Optimal Pairings

F. Vercauteren*

Department of Electrical Engineering, Katholieke Universiteit Leuven
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
frederik.vercauteren@esat.kuleuven.be

Abstract. In this paper we introduce the concept of an *optimal pairing*, which by definition can be computed using only $\log_2 r/\varphi(k)$ basic Miller iterations, with r the order of the groups involved and k the embedding degree. We describe an algorithm to construct optimal ate pairings on all parametrized families of pairing friendly elliptic curves. Finally, we conjecture that any non-degenerate pairing on an elliptic curve without efficiently computable endomorphisms different from powers of Frobenius requires at least $\log_2 r/\varphi(k)$ basic Miller iterations.

Keywords: Tate pairing, ate pairing, elliptic curves, finite fields.

1 Introduction

Ever since the inception of pairing based cryptography, there has been a huge interest in developing fast algorithms to compute bilinear pairings. A bilinear pairing (or simply pairing) is a map of the form

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$$

where $\mathbb{G}_1, \mathbb{G}_2$ are typically additive groups and $\mathbb{G}_T$ is a multiplicative group. Bilinearity means that the map is linear in each component. We only consider pairings between groups of large prime order r, which are non-degenerate, i.e. for which there exists $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$ such that $e(P, Q) \neq 1$. Note that due to bilinearity, there is essentially only one pairing. Indeed, every pairing is completely determined by its value on one set of generators of $\mathbb{G}_1, \mathbb{G}_2$: let $\mathbb{G}_1 = \langle P \rangle$, $\mathbb{G}_2 = \langle Q \rangle$ and $z = e(P, Q)$, then by bilinearity $e(aP, bQ) = z^{ab}$. If a second pairing is specified by P', Q', z' and $P' = \alpha P$, $Q' = \beta Q$, then clearly $e' = e^{\alpha\beta}$.

All fast algorithms are based on Miller's algorithm [19, 20] to compute the Weil and Tate pairings on (hyper)elliptic curves. Since then a large number of papers [3, 12, 6, 22, 23, 2, 15, 14, 18, 24, 17, 25] have incrementally improved efficiency, interspersed with the occasional jumps caused by fundamentally new approaches. One line of research is focused on shortening the loop in Miller's algorithm, which was initiated by Duursma-Lee [6] and extended by Barreto et

* Postdoctoral Fellow of the Research Foundation - Flanders (FWO)

al. [2] to supersingular abelian varieties using the η_T approach. The ate pairing introduced in [15] for elliptic curves and in [14] for hyperelliptic curves generalises this to all ordinary curves. More recently, several variants of the ate pairing were introduced thereby further reducing the loop length in Miller's algorithm, such as the optimized ate pairing [18], the ate$_i$ pairings [24] and finally the R-ate pairing [17].

So far, all variants of the ate pairing have a Miller loop of length at least $\log_2 r/\varphi(k)$, with k the embedding degree. In this paper, we introduce the notion of optimal pairings, which by definition attain this lower bound. Furthermore, we describe an algorithm to automatically construct optimal ate pairings on parametrized families of pairing friendly elliptic curves. This algorithm also explains why the bound $\log_2 r/\varphi(k)$ is a natural lower bound and we conjecture that any non-degenerate pairing on an elliptic curve without extra efficiently computable endomorphisms different from Frobenius requires at least $\log_2 r/\varphi(k)$ basic Miller operations, thereby justifying the term "optimal pairing". Since pairings on elliptic curves seem more useful than pairings on hyperelliptic curves [13], we limit the exposition to elliptic curves. It should be clear however that all results in this paper easily generalise to Jacobians of curves.

The remainder of this paper is organised as follows: Section 2 recalls the necessary background on pairings, including all variants of the ate pairing. Section 3 formally defines the notion of optimal pairing and describes an algorithm to automatically construct such pairings for families of pairing friendly elliptic curves. Section 4 applies the algorithm to an extensive list of families of pairing friendly curves and exhibits in each case an optimal ate pairing. Finally, Section 5 concludes the paper.

2 Background on Pairings

In this section, we briefly recall the definition of the Tate pairing, all variants of the ate pairing and Miller's algorithm to compute them. The necessary mathematical background can be found in [1] and an excellent overview on pairings is [11].

2.1 Tate Pairing

Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements where p is prime and let E be an elliptic curve defined over $\mathbb{F}_q$. The point at infinity is denoted by $\mathcal{O}$. Consider a large prime r such that $r \mid \#E(\mathbb{F}_q)$ and denote the embedding degree by k, i.e. the smallest positive integer such that r divides $q^k - 1$. Note that this implies that $r \mid \Phi_k(q)$ with $\Phi_k(x) \in \mathbb{Z}[x]$ the k-th cyclotomic polynomial. Throughout we will assume that $r^2 \nmid (q^k - 1)$. The embedding degree k is chosen in this way so as to ensure that both eigenspaces of Frobenius are $\mathbb{F}_{q^k}$-rational. When $k > 1$, this implies that the full r-torsion $E[r]$ of the elliptic curve is defined over the field $\mathbb{F}_{q^k}$, i.e. $E[r] \subset E(\mathbb{F}_{q^k})$.

For every $P \in E(\mathbb{F}_{q^k})$ and integer s, let $f_{s,P}$ be an $\mathbb{F}_{q^k}$-rational function with divisor

$$(f_{s,P}) = s(P) - ([s]P) - (s-1)\mathcal{O}\,.$$

Such function $f_{s,P}$ is called a Miller function and is determined uniquely up to multiplication by non-zero elements of $\mathbb{F}_{q^k}$.

Let $P \in E(\mathbb{F}_{q^k})[r]$ and $Q \in E(\mathbb{F}_{q^k})$, and consider the divisor $D = (Q+R) - (R)$ with R a random point in $E(\mathbb{F}_{q^k})$ such that D is coprime with $(P) - (\mathcal{O})$. Then the Tate pairing [9] is a well-defined, non-degenerate, bilinear pairing

$$\langle \cdot, \cdot \rangle_r : \begin{cases} E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to & \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r \\ (P,Q) & \mapsto \langle P, Q\rangle_r = f_{r,P}(D). \end{cases} \tag{1}$$

The output of this pairing is only defined up to a coset of $(\mathbb{F}_{q^k}^*)^r$, however for protocols we will require a unique element of $\mathbb{F}_{q^k}^*$. Hence to obtain a unique representative, one defines the reduced Tate pairing as

$$t(P,Q) = \langle P, Q\rangle_r^{(q^k-1)/r} = f_{r,P}(D)^{(q^k-1)/r} \in \mathbb{G}_T\,. \tag{2}$$

If the function $f_{r,P}$ in the definition is normalised, i.e. $(u_{\mathcal{O}}^r f_{r,P})(\mathcal{O}) = 1$ for some $\mathbb{F}_q$-rational uniformizer $u_{\mathcal{O}}$ at $\mathcal{O}$, then one can ignore working with the divisor D and simply work with the point Q, i.e. the reduced Tate pairing is

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

Remark 1. In the remainder of the paper we will assume that all Miller functions are normalised.

2.2 Ate Pairing

The ate pairing [15, 14] and its variations [18, 24, 17] are simply optimized versions of the Tate pairing when restricted to the eigenspaces of Frobenius. Denote with π_q the Frobenius endomorphism, i.e. $\pi_q : E \to E : (x,y) \mapsto (x^q, y^q)$ and define $\mathbb{G}_1 = E[r] \cap \mathrm{Ker}(\pi_q - [1]) = E(\mathbb{F}_q)[r]$ and $\mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\pi_q - [q])$.

A somewhat non-standard way to derive the ate pairing is the following: consider a fixed power $m \in \mathbb{Z}$ of the Tate pairing on $\mathbb{G}_2 \times \mathbb{G}_1$ (so with the arguments swapped)

$$t(Q,P)^m = f_{r,Q}(P)^{m(q^k-1)/r} = f_{mr,Q}(P)^{(q^k-1)/r}\,, \tag{3}$$

where the last step follows from $f_{mr,Q} = f_{r,Q}^m \cdot f_{m,[r]Q}$ and $rQ = \mathcal{O}$. In fact, it is easy to see that this holds in general, i.e. for all $a, b \in \mathbb{Z}$ we can take

$$f_{ab,Q} = f_{a,Q}^b \cdot f_{b,[a]Q}\,. \tag{4}$$

Since the Tate pairing is non-degenerate, the right hand side of (3) also defines a non-degenerate pairing for any $m \in \mathbb{Z}$ with $r \nmid m$. The main idea is then to find a nice multiple of r such that the evaluation $f_{mr,Q}(P)$ can be written as a power of the evaluation of a simpler function $f_{\lambda,Q}(P)$. This can be achieved by exploiting the fact that q-th powering corresponds to multiplication by q on $\mathbb{G}_2$ and leaves $\mathbb{G}_1$ invariant. Finally, multiplication by q on $\mathbb{G}_2$ is the same as multiplication by any λ such that $\lambda \equiv q \bmod r$.

Therefore, fix any λ such that $\lambda \equiv q \bmod r$ and note that $r|(\lambda^k - 1)$, since $r|(q^k - 1)$. Define $m = (\lambda^k - 1)/r$, then by the above derivation we have

$$t(Q,P)^m = f_{mr,Q}(P)^{(q^k-1)/r} = f_{\lambda^k-1,Q}(P)^{(q^k-1)/r} = f_{\lambda^k,Q}(P)^{(q^k-1)/r} .$$

Repeated application of (4) and using $[\lambda^i]Q = [q^i]Q$ gives

$$f_{\lambda^k,Q} = f_{\lambda,Q}^{\lambda^{k-1}} f_{\lambda,[q]Q}^{\lambda^{k-2}} \cdots f_{\lambda,[q^{k-1}]Q} .$$

Finally, by exploiting the action of q-th powering on both $\mathbb{G}_1$ and $\mathbb{G}_2$ we obtain

$$f_{\lambda^k,Q}(P) = f_{\lambda,Q}(P)^{\sum_{i=0}^{k-1} \lambda^{k-1-i} q^i} .$$

In conclusion: let $\lambda \equiv q \bmod r$ and $m = (\lambda^k - 1)/r$, then the (reduced) ate pairing a_λ

$$a_\lambda : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r : (Q,P) \mapsto f_{\lambda,Q}(P)^{(q^k-1)/r} ,$$

defines a bilinear pairing which is non-degenerate for $r \nmid m$. Note that the action of a_λ simply corresponds to a fixed power of the reduced Tate pairing.

A similar derivation also shows that when $k \mid \#\mathrm{Aut}(E)$ the twisted ate pairing a_λ^t

$$a_\lambda^t : \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r : (P,Q) \mapsto f_{\lambda,P}(Q)^{(q^k-1)/r} ,$$

defines a bilinear pairing that is non-degenerate for $r \nmid m$.

By choosing different multiples of r, other variants [18, 24] can be obtained such as setting $\lambda \equiv q^i \bmod r$ for any $i \in \mathbb{Z}$, since then $r \mid (\lambda^i)^{k/\gcd(i,k)} - 1$. Furthermore, by multiplying or dividing several variants of the ate pairing, one obtains new pairings as shown in [17] and [25]. All of these variants have a common goal, namely to make the constant λ as small as possible since this determines the length of the loop in Miller's algorithm.

The main idea in Section 3 will be to consider other multiples of r, in particular where the base-q expansion of mr has very small digits.

2.3 Miller's Algorithm

To compute the function $f_{s,P}$ for $s > 0$, one can use Miller's algorithm [19, 20], which is a double-and-add approach based on the following observation

$$f_{m+n,P} = f_{m,P} \cdot f_{n,P} \cdot \frac{l_{[m]P,[n]P}}{v_{[m+n]P}} ,$$

where $l_{[m]P,[n]P}$ is the equation of the line through $[m]P$ and $[n]P$ (or the tangent line when $[m]P = [n]P$) and $v_{[m+n]P}$ the equation of the vertical line trough $[m+n]P$.

Algorithm 1 Miller's algorithm for elliptic curves

Inputs: $s \in \mathbb{N}$ and $P, Q \in E[r]$ with $P \neq Q$
Outputs: $f_{s,P}(Q)$
  Write $s = \sum_{j=0}^{L} s_j 2^j$, with $s_j \in \{0,1\}$ and $s_L = 1$.
  $T \leftarrow P$, $f \leftarrow 1$.
  for $j = L - 1$ down to 0 **do**
    $f \leftarrow c^2 \cdot l_{T,T}(Q)/v_{[2]T}(Q)$.
    $T \leftarrow [2]T$
    if $s_j = 1$ **then**
      $f \leftarrow f \cdot l_{T,P}(Q)/v_{T \oplus P}(Q)$.
      $T \leftarrow T \oplus P$
    end if
  end for
  Return f.

For $s < 0$ it suffices to remark that $(f_{s,P}) = -(f_{-s,P}) - (v_{[s]P})$ with $v_{[s]P}$ the vertical line through $[s]P$, so we can take $f_{s,P} = 1/(f_{-s,P} v_{[s]P})$.

One execution of the main loop in Algorithm 1 will be called a *basic Miller iteration*, during which one doubling and at most one addition (and corresponding evaluation of the functions) is computed.

3 Optimal Pairings

3.1 Definition

It is not difficult to see that for the ate pairings with Miller function $f_{\lambda_i,Q}$ where $\lambda_i \equiv q^i \bmod r$, we have

$$r \mid \Phi_{k/d}(\lambda_i) \qquad \text{where } d = \gcd(i,k)\,,$$

which implies that the minimal value for λ_i is roughly $r^{1/\varphi(k/d)}$. For $\gcd(i,k) = 1$ we therefore obtain the smallest lower bound of roughly $r^{1/\varphi(k)}$. This bound is attained for several complete families of elliptic curves such as cyclotomic families [8]. Motivated by these bounds, we give the following definition.

Definition 1. *Let $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be a non-degenerate, bilinear pairing with $|\mathbb{G}_1| = |\mathbb{G}_2| = |\mathbb{G}_T| = r$, where the field of definition of $\mathbb{G}_T$ is $\mathbb{F}_{q^k}$, then $e(\cdot,\cdot)$ is called an* optimal pairing *if it can be computed in $\log_2 r/\varphi(k) + \varepsilon(k)$ basic Miller iterations, with $\varepsilon(k) \leq \log_2 k$.*

Note that the above definition does not specify that the pairing e should be computed as the evaluation of *one* Miller function $f_{\lambda,Q}$ as is the case for the ate pairings, but also allows for products of $f_{\lambda_i,Q}$ or other combinations as long as *all* $f_{\lambda_i,Q}$ can be computed in $\log_2 r/\varphi(k) + \varepsilon(k)$ basic Miller iterations.

As will be shown in the next section, the bound $\log_2 r/\varphi(k)$ is a natural one. The central idea for loop reduction in Miller's algorithm it to exploit efficiently computable endomorphisms, such as powers of the Frobenius endomorphism π_q^i for $i = 0, \ldots, k-1$ by decomposing a multiple of r as a sum of these endomorphisms. However, since $\Phi_k(q) \equiv 0 \bmod r$, higher powers of π_q^j for $j \geq \varphi(k)$ act on $\mathbb{G}_2$ as a linear combination with *small coefficients* of the $\varphi(k)$ endomorphisms π_q^i for $i = 0, \ldots, \varphi(k) - 1$. Therefore, only the latter ones should be considered as "independent", since the size of the coefficients of a linear combination of π_q^j for $j \geq \varphi(k)$ will only very slightly increase by reduction modulo Φ_k. Since this is essentially the best one can obtain for powers of Frobenius, we make the following conjecture, which also explains the terminology "optimal pairing".

Optimality Conjecture: any non-degenerate pairing on an elliptic curve without efficiently computable endomorphisms different from powers of Frobenius, requires at least $(1-\epsilon)\log_2 r/\varphi(k)$ basic Miller iterations for some $0 < \epsilon < 1/4$.

More generally, we can consider any set $\mathcal{E} \subset \mathrm{End}(E)$ of efficiently computable endomorphisms and remove those endomorphisms that satisfy linear dependencies with small coefficients when restricted to $\mathbb{G}_2$. The optimality conjecture can then be generalised by replacing $\varphi(k)$ with $\#\mathcal{E}$. Note that this is only useful when $\#\mathcal{E} > \varphi(k)$. In this case, the corresponding pairings are called *super-optimal*. An example of a super-optimal family of pairings will be given in Section 4.

3.2 More Ate Pairings

The basic idea to construct optimal ate pairings is to exploit equation (3) by finding a multiple $\lambda = mr$ that has base-q expansion $\lambda = \sum_{i=0}^{l} c_i q^i$ with small coefficients. Any such expansion gives rise to a bilinear pairing as shown in the following theorem.

Theorem 1. *Let $\lambda = mr$ with $r \nmid m$ and write $\lambda = \sum_{i=0}^{l} c_i q^i$ then*

$$a_{[c_0,\ldots,c_l]} : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r : (Q, P) \mapsto \left(\prod_{i=0}^{l} f_{c_i,Q}^{q^i}(P) \cdot \prod_{i=0}^{l-1} \frac{l_{[s_{i+1}]Q,[c_i q^i]Q}(P)}{v_{[s_i]Q}(P)} \right)^{(q^k-1)/r} \tag{5}$$

with $s_i = \sum_{j=i}^{l} c_j q^j$, defines a bilinear pairing. Furthermore, if

$$mkq^{k-1} \not\equiv ((q^k-1)/r) \cdot \sum_{i=0}^{l} i c_i q^{i-1} \bmod r\,,$$

then the pairing is non-degenerate.

Proof. Consider the m-th power of the reduced Tate pairing on $\mathbb{G}_2 \times \mathbb{G}_1$, then

$$t(Q,P)^m = f_{\lambda,Q}(P)^{(q^k-1)/r} = f_{\sum_{i=0}^{l} c_i q^i, Q}(P)^{(q^k-1)/r}\,.$$

The latter sum can be rewritten using the fact that

$$f_{c_i q^i, Q}(P) = f_{q^i,Q}^{c_i}(P) f_{c_i,[q^i]Q}(P) = f_{q^i,Q}^{c_i}(P) f_{c_i,Q}^{q^i}(P)$$

so we obtain

$$t(Q,P)^m = \left(\prod_{i=0}^{l} f_{q^i,Q}^{c_i}(P)\right)^{(q^k-1)/r} \cdot a_{[c_0,\ldots,c_l]}(Q,P)\,.$$

Note that the factor between brackets is a product of powers of ate pairings and thus bilinear, which shows that $a_{[c_0,\ldots,c_l]}$ is also bilinear. Furthermore, $a_{[c_0,\ldots,c_l]}$ will be non-degenerate unless $t(Q,P)^m$ equals the pairing between brackets. This can be computed explicitly by expressing both pairings as a power of the reduced ate pairing a_q. For the left hand side we obtain

$$t(Q,P)^m = a_q(Q,P)^{mkq^{k-1}((q^k-1)/r)^{-1} \bmod r}\,.$$

And for the pairing in between brackets

$$\left(\prod_{i=0}^{l} f_{q^i,Q}^{c_i}(P)\right)^{(q^k-1)/r} = a_q^{\sum_{i=0}^{l} ic_i q^{i-1}}\,.$$

In conclusion: if $mkq^{k-1} \not\equiv ((q^k-1)/r) \cdot \sum_{i=0}^{l} ic_i q^{i-1} \bmod r$, then is $a_{[c_0,\ldots,c_l]}$ non-degenerate. $\square$

Note that for k even, denominator elimination applies, so we can ignore all vertical lines $v_{[s_i]Q}(P)$. Furthermore, in the computation of the lines $l_{[s_{i+1}]Q,[c_i q^i]Q}$ one should replace all multipications by powers of q by Frobenius actions.

Since $r \mid \Phi_k(q)$, it would be tempting to take $\lambda = \Phi_k(q)$, for which the corresponding c_i will be extremely small and thus $a_{[c_0,\ldots,c_l]}$ extremely efficient. Unfortunately, this choice of λ will always result in a degenerate pairing, which can be seen as a corollary of the following trivial lemma.

Lemma 1. *For all $k \in \mathbb{N}_0$ we have*

$$kx^{k-1} \equiv \frac{(x^k-1)}{\Phi_k(x)} \cdot \Phi_k'(x) \bmod \Phi_k(x)\;.$$

Proof. Write $(x^k-1) = ((x^k-1)/\Phi_k(x)) \cdot \Phi_k(x)$ and take derivatives of both sides by applying the Leibniz' rule to the right hand side.

Corollary 1. *For $\lambda = \Phi_k(q) = \sum_{i=0}^{\varphi(k)} c_i q^i$, the pairing $a_{[c_0,\ldots,c_l]}$ is degenerate.*

Proof. Since $m = \Phi_k(q)/r$, we can rewrite the non-degeneracy condition in Theorem 1 as

$$mkq^{k-1} \not\equiv m(q^k-1)/\Phi_k(q)\Phi_k'(q) \bmod r\,,$$

which is false by the above lemma.

Note that any multiple of $\Phi_k(q)$ will also lead to a degenerate pairing.

3.3 An Algorithm for Optimal Ate Pairings

To avoid degenerate pairings and since modulo r the powers of q^i are related via $\Phi_k(q) \equiv 0 \bmod r$, which is a relation with *tiny* coefficients, it suffices to consider the powers q^i for $i = 0, \ldots, \varphi(k) - 1$ in Theorem 1.

It is clear that a necessary (but not sufficient) condition to obtain an optimal pairing is that the c_i in Theorem 1 should not be larger in absolute value than $r^{1/\varphi(k)}$. Such small c_i can be obtained in general by finding short vectors in the following $\varphi(k)$-dimensional lattice (spanned by the rows)

$$L := \begin{pmatrix} r & 0 & 0 & \cdots & 0 \\ -q & 1 & 0 & \cdots & 0 \\ -q^2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \\ -q^{\varphi(k)-1} & 0 & \ldots & 0 & 1 \end{pmatrix}.$$

The volume of L is easily seen to be r, so by Minkowski's theorem [21], there exists a short vector $V \in L$ with $\| V \|_\infty \leq r^{1/\varphi(k)}$, where $\| V \|_\infty = \max_i |v_i|$. This proves that the first condition can be satisfied for *all* pairing friendly elliptic curves. However, finding small c_i does not directly imply that the corresponding pairing $a_{[c_0,\ldots,c_l]}$ is optimal. This conclusion is only valid in a parallel computing model, but clearly not in a serial one.

The first approach to partially solve this problem is to look for short vectors with a minimal number of coordinates of size $r^{1/\varphi(k)}$. This can easily be achieved by listing all short vectors with norm smaller than $\delta\lambda_1(L)$ where $\lambda_1(L)$ is the length of the shortest vector in the lattice and δ a small integer. Note that this approach automatically finds the best linear combination by exhibiting the minimal number of "essential" c_i's.

If the above approach results in a vector with only one c_i of size $r^{1/\varphi(k)}$ we clearly obtain an optimal pairing. However, if there is more than one such c_i, it not clear how to compute the Miller functions using only $\log_2 r/\varphi(k)$ basic Miller iterations. If the c_i are completely independent, then the only optimisation possible would be to use some form of multi-exponentiation, and we would thus fail to attain the optimal number of basic Miller operations.

For pairing friendly elliptic curves in parametrized families however, the above approach can be executed on the polynomial representations of $r(x)$ and $q^i(x) \bmod r(x)$, thereby leading to short vectors where the $c_i(x)$ are automatically related since they are polynomial expressions in the same variable x. Exploiting this explicit relation often gives an optimal pairing, since all $f_{c_i(x),Q}$ in (5) will typically follow directly from $f_{x,Q}$.

The above reasoning shows that the bound $r^{1/\varphi(k)}$ can be achieved, but it provides no information on how good this bound is, i.e. how short the shortest vector is compared to Minkowski's bound. The following theorem resolves this problem.

Theorem 2. *The shortest vector V in L satisfies*

$$\|V\|_2 \geq \frac{r^{1/\varphi(k)}}{\|\Phi_k\|_2} \quad \textit{and} \quad \|V\|_\infty \geq \frac{r^{1/\varphi(k)}}{(\varphi(k)+1)\|\Phi_k\|_\infty} \,. \tag{6}$$

Proof. To obtain a lower bound on the length of the shortest vector, we consider the following equivalent problem. Let ξ_k denote a primitive k-th root of unity and consider the cyclotomic number field $\mathbb{Q}[\xi_k] \simeq \mathbb{Q}[x]/\Phi_k(x)$. For the prime r, we have $\Phi_k(q) \equiv 0 \bmod r$, so $\Phi_k(x)$ splits completely modulo r (since $\mathbb{Q}(\xi_k)$ is Galois). The ring of integers of $\mathbb{Q}[\xi_k]$ is $\mathbb{Z}[\xi_k]$ and the ideal $r\mathbb{Z}[\xi_k]$ factors as a product of $\varphi(k)$ different prime ideals $\mathfrak{p}_i = (r, \xi_k - s_i)$ with s_i the roots of $\Phi_k(x)$ modulo r. Consider the prime ideal $\mathfrak{p} = (r, \xi_k - q)$, then we have a one-to-one correspondence between vectors in L and elements in $\mathfrak{p}$ by

$$\Lambda : L \to \mathfrak{p} : V = [v_0, \ldots, v_{\varphi(k)-1}] \mapsto \sum_{i=0}^{\varphi(k)-1} v_i \xi_k^i \,.$$

Finding short vectors in L therefore corresponds to finding elements in $\mathfrak{p}$ of small norm. But the norm of elements in $\mathfrak{p}$ is always divisible by r (the norm of $\mathfrak{p}$) and thus we obtain

$$r \leq |\mathcal{N}(\sum_{i=0}^{\varphi(k)-1} v_i \xi_k^i)| = |\mathrm{Res}(V(x), \Phi_k(x))| \,.$$

By bounding the size of the resultant we finally obtain

$$r \leq \|V\|_2^{\varphi(k)} \|\Phi_k\|_2^{\varphi(k)-1} \leq (\varphi(k)+1)^{\varphi(k)} \|V\|_\infty^{\varphi(k)} \|\Phi_k\|_\infty^{\varphi(k)-1} \,,$$

which is precisely the bound given in (6). This shows that the shortest vector in the lattice can never be much shorter than Minkowski's bound. □

We can now combine Theorem 1 and 2 to provide further evidence for the optimality conjecture. Let $\lambda = mr$ with $r \nmid m$ and write $\lambda = \sum_{i=0}^{l} c_i q^i$ as in Theorem 1. Let $\lambda(x) = \sum_{i=0}^{l} c_i x^i$ and consider the division by $\Phi_k(x)$, i.e.

$$\lambda(x) = \alpha(x) \cdot \Phi_k(x) + \beta(x) \,,$$

with $\deg(\beta(x)) < \varphi(k)$. Since $r | \lambda$ and $r | \Phi_k(q)$, we conclude that $r | \beta(q)$ and thus that the coefficient vector of $\beta(x)$, denoted by β, is contained in L. There are now two possibilities for $\beta(x)$: either $\beta(x) = 0$ and we obtain a degenerate pairing as shown before, or $\beta(x) \neq 0$, but then $\|\beta\|_2 \geq r^{1/\varphi(k)}/\|\Phi_k\|_2$ since $\beta \in L$. However, this implies that not all original coefficients c_i can be very small either, since reduction modulo $\Phi_k(x)$ only causes a small increase in coefficient size. This shows once more that considering more general expressions $\lambda = \sum_{i=0}^{l} c_i q^i$ for $l \geq \varphi(k)$ will not lead to more efficient pairings than with the above algorithm.

4 Examples

In this section we apply the algorithm of the previous section to several polynomial families obtaining optimal ate pairings for all of them. An excellent overview of pairing friendly curves is given in [8].

BN-curves The family of BN-curves [4] has $k = 12$ and is given by the following parameterisations:

$$p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1 \qquad r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1\,.$$

The shortest vectors in the lattice L for the Euclidean norm are given by

$$V_1(x) = [x + 1, x, x, -2x] \qquad V_2(x) = [2x, x + 1, -x, x]\,.$$

Since there is such an easy relation between the $c_i(x)$, we already obtain an optimal pairing, since all $f_{c_i(x),Q}$ follow immediately from $f_{x,Q}$. Alternatively, we can look for short vectors with minimal number of coefficients of size x and obtain

$$W(x) = [6x + 2, 1, -1, 1]\,,$$

which gives another possibility for an optimal pairing. Since $f_{1,Q} = 1$ and $f_{-1,Q} = 1/f_{1,Q}v_Q$ (which disappears after final exponentiation), the pairing a_W can be computed as

$$a_W = \left(f_{6x+2,Q}(P) \cdot l_{Q_3,-Q_2}(P) \cdot l_{-Q_2+Q_3,Q_1}(P) \cdot l_{Q_1-Q_2+Q_3,[6x+2]Q}\right)^{(q^k-1)/r}\,,$$

where $Q_i = Q^{q^i}$ for $i = 1, 2, 3$.

Freeman curves The family of Freeman curves [7] has $k = 10$ and is given by the following parameterisations:

$$p(x) = 25x^4 + 25x^3 + 25x^2 + 10x + 3 \qquad r(x) = 25x^4 + 25x^3 + 15x^2 + 5x + 1\,.$$

The shortest vector in the lattice L for the Euclidean norm is given by

$$V = [x + 1, x, -x, -x]\,,$$

so again we obtain an optimal pairing since it suffices to compute $f_{x,Q}$. Listing all short vectors gives the following alternative: $W = [1, 1, -1, -5x - 1]$.

Supersingular elliptic curves with $\boldsymbol{k = 3}$ The following family represents supersingular curves with embedding degree $k = 3$ over $\mathbb{F}_q = \mathbb{F}_{p^2}$:

$$q(x) = (3x - 1)^2 \qquad r(x) = 9x^2 - 3x + 1\,.$$

The shortest vector is given by $V = [1, -3x + 1]$, which is already optimal. A slightly better choice is $W = [3x, 1]$.

Supersingular elliptic curves with $k = 6$ These curves are necessarily defined over $\mathbb{F}_{3^m}$ for some m and for odd m we have $t = \pm\sqrt{q}$. Popular values for m are $m = 97, 163, 193, 239, 353$. If $r = 3^x + 1 - 3^{(x+1)/2}$, then the shortest vector in L is given by $V = [3^{(x-1)/2}, 3^{(x-1)/2} - 1]$ and another nice choice is $W = [3^{(x+1)/2}, -1]$.

Cyclotomic family with $k = 10$ In [5], the authors describe the family parametrized by

$$p(x) = \frac{1}{4}(x^{12} - x^{10} + x^8 - 5x^6 + 5x^4 - 4x^2 + 4) \qquad r(x) = \Phi_{20}(x)\,,$$

which has embedding degree $k = 10$. Note that this is the first example where the degree of the polynomial $r(x)$ does not equal $\varphi(k)$, so we expect to find $c_i(x)$ of degree 2. The shortest vector in L is given by $V = [x^2 - 1, 1, -1, 1]$ and another nice short vector is given by $W = [1, -x^2, 0, 0]$.

Cyclotomic family with $k = 18$ In [16], the authors describe the family parametrized by

$$p(x) = \frac{1}{21}(x^8 + 5x^7 + 7x^6 + 37x^5 + 188x^4 + 259x^3 + 343x^2 + 1763x + 2401)$$

$$r(x) = \frac{1}{343}(x^6 + 37x^3 + 343)\,,$$

which for values $x \equiv 14 \bmod 42$ parametrises elliptic curves with embedding degree 18. The shortest vectors in the lattice L are given by three shifts of

$$V = [2z, 1, 0, z, 0, 0]$$

where $z = x/7$. Another nice short vector is given by $W = [1, 0, x, 2, 0, 0]$.

Scott's NSS curves This example illustrates a family of super-optimal curves, namely Scott's NSS curves [22]. These curves are defined over $\mathbb{F}_p$ with $p \equiv 1 \bmod 3$ and given by an equation of the form $y^2 = x^3 + B$. Since these curves have $k = 2$, we do not expect any speed-up by exploiting the Frobenius endomorphism alone. However, these curves admit an efficient endomorphism different from Frobenius given by $\phi : (x, y) \mapsto (\beta x, y)$, where β is a non-trivial cube root of unity. Furthermore, the action on r-torsion corresponds to multiplication by λ, where λ is a root of $\lambda^2 + \lambda + 1 \equiv 0 \bmod r$. Scott gives the example of $\lambda = 2^{87}$ and $r = (2^{174} + 2^{87} + 1)/73$. Note that multiplication by $73r$ corresponds to $\phi^2 + \phi + 1$ on $E[r]$, so we use a modification of the proof of Theorem 1. Consider the pairing

$$t(P, Q)^{73} = f_{73r,P}(Q)^E = f_{\lambda^2+\lambda+1,P}(Q)^E = f_{\lambda^2+\lambda,P}(Q)^E\,,$$

with $E = (p-1)(p+1)/r$. The latter function (without the final exponentiation) can be rewritten as

$$f_{\lambda(\lambda+1),P} = f_{\lambda,P}^{\lambda+1} \cdot f_{\lambda+1,[\lambda]P} = f_{\lambda,P}^{\lambda+1} \cdot f_{\lambda,[\lambda]P} \cdot l_{[\lambda]P,P}/v_{[\lambda+1]P} \,.$$

Since $[\lambda]P$ is given by $\phi(P) = (\beta x, y)$, we can simply compute $f_{\lambda,[\lambda]P}(Q)$ from $f_{\lambda,P}(Q)$ by replacing $x(P)$ by $\beta x(P)$. This shows that the Tate pairing on NSS curves can be computed using only $\lfloor \log_2 \lambda \rfloor$ basic Miller iterations and is therefore super-optimal. A similar derivation of Scott's results was described in [23].

Supersingular Genus 2 Curves with $k = 12$ To illustrate that the algorithm works equally well for hyperelliptic curves, we consider the family of curves introduced in [10]:

$$C_d : y^2 + y = x^5 + x^3 + d \qquad d \in \{0, 1\} \,,$$

over $\mathbb{F}_{2^m}$, with m coprime to 6. These curves are supersingular and have embedding degree $k = 12$. The order of the Jacobian J_C is given by the following table taken from [10].

$\#J_{C_d}(\mathbb{F}_{2^m})$	condition
$2^{2m} + (-1)^d 2^{(3m+1)/2} + 2^m + (-1)^d 2^{(m+1)/2} + 1$	$m \equiv 1, 7, 17, 23 \bmod 24$
$2^{2m} - (-1)^d 2^{(3m+1)/2} + 2^m - (-1)^d 2^{(m+1)/2} + 1$	$m \equiv 5, 11, 13, 19 \bmod 24$

For $m = 239$ and $m = 313$ we obtain a prime order Jacobian for $d = 1$. Since both cases correspond to the first line of the table, we assume that $r(m) = 2^{2m} - 2^{(3m+1)/2} + 2^m - 2^{(m+1)/2} + 1$. The shortest vector in the lattice L is given by

$$V = [2^{(m-1)/2}, -1, 0, -2^{(m-1)/2} + 1] \,.$$

However, a better short vector is given by

$$W = [2^{(m+1)/2}, -1, -1, 1] \,,$$

which clearly gives an optimal pairing.

5 Conclusion

In this paper we have introduced the concept of optimal pairings, which can be computed using $\log_2 r/\varphi(k)$ basic Miller iterations. We described a fully automatic procedure to construct optimal ate pairings on parametrized families of pairing friendly elliptic curves by exploiting the Frobenius endomorphism. In the presence of extra efficiently computable endomorphisms, super-optimal pairings are possible that require less than $\log_2 /\varphi(k)$ Miller iterations. Finally, we conjectured that any non-degenerate pairing requires at least $\log_2 r/\#\mathcal{E}$ basic Miller iterations with $\mathcal{E}$ a maximal set of independent efficiently computable endomorphisms.

Acknowledgements

The author wishes to thank Steven Galbraith and Mike Scott for providing useful suggestions and corrections.

References

1. R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of elliptic and hyperelliptic curve cryptography.* Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.
2. P.S.L.M. Barreto, S.D. Galbraith, C. Ó hÉigeartaigh, and M. Scott. Efficient pairing computation on supersingular abelian varieties. In *Designs, Codes and Cryptography*, vol 42(3), pages 239–271, 2007.
3. P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing-based cryptosystems. In *CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 354–368. Springer, 2002.
4. P.S.L.M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. In *SAC 2005 - Selected Areas in Cryptography*, volume 3897 of *Lecture Notes in Computer Science*, pages 319–331. Springer, 2006.
5. F. Brezing and A. Weng. Elliptic Curves Suitable for Pairing Based Cryptography. In *Designs, Codes and Cryptography*,vol 37(1), pages 133–141, 2005.
6. I.M. Duursma and H.-S. Lee. Tate Pairing Implementation for Hyperelliptic Curves $y^2 = x^p - x + d$. In *ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Computer Science*, pages 111–123. Springer, 2003.
7. D. Freeman. Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10. In *Algorithmic Number Theory Symposium ANTS-VII*, volume 4076 of *Lecture Notes in Computer Science*, pages 452–465. Springer-Verlag, 2006.
8. D. Freeman, M. Scott, and E. Teske. A taxonomy of pairing-friendly elliptic curves. Preprint 2006, Available from `http://eprint.iacr.org/2006/372`.
9. 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(206):865–874, 1994.
10. S.D. Galbraith. Supersingular curves in cryptography. In *ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 495–513. Springer-Verlag, 2002.
11. S.D. Galbraith. Pairings. *Advances in elliptic curve cryptography*, London Math. Soc. Lecture Note Ser. **317**, 183–213, Cambridge Univ. Press, 2005.
12. S.D. Galbraith, K. Harrison and S. Soldera. Implementing the Tate pairing. In *Algorithmic Number Theory Symposium – ANTS V*, volume 2369 of *Lecture Notes in Computer Science*, pages 324–337. Springer-Verlag, 2002.
13. S.D. Galbraith, F. Hess, and F. Vercauteren. Hyperelliptic pairings. In *Pairing 2007*, volume 2575 of *Lecture Notes in Computer Science*, pages 108–131. Springer-Verlag, 2007.
14. R. Granger, F. Hess, R. Oyono, N. Thériault and F. Vercauteren. Ate Pairing on Hyperelliptic Curves. In *EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Computer Science*, pages 430–447. Springer-Verlag, 2007.
15. F. Hess, N. Smart, and F. Vercauteren. The Eta-pairing revisited. *IEEE Transactions on Information Theory*, 52(10):4595–4602, 2006.

16. E.J. Kachisa, E.F. Schaefer and M. Scott. Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field. Preprint, 2007. Available from `http://eprint.iacr.org/2007/452`.
17. E. Lee, H.-S. Lee, and C.-M. Park. Efficient and Generalized Pairing Computation on Abelian Varieties. Preprint, 2008. Available from `http://eprint.iacr.org/2008/040`.
18. S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto. Optimised versions of the Ate and twisted Ate pairings. In *The 11th IMA International Conference on Cryptography and Coding*, volume 4887 of *Lecture Notes in Computer Science*, pages 302–312. Springer-Verlag, 2007.
19. V. S. Miller. Short programs for functions on curves. Unpublished manuscript 1986. Available at `http://crypto.stanford.edu/miller/miller.pdf`.
20. V. S. Miller. The Weil pairing, and its efficient calculation. *J. Cryptology*, 17(4):235–261, 2004.
21. H. Minkowski Geometrie der Zahlen. Leipzig und Berlin, Druck und Verlag von B.G. Teubner, 1910.
22. M. Scott. Faster Pairings Using an Elliptic Curve with an Efficient Endomorphism. In *INDOCRYPT 2005*, volume 3797 of *Lecture Notes in Computer Science*, pages. 258–269. Springer-Verlag, 2005.
23. C. Zhao, F. Zhang and J. Huang. Speeding up the Bilinear Pairings Computation on Curves with Automorphisms. Unpublished. 2006. Available from `http://eprint.iacr.org/2006/474`.
24. C. Zhao, F. Zhang and J. Huang. A Note on the Ate Pairing. Preprint, 2007. Available from `http://eprint.iacr.org/2007/247`.
25. C. Zhao, F. Zhang and J. Huang. All Pairings are in a Group. Preprint, 2008. Available from `http://eprint.iacr.org/2008/085`.