UNIVERSITÄT BAYREUTH

university of groningen

Explicit methods for hyperelliptic genus 4 Kummer varieties

Ludwig Fürst

Rational Points 2022

Schney
28.03.2022

Outline

- General Setup
- Explicit results for $g < 4$
- The case $g = 4$

General Setup

Let $F(X,Z) = f_0 Z^{2g+2} + \ldots + f_{2g+2} X^{2g+2}$ be a homogeneous polynomial of degree 2g+2 over a number field k with $Disc(F) \neq 0$, then $Y^2 = F(X,Z)$ defines a nonsingular curve C of genus g in the weighted projective plane (1 : g+1 : 1).

To this curve we associate its Jacobian $J(C) = Pic^0(C)$ and its Kummer variety $K(C) = J(C) / (-1)$.

The Kummer variety retains traces of the group law on the Jacobian such as *scalar multiplication*, addition of the *2-Torsion*, *Pseudo-Addition* and the notion of the *height of points*. Using the linear system of twice a Theta-divisor, we can embed K into the projective space of dimension 2^g-1.

Using such an embedding, we can make the above explicit.

The cases g < 4

- For *g=2* an embedding and many related objects have been constructed by *Flynn* (1993) and generalized by *Duquesne* (2007) and *Müller* (2010).

  The theory of heights was further developed by *Stoll* (1999,2002) and *Müller*,*Stoll* (2016).

- For *g=3* in the case of odd degree an embedding has been found by *Stubbs* (2000) in his thesis. This was further studied by *Duquesne* (2001) and *Müller* (2012). The general case was analyzed extensively in *Stoll* (2017).

- Some results have been found for arbitrary genus. So developed *Holmes* and *Müller* an height algorithm on the Jacobian using Arakelov intersection theory.

The case g = 4

For the following situations I found an explicit description:

- Embedding of the (dual) Kummer variety
- Defining equations of the Kummer (*)
- Addition of J[2]
- Duplication formulas
- Height algorithm (*)
- Pseudo-Addition (*)
- Lifting of points to the Jacobian

Embedding

- I represent a point on the Jacobian using the reduced *Mumford representation* (A,B,C) with $F = B^2 - AC$. This is in g = 4 *unique up to scaling and B mod A*. Behind this is the identification of J with $Pic^4(C)$.

- For a divisor of degree 4 (i.e. deg(A) = 4, deg(B) = 5, deg(C) = 6) we find functions on the Jacobian as invariant polynomials in the coefficients with certain weights.

  Using this I find a basis for L(2Θ) which gives my embedding $J \to K \to \mathbb{P}^{15}$

- The image of divisors of degree 2 can be found via a *specialization argument*

- The *dual* of the Kummer comes from $Pic^5(C)$ and corresponds to representations (A,B,C) with odd degree. Here I find a basis similar to the case of genus 3.

```
k1 := a0;
k2 := a1;
k3 := a2;
k4 := a3;
k5 := a4;

k6 := a0*a1*c3 - a0*b2^2 + a1*a3*c0 - 2*a1*b0*b3 - a2^2*c0 + 2*a2*b0*b2;
k7 := a0*a1*c4 + a0*a2*c3 - 2*a0*b2*b3 + a1*a4*c0 - 2*a1*b0*b4 - a2*a3*c0 + 2*a3*b0*b2;
k8 := a0*a2*c4 - a0*b3^2 + a2*a4*c0 - 2*a2*b0*b4 - a3^2*c0 + 2*a3*b0*b3;
k9 := -a0^2*c6 - a0*a4*c2 + 2*a0*b1*b5 - 2*a1*b0*b5 - a2*a4*c0 + 2*a4*b0*b2;
k10:= -a1*a3*c3 + a1*b3^2 + a2^2*c3 - 2*a2*b2*b3 + a3*b2^2;
k11:= -a0*a1*c6 - a0*a4*c3 + 2*a0*b2*b5 - 2*a2*b0*b5 - a3*a4*c0 + 2*a4*b0*b3;
k12:= -a0*a2*c6 - a0*a4*c4 + 2*a0*b3*b5 - 2*a3*b0*b5 - a4^2*c0 + 2*a4*b0*b4;
k13:= a0*a2*c6 - a1^2*c6 + 2*a1*b2*b5 + a2*a4*c2 - 2*a2*b1*b5 - a4*b2^2;
k14:= a0*a3*c6 - a1*a2*c6 + 2*a1*b3*b5 + a2*a4*c3 + a3*a4*c2 - 2*a3*b1*b5 - 2*a4*b2*b3;
k15:= a1*a3*c6 - a2^2*c6 + 2*a2*b3*b5 + a3*a4*c3 - 2*a3*b2*b5 - a4*b3^2;

k16:= -a0^2*a2*c4*c6 + a0^2*b3^2*c6 + a0*a1^2*c4*c6 - 2*a0*a1*b2*b3*c6 - 2*a0*a1*b2*b5*c4 + 2*a0*a1*b3*b5*c3 -
 a0*a2*a4*c0*c6 - a0*a2*a4*c2*c4 + a0*a2*a4*c3^2 + 2*a0*a2*b0*b4*c6 + 2*a0*a2*b1*b5*c4 + a0*a2*b2^2*c6 -
 2*a0*a2*b2*b5*c3 + a0*a3^2*c0*c6 - 2*a0*a3*b0*b3*c6 + a0*a4*b2^2*c4 - 2*a0*a4*b2*b3*c3 + a0*a4*b3^2*c2 -
 2*a0*b1*b3^2*b5 + 2*a0*b2^2*b3*b5 + a1^2*a4*c0*c6 - 2*a1^2*b0*b4*c6 - 2*a1*a2*a3*c0*c6 + 2*a1*a2*b0*b3*c6 +
 2*a1*a3*b0*b2*c6 - 2*a1*a3*b0*b5*c3 + 2*a1*a3*b3*b5*c0 - 2*a1*a4*b2*b5*c0 + 4*a1*b0*b2*b4*b5 -
 2*a1*b0*b3^2*b5 + a2^3*c0*c6 - 2*a2^2*b0*b2*c6 + 2*a2^2*b0*b5*c3 - 2*a2^2*b3*b5*c0 + 2*a2*a3*b2*b5*c0 -
 a2*a4^2*c0*c2 - 2*a2*a4*b0*b3*c3 + 2*a2*a4*b0*b4*c2 + 2*a2*a4*b1*b5*c0 + a2*a4*b3^2*c0 - 4*a2*b0*b1*b4*b5 +
 a3^2*a4*c0*c2 - 2*a3^2*b1*b5*c0 + 2*a3*a4*b0*b2*c3 - 2*a3*a4*b0*b3*c2 - 2*a3*a4*b2*b3*c0 +
 4*a3*b0*b1*b3*b5 - 2*a3*b0*b2^2*b5 + a4^2*b2^2*c0 - 2*a4*b0*b2^2*b4 + 2*a4*b0*b2*b3^2;
```

Picture 1: Basis for the Kummer variety

$$(0:0:0:0:0:$$

$$a_0^3 : a_0^2 a_1 : -a_0^2 a_2 + a_0 a_1^2 : a_0^2 a_2 : 2a_0 a_1 a_2 - a_1^3 : a_0 a_1 a_2 : a_0 a_2^2 : -a_0 a_2^2 + a_1^2 a_2 : a_1 a_2^2 : a_2^3 :$$

$$-a_0^4 c_8 + 2a_0^3 b_3 b_5 - 2a_0^2 a_1 b_2 b_5 + a_0^2 a_2^2 c_4 - 2a_0^2 a_2 b_1 b_5 - a_0^2 a_2 b_3^2 - a_0 a_1^2 a_2 c_4 + 2a_0 a_1^2 b_1 b_5 +$$
$$4a_0 a_1 a_2 b_0 b_5 + 2a_0 a_1 a_2 b_2 b_3 - 2a_0 a_2^2 b_0 b_4 - a_0 a_2^2 b_2^2 - 2a_1^3 b_0 b_5 + 2a_1^2 a_2 b_0 b_4 - 2a_1 a_2^2 b_0 b_3 -$$
$$a_2^4 c_0 + 2a_2^3 b_0 b_2)$$

Picture 2: Image of a degree 2 divisor

$$\eta_{ii} = b_i^2 - a_i c_i$$

$$\eta_{ij} = 2b_i b_j - a_i c_j - a_j c_i \text{ for } i < j$$

$$(1 : -\eta_{02} : \eta_{03} : -\eta_{04} : \eta_{22} : -\eta_{23} : -\eta_{05} : \eta_{33} : -\eta_{15} : \eta_{25} : -\eta_{35} :$$
$$-\eta_{02}\eta_{33} + \eta_{03}\eta_{23} - \eta_{04}\eta_{22} : -\eta_{02}\eta_{25} + \eta_{03}\eta_{15} + \eta_{05}\eta_{22} : \eta_{02}\eta_{35} - \eta_{04}\eta_{15} - \eta_{05}\eta_{23} :$$
$$-\eta_{03}\eta_{35} + \eta_{04}\eta_{25} + \eta_{05}\eta_{33} : -\eta_{22}\eta_{35} + \eta_{23}\eta_{25} - \eta_{15}\eta_{33})$$

Picture 3: Basis for the dual Kummer variety

Defining Equations

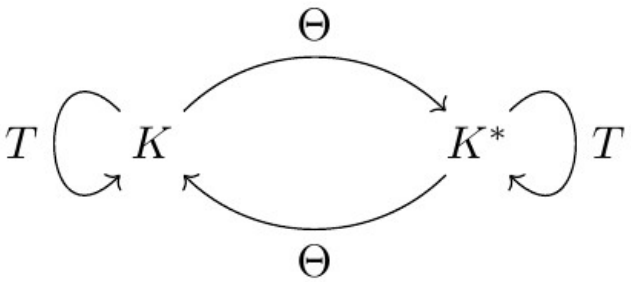
- The embedded Kummer variety can be definied by *1820 quartics*.
- There are *10 quadrics* vanishing on the Kummer and 16 independent cubics.
- Currently I am missing 40 quartics and the equations do not define the Kummer in *char(k) < 11*.

```
k1*k10 + k2*k8 - k3*k7 + k4*k6,
k1*k13 - k2*k11 + k3*k9 - k5*k6,
k1*k14 - k2*k12 + k4*k9 - k5*k7,
k1*k15 - k3*k12 + k4*k11 - k5*k8,
k2*k15 - k3*k14 + k4*k13 + k5*k10,
k1*k16 - k6*k12 + k7*k11 - k8*k9,
k2*k16 - k6*k14 + k7*k13 + k9*k10,
k3*k16 - k6*k15 + k8*k13 + k10*k11,
k4*k16 - k7*k15 + k8*k14 + k10*k12,
k5*k16 - k9*k15 + k11*k14 - k12*k13
```

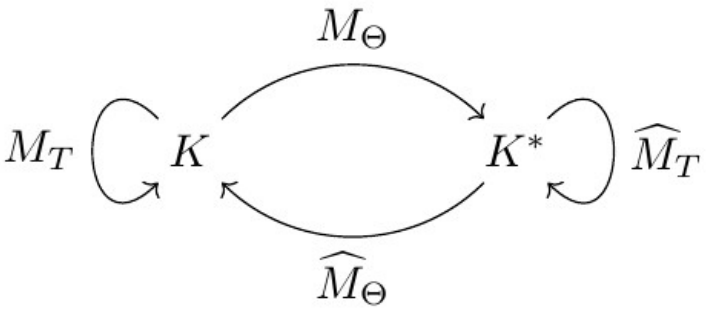
Picture 4: Quadrics vanishing on the (dual) Kummer

Addition of J[2]

- T ϵ J[2] is characterized by *F = GH* with *deg(G) even*, an odd degree factorization corresponds to a Θ-characteristic. Addition by this defines linear functions between the Kummer and its dual:



- These automorphisms are induced by automorphisms of the ambient projective space



Addition of J[2]

- The space of quadratic or quartic forms on the projective space can be acted on by (a covering of) J[2]. The representation of V_2 splits into *one-dimensional* subrepresentations.
- M_Θ for an even Θ-characteristic (resp. its dual) corresponds to the *quadratic form y_Θ (resp. z_Θ)* in such an eigenspace
- $\{y_\Theta\}$ and $\{z_\Theta\}$ form orthogonal bases of the quadr. Forms on K and K*
- The y_Θ for Θ-characteristics of degree (1,9) form another basis for the *Kummer quadrics*.
- The number of Kummer quadrics should generally be given by

$$2^{g-1}(2^g+1) - \tfrac{1}{2}\binom{2g+2}{g+1}$$

Duplication Formulas

- The duplication on K is induced by homogeneous quartics δ_1 ,…, δ_{16}. These are *invariant* under addition of J[2] and can be uniquely determined up to invariant quartics vanishing on K.

- The duplication polynomials can be defined with *integer coefficients over F* and fulfil

$$\delta_i = 4\xi_i\xi_{16}^3 + O(\xi_{16}^2) \text{ for } i < 16$$

$$\delta_{16} = \xi_{16}^4 + O(\xi_{16}^2)$$

- The eigenforms y_Θ of degree (5,5) fulfil

$$y_\Theta^2 =< \tau(\Theta), \delta > \text{ mod } E_4^{J[2]}$$

- The vanishing locus of the rational map δ can be determined explicitly for arbitrary F. The results are similar to the genus 3 case studied by *Stoll*.

Height Algorithm

- Using the duplication formulas and their behaviour mod primes, I can calculate the height of a point on the Kummer up to arbitrary precision following the algorithms in *Stoll* (2017).

- The necessary height bounds can be given via *Disc(F)* for the non-archimedian places and numerically by the coefficients of δ in the archimedian case.

- As in g<4, primes with valuation 1 in the discriminant don’t contribute to the height bound.

- More advanced algorithms cannot be used yet since there are no complete descriptions of the pseudo-addition or bounds of the denominator of $\mu_p/\log p$ in terms of the discriminant.

Pseudo-Addition

- Since there are quadrics vanishing on the Kummer variety, the map

$$Sym^2 L(2\Theta) \to L(4\Theta)^+$$

  is not surjective and pseudo-addition can not be defined solely by biquadratic forms.

- The formula describing pseudo-addition is similar to the case g=3:

$$B(\underline{\xi},\underline{\zeta}) = \frac{1}{16} \sum_{\Theta=(5,5)} y_\Theta(\underline{\xi}) y_\Theta(\underline{\zeta}) \cdot \widehat{M}_\Theta + \frac{1}{4} \sum_{\Theta=(1,9)} \sigma_\Theta(\underline{\xi}) \sigma_\Theta(\underline{\zeta}) \cdot \widehat{M}_\Theta$$

- The second summand can be made explicit in principle but currently is way too large to be stored efficiently.

Lifting of Points

- Since $J \to K$ is a 2-fold covering, the preimages of a rational point Q on K is generally only defined over an extension of degree 2 over k. To decide if it has a rat'l lift we check if a certain expression is a square over k.

- For a divisor of degree 4 we can use the square of an *odd function on the Jacobian*. In my case there are 20 simple function in $L(4\Theta)^{-}$.

  The product of two such functions are quartics in the Kummer coordinates. If the diagonal consists of squares, Q has a rat'l lift and it can be computed.

- Has the divisor degree 2, then we can find a lift directly using the explicit coordinates.

```
a0^2*b2 - a0*a1*b1 - a0*a2*b0 + a1^2*b0
a0^2*b3 - a0*a2*b1 - a0*a3*b0 + a1*a2*b0
a0^2*b4 - a0*a3*b1 - a0*a4*b0 + a1*a3*b0,
a0*a1*b3 - a0*a2*b2 - a1*a3*b0 + a2^2*b0
a0^2*b5 - a0*a4*b1 + a1*a4*b0,
a0*a1*b4 - a0*a3*b2 - a1*a4*b0 + a2*a3*b0,
a0*a2*b3 - a0*a3*b2 - a1^2*b3 + a1*a2*b2 + a1*a3*b1 - a2^2*b1
a0*a1*b5 - a0*a4*b2 + a2*a4*b0,
a0*a2*b4 - a0*a3*b3 - a2*a4*b0 + a3^2*b0,
a0*a2*b4 - a0*a4*b2 - a1^2*b4 + a1*a3*b2 + a1*a4*b1 - a2*a3*b1
-a0*a3*b4 + a0*a4*b3 + a1*a2*b4 - a1*a3*b3 - a2*a4*b1 + a3^2*b1,
a0*a2*b5 - a1^2*b5 + a1*a4*b2 - a2*a4*b1,
-a0*a2*b5 + a0*a4*b3 - a3*a4*b0
-a1*a3*b4 + a1*a4*b3 + a2^2*b4 - a2*a3*b3 - a2*a4*b2 + a3^2*b2,
a0*a3*b5 - a1*a2*b5 + a1*a4*b3 - a3*a4*b1,
-a0*a3*b5 + a0*a4*b4 - a4^2*b0
a1*a3*b5 - a2^2*b5 + a2*a4*b3 - a3*a4*b2,
a0*a4*b5 - a1*a3*b5 + a1*a4*b4 - a4^2*b1
a1*a4*b5 - a2*a3*b5 + a2*a4*b4 - a4^2*b2
a2*a4*b5 - a3^2*b5 + a3*a4*b4 - a4^2*b3
```

Picture 5: Functions in $L(4\Theta)^{-}$

Outlook

- I still have to find the missing defining equations of the variety. If possible define them over arbitrary odd characteristic.

- I want to find a more efficient way to compute the pseudo-addition

- I want to find an algorithm to search for points of bdd. height on the Kummer (or simply the Jacobian). This is the last missing ingredient to implement algorithms for the following:
  - Saturating a finite-index subgroup of J(k)
  - Finding generators of J(k)
  - Find all integral points on C

References

- S. Duquesne (2001): *‘Calculs effectifs des points entier et rationnels sur les courbes’*,
- S. Duquesne (2007): *‘Traces of the group law on the Kummer surface of a curve of genus 2 in characteristic 2’*
- E.V. Flynn (1993): *‘The group law on the jacobian of a curve of genus 2’*
- D. Holmes (2012): *‘An Arakelov-Theoretic Approach to Naive Heights on Hyperelliptic Jacobians’*
- J.S. Müller (2010): *‘Computing canonical heights on Jacobians’*
- J.S. Müller (2012): *‘Computing canonical heights using arithmetic intersection theory’*
- J.S. Müller (2014): *‘Explicit Kummer varieties of hyperelliptic Jacobian threefolds’*
- J.S. Müller, M. Stoll (2016): *‘Canonical heights on genus two Jacobians’*
- M. Stoll (1999): *‘On the height constant for curves of genus two’*
- M. Stoll (2002): *‘On the height constant for curves of genus two, II’*
- M. Stoll (2017): *‘An explicit theory of heights for hyperelliptic Jacobians of genus three’*
- A.G.J. Stubbs (2000): *‘Hyperelliptic curves’*

Thank You!