Edoardo Persichetti Lecture 8: Pairings 08/04/2014

Notes written by Grzegorz Milka

Pairings

A natural pairing in $\mathbb{R}^n$ is the inner product $\beta(u,v) = u \cdot v = \sum_{i=1}^{n} u_i v_i$.
Bilinearity means:

$$\begin{aligned} \beta(au+bv,w) &= a\beta(u,w) + b\beta(v,w) \\ \beta(u,av+bw) &= a\beta(u,v) + b\beta(u,w) \end{aligned}$$

In $\mathbb{R}^2$ if $u=(a,b), v=(c,d)$ then $\delta(u,v) = \det \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad-bc$ is a bilinear pairing.
An additional property of this pairing is called *alternating*:

$$\delta(v,u) = -\delta(u,v)$$

This implies that $\delta(u,u) = 0$ for every $u \in \mathbb{R}^2$.

Definition 1 (Divisor) A divisor is a formal sum that represents a compact notation for a certain number of elements, that is $D = \sum_j a_j (\alpha_j)$.

For example: $D = 2(1) + 3(-5)$ in $\mathbb{R}$.

Definition 2 (Principal Divisor) Let f be a rational function:

$$f(x) = \frac{a_0 + a_1 + \ldots + a_n x^n}{b_0 + b_1 + \ldots + b_m x^m} = \frac{(x-\alpha_1)^{e_1} \ldots (x-\alpha_r)^{e_r}}{(x-\beta_1)^{f_1} \ldots (x-\beta_s)^{f_s}} \tag{1}$$

The elements α_i and β_i are called respectively **zeros** and **poles** of the function.
We define the divisor associated to the rational function f as:

$$D = e_1(\alpha_1) + \ldots + e_r(\alpha_r) - f_1(\beta_1) - \ldots - f_s(\beta_s)$$

Divisors on Elliptic Curves

Definition 3 Given an elliptic curve $E(\mathbb{K})$ a divisor on E is defined as: $D = \sum_{P \in E(\mathbb{K})} n_P(P)$.

The following are fundamental notions about divisors:

- the **Support** of a divisor is the set of points P such that $n_P \neq 0$.
- the **Degree** of a divisor is $\deg(D) = \sum_P n_P$.
- the **Sum** of a divisor is $\text{sum}(D) = \sum_P n_P P$ (as points on the curve).

For example, let E be the elliptic curve defined by $y^2 = x^3 + 2x - 3$ and suppose we have a divisor $D = 5[P] - 7[Q]$, where $P = (2,3), Q = (1,0)$ are points on E. Then a rational function associated to D would be:

$$f(x,y) = \frac{(x-2)^5}{y^7}$$

Uniformizers

If we consider the curve defined by: $E : y^2 = x^3 - x$ and the rational function $f(x, y) = \frac{x}{y}$ what happens is that f is not defined in $(0, 0) \in E(K)$. However f is equivalent to $\frac{y}{x^2-1}$ on this curve and here it is defined in $(0, 0)$.

Theorem 1 *Let E be an elliptic curve. For each point P on E there exists a function u_P, with $u_P(P) = 0$, called **uniformizer** such that every function $f(x, y)$ can be written as:*

$$f = u_P^r g, r \in \mathbb{Z}, g(P) \notin \{0, \infty\}$$

Definition 4 (Order of f at P) We define the order of f at P as:

$$\mathrm{ord}_P(f) = r$$

For example, on the curve $y^2 = x^3 - x$ it can be shown that the function y is a uniformizer at $(0, 0)$. We have

$$x = y^2 \frac{1}{x^2 - 1}$$

and $\frac{1}{x^2-1}$ is nonzero and finite at $(0, 0)$. Therefore:

$$\mathrm{ord}_{(0,0)}(x) = 2,\ \mathrm{ord}_{(0,0)}\left(\frac{x}{y}\right) = 1$$

Definition 5 (Divisor of f) If f is a function on a curve E that is not identically zero then the *divisor* of f is:

$$\mathrm{div}(f) = \sum_{P \in E(\overline{\mathbb{K}})} \mathrm{ord}_P(f)[P] \in \mathrm{Div}(E)$$

Properties of divisors

Theorem 2 *Let E be an elliptic curve and let $f \neq 0$ be a rational function. Then:*

1. *f has finitely many zeros and poles.*
2. *If $div(f) = div(f')$ then there exists a constant c such that $f = cf'$.*
3. *$D = \sum_{P \in E(K)} n_p(P)$ then D is divisor of a function iff $\deg(D) = 0$ and $\mathrm{sum}(D) = \infty$.*
4. *If there are no zeros or poles ($\mathrm{div}(f) = 0$), then f is constant.*

Corollary 1 *If $P \in E[n]$ then $\exists f : \mathrm{div}(f) = n[P] - n[\infty]$.*

Proof By definition $nP = \infty$ so $n[P] - n[\infty]$ has degree zero and sum is ∞.

Consider for example the special case $n = 2 \Rightarrow P \in E[2]$. We know that $y = 0$ so $P = (\alpha, 0)$. It follows that

$$f_P = x - \alpha,\ \mathrm{div}(f_p) = 2[P] - 2[\infty]$$

Definition 6 (Equivalence of divisors)

$$D_1 \sim D_2 \Leftrightarrow D_1 = D_2 + \mathrm{div}(f)$$

Example 1 Let E be a curve defined by $y^2 = x^3 + 8x + 1$ on $\mathbb{F}_{61}$.
The following are points are on E: $P(57, 24), Q(25, 37), R(17, 32), S(42, 35)$.
Then $D_1 = [P] + [Q] + [R]$ and $D_2 = 4[\infty] - [S]$ are equivalent divisors, since if we compute $D_1 - D_2$ we will find out it has degree zero and sum ∞, hence it's divisor of a function f due to Corollary 1. The function f in this case is: $y = 33x^2 + 10x + 24$.

The Weil Pairing

Consider the elliptic curve E, a divisor $D = \sum_{P \in E} n_p[P]$, torsion points $P, Q \in E[n]$, and divisors $D_P = [P] - [\infty], D_Q = [Q] - [\infty]$.
We know that there exist functions $f_p, f_q : \mathrm{div}(f_p) = nD_P, \mathrm{div}(f_q) = nD_q$.

Definition 7 Let f, g be functions such that $\mathrm{div}(f) \sim nD_p, \mathrm{div}(g) \sim nD_q$ and the supports of both divisors are disjoint. The **Weil pairing** is $e_n : E[n] \times E[n] \to \mu_n = \{x : x^n = 1\}$ defined by $e_n = \dfrac{f(D_Q)}{g(D_P)}$, where $f(D) = \prod_{P \in E} f(P)^{n_p}$.

Note that we can't define the Weil pairing simply as $e_n = \frac{f_P(D_Q)}{f_Q(D_P)}$ since the supports are not disjoint. However, if $D'_P = [P + T] - [T], T \in E$ then $e_n(P, Q) = \frac{f_P(Q+T)}{f_P(T)} \frac{f_Q(-T)}{f_Q(P-T)}$.

Theorem 3 (Properties of Weil pairing) *The following properties hold:*

1. $e_n(P, Q)^n = 1$ *(that is, the Weil pairing always outputs a root of unity).*
2. ***Bilinearity*** $e_n(P_1 + P_2, Q) = e_n(P_1, Q) \cdot e_n(P_2, Q)$ *and similarly for the second argument.*
3. ***Alternating*** $\forall P \in E[n], e_n(P, P) = 1 \Leftrightarrow e_n(P, Q) = e_n(Q, P)^{-1}$.
4. ***Nondegenerate*** $\forall Q \in E[n], e_n(P, Q) = 1 \Rightarrow P = \infty$ *and similarly for the second argument.*
5. $e_n(\sigma(P), \sigma(Q)) = \sigma\left(e_n(P, Q)\right)$ *For all* $\sigma \in Aut\left(\overline{\mathbb{K}}\right)$ *that are the identity on the coefficients of* E*. Note that by writing* $\sigma(P)$ *we mean that we apply* σ *to both coordinates.*

We know that $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$. Let P_1, P_2 be the basis. Now if $e_n(P_1, P_2) = \zeta$, then if $P = a_P P_1 + b_P P_2, Q = a_Q P_1 + b_Q P_2$, then $e_n(P, Q) = \zeta^{\det A}, A = \begin{pmatrix} a_P & b_P \\ a_Q & b_Q \end{pmatrix}$.
Normally this is difficult to compute. However there is a fast algorithm by Miller that is a "double and add"-type algorithm which uses a constant times $\log q$ point additions.

The Tate-Lichtenbaum pairing

We define $E\left(\mathbb{F}_q\right)[n] = \{\text{Points of order that divides } n\}$. Let $P \in E(\mathbb{F}_q)[n], Q \in E[\mathbb{F}_q]$.
Then $D_P \sim [P] - [\infty]$.

Definition 8 (Tate pairing)

$$\tau_n : E\left(\mathbb{F}_q\right)[n] \times E\left(\mathbb{F}_q\right) / nE\left(\mathbb{F}_q\right) \to \mathbb{F}_q^* / \left(\mathbb{F}_q^*\right)^n$$

$\tau_n = f\left(D_Q\right) = e_n(P, R - \phi(R))$ where $R \in E\left(\mathbb{F}_q\right)$ such that $nR = Q$.

Definition 9 (Reduced/Modified Tate pairing)

$$T_n : E\left(\mathbb{F}_q\right)[n] \times E\left(\mathbb{F}_q\right) / nE\left(\mathbb{F}_q\right) \to \mu_n$$

$$T_n(P, Q) = \tau_n(P, Q)^{\frac{\#\mathbb{F}_q}{n}} \in \mu_n$$

Properties The Tate pairing is nondegenerate, bilinear and well-defined.

- Well-defined: $nR = Q, \infty = Q - \phi(Q) = n(R - \phi(R))$ so $R - \phi(R) \in E[n]$. Since $P \in E[n]$ then the Weil pairing $e_n(P, R - \phi(R))$ is well defined.

  Suppose that we have $R' : nR' = Q$ then let $T' = R' - R$. Then $nT = Q - Q = \infty$ so also $nT = \infty$ and $T \in E[n]$. So $e_n(P, R' - \phi(R)) = e_n(P, R - \phi(R)) + T - \phi(T) = \frac{e_n(P, R-\phi(R))e_n(P,T)}{e_n(P,\phi(T))}$, $P = \phi(P)$. Let $e_n(D, \phi(T)) = e_n(\phi(P), \phi(T)) = \phi(e_n(P, T)) = e_n(P, T)$. Thus, we have that $e_n(P, R' - \phi(R')) = e_n(P, R - \phi(R))$, which shows that the definition of the Tate pairing does not depend on the choice of R.

  Now let $Q' = Q + nU \in E(\mathbb{F}_q), nR = Q, R' = R + U, nR' = Q$. Then $e_n(P, R' - \phi(R')) = e_n(P, R - \phi(R) + U - \phi(U)) = e_n(P, R - \phi(R))$ since $U = \phi(U)$. Hence we can see that the Tate pairing is only defined modulo n.

- Bilinearity: Let $nR_1 = Q_1, nR_2 = Q_2$.

  $\tau_n(P, Q_1 + Q_2) = e_n(P, R_1 + R_2 - \phi(R_1) - \phi(R_2)) = e_n(P, R_1 - \phi(R_1))e_n(P, R_2 - \phi(R_2)) = \tau_n(P, Q_1)\tau_n(P, Q_2)$.

- Non-degeneracy: omitted.

Applications

Tri-partite Diffie-Helman With the Weil pairing we can perform tri-partite DH (that is, key exchange among three users).

MOV The MOV attack, that we saw in the previous lecture, is based on pairings.
Consider a curve E over $\mathbb{F}_q$ and a point $P \in E(\mathbb{F}_q)$ of order $n > \sqrt{p} + 1$, where p is a large prime.

1. Compute $\#E\left(\mathbb{F}_{q^k}\right) = N$. We know that $n|N$.
2. Choose random $T \in E\left(\mathbb{F}_{q^k}\right)$, but $T \notin E(\mathbb{F}_q)$.
3. Compute $T' = \frac{N}{n}T$. This could be two things. If $T' = \infty$ then restart with other T. Otherwise T' has order n.
4. Compute the Weil pairings $g = e_n(P, T'), h = e_n(Q, T')$. Note that $g, h \in \mu_n \subseteq \mathbb{F}_{q^k}$.

   So we have reduced ECDLP(P,Q) on F_q to DLP(g,h) on $\mathbb{F}_{q^k}$.
5. Solve $h = g^a$ (with fast methods such as index calculus).
6. It follows that $Q = aP$.