Genus 2 curves with given split Jacobian

Jasper Scholten
jasper.scholten@gmail.com

November 22, 2018

Abstract

Given 2 Elliptic Curves E_1 and E_2, we use some theory of elliptic Kummer surfaces to construct a hyperelliptic curve with Jacobian isogenous to $E_1 \times E_2$. We require the 2-torsion of E_1 and E_2 to be defined over the field we are working over.

1 Introduction

Let E_1 and E_2 be elliptic curves. The aim of this note is to construct an explicit genus 2 curve C on $E_1 \times E_2$.

The result of this paper was obtained 15 years ago. At that time I was preparing to write a paper on it, and made a reference to it in another paper [7]. In the proof of lemma 3.1 of [7] a reference to the current paper was made as being *in preparation*. Since then, results in [7] have been used by other researchers, see [5], [1], [3], [2], and I have been asked about the state of the current paper. This prompted me to finish it.

2 The construction

Let E_1 be an elliptic curve given by $y_1^2 = f(x_1)$ and E_2 an elliptic curve given by $y_2^2 = g(x_2)$, with f and g cubic monic polynomials with coefficients in some field k. Let S be the surface $E_1 \times E_2/\langle -1 \rangle$.

An affine equation for a surface that is birational to S is

$$f(x)y^2 - g(z) = 0, \tag{1}$$

with the projection $\pi : E_1 \times E_2 \to S$ given by

$$\pi(x_1, y_1, x_2, y_2) \mapsto (x, y, z) = (x_1, \frac{y_2}{y_1}, x_2).$$

Equation 1 occured in work of Kuwata, see for example [4]. It defines an affine part of the associated Kummer surface. See the next section for more on this.

At this point we can jump ahead to the construction of C. After the construction, we will introduce some theory (of elliptic Kummer surfaces) and show why our construction gives the curve we are looking for.

We can consider the equation $f(x)y^2 - g(z) = 0$ as a cubic curve over the rational function field $k(y)$. Call this curve $\mathbf{E}$. Assume that $f(x) = x(x-\alpha)(x-\beta)$ and $g(z) = z(z-\gamma)(z-\delta)$. The curve $\mathbf{E}$ has the following points: $(0,0), (0,\gamma)$, $(0,\delta)$, $(\alpha,0)$, $(\beta,0)$, (α,γ), (α,δ), (β,γ), (β,δ). By choosing $(0,0)$ as zero point, $\mathbf{E}$ becomes an elliptic curve with group law. Denote the group operation by $\oplus$. We can compute $(\alpha,\gamma) \oplus (\beta,\delta)$. This point over $k(y)$ can be considered as a curve R over k. It is a rational curve on the surface S, and its preimage $\pi^{-1}(R)$ is the genus 2 curve C on $E_1 \times E_2$ we are looking for.

3 Kummer surfaces

The surface S has singular points at the image of the fixed points of $[-1]$ on $E_1 \times E_2$. That is, at the image $\pi(T)$ for any 2-torsion point T on $E_1 \times E_2$. There are 16 of those. They are ordinary double points, and blowing them up once resolves the singular point, replacing each point with a $\mathbb{P}^1$. This resolution of singularities is called a Kummer surface. Let us call it K and the resulution map $\rho : K \to S$. Figure 1 shows some rational curves on K, and how they intersect:

The curves $\rho(F_i)$ are images $\pi(E_1 \times T)$ with T a 2-torsion point on E_2. $\rho(F_0)$ is the image when T is the zero point of E_2.

The curves $\rho(G_i)$ are images $\pi(T \times E_2)$ with T a 2-torsion point on E_1. $\rho(G_0)$ is the image when T is the zero point of E_1.

The 16 curves H_{ij} are curves created in the blow-ups of singular points on S.

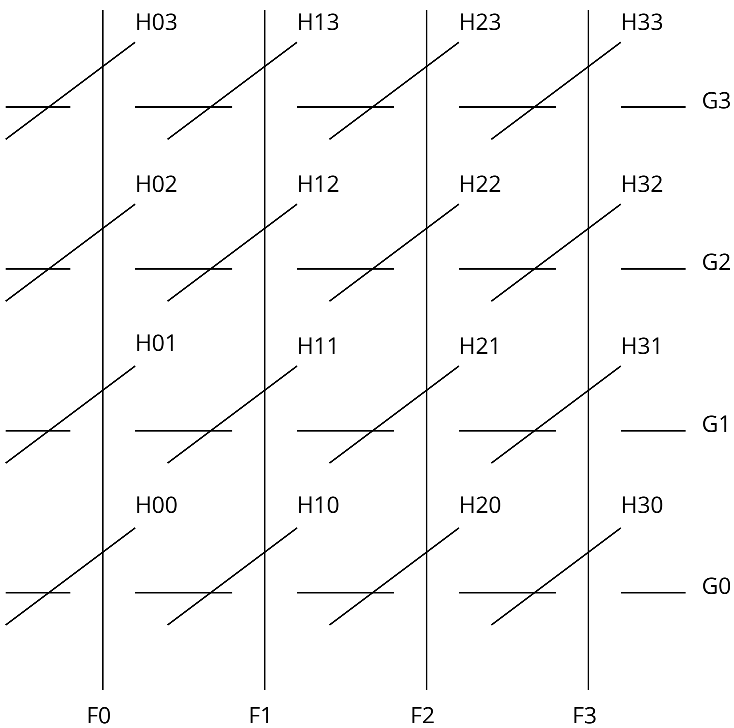

Figure 1: Some rational curves on Kummer surface

4 Elliptic Surfaces

See [8] for details on this section.

An elliptic surface is a surface X and curve D over a field k and map $\tau : X \to D$ and a section $O : D \to X$ with $\tau \circ O = \mathrm{Id}_D$ such that almost every fibre $\tau^{-1}(p)$ is an elliptic curve with zero $O(p)$. A section is a map $\psi : D \to X$ such that the composition $\tau \circ \psi$ is the identity map on D. The generic fibre of τ is an elliptic curve over the function field of D. Sections of the elliptic surface are in 1-1 correspondence with points on the generic fibre. We often use the same notation for a point on the generic fibre, its corresponding section $D \to X$, and the image of the section, which is a curve on X isomorphic to D.

Some notation: Given two sections F and G, we can add the images as divisors or elements of the Néron-Severi group. We will denote this sum by $F + G$. We can also add them using the elliptic curve group law on the generic fibre. This will result in a new section which we denote by $F \oplus G$.

Singular fibres of an elliptic surface were classified by Kodeira. Once X is *non-singular*, *complete* and *relatively minimal* (one can always find such a model) singular fibres are of type I_n, II, III, IV, IV^*, III^*, II^* or I_n^*.

The Néron-Severi group $NS(X)$ of a surface X is the group of divisors modulo algebraic equivalence. This group is finitely generated, and there is a pairing on the group, the intersection pairing. For an elliptic surface X, there is a close relationship between $NS(X)$ with the interesection pairing and the Modell-Weil group of its generic fibre with the pairing defined be the Néron-Tate height. One can define the Néron-Tate pairing of a point in terms of intersections of the corresponding section with fibre components and the zero-section. For sections (or points on generic fibre) P and Q denote the intersection pairing of P and Q by (P, Q) and the Néron-Tate height by $\langle P, Q\rangle$. Let χ be the arithmetic genus of X. Then

$$\begin{aligned} \langle P, Q\rangle &= \chi + (P, O) + (Q, O) - (P, Q) - \sum \mathrm{contr}_v(P, Q), \qquad (2) \\ \langle P, P\rangle &= 2\chi + 2(P, O) - \sum \mathrm{contr}_v(P, P). \end{aligned}$$

Here the sums runs over points v of D such that $\tau^{-1}(v)$ is reducible, and the $\mathrm{contr}_v(P, Q)$ are explicit numbers that depend on the Kodeira type of the fibre, and which component the sections P and Q intersect.

The elliptic surface we consider in this paper is a K3 surface, and it has arithmic genus $\chi = 2$ in the above height pairing formulas.

Any curve P on X that intersects with a fibre once (i.e. $(P, \tau^{-1}(v)) = 1$ for a v on D) is the image of a section.

5 Elliptic Kummer surfaces

A main reference for results in this section is [6].

On a Kummer surface K (or more generally a K3 surface) one can have several different maps to $\mathbb{P}^1$ that give it the structure of an elliptic surface. Let E be a divisor of K such that E is either an elliptic curve, or a reducible curve that is one of the Kodeira types. Then there is a way to give K the structure of an elliptic surface $K \to \mathbb{P}^1$ such that E is a fibre. The elliptic surface corresponds to the complete linear system $|E|$. A few examples of such E are:

- $E = 2F_0 + H_{00} + H_{01} + H_{02} + H_{03}$. This fibre has type I_0^* . This corresponds to the elliptic surface $S \to E_2/\langle -1 \rangle$ induced from the projection $E_1 \times E_2 \to E_2$. Other reducible fibres are $2F_i + H_{i0} + H_{i1} + H_{i2} + H_{i3}, i \leq 3$, all of type I_0^*.

- Similarly, $E = 2G_0 + H_{00} + H_{10} + H_{20} + H_{30}$ of type I_0^*, induced from $E_1 \times E_2 \to E_1$.

- $E = 3F_0 + 2H_{01} + 2H_{02} + 2H_{03} + G_1 + G_2 + G_3$. This has Kodeira type IV^*. This case corresponds to where consider $f(x)y^2 - g(z) = 0$ as an elliptic curve over $k(y)$. Here E is the reducible fibre over $y = 0$. There is another reducible fibre of type IV^* over $y = \infty$ given by $3G_0 + 2H_{10} + 2H_{20} + 2H_{30} + F_1 + F_2 + F_3$. The 9 curves $H_{i,j}$, $1 \leq i, j \leq 3$ are all images of sections (as they intersect the IV^*-fibres once). One can show that they generate a subgroup of the Mordell-Weil group of rank 4, but we won't need this. In fact, they generate the Mordell-Weil group if E_1 and E_2 are not isogenous. If E_1 and E_2 are isogenous then graphs of the isogenies can be used to construct more points, and the Mordell-Weil rank is $4 + \text{rank}(\text{Hom}(E_1, E_2))$.

6 Computation of intersections and heights

We consider the Kummer surface K with the two IV^* fibres from the previous sections. The elliptic curve $f(x)y^2 - g(z) = 0$ over $k(y)$ has nine points $(0, 0)$,

$(0,\gamma)$, $(0,\delta)$, $(\alpha,0)$, (α,γ), (α,δ), $(\beta,0)$, (β,γ), (β,δ), which by relabeling we assume to correspond to the sections H_{11}, H_{21}, H_{31}, H_{12}, H_{22}, H_{32}, H_{13}, H_{23}, H_{33} respectively. We choose $H_{11} = (0,0)$ as the zero for the elliptic curve group structure. The definition of the elliptic curve group law in terms of lines intersecting the cubic equation (1) in the (x,z)-affine plane over $k(y)$ immediately gives us the following relations:

$$\begin{aligned} H_{13} &= H_{22} \oplus H_{32}, \\ H_{12} &= H_{23} \oplus H_{33}, \\ H_{31} &= H_{22} \oplus H_{23}, \\ H_{21} &= H_{32} \oplus H_{33}. \end{aligned}$$

Let R denote the curve corresponding to the section $H_{23} \oplus H_{32}$. We will use the relation between height pairing and intersection pairing to compute the intersection of R with each of the 16 H_{ij}. Note that R is a rational curve, as it is a section of the elliptic surface over $\mathbb{P}^1$. We will find that $(R, H_{ij}) = 2$ for exactly 3 pairs (i,j) (namely $(i,j) = (0,0), (2,3)$ and $(3,2)$), and $(R, H_{ij}) = 0$ for all other (i,j). This means that the pullback of R on $E_1 \times E_2$ is unramified outside at most 6 points. The only possible ramification points are above where R intersects one of the H_{ij}. So the pullback on $E_1 \times E_2$ has genus at most 2. On the singular surface S the curve R has multiplicity 2 singularities at the points below the H_{ij} with $(R, H_{ij}) = 2$. For now we won't study in detail whether the cover ramifies does ramify at these points. In the last section we will obtain an explicit equation of the pullback on $E_1 \times E_2$, and observe that generically it has genus 2.

A IV^* fibre has 3 components of multiplicity 1. Each section must intersect 1 of these. The group structure of the elliptic curve induces a $\mathbb{Z}/3\mathbb{Z}$ group structure on the 3 components. We use this to determine which reducible fibre component intersects the sections we are studying. For a IV^* fibre, the $\mathrm{contr}_v(P,Q)$ values are the following:

- $\mathrm{contr}_v(P,Q) = 0$ if at least 1 of P and Q intersects the identity component.
- $\mathrm{contr}_v(P,Q) = \frac{4}{3}$ if P and Q intersect the same non-identity component.
- $\mathrm{contr}_v(P,Q) = \frac{2}{3}$ if P and Q intersect different non-identity components.

Now we can compute the height pairings and intersection pairings that we need. We start off with using the known intersections between the F_i, G_j and H_{ij} (see figure 1) to compute the height pairings between the 9 sections $H_{ij}, 1 \leq i, j \leq 3$, using (2). Then we use the bi-linearity of the height pairing to compute height pairings between other sections. Then we use (2) again to compute the intersection pairings we need.

$$
\begin{aligned}
\langle H_{ij}, H_{ij} \rangle &= 4 - \frac{4}{3} - \frac{4}{3} = \frac{4}{3} \quad \text{for } 2 \leq i, j \leq 3 \\
\langle H_{23}, H_{32} \rangle &= 2 - \frac{2}{3} - \frac{2}{3} = \frac{2}{3}, \\
4 = \frac{4}{3} + \frac{4}{3} + \frac{2}{3} + \frac{2}{3} &= \langle H_{23}, H_{23} \rangle + \langle H_{32}, H_{32} \rangle + \langle H_{23}, H_{32} \rangle + \langle H_{32}, H_{23} \rangle = \\
\langle R, R \rangle &= 4 + 2(R, O), \\
(R, O) &= 0, \\
2 = \langle R, H_{23} \rangle &= 2 - (R, H_{23}), \\
(R, H_{23}) &= 0, \qquad (R, H_{32}) = 0 \text{ is similar} \\
\langle H_{23}, H_{33} \rangle &= 2 + 0 + 0 - 0 - \frac{4}{3} - \frac{2}{3} = 0, \\
0 = \langle R, H_{33} \rangle &= 2 - (R, H_{33}), \\
(R, H_{33}) &= 2, \qquad (R, H_{22}) = 2 \text{ is similar} \\
2 = \langle R, H_{13} \rangle &= 2 - (R, H_{13}), \\
(R, H_{13}) &= 0, \\
(R, H_{ij}) &= 0 \text{ for } (i, j) = (1, 2), (2, 1), (3, 1) \text{ is similar}
\end{aligned}
$$

Note that R does not intersect F_0 and G_0 because they are fibre components with multiplicity > 1. And the group law on the component group tells us that it intersects F_1 and G_1, and it does not intersect F_2, G_2, F_3 and G_3.

Now we have computed $(R, H_{i,j})$ for every (i, j) except $(i, j) = (0, 0)$. Since H_{00} is not a fibre component or section of the elliptic fibration we chose, we can not use the above technique. However, we can use one of the elliptic fibrations with four I_0^* fibres. Using the intersections computed so far, we can see that R intersects 3 of these I_0^* fibres with multiplicity 2, hence it yields a degree 2 cover of $E_i/\langle -1 \rangle$. Therefore it must also intersect the fourth I_0^* with multiplicity 2, and this can only happen if $(R, H_{00}) = 2$.

7 Explicit Equations

Given the elliptic curve $f(x)y^2 - g(z) = 0$ over $k(y)$ as before, we can use the group law to evaluate

$$(\alpha, \delta) \oplus (\beta, \gamma) = \left(\tfrac{(\alpha\delta-\beta\gamma)(\gamma-\delta)^2}{(\alpha-\beta)^3 y^2-(\gamma-\delta)^3} \quad , \quad \tfrac{(\alpha\delta-\beta\gamma)(\alpha-\beta)^2 y^2}{(\alpha-\beta)^3 y^2-(\gamma-\delta)^3} \right)$$

To find the Weierstrass points of the genus 2 curve C we are after, we solve for which y this points passes through (∞, ∞), (α, γ) and (β, δ). Our computation of intersection numbers in the previous section ensures that the curve passes through each of these points twice. An easy computation shows that this happens at

$$y^2 = \frac{(\gamma - \delta)^3}{(\alpha - \beta)^3},$$
$$y^2 = \frac{\gamma(\gamma - \delta)^2}{\alpha(\alpha - \beta)^2},$$
$$y^2 = \frac{\delta(\gamma - \delta)^2}{\beta(\alpha - \beta)^2}.$$

So up to a twist, C has equation

$$Y^2 = \big((\alpha - \beta)X^2 - (\gamma - \delta)\big) \big(\alpha X^2 - \gamma\big) \big(\beta X^2 - \delta\big)$$

(The $\frac{(\gamma-\delta)^2}{(\alpha-\beta)^2}$ factor can be removed with a straightforward coordinate transformation).

Theorem 1. *The curve C defined by equation*

$$(\delta\alpha - \beta\gamma)\, Y^2 = \big((\alpha - \beta)X^2 - (\gamma - \delta)\big) \big(\alpha X^2 - \gamma\big) \big(\beta X^2 - \delta\big) \tag{3}$$

maps to both elliptic curves E_1 and E_2.

Proof. Replacing X^2 with X maps C to the elliptic curve

$$(\delta\alpha - \beta\gamma)\, Y^2 = ((\alpha - \beta)X - (\gamma - \delta))\, (\alpha X - \gamma)\, (\beta X - \delta) \tag{4}$$

Replacing X with

$$\frac{\alpha\delta - \beta\gamma}{(\alpha - \beta)\alpha\beta} X + \frac{\gamma - \delta}{\alpha - \beta}$$

transforms equation (4) to

$$\frac{\alpha^2\beta^2}{(\delta\alpha-\beta\gamma)^2}Y^2 = X(X-\beta)(X-\alpha)$$

which is isomorphic to E_1. If we swap α and γ, and we swap β and δ in equation 3, then the resulting equation defines a curve isomorphic to C (map X to $\frac{1}{X}$ and rescale Y). So C also maps to E_2. $\square$

In the proof of lemma 3.1 of [7] we made use of (a transformation of) equation (3).

References

[1] Daniel J. Bernstein and Tanja Lange. Hyper-and-elliptic-curve cryptography. Cryptology ePrint Archive, Report 2014/379, 2014. `https://eprint.iacr.org/2014/379`.

[2] Craig Costello. Computing supersingular isogenies on kummer surfaces. Cryptology ePrint Archive, Report 2018/850, 2018. `https://eprint.iacr.org/2018/850`.

[3] Antoine Joux and Vanessa Vitse. Cover and decomposition index calculus on elliptic curves made practical. application to a seemingly secure curve over F_{p^6}. Cryptology ePrint Archive, Report 2011/020, 2011. `https://eprint.iacr.org/2011/020`.

[4] M. Kuwata and T. Shioda. Elliptic parameters and defining equations for elliptic fibrations on a Kummer surface. *ArXiv Mathematics e-prints*, September 2006. Available at `https://arxiv.org/abs/math/0609473`.

[5] Fumiyuki Momose and Jinhui Chao. Scholten forms and elliptic/hyperelliptic curves with weak weil restrictions. Cryptology ePrint Archive, Report 2005/277, 2005. `https://eprint.iacr.org/2005/277`.

[6] Keiji Oguiso. On jacobian fibrations on the kummer surfaces of the product of non-isogenous elliptic curves. *J. Math. Soc. Japan*, 41(4):651–680, 10 1989.

[7] Jasper Scholten. Weil Restriction of an Elliptic Curve over a Quadratic Extension. 2003. Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.118.7987&rep=rep1&type=pdf.

[8] Tetsuji Shioda. On the mordell-weil lattices. *Commentarii Mathematici Universitatis Sancti Pauli*, 39(2):211–240, 1990.