} \\ &= -w' \left(\prod_{j=0}^{e-1} \left(f_{s,P}(\alpha^j(Q)) / f_{s,Q}(\alpha^{-j}(P)) \right)^{s^{e-1-j} q^{dj}} \right)^c \\ &= -w'' \left(\prod_{j=0}^{e-1} \left(f_{s,P}(\alpha^j(Q)) / f_{s,\alpha^j(Q)}(P) \right)^{s^{e-1-j} q^{dj}} \right)^c \end{aligned} \tag{9}$$

with $c = \sum_{i=0}^{k'-1} (s^e)^{k'-1-i} (q^{ed})^i \not\equiv 0 \bmod r$ as above, where the last equation holds because α is an automorphism with $\alpha(\mathcal{O}) = \mathcal{O}$. The elements $w', w'' \in \mathbb{F}_q$ are again n-th roots of unity. Since $s \equiv 0 \bmod (q^k-1)/r^\nu$ we get $s \equiv 0 \bmod r'$ for all prime numbers $r' \neq r$ dividing $q^k - 1$. Then $c \equiv q^{ed(k'-1)} \not\equiv 0 \bmod r'$ and $\gcd(c, q^k-1) = 1$, so c can be omitted from the final exponentiation. Let $\bar{c}c \equiv 1 \bmod q^k - 1$. Since s is even we have that q is even or precisely one of the exponents $s^{e-1-j} q^{dj}$ is odd. Also $w^s = 1$ and $w^q = w$ for any n-th root of unity $w \in \mathbb{F}_q$. We can thus write

$$\begin{aligned} e_{s,r}(P,Q)^{\bar{c}(s^n-1)/r} &= -w \prod_{j=0}^{e-1} \left(f_{s,P}(\alpha^j(Q)) / f_{s,\alpha^j(Q)}(P) \right)^{s^{e-1-j} q^{dj}} \\ &= \prod_{j=0}^{e-1} \left(-w f_{s,P}(\alpha^j(Q)) / f_{s,\alpha^j(Q)}(P) \right)^{s^{e-1-j} q^{dj}} \end{aligned} \tag{10}$$

for some n-th root of unity $w \in \mathbb{F}_q$. We know that (10) defines an element in μ_r. Since $s \equiv 0 \bmod (q^k-1)/r^\nu$ the factors of the product in (10) are elements in μ_{r^ν} for $0 \leq j < e-1$. We obtain that the factor for $j = e-1$ is an element of μ_{r^ν} as well. Since its exponent $q^{(e-1)d}$ is coprime to r^ν and since $\alpha^j(Q)$ runs through all points of G_2 we get that

$$-w f_{s,P}(\alpha^j(Q)) / f_{s,\alpha^j(Q)}(P) \in \mu_{r^\nu} \tag{11}$$

for all $0 \leq j \leq e-1$. Now $s^{e-1-j} q^{dj} \equiv s^{e-1} v^j \bmod r^\nu$ by assumption. Let $\bar{s}s \equiv 0 \bmod r$. We replace the exponents $s^{e-1-j} q^{dj}$ by $s^{e-1} v^j$ and raise (10) to the power $\bar{s}^{e-1}$. This gives

$$e_{s,r}(P,Q)^{\bar{s}\bar{c}(s^n-1)/r} = \prod_{j=0}^{e-1} \left(-w f_{s,P}(\alpha^j(Q)) / f_{s,\alpha^j(Q)}(P) \right)^{v^j}, \tag{12}$$

and the left hand side of this equation shows that the right hand side defines a bilinear pairing that is non-degenerate if and only if the condition $s^n \not\equiv 1 \bmod r^2$ holds. Now

$$f_{r^2,P}(\alpha^j(Q))/f_{r^2,\alpha^j(Q)}(P) = e(P,\alpha^j(Q))^r = 1. \tag{13}$$

Multiplying the right hand side of (12) with the left hand side of (13) to the power λv^j for $0 \le j \le e-1$ gives

$$e_{s,r}(P,Q)^{\overline{s}\overline{c}(s^n-1)/r} = \prod_{j=0}^{e-1}\left(-w f_{s+\lambda r^2,P}(\alpha^j(Q))/f_{s+\lambda r^2,\alpha^j(Q)}(P)\right)^{v^j}. \tag{14}$$

This finally shows that the right hand side of (12) depends only on the value of s modulo r^2 and thus also only on the value of v modulo r^2. So we can replace the additional assumptions on ν, s, u, v made in the proof before (9) by $\nu = \min(2, v_r(q^k-1))$ and $v = s^{-1}q^d \bmod r^\nu$. This finishes the proof. □

5 Extended Pairing Functions of Lowest Degree

With the extended pairings we obtain an extended version of Theorem 1.

Theorem 3 *We use the notation and assumptions from the beginning of section 3 and from Theorem 2. We additionally assume* $s^n \equiv 1 \bmod r^2$.

Let $h \in \mathbb{Z}[x]$ *with* $h(s) \equiv 0 \bmod r$. *Then there is* $w \in \mathbb{F}_q \cap \mu_{\mathrm{lcm}(2,n)}$ *such that*

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

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

$$e_{s,h} : G_1 \times G_2 \to \mu_r,\ (P,Q) \mapsto w\prod_{j=0}^{e-1}\left(f_{s,h,P}(\alpha^j(Q))/f_{s,h,\alpha^j(Q)}(P)\right)^{v^j}$$

define bilinear pairings whenever the respective assumptions for a_s, a_s^{twist} *and* e_s *of Theorem 2 are met.*

Each pairing $a_{s,h}$, $a_{s,h}^{\text{twist}}$ and $e_{s,h}$ is non-degenerate if and only if $h(s) \not\equiv 0 \bmod r^2$. The relation with the Tate and Weil pairing is

$$a_{s,h}(Q,P) = t(Q,P)^{eh(s)/r}, \quad a_{s,h}^{\text{twist}}(P,Q) = t(P,Q)^{eh(s)/r},$$
$$e_{s,h}(P,Q) = e(P,Q)^{eh(s)/r}.$$

There exists an efficiently computable $h \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod r$, $\deg(h) \leq \varphi(n) - 1$ and $\|h\|_1 = O(r^{1/\varphi(n)})$ such that the above pairings are non-degenerate. The O-constant depends only on n.

Any $h \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod r$ such that the above pairings are non-degenerate satisfies $\|h\|_1 \geq r^{1/\varphi(n)}$.

Proof. The theorem is an instantiation of the generic Theorem 6 for the three different pairing functions. In the following proof we will thus use the notation from Theorem 6.

Let $h, g \in \mathbb{Z}[x]$ and $R \in E(\mathbb{F}_{q^k})[r]$. Since $f_{s,g(x)(x^n-1)+h(x),R} = f_{s,h(x),R}$ 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. Observing $h(s) \equiv 0 \bmod r$ it is then clear that we have three functions

$$a_s, a_s^{\text{twist}} : I^{(1)} \to W_1, \quad e_s : I^{(1)} \to W_n$$

where $h \in I^{(1)}$ is mapped to $a_{s,h}, a_{s,h}^{\text{twist}}$ and $e_{s,h}$ respectively. Note that for e_s we do not need to know w since $e_{s,h} \in W_n$. Theorem 1 follows directly from Theorem 6 if we prove the three properties of Theorem 6 for a_s, a_s^{twist} and e_s.

Property 1 is clear for a_s, a_s^{twist} and e_s, since

$$f_{s,h+g,R} = f_{s,h,R} f_{s,g,R}$$

for any $h, g \in I^{(1)}$ and $R \in E(\mathbb{F}_{q^k})[r]$.

To show property 2 observe that

$$f_{s,hx,R} = f_{s,h,sR}$$

for any $h \in I^{(1)}$ and $R \in E(\mathbb{F}_{q^k})[r]$. Let b denote a_s or a_s^{twist}. Let T, S be admissible input points of b_h and assume $b_h \in W_1^{\text{bilin}}$. Then

$$b_{hx}(T,S) = b_h(sT,S) = b_h(T,S)^s,$$

as was to be shown. The case of e_s is a little more complicated. Consider $\beta \in \text{Aut}(E)$ from the proof of Theorem 2 with $\beta(P) = sP$. Then

$\beta(\alpha^j(sQ)) = \alpha^j(Q)$ and $f_{s,h,\alpha^j(sQ)}(P) = w f_{s,h,\alpha^j(Q)}(sP)$ for some n-th root of unity $w \in \mathbb{F}_q$ independent of P and Q, where application of β to the left hand side of the equation yields the right hand side. Assuming $e_{s,h} \in W_n^{\text{bilin}}$ we get (working with some fixed class representatives for $e_{s,hx}$ and $e_{s,h}$)

$$\begin{aligned} e_{s,hx}(P,Q) &\sim \prod_{j=0}^{e-1} \left(f_{s,hx,P}(\alpha^j(Q))/f_{s,hx,\alpha^j(Q)}(P)\right)^{v^j} \\ &= \prod_{j=0}^{e-1} \left(f_{s,h,sP}(\alpha^j(Q))/f_{s,h,\alpha^j(sQ)}(P)\right)^{v^j} \\ &= \prod_{j=0}^{e-1} \left(w^{-1} f_{s,h,sP}(\alpha^j(Q))/f_{s,h,\alpha^j(Q)}(sP)\right)^{v^j} \\ &\sim e_{s,h}(sP,Q) \sim e_{s,h}(P,Q)^s \end{aligned}$$

where $\sim$ means equality up to multiplication by some fixed elements from $\mathbb{F}_q \cap \mu_{\text{lcm}(2,n)}$ that are indepenent of P and Q. We thus obtain $e_{s,hx} = e_{s,h}^s$ in W_n, as required.

Finally we prove property 3. Consider $\alpha \in \text{Aut}(E)$ from Theorem 2 with $\alpha(Q) = uQ$ and thus $\alpha^{-1}(P) = uP$. Then

$$\begin{aligned} a_{s,r}(Q,P) &= \left(\prod_{j=0}^{e-1} f_{s,r,Q}(\alpha^{-j}(P))^{v^j}\right)^{(q^k-1)/r} = \prod_{j=0}^{e-1} t(Q,\alpha^{-j}(P))^{v^j} \\ &= \prod_{j=0}^{e-1} t(Q,u^j(P))^{v^j} = t(Q,P)^e \end{aligned}$$

and similarly

$$\begin{aligned} a_{s,r}^{\text{twist}}(P,Q) &= \left(\prod_{j=0}^{e-1} f_{s,r,P}(\alpha^j(Q))^{v^j}\right)^{(q^k-1)/r} = \prod_{j=0}^{e-1} t(P,\alpha^j(Q))^{v^j} \\ &= \prod_{j=0}^{e-1} t(P,u^j(Q))^{v^j} = t(P,Q)^e. \end{aligned}$$

Furthermore,

$$e_{s,r}(P,Q) \sim \prod_{j=0}^{e-1} \left(f_{s,r,P}(\alpha^j(Q))/f_{s,r,\alpha^j(Q)}(P)\right)^{v^j}$$
$$= \prod_{j=0}^{e-1} e_s(P,\alpha^j(Q))^{v^j} = \prod_{j=0}^{e-1} e_s(P,u^j(Q))^{v^j} = e_s(P,Q)^e,$$

so that we have $e_{s,r} = e_s^e$ in W_n. The functions $a_{s,x-s}$, $a_{s,x-s}^{\text{twist}}$ and $e_{s,x-s}$ are equal to the respective pairings a_s, a_s^{twist} and e_s from Theorem 2. Because $s^n \equiv 1 \bmod r^2$ they are all degenerate. This concludes the proof of Theorem 3. □

We remark that the comments after Theorem 1 apply to Theorem 3 as well.

Since the automorphism group of ordinary elliptic curves is rather small the best improvement we can get in Theorem 3 is for $\varphi(n) = 2\varphi(k)$. This happens precisely when

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

where D denotes the discriminant of the endomorphism ring. In all other cases, $\varphi(n) = \varphi(k)$.

It is interesting to look for further extensions. The key point with the ate pairing reduction is equation (5). But every purely inseparable function of degree q^i is of the form $\gamma\pi^i$ with $\gamma \in \text{Aut}(E)$. Thus we cannot do better than Theorem 3.

On the other hand, we could choose to not use (5). Based on solely (4) it is indeed possible to define non-degenerate bilinear pairings. The following theorem states this for the ate pairing case, the twisted ate pairing and Weil pairing cases are left to the reader. We continue to use the notation from the beginning of section 3.

Theorem 4 *Let n be any divisor of $r-1$ and s a primitive n-th root of unity modulo r^2.*

Let $h \in \mathbb{Z}[x]$ with $h(s) \equiv 0 \bmod r$. Then

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

is a bilinear pairing that is non-degenerate if and only if $h(s) \not\equiv 0 \bmod r^2$. *The relation with the Tate pairing is*

$$a_{s,h}(Q,P) = t(Q,P)^{ns^{n-1}h(s)/r}.$$

There exists an efficiently computable $h \in \mathbb{Z}[x]$ *with* $h(s) \equiv 0 \bmod r$, $\deg(h) \leq \varphi(n)-1$ *and* $\|h\|_1 = O(r^{1/\varphi(n)})$ *such that* $a_{s,h}$ *is non-degenerate. The* O*-constant depends only on* n.

Any $h \in \mathbb{Z}[x]$ *with* $h(s) \equiv 0 \bmod r$ *such that* $a_{s,h}$ *is a non-degenerate bilinear pairing satisfies* $\|h\|_1 \geq r^{1/\varphi(n)}$.

Proof. Using equation (4) with $T = Q, S = P$ to the power of $(q^k-1)/r$ we find that $a_{s,x-s}$ defines a bilinear pairing that is degenerate. Also $a_{s,r} = t^{ns^{n-1}}$ is quite directly seen. From here 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 3. 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 γ such that $\gamma(Q) = sQ$. An example for a similar construction, which does give a fast pairing, are the NSS curves from [8]. See also [9], 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 with the computer and n with $k \,|\, n$ and determined all functions in $\mathbb{F}_{q^k}(E)$ supported in $Z_s = \{s^iQ \,|\, 0 \leq i \leq n-1\}$ that would define a bilinear (non-degenerate) pairing. Except for the already known functions supported on $Z = \{q^iQ \,|\, 0 \leq i \leq k-1\} \subseteq Z_s$ we did not find any new functions. This suggests that on G_1 and G_2, at least generically, all functions defining pairings are in fact of the form like in Theorem 1.

6 Parametric Families

For parametric families of pairing friendly elliptic curves we get the following theorem. We continue to use the notation from the beginning of section 3. A non-zero polynomial $f \in \mathbb{Z}[t]$ is called primitive if the greatest common divisor of its coefficients is equal to 1.

Theorem 5 *Assume that $n, k \geq 2$ are integers and q, s, r are non-constant polynomials in $\mathbb{Z}[t]$, such that s is a primitive n-th root of unity modulo r^2 and r is a primitive polynomial. Assume furthermore that for all $t_0 \in J$ with J a suitable unbounded subset of $\mathbb{Z}$ 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 $k = n$), Theorem 3 or Theorem 4.*

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

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

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

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

Proof. Follows immediately from Theorem 7.

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

The polynomial h can be computed in the same way as the polynomial h from Theorem 1, using the function field LLL (see e.g. [7] and the discussion before Lemma 6) instead of the standard LLL algorithm.

We refer to [9] for examples of this construction.

7 Generic Results

This last section of the paper contains some technical lemmas dealing with the ring A and its ideals $I^{(i)}$ that occured in the proofs of Theorems 1, 3, 4 and 5.

In the following we will work with $R = \mathbb{Z}$ and $R = \mathbb{Q}[t]$. It is hence convenient to deal with these cases simultaneously for a moment. The following notation and assumptions will however be in place for the rest of this section.

Let R be a (principal ideal) domain and let $r, s \in R$ such that $r \neq 0$ is not a unit and s has order $n \geq 2$ in $(R/rR)^\times$. In other words, s is a primitive n-th root of unity modulo r. Define the R-algebra and its ideals

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

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 $j \leq i$. Also $I^{(i),n} = I^{(i)}$.

7.1 Ideal Structure

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. *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 applied to the basis $r^i, x-s, x(x-s), \ldots, x^{m-2}(x-s)$ of $I^{(i),m}$.

The third assertion follows using polynomial division by Φ_n with remainder: The projection $I^{(i),m} \to I^{(i),\varphi(n)}$, $h \mapsto h \bmod \Phi_n$ is split by the inclusion $I^{(i),\varphi(n)} \to I^{(i),m}$. 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 $h \in I^{(i)}$.

7.2 Lattice Arguments for $R = \mathbb{Z}$

We keep the notation and assumptions from the beginning of Section 7 for $R = \mathbb{Z}$ and $r \geq 2$. For $h = \sum_{i=0}^{d} h_i x^i \in \mathbb{Z}[x]$ define

$$\|h\|_1 = \sum_{i=0}^{d} |h_i| \quad \text{and} \quad \|h\|_2 = \left(\sum_{i=0}^{d} |h_i|^2 \right)^{1/2}.$$

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 $i \geq 1$ satisfies $s^n \equiv 1 \bmod r^i$ 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-th 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 $h(\zeta) \in \mathfrak{a}\backslash\{0\}$ by assumption on h and therefore

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

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*

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

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 $M = \{h \in I^{(1),m} \,|\, h \equiv 0 \bmod \Phi_n\}$. Thus there are at least $\varphi(n)$ basis vectors v_i of $I^{(1),m}$ 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.

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, which is a contradiction. 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. In this case the element relations will hold. Note that, unconditionally, any (LLL-reduced) basis of $I^{(1),m}$ must contain at least one basis element that is not in $I^{(2)}$.

7.3 Lattice Arguments for $R = \mathbb{Q}[t]$

The results of this section are needed for the proof of Theorem 5. We keep the notation and assumptions from the beginning of Section 7 for $R = \mathbb{Q}[t]$ and $\deg(r) \ge 1$. 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 $\le n-1$ in x. This makes $I^{(i)}$ into a lattice[2] with respect to deg.

Lemma 5 *Suppose $i \ge 1$ satisfies $s^n \equiv 1 \bmod r^i\mathbb{Q}[t]$ 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 (i.e. without non-zero

[2] This means that $I^{(i)}$ is a free $\mathbb{Q}[t]$-module of finite rank such that subsets of bounded deg-value are finite dimensional $\mathbb{Q}$-vector spaces.

powers of t) complex conjugates $\zeta^{(j)}$ of ζ and thus satisfy $\deg(\zeta^{(j)}) = 0$. Hence $\deg(h(\zeta^{(j)})) \leq \deg_t(h)$ and

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

Combining the two inequalities proves the assertion. □

The following lemma uses the function field LLL (e.g. [7]). 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 basis $v_1, \ldots, v_m$ of $I^{(1),m}$ satisfies*

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

Proof. The assertion and proof are exactly analogous to Lemma 4 (using the analogy $\deg_t = \log(\|\cdot\|_2)$). □

7.4 Pairing Lattices

Let V_n be the multiplicative group

$$V_n = \{wf \mid w \in \mathbb{F}_q \cap \mu_{\mathrm{lcm}(2,n)} \text{ and } f : G_1 \times G_2 \to \mu_r\}$$

where G_1 and G_2 are cyclic groups of prime order r and $\gcd(n, r) = 1$. Let W_n denote the factor group of V_n obtained by factoring out the constant functions with values in $\mathbb{F}_q \cap \mu_{\mathrm{lcm}(2,n)}$. The elements of W_n are thus functions $G_1 \times G_2 \to \mu_r$ that are defined up to scalar multiples from $\mathbb{F}_q \cap \mu_{\mathrm{lcm}(2,n)}$. Let W_n^{bilin} denote the subgroup of W_n that is generated by bilinear functions.

We can finally wrap up and state our main generic theorems.

Theorem 6 *Assume that r is a prime number, that n is coprime to r and that s is a primitive n-th root of unity modulo r^2. Let*

$$a_s : I^{(1)} \to W_n, \quad h \mapsto a_{s,h}$$

be a map with the following properties:

1. $a_{s,g+h} = a_{s,g}a_{s,h}$ *for all* $g, h \in I^{(1)}$,
2. $a_{s,hx} = a_{s,h}^s$ *for all* $h \in I^{(1)}$ *with* $a_{s,h} \in W_n^{\mathrm{bilin}}$,
3. $a_{s,r} \in W_n^{\mathrm{bilin}} \backslash \{1\}$ *and* $a_{s,t-s} = 1$.

Then $\mathrm{im}(a_s) = W_n^{\mathrm{bilin}}$ *and* $\ker(a_s) = I^{(2)}$. *More precisely,*

$$a_{s,h} = a_{s,r}^{h(s)/r}$$

for all $h \in I^{(1)}$.

There exists an efficiently computable $h \in I^{(1),\varphi(n)}$ *with* $\|h\|_1 = O(r^{1/\varphi(n)})$ *and* $a_{s,h} \neq 1$. *The O-constant depends only on n.*

Any $h \in I^{(1)}$ *with* $a_{s,h} \neq 1$ *satisfies* $\|h\|_1 \geq r^{1/\varphi(n)}$.

Proof. From properties 1 and 2 we see

$$a_{s,hg} = a_{s,h}^{g(s)}$$

for all $h \in I^{(1)}$ with $a_{s,h} \in W_n^{\mathrm{bilin}}$ and $g \in A$. We have $I^{(1)} = rA + (x-s)A$ by Lemma 2, so every $h \in I^{(1)}$ is of the form $h = g_1 r + g_2(x-s)$ with $g_1, g_2 \in A$. Then, using property 3,

$$a_{s,h} = a_{s,g_1 r + g_2(x-s)} = a_{s,r}^{g_1(s)} a_{s,x-s}^{g_2(s)} = a_{s,r}^{g_1(s)} \in W_n^{\mathrm{bilin}} \tag{15}$$

and thus $\mathrm{im}(a_s) \subseteq W_n^{\mathrm{bilin}}$. Since $a_{s,r} \neq 1$ and r is prime, we have $\mathrm{im}(a_s) = W_n^{\mathrm{bilin}}$.

The properties of a_s shown so far can be conveniently summarised as follows. We make W_n^{bilin} into an A-module via $f^g = f^{g(s)}$ for $f \in W_n^{\mathrm{bilin}}$ and $g \in A$. Then a_s is an epimorphism of the A-modules $I^{(1)}$ and W_n^{bilin}.

The kernel of a_s is an A-submodule of $I^{(1)}$ and hence an ideal of A contained in $I^{(1)}$. Since a_s is surjective, the index satisfies

$$(I^{(1)} : \ker(a_s)) = \#W_n^{\mathrm{bilin}} = r.$$

But $r^2, x - s \in \ker(a_s)$ so $I^{(2)} = r^2 A + (x-s)A \subseteq \ker(a_s)$ by Lemma 2. Again by Lemma 2 we have $(I^{(1)} : I^{(2)}) = r$, so $\ker(a_s) = I^{(2)}$ follows.

Looking at (15) we see that $g_1(s) = h(s)/r \bmod r$ and thus

$$a_{s,h} = a_{s,r}^{h(s)/r},$$

which shows the relation of $a_{s,h}$ with the generator $a_{s,r}$ of W_n^{bilin}.

Using $\ker(a_s) = I^{(2)}$, the rest of the theorem follows directly from Lemma 4 with $m = \phi(n)$, the LLL algorithm and Lemma 3. □

The ideal $I^{(1)}$ together with the map $a_s : I^{(1)} \to W_n$ satisfying the properties stated in Theorem 6 is called a pairing lattice with pairing lattice function a_s.

Theorem 7 *Assume that $n \geq 2$ and r, s are non-constant polynomials in $\mathbb{Z}[t]$ such that s is a primitive n-th root of unity modulo r^2 and r is a primitive polynomial. Assume furthermore that there is a pairing lattice function*

$$a_{s(t_0)} : I^{(1)}_{r(t_0),s(t_0)} \to W^{\text{bilin}}_{n,r(t_0)}$$

for all $t_0 \in J$ with J a suitable unbounded subset of $\mathbb{Z}$.

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

$$a_{s(t_0),h(t_0,x)} \neq 1$$

for all sufficiently large $t_0 \in J$. The polynomial h can be efficiently computed.

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

Proof. There are only finitely many $t_0 \in J$ such that $s(t_0)$ has order less than n modulo r^2, because these t_0 must be zeros of $s^m - 1 \bmod r$ for $m < n$. Since t_0 is to be chosen large enough we may assume that $s(t_0)$ is a primitive n-th root of unity modulo r^2.

We define $A, I^{(1)}, I^{(2)}$ for r, s and $R = \mathbb{Q}[t]$ as at the beginning of section 7. From Lemma 6 with $m = \phi(n)$ and the function field LLL we see that there is $v_i \in \mathbb{Q}[t][x]$ with $v_i(s) \equiv 0 \bmod r\mathbb{Q}[t]$, $\deg(v_i) \leq \phi(n) - 1$ and $\deg_t(v_i) = 1/\varphi(n)\deg(r)$ for $1 \leq i \leq \phi(n)$. Let $h \in \mathbb{Z}[t][x]$ be the product of v_i with the least common multiple of all denominators of all $\mathbb{Q}$-coefficients of v_i. Then $h(s) \in \mathbb{Z}[t]$ and $h(s) \equiv 0 \bmod r\mathbb{Z}[t]$ by the lemma of Gauss [3, p. 181], since r was assumed to be primitive.

Substituting t_0 for t in this congruence we get $h(t_0, s(t_0)) \equiv 0 \bmod r(t_0)$. From $\deg_t(h) = 1/\varphi(n)\deg(r)$ we see $\|h(t_0, x)\|_1 = O(r(t_0)^{1/\varphi(n)})$. Lemma 3 implies $h(t_0, s(t_0)) \not\equiv 0 \bmod r(t_0)^2$. We conclude that $a_{s(t_0),h(t_0,x)}$ defines a non-degenerate pairing by Theorem 1.

The last statement on the degrees follows since $\|h(t_0, x)\|_1 \geq r(t_0)^{1/\varphi(n)}$ by Lemma 3 for t_0 tending to infinity. □

Acknowledgement

The author thanks Steven Galbraith for a careful reading of a prior version of the paper.

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. S. Lang "Algebra", GTM 211, Springer-Verlag (2002)
4. 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`
5. 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.
6. V. S. Miller. The Weil pairing, and its efficient calculation. *J. Cryptology*, 17(4):235–261, 2004.
7. S. Paulus. "Lattice basis reduction in function fields", *ANTS-III*, Lecture Notes in Computer Science 1423, Springer-Verlag (1998), pp. 567–575.
8. 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.
9. F. Vercauteren. "Optimal Pairings", *Cryptology ePrint Archive*, Report 2008/096, 2008. `http://eprint.iacr.org/2008/096`
10. 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`
11. C.-A. Zhao, F. Zhang. "Reducing the Complexity of the Weil Pairing Computation", *Cryptology ePrint Archive*, Report 2008/212, 2008. `http://eprint.iacr.org/2008/212`