Fast change of level and applications to isogenies

David Lubicz, Damien Robert

Université de Rennes 1 and Mathematic Institute of Bordeaux.

Outline

Outline

The aim of this talk

In this talk, we are going to present:

- change of level algorithm for theta functions;
- an application to isogeny computation between Abelian varieties.

The results apply to a fairly general situation (Abelian varieties of any dimension over any base field) but we will specialize to $\mathbb{C}$ for the sake of simplicity.

Abelian varieties

Definition

An Abelian variety is a smooth complete connected group variety over a base field k.

Abelian variety = subset of a projective space given as the zero of homogeneous polynomials together with an Abelian group law given by rational functions .

Example

- Elliptic curves= Abelian varieties of dimension 1;
- If C is a (smooth) curve of genus g, its Jacobian is an Abelian variety of dimension g;
- In dimension $g \geqslant 4$, not every Abelian variety is a Jacobian.

Abelian varieties over $\mathbb{C}$

- In this talk, we consider Abelian varieties over $\mathbb{C}$;
- Let $\mathbb{H}_g$ be the Siegel upper-half space;
- For $\Omega \in \mathbb{H}_g$, let $\Lambda_\Omega = \mathbb{Z}^g + \Omega\mathbb{Z}^g \subset \mathbb{C}^g$.

Definition

- The analytic Abelian variety A associated to Ω is $\mathbb{C}^g/\Lambda_\Omega$;
- A (principally polarized) Abelian variety A over $\mathbb{C}$ is isomorphic to an analytic Abelian variety.

Projective embedding

- Let $\Lambda = \mathbb{Z}^g + \Omega\mathbb{Z}^g$;
- A projective embedding of $A = \mathbb{C}^g/\Lambda$ can be given by quasi-periodic functions with respect to Λ.

Definition

A Λ-quasi-periodic function of level n is a function f on $\mathbb{C}^g$ such that for all $z \in \mathbb{C}^g$ and $\lambda \in \mathbb{Z}^g$:

$$f(z+\lambda) = f(z), \quad f(z+\Omega\lambda) = \exp(-\pi i \, n \, {}^t\lambda\Omega\lambda - 2\pi i \, n \, {}^t z\lambda) f(z).$$

Let R_Ω^n be a vector space of level n functions.

Theta functions I

Definition

For $a, b \in \mathbb{Q}^g$, the theta function with rational characteristics (a, b) is a function $\mathbb{C}^g \times \mathbb{H}_g \to \mathbb{C}$ given by:

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

Theta functions II

Definition

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

$$\theta_i(z) = \theta \begin{bmatrix} 0 \\ i/n \end{bmatrix} (z, \Omega/n), \text{ for } i \in Z(n).$$

- The $(\theta_i(z))_{i \in \mathbb{Z}(n)}$ form a basis a R_Ω^n.
- An embedding of $A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$ in $\mathbb{P}^{Z(n)}$ if $n \geqslant 3$:

$$\varphi_{n,\Omega} : z \mapsto (\theta_i(z))_{i \in Z(n)}.$$

- The point $\varphi_{n,\Omega}(0) \in \mathbb{P}^{Z(n)}(\mathbb{C})$ is called the Theta null point of $\varphi_{n,\Omega}$.

Change of level algorithm

Definition

Let ℓ, n positive integers, a change of level algorithm is an algorithm to compute a theta basis of R^n_Ω from the knowledge of a theta basis $R^{\ell n}_\Omega$ (going down) and the other way around (going up).

Previous results:

- duplication formula: going up from level n to level $2n$ and the other way around.
- Koizumi formula: going down from the level ℓn to level n.

We want to expand these results and improve the complexity of change of level algorithms.

Algebraic representation

We suppose that n is even:

- The Theta null point $\varphi_{n,\Omega}(0)$ is rational.
- Riemann's equations parametrized by $\varphi_{n,\Omega}(0)$ provides a complete set of quadratic equation for $\varphi_{n,\Omega}(\mathbb{C}^g)$.
- Riemann's equations allows to recover the arithmetic of A inside $\mathbb{P}^{Z(n)}$.
- Theta functions can be regarded as sections of the line bundle $\mathscr{L}^n = \varphi_{n,\Omega}^*(\mathscr{O}_{\mathbb{P}^{Z(n)}}(1))$ (where $\mathscr{L}$ is a principal line bundle).

Locus of theta null points

It is clear that from Ω one can recover the theta null point $\varphi_{n,\Omega}(0)$. Reciprocally, we have:

Theorem (Mumford-Kempf)

If $n \geqslant 4$ even, the function of Ω, $\varphi_{n,\Omega}(0)$ is an embedding of $\mathcal{A}_g(n) = \mathbb{H}_g/\Gamma(n,2n)$ into $\mathbb{P}^{Z(n)}$, where $\Gamma(n,2n)$ is a congruence subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z})$ (Igusa level n subgroups).

Theta structure

The following data are equivalent:

- A theta null point $\varphi_{n,\Omega}(0)$;
- A point of $\mathcal{A}_g(n)$;
- A suitable basis $(\theta_i(z))_{i \in Z(n)}$ of $H^0(\mathscr{L}^n)$.

Definition

We call it a level n (symmetric) theta structure .

If Θ^n is a level n theta structure for A, we denote by $\varphi^{\Theta^n} : A \to \mathbb{P}^{Z(n)}$ the associated embedding.

Compatible theta structure

Definition

Two theta structures of level n_1 and n_2 given by $\Omega_1, \Omega_2 \in \mathbb{H}_g$ are compatible if there exists ℓ such that $n_1 = \ell n_2$ and there exists $\Omega \in \mathbb{H}_g$ such that $\Omega/n_i \cong \Omega_i \mod \Gamma(n_i, 2n_i)$ for $i = 1, 2$.

Outline

Change of level algorithms

Let ℓ and n be two relatively prime integers, let $(A, \Theta_A^{\ell n})$ be an Abelian variety together with a level ℓn theta structure:

- From $\varphi^{\Theta^{\ell n}}(0)$, one can recover $A[\ell] = A_1[\ell] \oplus A_2[\ell]$ a symplectic decomposition for the Weil pairing.
- Reciprocally, given (A, Θ_A^n) by $\varphi^{\Theta_A^n}(0)$ and $A[\ell] = A_1[\ell] \oplus A_2[\ell]$ can we compute $\varphi^{\Theta_A^{\ell n}}(0)$?

A result

Theorem

Let (A, Θ_A^n) and let $A[\ell] = A_1[\ell] \oplus A_2[\ell]$ be a symplectic decomposition for the Weil pairing. Suppose ℓ odd, there exists a unique theta structure $\Theta_A^{\ell n}$ compatible with the preceding data. One can compute $\varphi^{\Theta^{\ell n}}(0)$ from the knowledge of $\varphi^{\Theta^n}(0)$ and the decomposition $A[\ell] = A_1[\ell] \oplus A_2[\ell]$ at the expense of $O(n^g \ell^{2g} \log(\ell))$ operations in the base field.

We have a similar result for going down with complexity $O(n^g \ell^g log(\ell))$.

Outline

Link with isogeny computations

The problem:

- Let A an Abelian variety and K an isotropic sub-group of $A[\ell]$ for the Weil pairing;
- Compute $B = A/K$ and the isogeny $f : A \to B$.

Representation:

- A is given by its theta null point of level n (n^g coordinates);
- K is given as a subvariety of $A \subset \mathbb{P}^{Z(n)}$.

Previous results

To compute isogenies, we have at least the following general algorithms:

- dimension 1: Vélu's formula;
- dimension g, ℓ-isogenies Cosset-L.-Robert :
  - $\widetilde{O}(\ell^g)$ if $\ell \equiv 1 \mod 4$;
  - $\widetilde{O}(\ell^{2g})$ if $\ell \equiv 3 \mod 4$.
- dimension g, cyclic isogenies Dudeau-Jetchev-Robert-Vuile, linear complexity but not practical;
- dimension 2: Couveignes, ℓ-isogenies in $\widetilde{O}(\ell^2)$.

Link with change of level

We have to endow B with a theta structure Θ_B^n. Two approaches:

- Compute $\hat{f}^*(\Theta_A^n)$ via the isogeny theorem (a level ℓn theta structure for B), then going down from level ℓn to level n:

$$\begin{tikzcd}
 & (B, \hat{f}^*(\Theta_A^n)) \arrow[dl, "\hat{f}"'] \arrow[d] \\
(A, \Theta_A^n) & (B, \Theta_B^n)
\end{tikzcd}$$

- go up from level n to level ℓn then compute f via the isogeny theorem:

$$\begin{tikzcd}
(A, \Theta_A^{n\ell}) \arrow[dr, "f"] & \\
(A, \Theta_A^n) \arrow[u] & (B, \Theta_B^n)
\end{tikzcd}$$

A result

Theorem

Let (A, Θ_A^n) an Abelian variety. Let $K \subset A[\ell]$ be a subgroup isotropic for the Weil pairing and let $B = A/K$. One can compute the theta null point associated to (B, Θ_B^n) and the isogeny $f : A \to B$ in time $O((n\ell)^g \log(\ell))$ operations in the base field.

Representations

For practical implementation, we work in:

- level 4: 4^g coordinates, gives a projective embedding of A;
- level 2: 2^g coordinates, gives a projective embedding of $K = A/(-1)$.

Computation of level 2 or 4 theta null points:

- via Thomae's like formulas when $A = J(C)$;
- by picking up a point of $\mathcal{A}_g(4)$ a projective embedding of which is given by Riemann and symmetry equations.

Implementations

There are two implementations available:

- a magma implementation: AVIsogeny by Bisson-Cosset-Robert.
- a sagemath implementation by Somoza.

All the details and link to implementations are in the paper !

Other applications and open questions

Ohter application of change of level formulas:

- Higher level Thomae formulas;
- Computation of modular functions of arbitrary level.

Open question:

- The case $\ell = 2$;
- Change of level algorithm to compute modular forms.

Thanks for your attention