

# Fast change of level and applications to isogenies

**David Lubicz**, Damien Robert

Université de Rennes 1 and Mathematic Institute of Bordeaux.

# Outline

- 1 Introduction
- 2 The results
- 3 Consequences

# Outline

- 1 Introduction
- 2 The results
- 3 Consequences

# 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  $g \geq 4$ , 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  $\Omega$  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  $\Lambda$ .

## Definition

A  $\Lambda$ -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  $R_\Omega^n$  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  $\mathbb{C}^g \times \mathbb{H}_g \rightarrow \mathbb{C}$  given by:

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



# Theta functions II

## Definition

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

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

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

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

- 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  $\ell, n$  positive integers, a **change of level algorithm** is an algorithm to compute a theta basis of  $R_{\Omega}^n$  from the knowledge of a theta basis  $R_{\Omega}^{\ell n}$  (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  $\ell n$  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  $\mathcal{L}^n = \varphi_{n,\Omega}^*(\mathcal{O}_{\mathbb{P}^{Z(n)}}(1))$  (where  $\mathcal{L}$  is a principal line bundle).

# Locus of theta null points

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

## Theorem (Mumford-Kempf)

*If  $n \geq 4$  even, the function of  $\Omega$ ,  $\varphi_{n,\Omega}(0)$  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  $H^0(\mathcal{L}^n)$ .

## Definition

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

If  $\Theta^n$  is a level  $n$  theta structure for  $A$ , we denote by  $\varphi^{\Theta^n} : A \rightarrow \mathbb{P}^{Z(n)}$  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  $\ell$  such that  $n_1 = \ell n_2$  and there exists  $\Omega \in \mathbb{H}_g$  such that  $\Omega/n_i \cong \Omega_i \pmod{\Gamma(n_i, 2n_i)}$  for  $i = 1, 2$ .

# Outline

- 1 Introduction
- 2 The results
- 3 Consequences

# Change of level algorithms

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

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

- 1 Introduction
- 2 The results
- 3 Consequences**

# 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  $f : A \rightarrow B$ .

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

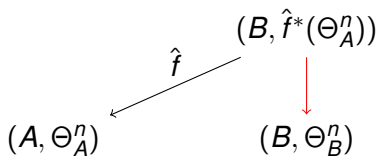
To compute isogenies, we have at least the following general algorithms:

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

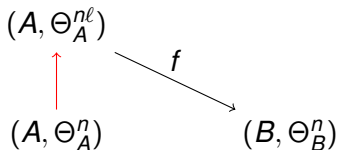
# Link with change of level

We have to endow  $B$  with a theta structure  $\Theta_B^n$ . Two approaches:

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



- go up from level  $n$  to level  $\ell n$  then compute  $f$  via the isogeny theorem:



# A result

## Theorem

*Let  $(A, \Theta_A^n)$  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  $(B, \Theta_B^n)$  and the isogeny  $f : A \rightarrow B$  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

Other 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