Calcul des Couplages par les *Elliptic Nets*

Emmanuel FOUOTSA

Université de Bamenda, Cameroun
Ecole Normale Supérieure de Bambili
Département de Mathématiques

FAST, Institut de Mathématiques de Bordeaux, France

September 6, 2017

Sommaire

Suite de divisibilité elliptique

Elliptic net de rang 1

C'est une suite définie par la relation de recurrence

$$W_{n+m}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2$$

for positive integers $m > n$

- W_1, W_2, W_3, W_4 given
- Exemple: 1, 2, 3, 4, 5, ...

Suite de divisibilité elliptique associée à une courbe elliptique

Soit F_q un corps fini et $P(x,y) \in E(F_q)$ où
$E(F_q) = \{(x,y) \in F_q^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$ Posons
$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6$
$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$

Alors $[n]P = (\frac{\phi_n(P)}{\psi_n(P)^2}, \frac{\omega_n(P)}{\psi_n(P)^3})$ où

1. $\psi_1 = 1, \quad \psi_2 = 2y + a_1x + a_3$
2. $\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8$
3. $\psi_4 = (2y+a_1x+a_3)(2x^6+b_2x^5+5b_4x^4+10b_6x^3+10b_8x^2+(b_2b_8-b_4b_6)x+b_4b_8-b_6^2)$
4. $\psi_{n+m}\psi_{n-m} = \psi_{n+1}\psi_{n-1}\psi_m^2 - \psi_{m+1}\psi_{m-1}\psi_n^2, \quad$ (II)

$W_n(P) = \psi_n(P)$ est donc une suite de divisibilité elliptique.

Generalisation des suites de divisibilité elliptique

$$\{W_n(P)\} \leftrightarrow [n]P$$

On voudrait generaliser

$$\{W_{n,m}(P,Q)\} \leftrightarrow [n]P + [m]Q$$

$$\{W_{n,m,s}(P,Q,R)\} \leftrightarrow [n]P + [m]Q + [s]R$$

Elliptic Nets

Définition [Stange]

Soit $\mathcal{A}$ un anneau intègre. Un Elliptic Net est une suite $W : \mathbb{Z}^n \to \mathcal{A}$ qui vérifie la relation

$$W(p+q+s)W(p-q)W(r+s)W(r) + W(q+r+s)W(q-r)W(p+s)W(p) + \quad (1)$$
$$W(r+p+s)W(r-p)W(q+s)W(q) = 0 \quad (2)$$

Soit $\{e_i\}$, la base naturelle de $\mathbb{Z}^n$

1. $n = 1$, on a une suite de divisibilité elliptique.
2. W est normalisée si $W(e_i) = 1$ pour tout i et $W(e_i + e_j) = 1$ pour tout $1 \leq i < j \leq n$.
3. W est non-dégénérée si $W(e_i) \neq 0,\ W(e_i + e_j) \neq 0,\ W(e_i - e_j) \neq 0,\ \ W(2e_i) \neq 0.$

On s'interesse aux elliptic nets de rang $n = 2$

De l'Elliptic Net à une courbe elliptique

Soit $W : \mathbb{Z}^2 \to \mathcal{A}$ un elliptic net normalisé et non-degeneré de rang 2

La courbe d'équation

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{3}$$

où

$$a_1 = \frac{W(2,0) - W(0,2)}{W(2,1) - W(1,2)} \tag{4}$$

$$a_2 = 2W(2,1) - W(1,2) \tag{5}$$

$$a_3 = W(2,0), \quad a_4 = (W(2,1) - W(1,2))W(2,1), \quad a_6 = 0 \tag{6}$$

$$\tag{7}$$

définit une courbe elliptique et $P = (0,0)$ et $Q = (W(1,2) - W(2,1), 0)$ sont des points non singuliers

D'une Courbe elliptique à un Elliptic Net

Soit $E(\mathbb{C})$ une courbe elliptique et Γ le réseau correspondant. Soit (P_1, P_2) deux points linéairement indépendants de E et (z_1, z_2) les complexes correspondants via l'isomorphisme $\mathbb{C}/\Gamma \cong E(\mathbb{C})$.

Construction de Stange 2007

Soit $v(v_1, v_2) \in \mathbb{Z}^2$,

$$\psi_v(z_1, z_2) = \frac{\sigma(v_1 z_1 + v_2 z_2; \Gamma)}{\sigma(z_1)^{v_1^2 - v_1 v_2} \sigma(z_1 + z_2)^{v_1 v_2} \sigma(z_2)^{v_2^2 - v_1 v_2}} \tag{8}$$

D'une Courbe elliptique à un Elliptic Net

$$\begin{array}{rccc} W: & \mathbb{Z}^2 & \to & \mathbb{C} \\ & (v_1, v_2) & \longmapsto & \psi_{v_1,v_2}(z_1, z_2) \end{array} \tag{9}$$

est un elliptic net associé à la courbe E et aux points P_1 et P_2

1. $W(v_1, v_2) = 0 \Longleftrightarrow [v_1]P_1 + [v_2]P_2 = \mathcal{O}$
2. $W(v_1, 0)$ et $W(0, v_2$ correspondent aux polynômes de division pour $[v_1]P_1$ et $[v_2]P_2$
3. $W(1, 0) = W(0, 1) = W(1, 1) = 1$
4. Sont les dénominateurs de $[v_1]P_1 + [v_2]P_2$?

Stange étend le résultat à tout corps $\mathbb{K}$

A quoi ça ressemble

Let K be a field and $P(x_1, y_1),\ Q(x_2, y_2) \in E(K)$ where
$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$. then

- $W_{(1,0)} = W_{(0,1)} = W_{(1,1)} = 1$
- $W_{(1,-1)} = x_2 - x_1, W_{(-1,1)} = x_1 - x_2,$
- $W_{(2,1)} = 2x_1 + x_2 - (\frac{y_2-y_1}{x_2-x_1})^2 - a_1(\frac{y_2-y_1}{x_2-x_1}) + a_2$
- $W_{(1,2)} = x_1 + 2x_2 - (\frac{y_2-y_1}{x_2-x_1})^2 - a_1(\frac{y_2-y_1}{x_2-x_1}) + a_2.$

Théorème des Elliptic Nets

Il y a donc bijection entre

L'ensemble des courbes elliptiques et deux points P et Q, $P, Q, P+Q, P-Q \neq \mathcal{O}$

et

l'ensemble des elliptic Nets $W_{n,m}$ verifiant $W_{(1,0)} = W_{(0,1)} = W_{(1,1)} = 1$ et $W_{1,-1} \neq 0$

Et ça marche bien pour les rangs supérieurs

$E(\mathbb{F}_q)$ est une courbe elliptique dont l'odre du groupe est divisible par un grand facteur premier m. Soit $P \in E(\mathbb{F}_q)[m]$ et $Q \in E(\mathbb{F}_{q^k})/mE(\mathbb{F}_{q^k})$. Soit $f_{m,P}$ de diviseur $\mathrm{Div}(f_{m,P}) = m(P) - m(P_0)$. Soit D_Q un diviseur de support disjoint avec $\mathrm{Div}(f_{m,P})$

Le couplage de Tate

Le couplage de Tate est l'application

$$\begin{array}{rccc} e_m : & E(\mathbb{F}_q)[m] \times E(\mathbb{F}_{q^k})/mE(\mathbb{F}_{q^k}) & \to & \mathbb{F}^\star_{q^k}/(\mathbb{F}^\star_{q^k})^m \\ & (P,Q) & \mapsto & f_{m,P}(D_Q) \end{array}$$

L'algorithme de Miller

On considère les fonctions f_i telles que $\mathrm{Div}(f_{i,P}) = i(P) - (iP) - (i-1)(P_0)$ qui verifient

1. $f_{1,P} = 1$
2. $f_{i+j,P} = f_{i,P} f_{j,P} \frac{H_{iP,jP}}{d_{(i+j)P}}$
3. $f_{ij,P} = f_{i,P}^{j} f_{j,iP} = f_{j,P}^{i} f_{i,jP}$

1. Calcule la fonction $f_{m,P}(Q)$ à partir des $f_{i,P}$
2. on decompose $m = (1, m_{r-1}, ...m_1, m_0)_2$
3. C'est un double and add algorithm

L'algorithme de Miller pour calculer le couplage

Input: $P \in E(\mathbb{F}_q)[m]$, $Q \in E(\mathbb{F}_{q^k})[m]$,
$m = (1, m_{r-1}, ...m_1, m_0)_2$.
Output: *The Tate pairing of* P *and* Q : $e_m(P,Q)$

1. *do* $f \leftarrow 1$ *and* $R \leftarrow P$
2. *for* $i = r-1$ *à* 0
   - 2.1 *do* $f \leftarrow f^2 \cdot H_{R,R}(D_Q)$ *and* $R \leftarrow 2R$
   - 2.2 *if* $m_i = 1$ *then* $f \leftarrow f \cdot H_{R,P}(D_Q)$ *and* $R \leftarrow R + P$
3. $e_m(P,Q) \leftarrow f^{\frac{q^k-1}{m}}$

Le Couplage de Tate en termes d' Elliptic Nets

On considère la fonction $\psi_{1,v_2,v_3}(-S,P,Q)$ associée à la combinaison linéaire $-S+[v_2]P+[v_3]Q$ où S est quelconque. Grâce aux proprietés de la fonction σ de Weiertrass on peut demontrer que

$$Div(\psi_{1,v_2,v_3}(-S,P,Q)) = ([v_2]P+[v_3]Q) - \{v_2(P)+v_3(Q)\} - \{1-v_2-v_3\}(\mathcal{O}) \quad (10)$$

où les v_i sont les entiers et P,Q sont les points de la courbe elliptique.

On vérifie alors que

$$Div(\psi_{1,0,0}) = O, \qquad Div(\psi_{1,m,0}) = -m(P)+m(\mathcal{O})$$

$$Div(\psi_{1,0,1}) = O \qquad Div(\psi_{1,m,1}) = -m(P)+m(\mathcal{O})$$

Le couplage de Tate en termes d' Elliptic Nets

On déduit

$$Div(\frac{\psi_{1,0,0}(-S,P,Q)}{\psi_{1,m,0}(-S,P,Q)}) = Div(f_{m,P}) \tag{11}$$

ce qui conduit à

$$f_{m,P}(S) = \frac{\psi_{1,0,0}(-S,P,Q)}{\psi_{1,m,0}(-S,P,Q)}$$

Soit D_Q, le diviseur $(-S) - (-S-Q)$. On a

$$\begin{aligned} f_{m,P}(D_Q) &= \frac{f_{m,P}(-S)}{f_{m,P}(-S-Q)} \\ &= \frac{\psi_{1,0,0}(S,P,Q)\psi_{1,m,0}(S+Q,P,Q)}{\psi_{1,m,0}(S,P,Q)\psi_{1,0,0}(S+Q,P,Q)} \\ &= \frac{\psi_{1,0,0}(S,P,Q)\psi_{1,m,1}(S,P,Q)}{\psi_{1,m,0}(S,P,Q)\psi_{1,0,1}(S,P,Q)} \end{aligned}$$

Couplage de Tate en termes d'Elliptic Nets

En posant $S = P$,

$$T_{m,P}(P,Q) = \frac{W_{P,Q}(m+1,1)W_{P,Q}(1,0)}{W_{P,Q}(m+1,0)W_{P,Q}(1,1)} \tag{12}$$

where $W_{P,Q}(m+1,i) = \psi_{1,m,i}(S,P,Q)|_{S=P}$.

qui est le couplage de Tate (- *l'expo finale*) qui se simplifie grâce aux proprietés de l'elliptic net

$$T_{m,P}(P,Q) = \frac{W_{P,Q}(m+1,1)}{W_{P,Q}(m+1,0)} \tag{13}$$

Calcul

$$T_{m,P}(P,Q) = \frac{W_{P,Q}(m+1,1)}{W_{P,Q}(m+1,0)} \tag{14}$$

moins l'expo finale

Pour calculer $T_{m,P}(P,Q)$, il faut calculer $W_{P,Q}(m+1,1)$ et $W_{P,Q}(m+1,0)$ en premier et pour le faire, l'on devrait utiliser la rélation de récurrence des elliptic nets.

D'un block V à un block Double(V) ou DoubleAdd(V)

L'Algorithme de Stange

Table: Block V centré en k

		(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)

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

		(2k,1)	(2k+1,1)	(2k+2,1)			
(2k-2,0)	(2k-1,0)	(2k,0)	(2k+1,0)	(2k+2,0)	(2k+3,0)	(2k+4,0)	(2k+5,0)

Le bloc centré en m est obtenue après $\log(m)$ steps.

Formules de Duplication

Des termes initiaux sont connus:
$a = W(2,0)$, $b = W(3,0)$, $c = W(4,0)$, $d = W(2,1)$, $e = W(-1,1)$,
$f = W(2,-1)$, $g = W(1,1)$ et $W(1,0) = W(0,1) = 1$

Outil de calcul du premier vecteur

$$W(2i-1,0) = W(i+1,0)W(i-1,0)^3 - W(i-2,0)W(i,0)^3$$
$$W(2i,0) = (W(i,0)W(i+2,0)W(i-1,0)^2 - W(i,0)W(i-2,0)W(i+1,0)^2)/W(2,0)$$

Outil de calcul du second vecteur

$$W(2k-1,1) =$$
$$(W(k+1,1)W(k-1,1)W(k-1,0)^2 - W(k,0)W(k-2,0)W(k,1)^2)/W(1,1)$$
$$W(2k,1) = W(k-1,1)W(k+1,1)W(k,0)^2 - W(k-1,0)W(k+1,0)W(k,1)^2$$
$$W(2k+1,1) =$$
$$(W(k-1,1)W(k+1,1)W(k+1,0)^2 - W(k,0)W(k+2,0)W(k,1)^2)/W(-1,1)$$
$$W(2k+2,1) =$$
$$(W(k+1,0)W(k+3,0)W(k,1)^2 - W(k-1,1)W(k+1,1)W(k+2,0)^2)/W(2,-1)$$

L'algorithme des Elliptic Nets

Algorithme 1 Double(V) et DoubleAdd(V)

Entrées : Les termes
initiaux $a = W(2,0)$, $b = W(3,0)$, $c = W(4,0)$, $d = W(2,1)$, $e = W(-1,1)$,
$f = W(2,-1)$, $g = W(1,1)$ d'un "ellipti net" satisfaisant $W(1,0) = W(0,1) = 1$ et
l'entier $m = (m_l m_{l-1} \cdots m_1)_2$.
Sorties : Les termes $W(m,0)$ et $W(m,1)$ de "l'elliptic net".

L'algorithme des Elliptic Nets

1: $V \leftarrow [[-a, -1, 0, 1, a, b, c, a^3c - b^3]; [1, g, d]]$
2: Pour i allant de $l - 1$ à 1 faire
3: si i=0 alors
4: $V \leftarrow Double(V)$
5: sinon
6: $V \leftarrow DoubleAdd(V)$
7: fin si
8: fin Pour
9: Sortie : $V[0, 3]$, $V[1, 1]$ i.e $\{W(m, 0)$ et $W(m, 1)\}$

L'algorithme des Elliptic Nets

Algorithme 1

Entrées : Block V centré en k d'un "elliptic net" satisfaisant $W(1,0) = W(0,1) = 1, A = W(2,0)^{-1}, E = W(-1,1)^{-1}, F = W(2,-1)^{-1}, G = W(1,1)^{-1}$, et $add \in \{1,0\}$

Sorties : Block centré en $2k$ si $add == 0$ et centré en $2k+1$ si $add == 1$.

1: $S \leftarrow [0,0,0,0,0,0]$

2: $P \leftarrow [0,0,0,0,0,0]$

3: $S_0 \leftarrow V[1,1]^2$ $1S_k$

4: $P_0 \leftarrow V[1,1]V[1,2]$ $1M_k$

L'algorithme des Elliptic Nets

5: Pour i allant de 0 à 5 faire	
6: $S[i] \leftarrow V[0,i+1]^2$	$6 \cdot (1S)$
7: $P[i] \leftarrow V[0,i]V[0,i+2]$	$6 \cdot (1M)$
8: fin Pour	
9: Si $add == 0$ alors	
10: Pour i allant de 1 à 4 faire	
11: $V[0,2i-2] \leftarrow S[i-1]P[i] - S[i]P[i-1]$	$8 \cdot (2M)$
12: $V[0,2i-2] \leftarrow (S[i-1]P[i+1] - S[i+1]P[i-1])A$	
13: fin Pour	
14: $V[1,0] \leftarrow (S[1]P_0 - S_0P[1])G$	$2kM + M_k$
15: $V[1,1] \leftarrow S[2]P_0 - S_0P[2]$	$2kM$
16: $V[1,2] \leftarrow (S[3]P_0 - S_0P[3])E$	$2kM + M_k$

L'algorithme des Elliptic Nets

17: sinon
18: Pour i allant de 1 à 4 faire
19: $V[0, 2i-2] \leftarrow (S[i-1]P[i+1] - S[2]P[0])A$ $4 \cdot (3M)$
20: $V[0, 2i-2] \leftarrow S[i]P[i+1] - S[i+1]P[i]$ $4 \cdot (2M)$
21: fin Pour
22: $V[1, 0] \leftarrow S[0]P_0 - S_0P[0]$ $2kM$
23: $V[1, 1] \leftarrow (S[3]P_0 - S_0P[3])E$ $2kM + M_k$
24: $V[1, 2] \leftarrow (S_0P[4] - S[4]P_0)F$ $2kM + M_k$
25: fin Pour
26: Sortie : V

Complexité et Comparaison: Stange 2007

1. On peut trouver des elliptic nets equivalent pour lesquels on obtient $A = W(2,0)^{-1} = W(1,1)^{-1} = W(2,-1)^{-1} = 1$
2. L'elliptic net equivalent qui donne $W(-1,1) = 1$ donne entre autre $W(1,1) = x_P - x_Q$ on utilise les tordues de courbes elliptiques pour choisir Q.

Evaluation des coûts

Algorithme	**"Elliptic nets"**
Double :	$6S + (6k+26)M + S_k + \frac{3}{2}M_k$
DoubleAdd :	$6S + (6k+26)M + S_k + 2M_k$

Algorithme	**Algorithme de Miller**
Double :	$4S + (k+7)M + S_k + M_k$
DoubleAdd :	$7S + (2k+19)M + S_k + 2M_k$

Une recente optimisation ?

$$T_{m,P}(P,Q) = \frac{W_{P,Q}(m+1,1)}{W_{P,Q}(m+1,0)} \tag{15}$$

moins l'expo finale

Ogura, Kanayama, Uchiyana, Okamoto[2016]

Proposition:
Soit E une courbe définie sur le corps fini F_q. Soit $k > 1$, m un très grand nombre premier qui divise l'ordre de $E(F_q)$ et $(m,q) = 1$. Alors, pour $P \in E(F_q)$ et $Q \in E(F_{q^k})$,

$$T_m(P,Q) = f_{m,P}(Q)^{(q^k-1)/m} = W_{(m,1)}(P,Q)^{(q^k-1)/m} \tag{16}$$

- On gagne une inversion et une multiplication juste avant l'exponentiation finale
- Mais on ne gagne rien dans l'algorithme car le calcul de $W_{m,0}$ et $W_{m,1}$ sont liés.

Questions

1. Trouver d'autres formules de duplications qui ameliore le coût de calcul simultané de $W_{m,0}$ et $W_{m,1}$