Improving the AGM point counting algorithm

David Lubicz, Damien Robert

Outline

1. Generalities about point counting algorithms
2. Mestre's algorithm
3. Improving the AGM point counting algorithm
   - The genus 1 case
   - The genus 2 case
   - The higher genus case

Point counting algorithms

Quick version:

- Input: a curve $\mathbf{X}$ of genus $\mathbf{g}$ over $\mathbb{F}_{\mathbf{q}}$, $q = p^n$;
- Output: $\#X(\mathbb{F}_q)$.

Point counting algorithms

Longer version :

Zeta function of X

- $\chi(X, T) = \sum_n A_n T^n$, $A_n = \#\{D \in DivC | D \geqslant 0, \deg D = n\}$;
- $\chi(X, T) = \frac{\chi_p(X,T)}{(1-T)(1-qT)}$, $\chi_p(X, T) = \sum_{i=0}^{2g} a_i T^i \in \mathbb{Z}[T]$, $a_{2g} = 1, a_0 = q^g$.

- Input: a curve X of genus g over $\mathbb{F}_q$;
- Output: $\chi_p(X, T)$.

Remark

Remark : $\chi_p(X, 1) = \#J(X)(\mathbb{F}_q)$ *has cryptographic applications.*

Canonical lift point counting algorithms

- Let $\overline{E}$ be the elliptic curve:

$$\boxed{\overline{E} : y^2 = x^3 + \overline{a}x + \overline{b}}, \text{ for } \overline{a}, \overline{b} \in \mathbb{F}_q, (q = p^n,\ p \neq 2, 3).$$

- Let $W(\mathbb{F}_q)$ be the degree n unramified extension of $\mathbb{Z}_p$;
- The reduction morphism $\pi : W(\mathbb{F}_q) \to \mathbb{F}_q,\ x \mapsto x \mod p$.

Definition

A lift E of $\overline{E}$ is a curve over $W(\mathbb{F}_q)$:

$$\boxed{E : y^2 = x^3 + ax + b}, \text{ for } a, b \in W(\mathbb{F}_q),$$

which reduces to E *mod* p i.e. such that $\overline{a} = a \mod p$ and $\overline{b} = b \mod p$.

Canonical lift point counting algorithms

Definition

If $\overline{E}$ is ordinary there's a unique canonical lift E of $\overline{E}$ such that $End(\overline{E}) = End(E)$.

- In particular, q-Frobenius of $\overline{E}$ has a lift Σ in $End(E)$;
- Σ acts by $x \mapsto \lambda x$, $\lambda \in W(\mathbb{F}_q)$ on $T_0^*(X)$ the 1-dimensional (co)tangent space in 0 of E;
- then $\chi_p(X, T) = T^2 + (\lambda + q/\lambda)T + q$.

Remark

Generalize to higher genus curves (need to distinguish X and $J(X)$).

Framework of canonical lift algorithms

General framework of Satoh-Mestre algorithms:

- Input: an ordinary curve $\mathbf{X}$ of genus $\mathbf{g}$ over $\mathbb{F}_{\mathbf{q}}$, $q = p^n$;
- Output: $\chi_p(X, T)$ the characteristic polynomial of the Frobenius.

1. Compute the canonical lift of $J(X)$ over $W(\mathbb{F}_q)$;
2. Compute the action M of the Frobenius morphism on $T_0(J(X))$;
3. Compute $\chi_1(X, T) = \det(M - TI)$;
4. Recover $\chi_p(X, T) = T^g \chi_1(X, q/T) \chi_1(X, T)$.

Idea of Mestres's algorithm

- Main idea: the canonical lift is a fixed point for the Frobenius action;
- Compute the canonical lift by iterating the Frobenius: actually we use the p-Frobenius isogeny because of its small degree;
- the Frobenius action: easily computed by an isomorphism between Weierstrass models of elliptic curves.

By the way, where is the AGM ? Characteristic 2 case !

- Define an AGM sequence by: $(a_0, b_0) \in W(\mathbb{F}_{2^n})$,

$$\boxed{(a_{k+1}, b_{k+1}) = \left(\frac{a_k+b_k}{2}, \sqrt{a_k b_k}\right)}.$$

- Let $\widetilde{E}_{a_k,b_k}$ be the elliptic curves over $\mathbb{Q}_{2^n}$ given by :

$$\boxed{y^2 = x(x - a_k^2)(x - b_k^2).}$$

- Then there is a sequence of 2-isogeny:

$$\boxed{E_{a_0,b_0} \longrightarrow E_{a_1,b_1} \longrightarrow \cdots \longrightarrow E_{a_k,b_k} \longrightarrow \cdots}$$

Scheme of the algorithm

- Let $\overline{E}_0$ over $\mathbb{F}_{2^n}$, suppose that E_{a_0,b_0} is a lift of E_0.
- Then we have the diagram of isogenies:

$$
\begin{tikzcd}
E_{a_n,b_n} \arrow[r] & E_{a_{n+1},b_{n+1}} \arrow[r] & \cdots \arrow[r] & E_{a_{2n-1},b_{2n-1}} \\
E_{a_0,b_0} \arrow[r] \arrow[d] & E_{a_1,b_1} \arrow[r] \arrow[d] & \cdots \arrow[r] & E_{a_{n-1},b_{n-1}} \arrow[d] \arrow[ulll, bend left] \\
\overline{E}_0 \arrow[r] & \overline{E}_1 \arrow[r] & \cdots \arrow[r] & \overline{E}_{n-1} \arrow[lll, bend left]
\end{tikzcd}
$$

Generalisations and algorithmic improvements

- Higher genus generalisation by Mestre: theta interpretation of theta AGM;
- Generalisation to the odd characteristic case;
- Algorithmic improvement: compute the canonical lift with a kind of Hensel lift.

We obtain a quasi-quadratic algorithm in n for point counting over $\mathbb{F}_{p^n}$.

Theta functions

Definition

Let $\mathcal{H}_g$ be the Siegel upper-half space. For $a, b \in \mathbb{Q}^g$, and $\Omega \in \mathcal{H}_g$, the theta function with rational characteristics (a, b) is given by:

$$\theta\left[\begin{smallmatrix} ab(z \\ \Omega \end{smallmatrix}\right]) = \sum_{n \in \mathbb{Z}^g} \exp\left[\pi i^t(n+a).\Omega.(n+a) + 2\pi i^t(n+a).(z+b)\right]. \quad (1)$$

Theta functions

Definition

For $\ell \geqslant 2$, let $Z(\ell) = \mathbb{Z}/\ell\mathbb{Z}$, the ℓ^g level ℓ theta functions are:

$$\theta_i(z) = \theta \left[\begin{smallmatrix} 0 i/\ell (z \\ \Omega \end{smallmatrix} \right] /\ell), \text{ for } i \in Z(\ell).$$

- Ω fixed: embedding of $A_\Omega = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$ in $\mathbb{P}^{Z(\ell)}$ if $\ell \geqslant 4$:
$$z \mapsto (\theta_i^A(z)).$$
- $z = 0$: embedding of $\mathcal{A}_g = \mathcal{H}_g/\Gamma$, Γ some congruence subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z})$ in $\mathbb{P}^{Z(\ell)}$:
$$\Omega \mapsto (\theta_i(0, \Omega)).$$

Application to AGM algorithm

Remark

If $\ell = 2$, $\theta_i^A(z) = \theta_i^A(-z)$ and θ_i^A gives an embedding of $K = A/(-1)$ the Kummer variety of A.

Theta function theory gives formulas:

- recover level 2 $\theta_i^A(0)$ from the knowledge of the ramification points of an hyperelliptic curve : Thomae formulas;
- compute 2^g-isogenies: duplications formulas;
- recover $\prod_{i=1}^g \lambda_i$, λ_i Eigenvalues of the Frobenius morphism which are unit mod 2: transformation formula.

Limitation of AGM point counting algorithms

Bad behavior with respect to the genus:

- 2^g coordinates;
- Recovering λ_i from $\prod_{i=1}^g \lambda_i$ is painful:
  - consider P_{sym} symmetric polynomial whose roots are products in pairs $\{\lambda_i, \overline{\lambda_i}\}$;
  - need to increase the precision of computations;
  - LLL algorithm with a matrix of size 2^g
- starting from $g = 4$ does not characterise isogeny class of Abelian varieties (counter example of Mestre).

Aim of this talk

Let X be a curve over $\mathbb{F}_q$, $q = p^n$, let A be a canonical lift of $J(X)$, we explain :

- How to recover $\chi_P(X, T)$;
- More : the similarity class of the action of the Frobenius on differential forms;
- Efficiently : no increase of precision, almost in the same time complexity as the lift step.

We suppose that $p = 2$ for the sake of simplicity.

Notations

- Let X be a curve over $\mathbb{F}_{2^n}$;
- $\overline{A}_0 = J(X)$, A_0 a canonical lift of $\overline{A}_0$;
- v_i (resp. V_i) is the dual of σ_i (resp. Σ_i);
- the absolute Frobenius gives isomorphisms $\overline{A}_{i+1} \simeq \overline{A}_i \otimes_{\sigma_i} \mathbb{F}_{2^n}$ which lifts to $A_{i+1} \simeq A_i \otimes_{\Sigma_i} \mathbb{Q}_{2^n}$

$$
\begin{tikzcd}
A_0 \arrow[r, "\Sigma_0"] \arrow[d] & A_1 \arrow[r, "\Sigma_1"] \arrow[d] & \cdots \arrow[r, "\Sigma_{n-2}"] & A_{n-1} \arrow[d] \arrow[lll, bend right, "\Sigma_{n-1}"'] \\
\overline{A}_0 \arrow[r, "\sigma_0"] & \overline{A}_1 \arrow[r, "\sigma_1"] & \cdots \arrow[r, "\sigma_{n-2}"] & \overline{A}_{n-1} \arrow[lll, bend left, "\sigma_{n-1}"]
\end{tikzcd}
$$

Guiding principle

- Let $\Sigma^q : A_0 \to A_0$ be the q^{th}-Frobenius, V^q its dual;
- Aim : compute $V^{q*} : T_0^*(A_0) \to T_0^*(A_0)$;
- By standard argument it suffices to:
  - Compute the matrix M of

$$V_0^* : T_0^*(A_0) \to T_0^*(A_1)$$

    in basis $(x_i)_{i=1,\dots,g}$ of $T_0^*(A_0)$ and $(x_i \otimes_{\Sigma_0} \mathbb{Q}_{2^n})_{i=1,\dots,g} = (x_i^{\Sigma_0})_{i=1,\dots,g}$ of $T_0^*(A_1)$;
  - Then the matrix of V^{q*} is similar to

$$\mathrm{Norm}_{\mathbb{Q}_{2^n}/\mathbb{Q}_2}(M).$$

Guiding principle

- Generically, level 4 $(\theta_i^{A_0}/\theta_0^{A_0})_{i=1,\dots,g}$ gives local parameters in 0 of A_0;
- Duplication formulas give expression for V_0;
- So what's the problem?

- We lose because we are using 4^g coordinates;
- We would like to stay in level 2 but...
- Level 2 theta functions does not provide an embedding of A_0 but rather that of $K_0 = A_0/(-1)$.

Guiding principle

- Generically, level 4 $(\theta_i^{A_0}/\theta_0^{A_0})_{i=1,\dots,g}$ gives local parameters in 0 of A_0;
- Duplication formulas give expression for V_0;
- So what's the problem?

- We lose because we are using 4^g coordinates;
- We would like to stay in level 2 but...
- Level 2 theta functions does not provide an embedding of A_0 but rather that of $K_0 = A_0/(-1)$.

Outline

1. Generalities about point counting algorithms
2. Mestre's algorithm
3. Improving the AGM point counting algorithm
   - The genus 1 case
   - The genus 2 case
   - The higher genus case

The Kummer line

- $x_{A_0} = \theta_1^{A_0}/\theta_0^{A_0}$ local parameter in 0 of $K_0 = A_0/(-1) \simeq \mathbb{P}^1$;
- Duplication give expression for $V_0 : K_1 \to K_0$:

$$x_{A_0} = \frac{(A+B)x_{A_1}^2 + A - B}{(A-B)x_{A_1}^2 + A + B},$$

A,B depend of level 2 theta constants of A_0 and A_1. Then,

$$dx_{A_0} = dx_{A_1} \frac{4xAB}{(A-B)x^2 + A + B)^2}.$$

The Kummer line

- It seems reasonable to obtain the action of the Frobenius as:

$$\boxed{t = \mathrm{Norm}_{\mathbb{Q}_{2^n}/\mathbb{Q}_2}\left(\sqrt{\frac{4xAB}{(A-B)x^2+A+B)^2}}\right)}.$$

- It works ! Trace of Frobenius morphism up to a sign:

$$\boxed{t + 2^n/t}.$$

Outline

1. Generalities about point counting algorithms
2. Mestre's algorithm
3. Improving the AGM point counting algorithm
   - The genus 1 case
   - The genus 2 case
   - The higher genus case

Some difficulties

- For $g \geqslant 2$, the Kummer line is singular in 0;
- We still have a description of $V_0 : A_1 \to A_0$
- $3 = \dim T_0^* K_0 \geqslant 2$;
- How to recover a 2×2 matrix from a 3×3 matrix?

Tangent cone I

Definition

Let $(R, \mathfrak{M})$ be a local ring, its associated graduated ring is:

$$\mathrm{Gr}(R) = \bigoplus_i \mathfrak{M}^i / \mathfrak{M}^{i+1}.$$

Definition

Let $(V, \mathscr{O})$ an algebraic variety and $x \in V$ a point with associated local ring $(\mathscr{O}_x, \mathfrak{M})$. The tangent cone $T_x^c(V)$ of V in x is $\mathrm{Spec}(\mathrm{Gr}(\mathscr{O}_x))$.

Remark

$\mathfrak{M}/\mathfrak{M}^2$ is the co-tangent space of V in x.

Tangent cone II

Definition

For $P \in R = k[x_1, \ldots, x_g]$ let P_0 be its lowest degree homogeneous component. If $I \subset R$ is an ideal let I_0 be the ideal generated the set $\{P_0, P \in I\}$.

Definition

If V is an affine variety over k with ring of functions $k[x_1, \ldots, x_g]/I$. Suppose that $0 \in V(k)$, $T_0^c(V)$ is the affine variety defined by the ideal I_0.

Tangent cone III

Example

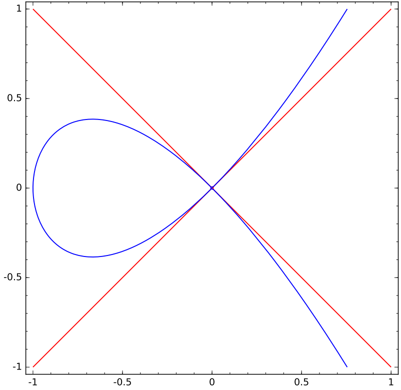
The affine curve:

$$y^2 = x^3 + x^2.$$

has tangent cone in $(0,0)$:

$$y^2 = x^2.$$

Limit of directions lines when approaching $(0,0)$.



Tangent cone IV

Tangent cone generalizes tangent space:

- If R is a regular local ring of dimension g then $\mathrm{Gr}(R) = k[x_1, \dots, x_g] \Rightarrow \mathrm{Spec}(\mathrm{Gr}(R))$ tangent space;
- The dimension of the tangent cone is equal to that of the variety;
- Functoriality property.

Tangent cone and genus 2 Kummer variety

The genus 2 Kummer variety embedded in $\mathbb{P}^3$ with level 2 theta is given:

$$f(x_1, \dots, x_4) = \sum a_i X^i,$$

f homogeneous, $\deg f = 4$. The theta null point (θ_i) verify $f(\theta_i) = 0$. Compute its tangent cone:

- make affine: $f_a(x_1, x_2, x_3) = f(x_1, x_2, x_3, 1)$, $\deg f_a = 4$;
- localize around the origin: $f_{loc}(\vartheta_i) = f_a(x_i + \frac{\theta_i}{\theta_4})$;
- write $f_{loc}(\vartheta_i) = \sum_j h_j(\vartheta_i)$, where h_j degree i homogeneous component;
- $h_0 = h_1 = 0$, $h_2(\vartheta_i) = Q_f(\vartheta_i) \neq 0$ is the quadratic equation of the tangent cone at the origin.

An idea

$$\begin{tikzcd} A \arrow[loop above, "-1"] \arrow[d] \\ K \end{tikzcd} \qquad \begin{tikzcd} \mathrm{Spec}(k[x_1,x_2]) \arrow[loop above, "-1"] \arrow[d] \\ ? \end{tikzcd}$$

An idea

$$\begin{tikzcd} A \arrow[loop above, "-1"] \arrow[d] \\ K \end{tikzcd} \qquad \begin{tikzcd} \mathrm{Spec}(k[x_1,x_2]) \arrow[loop above, "-1"] \arrow[d] \\ k[x_1^2, x_2^2, x_1 x_2] \end{tikzcd}$$

An idea

$$\begin{tikzcd} A \arrow[loop above, "-1"] \arrow[d] \\ K \end{tikzcd} \qquad \begin{tikzcd} \mathrm{Spec}(k[x_1,x_2]) \arrow[loop above, "-1"] \arrow[d] \\ \dfrac{k[u,v,w]}{uv-w^2} \end{tikzcd}$$

An idea

$$\begin{tikzcd} A \arrow[loop above, "\Sigma^q"] \arrow[d] \\ K \end{tikzcd}$$

$$\begin{tikzcd} \mathrm{Spec}(k[x_1,x_2]) \arrow[loop above, "\Sigma"] \arrow[d] \\ \frac{k[u,v,w]}{uv-w^2} \end{tikzcd}$$

Action of Σ on $k[x_1, x_2]$:

$$\Sigma(x_1) = ax_1 + bx_2$$

$$\Sigma(x_2) = cx_2 + dx_2$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k)$$

An idea

$$\begin{tikzcd} A \arrow[loop above, "\Sigma^q"] \arrow[d] \\ K \end{tikzcd}$$

$$\begin{tikzcd} \mathrm{Spec}(k[x_1,x_2]) \arrow[loop above, "\Sigma"] \arrow[d] \\ \frac{k[u,v,w]}{uv-w^2} \end{tikzcd}$$

Action of Σ on $k[x_1^2, x_2^2, x_1x_2]$:

$$\Sigma(x_1^2) = a^2x_1^2 + b^2x_2^2 + 2abx_1x_2$$

$$\Sigma(x_2^2) = c^2x_1^2 + d^2x_2^2 + 2cdx_1x_2$$

$$\Sigma(x_1x_2) = acx_1^2 + bdx_2^2 + (ad + bc)x_1x_2$$

$$M = \begin{pmatrix} a^2 & b^2 & 2ab \\ c^2 & d^2 & 2cd \\ ac & db & (ad+bc) \end{pmatrix} \in \mathrm{SO}(Q)$$

$$Q = uv - w^2$$

An idea

$$\begin{tikzcd} A \arrow[loop above, "\Sigma^q"] \arrow[d] \\ K \end{tikzcd} \qquad \begin{tikzcd} \mathrm{Spec}(k[x_1,x_2]) \arrow[loop above, "\Sigma"] \arrow[d] \\ \frac{k[u,v,w]}{uv-w^2} \end{tikzcd}$$

Action of Σ on $k[x_1^2, x_2^2, x_1x_2]$:

$$\Sigma(x_1^2) = a^2x_1^2 + b^2x_2^2 + 2abx_1x_2$$

$$\Sigma(x_2^2) = c^2x_1^2 + d^2x_2^2 + 2cdx_1x_2$$

$$\Sigma(x_1x_2) = acx_1^2 + bdx_2^2 + (ad+bc)x_1x_2$$

$$M = \begin{pmatrix} a^2 & b^2 & 2ab \\ c^2 & d^2 & 2cd \\ ac & db & (ad+bc) \end{pmatrix} \in \mathrm{SO}(Q)$$

$$Q = uv - w^2$$

Remark

From M we recover $\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

A first result

Proposition

Let $(R, \mathfrak{M})$ be a dimension 2 regular local ring over k and let σ be an automorphism of R which acts like (-1) on $\mathfrak{M}/\mathfrak{M}^2$. Then:

$$\kappa : \mathrm{Gr}(R^\sigma) \simeq (\mathrm{Gr} R)^\sigma.$$

Remark

Let x_1, x_2 be local parameters of R:

- $(\mathrm{Gr} R) = k[x_1, x_2]$, $(\mathrm{Gr} R)^\sigma = k[x_1^2, x_2^2, x_1 x_2]$;
- *If R is the local ring at origin of A then $\mathrm{Gr}(R^\sigma)$ is the coordinate ring of $T_0^c(K)$;*
- *Isomorphism between $T_0^c(K)$ and "standard" tangent cone.*

An idea

$$\begin{tikzcd}
T_0^*(A_0), (x_1, x_2) \arrow[r, "M(V_0^*) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}"] \arrow[d] & T_0^*(A_1), (x_1, x_2) \otimes_\Sigma \mathbb{Q}_{2^n} \arrow[d] \\
T_c^*(K_0), (x_1^2, x_2^2, x_1 x_2) \arrow[r, "\begin{pmatrix} a^2 & b^2 & 2ab \\ c^2 & d^2 & 2cd \\ ac & bd & ad+bc \end{pmatrix}"] \arrow[d, "\kappa"'] & T_c^*(K_1), (x_1^2, x_2^2, x_1 x_2) \otimes_\Sigma \mathbb{Q}_{2^n} \arrow[d, "\kappa \otimes_\Sigma \mathbb{Q}_{2^n}"] \\
T_c^*(K_0), (\vartheta_i) \arrow[r, "M_c(V_0^*)"] & T_c^*(K_1), (\vartheta_i) \otimes_\Sigma \mathbb{Q}_{2^n}
\end{tikzcd}$$

We want to compute:

$$\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 & b^2 & 2ab \\ c^2 & d^2 & 2cd \\ ac & bd & ad+bc \end{pmatrix} = (M_\kappa \otimes_\Sigma \mathbb{Q}_{2^n})^{-1} M_c(V_0^*) M_\kappa .$$

A second good news

Keeping the notations of the proposition:

Proposition

The isomorphism $\kappa : (\mathrm{Gr} R^\sigma) \simeq (\mathrm{Gr} R)^\sigma$ *is linear. Let* T *be the matrix of this ismorphism in the basis* $(x_1^2, x_2^2, x_1 x_2)$ *and* (ϑ_i)*:*

$$^t T\, M(Q_f)\, T = M(Q),$$

$M(Q_f)(\vartheta_i)$ *matrix of* Q_f *and* $M(Q) = M(uv - w^2) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}$.

Because...

- κ induce a linear isomorphism $k[x_1^2, x_2^2, x_1 x_2] \to \mathfrak{M}_{R^\sigma}/\mathfrak{M}_{R^\sigma}^2$;
- but such a linear isomorphism determines uniquely κ;
- moreover $\kappa^*(Q_f) = Q$.

Computing the matrix M

Computing M:

- $Q = uv - w^2$ is the orthogonal sum of an hyperbolic plane and definite one dimensional quadratic form;
- to compute M:
  1. find an isotropic vector v for Q_f;
  2. take any w such that $Q_f(v, w) \neq 0$;
  3. find λ such that $w' = w + \lambda v$, $Q_f(w') = 0$ and scale s.t. $Q_f(v, w') = 1$;
  4. compute an orthogonal vector to the plane (v, w').

Finding an isotropic vector

- Use Gram-Schmidt : we have to solve $Q_f \sim aX^2 + bY^2 + cZ^2 \sim X^2 + baY^2 + caZ^2 = 0$
- If $-ba$ is a square α^2 in $\mathbb{Q}_{2^n}$ then $(\alpha, 1, 0)$ is a solution;
- If no we have to solve a norm equation in $\mathbb{Q}_{2^n}(\sqrt{-ab})$: efficient algorithm.

A new problem

Remark

If M is such that ${}^t M\, M(Q_f)\, M = M(Q)$ then for any $T \in SO(Q)$ MT is another solution !

The fix

Proposition

We have an exact sequence:

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow Sl_2(\mathbb{Q}_{2^r}) \xrightarrow{\mu} SO(Q) \longrightarrow 0$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} a^2 & b^2 & 2ab \\ c^2 & d^2 & 2cd \\ ac & bd & ad+bc \end{pmatrix}$$

The fix II

$$
\begin{tikzcd}
T_0^*(A_0),(x_1',x_2') \arrow[r, "T"] \arrow[d] & T_0^*(A_0),(x_1,x_2) \arrow[r, "M(V_0^*)"] \arrow[d] & T_0^*(A_1),(x_1,x_2)^\Sigma \arrow[d] & T_0^*(A_1),(x_1',x_2')^\Sigma \arrow[l, "T^\Sigma"'] \arrow[d] \\
T_c^*(K_0),(u',v',w') \arrow[r, "\mu(T)"] \arrow[dr, "\kappa'"] & T_c^*(K_0),(u,v,w) \arrow[r, "\mu(M(V_0^*))"] \arrow[d, "\kappa"] & T_c^*(K_1),(u,v,w)^\Sigma \arrow[r, "\mu(T^\Sigma)"] \arrow[d, "\kappa^\Sigma"] & T_c^*(K_1),(u',v',w')^\Sigma \arrow[dl, "\kappa'^\Sigma"] \\
& T_c^*(K_0),(\vartheta_i) \arrow[r, "M_c(V_0^*)"] & T_c^*(K_1),(\vartheta_i)^\Sigma &
\end{tikzcd}
$$

- what we are computing is $\pm T\, M_\Sigma\, T^{\Sigma-1}$;
- taking the norm we obtain: $\pm T\, M_{\Sigma^q}\, T^{-1}$ same similarity class as M_{Σ^q}.

Description of the algorithm

- **Input** : (θ_i) the theta null point of a canonical lift of $J(X)$ (up to the right p-adic precision);
- **Output** : $\chi_1(X, T)$;

1. compute the quadratic equation Q_f of $T_c(K_0)$;
2. compute a matrix M such that ${}^t M\, Q_f\, M = Q$;
3. compute the matrix of $M_c(V_0^*)$ of partial derivatives of the dual of the Frobenius;
4. compute $M_0 = M^{-1}\, M_c(V_0^*)\, M^{\Sigma}$;
5. compute $Norm_{\mathbb{Q}_{2^n}/\mathbb{Q}_2}(M_0) = \begin{pmatrix} a^2 & b^2 & 2ab \\ c^2 & d^2 & 2cd \\ ac & bd & ad+bc \end{pmatrix}$;
6. recover $M = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and compute $\det(M - TI)$.

Some remarks

Remark

- *It can be shown that the coefficients of M are in $\mathbb{Q}_{2^n}$ and its trace and determinant are in $\mathbb{Q}_2$.*
- *The matrix T s.t. ${}^tT\,M(Q_f)\,T = M(Q)$ is not in general defined over $\mathbb{Q}_{2^n}$. We have to work with the basis tx_1^2, x_2^2, x_1x_2 in order to stay rational and pay attention to the fact that the Frobenius morphism is semi-linear.*

Outline

1. Generalities about point counting algorithms
2. Mestre's algorithm
3. Improving the AGM point counting algorithm
   - The genus 1 case
   - The genus 2 case
   - The higher genus case

List of ingredients to generalize

We have to generalize:

- Equations for K_0 embedded with 2 theta functions;
- Isomorphism between $T_c^*(K_0)$ and normalized tangent cone;
- Equations for $T_c^*(K_0)$;
- Computation of the isomorphism;
- Computation of the matrix $M_c(V_0^*)$;
- Recovering the dual of the Frobenius matrix.

List of ingredients to generalize

We have to generalize:

- Equations for K_0 embedded with 2 theta functions;
- Isomorphism between $T_c^*(K_0)$ and normalized tangent cone;
- Equations for $T_c^*(K_0)$;
- Computation of the isomorphism;
- Computation of the matrix $M_c(V_0^*)$;
- Recovering the dual of the Frobenius matrix.

List of ingredients to generalize

We have to generalize:

- Equations for K_0 embedded with 2 theta functions;
- Isomorphism between $T_c^*(K_0)$ and normalized tangent cone;
- Equations for $T_c^*(K_0)$;
- Computation of the isomorphism;
- Computation of the matrix $M_c(V_0^*)$;
- Recovering the dual of the Frobenius matrix.

List of ingredients to generalize

We have to generalize:

- Equations for K_0 embedded with 2 theta functions;
- Isomorphism between $T_c^*(K_0)$ and normalized tangent cone;
- Equations for $T_c^*(K_0)$;
- Computation of the isomorphism;
- Computation of the matrix $M_c(V_0^*)$;
- Recovering the dual of the Frobenius matrix.

Normalized tangent cone

Remark

The normalized tangent cone has coordinate ring:

$$k[x_i^2, x_i x_j | i = 1 \dots g, j = 1 \dots g] = \frac{k[u_i, w_{ij}]}{u_i u_j - w_{ij}^2}$$

It is a g-dimensional variety embedded in a $g(g+1)/2$ tangent space.

The proof of the isomorphism is the same.

A funny side remark

Remark

A consequence of the isomorphism is that the tangent space in 0 *of* K_0 *has dimension* $g(g+1)/2$*.*

List of ingredients to generalize

We have to generalize:

- Equations for K_0 embedded with 2 theta functions;
- Isomorphism between $T_c^*(K_0)$ and normalized tangent cone;
- Equations for $T_c^*(K_0)$;
- Computation of the isomorphism;
- Computation of the matrix $M_c(V_0^*)$;
- Recovering the dual of the Frobenius matrix.

List of ingredients to generalize

We have to generalize:

- Equations for K_0 embedded with 2 theta functions;
- Isomorphism between $T_c^*(K_0)$ and normalized tangent cone;
- Equations for $T_c^*(K_0)$;
- Computation of the isomorphism;
- Computation of the matrix $M_c(V_0^*)$;
- Recovering the dual of the Frobenius matrix.

List of ingredients to generalize

We have to generalize:

- Equations for K_0 embedded with 2 theta functions;
- Isomorphism between $T_c^*(K_0)$ and normalized tangent cone;
- Equations for $T_c^*(K_0)$;
- Computation of the isomorphism;
- Computation of the matrix $M_c(V_0^*)$;
- Recovering the dual of the Frobenius matrix.

List of ingredients to generalize

We have to generalize:

- Equations for K_0 embedded with 2 theta functions;
- Isomorphism between $T_c^*(K_0)$ and normalized tangent cone;
- Equations for $T_c^*(K_0)$;
- Computation of the isomorphism;
- Computation of the matrix $M_c(V_0^*)$;
- Recovering the dual of the Frobenius matrix.

A problem

- The tangent cone is embeded in $\mathbb{P}^{2^g-1}$;
- Closed subvariety given by $\mathcal{E}_1, \ldots, \mathcal{E}_k$ equations $k \geqslant 2^g - 1 - g$;
- Let $I_1 = (\mathcal{E}_{i,0})$;
- Problem $I_1 \neq I_0 = \{P_0 | P \in I\}$;
- Burberger like algorithm to compute the tangent cone: very inefficient;
- In the $\mathcal{E}_{i,0}$ there are:
  - at least $2^g - 1 - g(g+1)/2$ linear equations $\{\mathcal{E}_{i,0}\}_{i \in L}$;
  - equations of degree 2: $\{\mathcal{E}_{i,0}\}_{i \in M}$;
  - equations of degree $\geqslant 2$.

Tangent cone (almost) for free

Proposition

The degree 1 and 2 equations $\{\mathcal{E}_{i,0}\}_{i \in L}$ and $\{\mathcal{E}_{i,0}\}_{i \in M}$ generate the ideal of the tangent cone of K_0.

- Normalized tangent cone:
  - has dimension g;
  - $g(g-1)/2$ equations inside a space of dimension $g(g+1)/2$.
  - degree of the variety: $2^{g(g-1)/2}$.
- Kummer tangent cone $T_c(K_0)$:
  - at least $g(g-1)/2$ equations;
  - of degree $\geqslant 2$, if equations of degree > 3 $\deg(T_c(K_0)) > 2^{g(g-1)/2}$ contradiction.

List of ingredients to generalize

We have to generalize:

- Equations for K_0 embedded with 2 theta functions;
- Isomorphism between $T_c^*(K_0)$ and normalized tangent cone;
- Equations for $T_c^*(K_0)$;
- Computation of the isomorphism;
- Computation of the matrix $M_c(V_0^*)$;
- Recovering the dual of the Frobenius matrix.

Computation of the isomorphism of tangent cones

- The underlying problem is difficult but:
- no need to be smart: it involves computing with $g \times g$ matrices;
- We have somewhat good solution involving computing determinant of matrices.

A word about the complexity

- Dominant step : computation of the tangent space;
- Gaussian elimination in a matrix of dimension 2^g with coefficients in $\mathbb{Z}_{2^n}$ with precision $n^{g/2}$;
- Time complexity: $O(2^{3g} n^{g/2})$.

The end

Questions ?