GLUEING JACOBIANS

JEROEN HANSELMAN, SAM SCHIAVONE, AND JEROEN SIJSLING

Contents

I. Introduction

In [FK91] the authors describe a method for glueing two elliptic curves E_1 and E_2 along their torsion subgroups to produce a genus 2 curve that covers both of them. In this article, we extend this method to genus 3: we glue a genus 1 curve X_1 to the Jacobian variety of a genus 2 curve X_2. This produces an abelian 3-fold which, since all abelian 3-folds are principally polarized, is the Jacobian variety of a genus 3 curve X_3. We determine explicit equations for X_3, given the data of blah. We have implemented this method in Magma, and conclude the paper with several examples.

[Other papers to mention? Howe? Howe, Leprovost, Poonen? Broker, Lauter, Stevenhagen, etc.?]

II. Background

Encoding divisors as polynomials as in Mumford and Cantor. Describe construction of the Kummer as in Mueller.

II.1. **Definitions and conventions.** Throughout, let k be a field of characteristic $\neq 2$. A *hyperelliptic curve* over k is a curve C of genus $g \geq 2$ with a model of the form $y^2 = f(x)$, where $f \in k[x]$ has distinct roots. Then $\deg(f)$ is either $2g+1$ or $2g+2$—we call the model *odd* or *even* according to the parity of $\deg(f)$. Note that an odd model has the single point $\infty = (1 : 0 : 0)$ at infinity while an even model has two: letting c be the leading

Date: October 2, 2019.

coefficient of f, then the two points at infinity are $\infty = (1 : \sqrt{c} : 0)$ and $\infty' = (1 : -\sqrt{c} : 0)$. Let

$$\widehat{\infty} = \begin{cases} \infty + \infty' & \text{if } \deg(f) \text{ is even;} \\ 2\infty & \text{if } \deg(f) \text{ is odd.} \end{cases} \tag{1}$$

We denote by $\iota : C \to C$ the hyperelliptic involution that maps $(x, y) \mapsto (x, -y)$.

II.2. **Representing divisors.** Let C be a hyperelliptic curve, $\mathrm{Div}_k(C)$ be the group of k-divisors on C [define?], $\mathrm{Div}_k^0(C)$ be the subgroup of divisors of degree 0, and $\mathrm{Jac}(C)$ be its Jacobian variety. Denote by $\equiv$ the equivalence relation of linear equivalence on $\mathrm{Div}_k(C)$. We describe how points of $\mathrm{Jac}(C)$ can be represented as pairs of polynomials, as presented in [Can87] and [Mum07, §1].

Given a point $P = (u, v)$ on C, then $\iota(P) = (u, -v)$ also lies on C. Since $\mathrm{div}(x - a) = P + \iota(P) - \widehat{\infty}$, then $-P' \equiv P - \widehat{\infty}$. Then each divisor $D \in \mathrm{Div}_k^0(C)$ is linearly equivalent to one the form [TODO: fix this to make it work in the even model case, too]

$$\sum_{i=1}^{r} P_i - r\widehat{\infty} \tag{2}$$

[Again, Cantor and Mumford only consider odd models, so have ∞, not $\widehat{\infty}$.] satisfying the following conditions:

(1) $P_i \notin \{\infty, \infty'\}$ for all i; and
(2) $P_j \neq \iota(P_i)$ for all $j \neq i$, i.e., at most one of P_i and $\iota(P_i)$ appears.

A divisor of this form is called *semireduced*.

Given a semireduced divisor $D = \sum_{i=1}^{r} P_i - r\widehat{\infty}$, we produce a pair $(a(x), b(x))$ of polynomials. Writing $P_i = (u_i, v_i)$ for each i, let $a(x) = \prod_{i=1}^{r}(x - u_i)$ and $b(x)$ be the unique polynomial of degree at most $r - 1$ such that $b(u_i) = v_i$ for all i [TODO: add statement about multiplicities here]. In the case where all the P_i are distinct, we can write b explicitly using Lagrange interpolation as

$$b(x) = \sum_{i=1}^{r} v_i \prod_{j \neq i} \frac{x - u_j}{u_i - u_j}.$$

[Put some statement about a bijection between pairs of polynomials and semireduced divisors here?]

II.3. **Embedding the Kummer variety.** Let X be a curve of genus g. Let $X^{(g)} = X^g / S_g$ be the g^{th} symmetric power of X. Fixing a basepoint $P_0 \in X$, recall that the map

$$\begin{aligned} X^{(g)} &\to \mathrm{Jac}(X) \\ \{P_1, \ldots, P_g\} &\mapsto [P_1] + \cdots + [P_g] - g[P_0] \end{aligned}$$

is surjective.

Let

$$f(x) = f_6 x^6 + f_5 x^5 + \cdots + f_1 x + f_0 \in k[x]$$

be a polynomial with no repeated roots (in the algebraic closure k^{al}). Then

$$X_2 : y^2 = f(x)$$

is a genus 2 hyperelliptic curve over k.

Let

$$F_0(x,u) = 2f_0 + f_1(x+u) + 2f_2xu + f_3(x+u)xu + 2f_4(xu)^2 + f_5(x+u)xu + 2f_6(xu)^3 .$$

The image of κ is a quartic surface given by

$$K_2(\kappa_1,\kappa_2,\kappa_3)\kappa_4^2 + K_1(\kappa_1,\kappa_2,\kappa_3)\kappa_4 + K_0(\kappa_1,\kappa_2,\kappa_3)\,,$$

where

$$\begin{aligned}
K_2(\kappa_1,\kappa_2,\kappa_3) &= \kappa_2^2 - 4\kappa_1\kappa_3\\
K_1(\kappa_1,\kappa_2,\kappa_3) &= -4\kappa_1^3 f_0 - 2\kappa_1^2\kappa_2 f_1 - 4\kappa_1^2\kappa_3 f_2 - 2\kappa_1\kappa_2\kappa_3 f_3 - 4\kappa_1\kappa_3^2 f_4 - 2\kappa_2\kappa_3^2 f_5 - 4\kappa_3^3 f_6\\
K_0(\kappa_1,\kappa_2,\kappa_3) &= -4\kappa_1^4 f_0 f_2 + \kappa_1^4 f_1^2 - 4\kappa_1^3\kappa_2 f_0 f_3 - 2\kappa_1^3\kappa_3 f_1 f_3 - 4\kappa_1^2\kappa_2^2 f_0 f_4 + 4\kappa_1^2\kappa_2\kappa_3 f_0 f_5\\
&\quad - 4\kappa_1^2\kappa_2\kappa_3 f_1 f_4 - 4\kappa_1^2\kappa_3^2 f_0 f_6 + 2\kappa_1^2\kappa_3^2 f_1 f_5 - 4\kappa_1^2\kappa_3^2 f_2 f_4 + \kappa_1^2\kappa_3^2 f_3^2\\
&\quad - 4\kappa_1\kappa_2^3 f_0 f_5 + 8\kappa_1\kappa_2^2\kappa_3 f_0 f_6 - 4\kappa_1\kappa_2^2\kappa_3 f_1 f_5 + 4\kappa_1\kappa_2\kappa_3^2 f_1 f_6 - 4\kappa_1\kappa_2\kappa_3^2 f_2 f_5\\
&\quad - 2\kappa_1\kappa_3^3 f_3 f_5 - 4\kappa_2^4 f_0 f_6 - 4\kappa_2^3\kappa_3 f_1 f_6 - 4\kappa_2^2\kappa_3^2 f_2 f_6 - 4\kappa_2\kappa_3^3 f_3 f_6 - 4\kappa_3^4 f_4 f_6\\
&\quad + \kappa_3^4 f_5^2\,.
\end{aligned}$$

III. Overview of method

Our construction proceeds as follows. We take as input an elliptic curve X_1 and a genus 2 curve X_2 over a number field k [or more genenerally, any field? characteristic $\neq 2$?] given in Weierstrass form

$$X_1 : y^2 + u(x)y = v(x) \qquad X_2 : y^2 + h(x)y = f(x)\,.$$

Letting J_2 be the Jacobian variety of X_2, then J_2 is an abelian surface with 16 2-torsion points. The Kummer variety K_2 of X_2 is obtained by forming the quotient of J_2 by the negation map $[-1]$. This quotient map $\pi : J_2 \to K_2$ is injective on the 2-torsion points of J_2, whose images are the singular points of K_2. [Nodes, I guess?] Using the explicit embedding given in [Mül10] (which in turn is a generalization of [CF96]), we can realize K_2 as a quartic surface in $\mathbb{P}^3$.

Fix two nodes T_1, T_2 of K_2. Consider the pencil of planes $\mathcal{H} = \{H_\mu : \mu \in \mathbb{P}^1\}$ passing through T_1 and T_2. The intersection of a plane $H_\mu \in \mathcal{H}$ with K_2 is a quartic plane curve C_μ with two nodes. By the usual degree-genus formula for plane curves, C_μ has genus 1 for each $\mu \in \mathbb{P}^1$. We will endow C_μ with the structure of an elliptic curve and compute its j-invariant as a function of μ.

To a point $Q \in C_\mu$ we associate the line ℓ_Q passing through T_1 and Q. The association $Q \mapsto \ell_Q$ defines a degree 2 map $C_\mu \to \mathbb{P}^1$ ramified at 4 points. Computing the cross-ratio of these 4 points yields the λ-invariant of C_μ, allowing us to find a Legendre model

$y^2 = x(x-1)(x-\lambda)$ for C_μ. We can then compute the j-invariant of C_μ using the standard formula

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda-1)^2}.$$

Note that computing the λ-invariant of C_μ not only endows C_μ with the structure of an elliptic curve, but also with level 2 structure: the Legendre model $E_{\mathrm{Leg}} : y^2 = x(x-1)(x-\lambda)$ comes equipped with the basis $\{(0,0),(1,0)\}$ for $E_{\mathrm{Leg}}[2]$, and we may pull back this basis along the isomorphism $C_\mu \xrightarrow{\sim} E_{\mathrm{Leg}}$ to obtain a basis for $C_\mu[2]$.

Lemma 1. *The composite map*

$$\begin{array}{ccccccc} \varphi : \mathbb{P}^1 & \longrightarrow & \mathcal{M}_1 & \longrightarrow & X(2) & \longrightarrow & X(1) \\ \mu & \longmapsto & C_\mu & \longmapsto & \lambda(C_\mu) & \longmapsto & j(\lambda(C_\mu)) \end{array}$$

has degree 12*.*

Proof. By the classical theory of modular functions, the map $X(2) \to X(1)$, $\lambda \mapsto j(\lambda)$ has degree 6, corresponding to the 6 permutations of $0, 1, \infty$ acted on by S_3. As the map $\mu \mapsto C_\mu$ has degree 1, it suffices to show that the map $\mathcal{M}_1 \to X(2)$ has degree 2. [I think this just follows from the fact that we could've chosen to the other node and taken lines through T_2 and Q to obtain a map to $\mathbb{P}^1$. I guess we have to show that this would produce the same λ...] ∎

Thus the composite map in the above lemma is a rational function of degree 12 in μ. Let $j_1 = j(X_1)$. In order to find a value of μ that yields an elliptic curve C_μ isomorphic to our original curve X_1, we solve the equation $\varphi(\mu) = j_1$. The solutions μ to this equation may not lie in the ground field, so it may be necessary to base change our curve to an algebraic extension. [I think in all the examples so far we've only needed quadratic extensions of the base field...] [One more interesting note: I think in all the examples we've done so far, $\varphi(\mu) - j_1$ has an interesting factorization. The numerator is a product of quadratics, and the denominator is a product of linear factors squared. Is this expected?]

IV. Applications

Constructing abelian three-folds with interesting torsion?

V. Examples

References

[Can87] David G. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, 48(177):95–101, 1987.

[CF96] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus* 2, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.

[FK91] Gerhard Frey and Ernst Kani. Curves of genus 2 covering elliptic curves and an arithmetical application. In *Arithmetic algebraic geometry (Texel, 1989)*, volume 89 of *Progr. Math.*, pages 153–176. Birkhäuser Boston, Boston, MA, 1991.

[Mül10] Jan Steffen Müller. Explicit Kummer surface formulas for arbitrary characteristic. *LMS J. Comput. Math.*, 13:47–64, 2010.

[Mum07] David Mumford. *Tata lectures on theta. II*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura, Reprint of the 1984 original.