The Tate Pairing via Elliptic Nets

Katherine Stange

Department of Mathematics
Brown University
http://www.math.brown.edu/~stange/

Pairing,
Tokyo, Japan, 2007

Outline

Definition of an elliptic net

Definition (KS)

Let R be an integral domain, and A a finite-rank free abelian group. An *elliptic net* is a map $W : A \to R$ such that the following recurrence holds for all $p, q, r, s \in A$.

$$\begin{aligned} W(p+q+s)W(p-q)W(r+s)W(r) \\ + W(q+r+s)W(q-r)W(p+s)W(p) \\ + W(r+p+s)W(r-p)W(q+s)W(q) = 0 \end{aligned}$$

- The recurrence generates the net from finitely many initial values.

Elliptic Nets in their Natural Habitat

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

$\circ$ $[3]Q$	$\circ$ $[1]P + [3]Q$	$\circ$ $[2]P + [3]Q$
$\circ$ $[2]Q$	$\circ$ $[1]P + [2]Q$	$\circ$ $[2]P + [2]Q$
$\circ$ $[1]Q$	$\circ$ $[1]P + [1]Q$	$\circ$ $[2]P + [1]Q$
$\circ$ ∞	$\circ$ $[1]P$	$\circ$ $[2]P$

Elliptic Nets in their Natural Habitat

$$E: y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

$\left(\frac{56}{25}, \frac{371}{125}\right)$	$\left(-\frac{95}{64}, \frac{495}{512}\right)$	$\left(\frac{328}{361}, -\frac{2800}{6859}\right)$
$\left(\frac{6}{1}, -\frac{16}{1}\right)$	$\left(\frac{1}{9}, -\frac{19}{27}\right)$	$\left(\frac{39}{1}, \frac{246}{1}\right)$
$\left(\frac{1}{1}, \frac{0}{1}\right)$	$\left(-\frac{2}{1}, -\frac{1}{1}\right)$	$\left(\frac{5}{4}, -\frac{13}{8}\right)$
∞	$\left(\frac{0}{1}, \frac{0}{1}\right)$	$\left(\frac{3}{1}, \frac{5}{1}\right)$

Elliptic Nets in their Natural Habitat

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

$\circ\ \left(\frac{56}{5^2}, \frac{371}{5^3}\right)$ $\circ\ \left(-\frac{95}{8^2}, \frac{495}{8^3}\right)$ $\circ\ \left(\frac{328}{19^2}, -\frac{2800}{19^3}\right)$

$\circ\ \left(\frac{6}{1^2}, -\frac{16}{1^3}\right)$ $\circ\ \left(\frac{1}{3^2}, -\frac{19}{3^3}\right)$ $\circ\ \left(\frac{39}{1^2}, \frac{246}{1^3}\right)$

$\circ\ \left(\frac{1}{1^2}, \frac{0}{1^3}\right)$ $\circ\ \left(-\frac{2}{1^2}, -\frac{1}{1^3}\right)$ $\circ\ \left(\frac{5}{2^2}, -\frac{13}{2^3}\right)$

$\circ\ \infty$ $\circ\ \left(\frac{0}{1^2}, \frac{0}{1^3}\right)$ $\circ\ \left(\frac{3}{1^2}, \frac{5}{1^3}\right)$

Elliptic Nets in their Natural Habitat

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

5	8	19
1	3	1
1	1	2
0	1	1

Elliptic Nets in their Natural Habitat

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

$\circ\ -5$	$\circ\ +8$	$\circ\ -19$
$\circ\ +1$	$\circ\ +3$	$\circ\ -1$
$\circ\ +1$	$\circ\ +1$	$\circ\ +2$
$\circ\ +0$	$\circ\ +1$	$\circ\ +1$

Curve + Points give Net

Theorem (KS)

Let E be an elliptic curve defined over a field K. For all $\mathbf{v} \in \mathbb{Z}^n$, there exist functions

$$\Psi_{\mathbf{v}} : E^n \to K$$

such that the following holds:

1. *Each $\Psi_{\mathbf{v}}$ is elliptic in each variable.*
2. *For any fixed $\mathbf{P} \in E^n$, the function $W : \mathbb{Z}^n \to K$ defined by*
$$W(\mathbf{v}) = \Psi_{\mathbf{v}}(\mathbf{P})$$
is an elliptic net.

Characterising Functions $\Psi_{\mathbf{v}}$

The functions $\Psi_{\mathbf{v}}$ may be characterised uniquely by the additional assumptions that

1. $\Psi_{\mathbf{v}}(\mathbf{P})$ vanishes exactly when $\mathbf{v} \cdot \mathbf{P} = 0$ on E.
2. $\Psi_{\mathbf{v}} = 1$ whenever $\mathbf{v}$ is $\mathbf{e}_i$ or $\mathbf{e}_i + \mathbf{e}_j$ for some standard basis vectors $\mathbf{e}_i \neq \mathbf{e}_j$.

- We call W the elliptic net associated to $E, P_1, \ldots, P_n$, and write $W_{E,\mathbf{P}}$.
- We call $P_1, \ldots, P_n$ the basis of $W_{E,\mathbf{P}}$.

Division Polynomials

Any elliptic curve E has a Weierstrass equation. Suppose

$$E : y^2 = x^3 + Ax + B \ .$$

The elliptic functions Ψ_k are the **Division Polynomials** in terms of x, y, A, B:

$$\begin{aligned}
\Psi_1 &= 1, \\
\Psi_2 &= 2y, \\
\Psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2, \\
\Psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),
\end{aligned}$$

Net Polynomial Examples

In higher rank case, we also have such polynomial representations.

$$\Psi_{-1,1} = x_1 - x_2 \quad ,$$

$$\Psi_{2,1} = 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \quad ,$$

$$\Psi_{2,-1} = (y_1 + y_2)^2 - (2x_1 + x_2)(x_1 - x_2)^2 \quad ,$$

$$\Psi_{1,1,1} = \frac{y_1(x_2 - x_3) + y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)} \quad ,$$

Can calculate more via the recurrence...

$$\begin{aligned}\Psi_{3,1} = (x_2 - x_1)^{-3}(&4x_1^6 - 12x_2x_1^5 + 9x_2^2x_1^4 + 4x_2^3x_1^3 \\ &- 4y_2^2x_1^3 + 8y_1^2x_1^3 - 6x_2^4x_1^2 + 6y_2^2x_2x_1^2 - 18y_1^2x_2x_1^2 \\ &+ 12y_1^2x_2^2x_1 + x_2^6 - 2y_2^2x_2^3 - 2y_1^2x_2^3 + y_2^4 - 6y_1^2y_2^2 \\ &+ 8y_1^3y_2 - 3y_1^4) \quad .\end{aligned}$$

Elliptic nets calculate the group law

Consider the one-dimensional case. Suppose we have

$$E : y^2 = x^3 + Ax + B \ .$$

Define

$$\phi_k = x\Psi_k^2 - \Psi_{k+1}\Psi_{k-1} \ ,$$

$$4y\omega_k = \Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2 \ .$$

Then we have

$$[k]P = \left(\frac{\phi_k(P)}{\Psi_k(P)^2}, \frac{\omega_k(P)}{\Psi_k(P)^3} \right) \ .$$

In general, the elliptic net calculates the coordinates of any linear combination of its basis points.

Example

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

-5	8	-19			
1	3	-1			
1	1	2			
0	1	1			

$\uparrow$ Q

$P \rightarrow$

Example

$$E: y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

	4335	5959	12016	-55287	23921	1587077
	94	479	919	-2591	13751	68428
	-31	53	-33	-350	493	6627
	-5	8	-19	-41	-151	989
	1	3	-1	-13	-36	181
$\uparrow$	1	1	2	-5	7	89
Q	0	1	1	-3	11	38
	$P \rightarrow$					

Example

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

4335	5959	12016	−55287	23921	1587077
94	479	919	−2591	13751	68428
−31	53	−33	−350	493	6627
−5	8	−19	−41	−151	989
1	3	−1	−13	−36	181
1	1	2	−5	7	89
0	1	1	−3	11	38

$\uparrow$ Q

$P \rightarrow$

Example

$$E : y^2 + y = x^3 + x^2 - 2x; P = (0,0), Q = (1,0)$$

	4335	5959	12016	−55287	23921	1587077
	94	479	919	−2591	13751	68428
	−31	53	−33	−350	493	6627
	−5	8	−19	−41	−151	989
	1	3	−1	−13	−36	181
$\uparrow$	1	1	2	−5	7	89
Q	0	1	1	−3	11	38
	$P \rightarrow$					

Lattice Property

- For an integer elliptic net, for each prime p, there exists a **Lattice of Apparition** $L \subset A$ such that

$$W(\mathbf{v}) \equiv 0 \mod p \iff \mathbf{v} \in L$$

- Let $\widetilde{E}, \widetilde{P}_1, \ldots, \widetilde{P}_n$ be the images of $E, P_1, \ldots, P_n$ under reduction modulo p.
- Then $W_{\widetilde{E},\widetilde{\mathbf{P}}}$ (taking values in $\mathbb{F}_p$) is simply the reduction of the values of $W_{E,\mathbf{P}}$ modulo p.
- In particular, $W_{E,\mathbf{P}}(\mathbf{v}) \equiv 0 \mod p$ if $\mathbf{v} \cdot \mathbf{P} = 0$ on $\widetilde{E}$.

Example of Reduction Mod 5 of an Elliptic Net

	0	4	4	3	1	2	4
	4	4	4	4	1	3	0
	4	3	2	0	3	2	1
	0	3	1	4	4	4	4
	1	3	4	2	4	1	0
$\uparrow$	1	1	2	0	2	4	1
Q	0	1	1	2	1	3	4
	$P \longrightarrow$						

Example of Reduction Mod 5 of an Elliptic Net

	0	4	4	3	1	2	4
	4	4	4	4	1	3	0
	4	3	2	0	3	2	1
	0	3	1	4	4	4	4
	1	3	4	2	4	1	0
$\uparrow$	1	1	2	0	2	4	1
Q	0	1	1	2	1	3	4
	$P \longrightarrow$						

Example of Reduction Mod 5 of an Elliptic Net

	0	4	4	3	1	2	4
	4	4	4	4	1	3	0
	4	3	2	0	3	2	1
	0	3	1	4	4	4	4
	1	3	4	2	4	1	0
$\uparrow$	1	1	2	0	2	4	1
Q	0	1	1	2	1	3	4
	$P \longrightarrow$						

Example of Reduction Mod 5 of an Elliptic Net

0	4	4	3	1	2	4
4	4	4	4	1	3	0
4	3	2	0	3	2	1
0	3	1	4	4	4	4
1	3	4	2	4	1	0
1	1	2	0	2	4	1
0	1	1	2	1	3	4

$\uparrow Q$ $P \longrightarrow$

- The elliptic net is not periodic modulo the lattice of apparition.

Example of Reduction Mod 5 of an Elliptic Net

0	4	4	3	1	2	4
4	4	4	4	1	3	0
4	3	2	0	3	2	1
0	3	1	4	4	4	4
1	3	4	2	4	1	0
1	1	2	0	2	4	1
0	1	1	2	1	3	4

$\uparrow Q$

$P \rightarrow$

- The elliptic net is not periodic modulo the lattice of apparition.
- The appropriate translation property should tell how to obtain the green values from the blue values.

Example of Reduction Mod 5 of an Elliptic Net

0	4	4	3	1	2	4
4	4	4	4	1	3	0
4	3	2	0	3	2	1
0	3	1	4	4	4	4
1	3	4	2	4	1	0
1	1	2	0	2	4	1
0	1	1	2	1	3	4

$\uparrow Q$

$P \longrightarrow$

- The elliptic net is not periodic modulo the lattice of apparition.
- The appropriate translation property should tell how to obtain the green values from the blue values.
- There are such translation properties, and it is within these that the Tate pairing information lies.

Elliptic Nets and Linear Combinations of Points

- If W_i is the elliptic net associated to E, P_i, Q_i for $i = 1, 2$, and

$$[a_1]P_1 + [b_1]Q_1 = [a_2]P_2 + [b_2]Q_2$$

then

$$W_1(a_1, b_1) \text{ is not necessarily equal to } W_2(a_2, b_2) \quad .$$

- So how do we propose to compare two elliptic nets supposedly associated to the same linear combinations?

Defining a Net on a Free Abelian Cover

- Let K be a finite or number field. Let $\hat{E}$ be any finite rank free abelian group surjecting onto $E(K)$.

$$\pi : \hat{E} \to E(K)$$

- For a basis P_1, P_2, choose $p_i \in \hat{E}$ such that $\pi(p_i) = P_i$.
- We specify an identification

$$\mathbb{Z}^2 \cong \langle p_1, p_2 \rangle$$

  via $\mathbf{e}_i \mapsto p_i$.
- The elliptic net W associated to E, P_1, P_2 and defined on $\mathbb{Z}^2$ is now identified with an elliptic net W' defined on $\hat{E}$.
- This allows us to compare elliptic nets associated to different bases.

Defining a Special Equivalence Class

Definition

Let $W_1, W_2 : A \to K$. Suppose $f : A \to K^*$ is a quadratic function. If

$$W_1(\mathbf{v}) = f(\mathbf{v}) W_2(\mathbf{v})$$

for all $\mathbf{v}$, then we say W_1 *is equivalent to* W_2.

- The basis change formula is an equivalence, when the elliptic nets are viewed as maps on $\hat{E}$ as explained in the previous slide.
- In this way, we can associate an equivalence class to a subgroup of $E(K)$.

Statement of Theorem

Theorem (KS)

Fix a positive $m \in \mathbb{Z}$. Let E be an elliptic curve defined over a finite field K containing the m-th roots of unity. Let $P, Q \in E(K)$, with $[m]P = \mathcal{O}$. Choose $S \in E(K)$ such that $S \notin \{\mathcal{O}, -Q\}$. Choose $p, q, s \in \hat{E}$ such that $\pi(p) = P$, $\pi(q) = Q$ and $\pi(s) = S$. Let W be an elliptic net in the equivalence class associated to a subgroup of $E(K)$ containing P, Q, and S. Then the quantity

$$T_m(P,Q) = \frac{W(s + mp + q)W(s)}{W(s + mp)W(s + q)}$$

is the Tate pairing.

Choosing an Elliptic Net

Corollary

Let E be an elliptic curve defined over a finite field K, m a positive integer, $P \in E(K)[m]$ and $Q \in E(K)$. Then

$$\tau_m(P, P) = \frac{W_{E,P}(m+2)W_{E,P}(1)}{W_{E,P}(m+1)W_{E,P}(2)} ,$$

and

$$\tau_m(P, Q) = \frac{W_{E,P,Q}(m+1,1)W_{E,P,Q}(1,0)}{W_{E,P,Q}(m+1,0)W_{E,P,Q}(1,1)} .$$

Elliptic Net Algorithm

Algorithm Outline

1. Given E, P, Q with $[m]P = 0$, calculate the initial terms of $W_{E,P,Q}$.
2. Using the recurrence relation, calculate the terms $W(m+1,0)$, $W(m+1,1)$.
3. Calculate $T_m(P,Q) = W(m+1,1)/W(m+1,0)$.
4. Perform final exponentiation exactly as in Miller's algorithm.

Remarks:

- There are polynomial formulae for the initial terms of Step 1.
- Step 4 is also performed in Miller's algorithm and the same efficient methods apply here.
- The challenge lies in efficient computation of large terms of the net $W_{E,P,Q}$.

Computing Terms of $W_{E,P,Q}$

		(k-1,1)	(k,1)	(k+1,1)			
(k-3,0)	(k-2,0)	(k-1,0)	(k,0)	(k+1,0)	(k+2,0)	(k+3,0)	(k+4,0)

Figure: A block centred at k

Computing Terms of $W_{E,P,Q}$

Double and add algorithm:

$$\begin{tikzcd}[column sep=small] & \text{Block centred at } k \arrow[dl] \arrow[dr] & \\ \text{Block centred at } 2k & & \text{Block centred at } 2k+1 \end{tikzcd}$$

Each term of the new block requires one instance of the recurrence relation, i.e. several multiplications and an addition.

Complexity

Let k be the embedding degree. Let $P \in E(\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_{q^k})$.

S	squaring in $\mathbb{F}_q$
S_k	squaring in $\mathbb{F}_{q^k}$
M	multiplication in $\mathbb{F}_q$
M_k	multiplication in $\mathbb{F}_{q^k}$

Algorithm:	Elliptic Net
Double:	$6S + (6k+26)M + S_k + \frac{3}{2}M_k$
DoubleAdd:	$6S + (6k+26)M + S_k + 2M_k$

Algorithm:	Optimised Miller's [1]
Double:	$4S + (k+7)M + S_k + M_k$
DoubleAdd:	$7S + (2k+19)M + S_k + 2M_k$

[1] Koblitz N., Menezes A., *Pairing-based cryptography at high security levels*, 2005

In Practice

Thank you to Michael Scott, Augusto Jun Devigili and Ben Lynn for implementing the algorithm. A timing comparison program is bundled with Ben Lynn's Pairing-Based Cryptography Library at http://crypto.stanford.edu/pbc/

- **type a**: 512 bit base-field, embedding degree 2, 1024 bits security, $y^2 = x^3 + x$, group order is a Solinas prime.
- **type f**: 160 bit base-field, embedding degree 12, 1920 bits security, Barreto-Naehrig curves [*Pairing Friendly Elliptic Curves of Prime Order*, SAC 2005]

Algorithm:	Miller's	Elliptic Net
type a	19.8439 ms	40.6252 ms
type f	238.4378 ms	239.5314 ms

average time of a test suite of 100 randomly generated pairings in each of the two cases

Potential Advantages

- Naturally inversion-free.
- Naturally deterministic.
- Since Double and DoubleAdd steps are similar or the same, is independent of hamming weight and avoids side-channel attacks.
- Lends itself to time-saving precomputation for repeated pairings $e_m(P, Q)$, e.g. where E, m, and P are fixed.
- Code is simple.

Improving the Algorithm

To compute a given pairing, we have many choices:

- Choice of a point S.
- Choice of lifts of P, Q, S.
- Choice of a subgroup of $E(K)$ containing P and Q, and S.
- Choice of an elliptic net in the given equivalence class.
- Choice of scaling of the chosen net.
- Choice of recurrences used to compute the terms of the net.
- Choice of order of operations for the computations.

In the algorithm I have given, I have made apparently convenient choices for these things. It is very probable significant improvement is possible.

Summary

- Elliptic nets provide an alternate computational model for elliptic curves.
- The terms of an elliptic net compute the Tate and Weil pairings.
- The resulting algorithm is of comparable complexity to Miller's Algorithm and is likely to yield to further optimisation.
- The algorithm may have inherent security and computational benefits.

Slides and Pari/GP scripts available at
http://www.math.brown.edu/~stange/