Pairs of isogenous Jacobians of hyperelliptic curves of arbitrary genus

Couples de Jacobiennes isogènes de courbes hyperelliptiques de genre arbitraire

J.-F. Mestre

Translated from the original preprint arXiv:0902.3470 (2009) by Benjamin Smith

This version was compiled on October 4, 2011

1 Introduction

Let C be a genus g curve, J_C its Jacobian, and H a Weil-isotropic rank-g subgroup of $J_C[2]$; the quotient abelian variety $A = J_C/H$ is principally polarized, but for $g \geq 4$ is generally not a Jacobian. *A fortiori*, if C is hyperelliptic and $g \geq 3$, then A is generally not the Jacobian of a hyperelliptic curve.

It does not seem well-known that, for large enough g, there exists at least one pair of hyperelliptic curves C, C' of genus g whose Jacobians are $(2,\ldots,2)$-isogenous. We note nevertheless that B. Smith has obtained some families[1] with 3 (resp. 2, resp. 1) parameters of such pairs of curves of genus $6,12,14$ (resp. $3,6,7$, resp. $5,10,15$).

We show here that for all $g \geq 2$, there exists a $(g+1)$-parameter family of pairs of hyperelliptic curves (C, C') whose Jacobians are connected by an isogeny with kernel isomorphic to $(\mathbb{Z}/2\mathbb{Z})^g$. More precisely,

Theorem. *Let g be a positive integer, and let $K = \mathbb{Q}(a_1,\ldots,a_g,v)$ where $a_1,\ldots,a_g,v$ are indeterminates. There exists a 2-2 correspondence between the curves C and C' defined by*

$$C : y^2 = (x-v)(vx-1)(x^2-a_1)\cdots(x^2-a_g)$$

and

$$C' : y^2 = (x-v)(vx-(-1)^g)(x^2-b_1)\cdots(x^2-b_g),$$

where $b_i = (a_i v^2 - 1)/(a_i - v^2)$ for $1 \leq i \leq g$, inducing a $(2,\ldots,2)$-isogeny between their Jacobians.

The Jacobian of C is absolutely simple; further, when we specialize the a_i and v at elements of $\mathbb{C}$, the image of the curves C in the moduli space of hyperelliptic curves of genus g over $\mathbb{C}$ has dimension $g+1$.

Remark 1. When g is even, this allows us to obtain a $(g/2+1)$-dimensional family of hyperelliptic curves whose Jacobians have endomorphism rings containing $\mathbb{Z}[\sqrt{2}]$: if v and a_i (with $1 \leq i \leq g/2$) are arbitrary, then we take $a_{g/2+i} = (a_i v^2 - 1)/(a_i - v^2)$ for $1 \leq i \leq g/2$.

Remark 2. In the case $g = 2$, we recover the Richelot correspondence (see, for example, [1], [2], and [3]).

[1] This work has now appeared. See B. Smith, *Families of Explicit Isogenies of Hyperelliptic Jacobians*, in *Arithmetic, Geometry, Cryptography and Coding Theory 2009*, Contemp. Math. **521** (2009), 121–144 (also `http://hal.inria.fr/inria-00420605`). Specifically, it defines three-dimensional hyperelliptic families for $g = 6,12,14$; two-dimensional families for $g = 3,6,7,10,20,30$; and one-dimensional families for $g = 5,10,15$. The kernels of the isogenies are not all of the form $(\mathbb{Z}/2\mathbb{Z})^g$. A related construction, yielding non-hyperelliptic families in arbitrarily high genus, has also appeared: see B. Smith, *Families of explicitly isogenous Jacobians of variable-separated curves*, LMS J. Comput. Math. **14** (2011), 179–199 (also `http://hal.inria.fr/inria-00516038`).

2 Proof

We maintain the notation of the theorem. We write $p_0(x) = q_0(x) = (x - v)(vx - 1)$ and $p_i(x) = x^2 - a_i$ and $q_i(x) = x^2 - b_i$ for $1 \le i \le g$; if we set

$$S(x, z) = x^2 z^2 - v^2(x^2 + z^2) + 1,$$

where z is an indeterminate, then we have the identities

$$p_2(v)p_1(x)q_2(z) - p_1(v)p_2(x)q_1(z) + (a_1 - a_2)S(x, z) = 0$$

and

$$(1 - v^2)S(x, z) = 2p_0(x)q_0(z) - (v^2 + 1)(1 - xv - zv + xz)^2,$$

whence

$$p_2(v)p_1(x)q_2(z) \equiv p_1(v)p_2(x)q_1(z) \pmod{S}$$

and

$$2p_0(x)q_0(z) \equiv (v^2 + 1)(1 - xv - zv + xz)^2 \pmod{S}.$$

2.1 The case where g is even

First, suppose that g is even: then for $1 \le i \le g$, the equation above yields

$$p_{2i}(v)p_{2i-1}(x)q_{2i}(z) \equiv p_{2i-1}(v)p_{2i}(x)q_{2i-1}(z) \pmod{S} \quad \text{for } 1 \le i \le g/2.$$

It follows, writing

$$M(x, z) = p_2(v)p_4(v)\cdots p_g(v)p_1(x)q_2(z)p_3(x)q_4(z)\cdots p_{g-1}(x)q_g(z),$$

that

$$\prod_{i=1}^{g} p_i(v)p_i(x) \prod_{i=1}^{g} q_i(z) \equiv M(x, z)^2 \pmod{S}.$$

If C is the curve defined by

$$C : y^2 = A \prod_{i=0}^{g} p_i(x) \quad \text{where } A = 2(v^2 + 1) \prod_{i=1}^{g} p_i(v)$$

and C' the curve defined by

$$C' : t^2 = \prod_{i=0}^{g} q_i(z),$$

then we have a correspondence Γ on $C \times C'$ defined by

$$\Gamma : \begin{cases} S(x, z) = 0, \\ yt = M(x, z)(v^2 + 1)(1 - xv - zv + xz). \end{cases}$$

By construction, the classes of the divisors $(\sqrt{a_i}, 0) - (-\sqrt{a_i}, 0)$ are in the kernel of the homomorphism $J_C \to J_{C'}$ induced by Γ, which therefore contains the subgroup of order 2^g of $J_C[2]$ generated by these classes. The theorem for even g then follows from the following proposition:

Proposition. *Let $\Gamma' \subset C' \times C$ be the transpose of Γ; then $\Gamma \circ \Gamma$ acts on $\mathrm{Pic}^0(C)$ by $D \mapsto 2D$.*

We prove without difficulty, using the defining equations for Γ, that the image of a point $P = (X, Y)$ of C under $\Gamma' \circ \Gamma$ is the divisor $2P + P_1 + w(P_1)$, where P_1 is a point of C with $x(P_1) = -X$ and w is the hyperelliptic involution of C; the action on degree-0 divisor classes is therefore multiplication by 2.

2.2 The case where g is odd

To prove the theorem for odd g it is enough to specialize $a_g \to 0$ in the construction above. The curves C and C' are then of genus $g-1$; an easy calculation gives the defining equation for C' in the theorem.

2.3 Dimension in the moduli space

1) The case $g = 2$**.** The generic hyperelliptic curve of genus 2 is in the form of C above: indeed, if $P_1, \ldots, P_6$ are six generic points on the projective line, then there exists a unique involution u such that $u(P_1) = P_2$ and $u(P_3) = P_4$; there then exists a unique involution w, commuting with u, such that $w(P_5) = P_6$. Choosing coordinates such that u maps $x \mapsto -x$, the involution w has the form $x \mapsto t/x$, which we can bring into the form $x \mapsto 1/x$ by a homothety.

2) The case $g \geq 3$**.** Two hyperelliptic curves are isomorphic if and only if there exists a homography mapping the Weierstrass points of one onto those of the other. It therefore suffices to prove that if $v, x_1, \ldots, x_g$ are generic points of $\mathbb{P}^1$, and if $h : x \mapsto (ax+b)/(cx+d)$ is a homography such that the set $A = \{h(v), h(1/v), h(x_1), \ldots, h(x_g), h(-x_1), \ldots, h(-x_g)\}$ is in the form $\{w, 1/w, y_1, \ldots, y_g, -y_1, \ldots, -y_g\}$, then h is of the form $x \mapsto \pm x$ or $x \mapsto \pm 1/x$.

Let $B = h^{-1}(\{y_1, -y_1, y_2, -y_2, y_3, -y_3\})$; then B is (globally) fixed by the involution $h^{-1}uh$, where u is the involution $x \mapsto -x$. However, if $a_1, \ldots, a_6$ are six distinct field elements, then there exists an involution permuting a_{2i-1} and a_{2i} for $1 \leq i \leq 3$ if and only if

$$\begin{aligned} &a_6a_5a_3 + a_6a_5a_4 + a_6a_2a_1 + a_5a_2a_1 + a_1a_4a_3 + a_2a_4a_3 \\ &= a_6a_5a_1 + a_6a_5a_2 + a_6a_4a_3 + a_5a_4a_3 + a_2a_1a_3 + a_2a_1a_4. \end{aligned}$$

It follows that each element of B is algebraically dependent on the others; hence, if b is an element of B in the form $\pm x_i$ then $\{x_i, -x_i\} \subset B$, and if b is equal to v or $1/v$ then $\{v, 1/v\} \subset B$. Up to a permutation of $\{1, \ldots, g\}$, the set B must have the form $B_1 = \{x_1, -x_1, x_2, -x_2, v, 1/v\}$ or $B_2 = \{x_1, -x_1, x_2, -x_2, x_3, -x_3\}$.

As shown above, six generic points of $\mathbb{P}^1$ can be written (in a suitable coordinate system) in the form $\{x_1, -x_1, x_2, -x_2, v, 1/v\}$; hence, generically there is no involution fixing B_1, so B is of the form B_2 and $h(\{v, 1/v\}) = \{w, 1/w\}$. But the generic genus 2 curve with automorphism group $(\mathbb{Z}/2\mathbb{Z})^2$ is in the form $y^2 = (x^2 - x_1^2)(x^2 - x_2^2)(x^3 - x_3^2)$, its automorphism group formed by the four elements $(x, y) \mapsto (\pm x, \pm y)$. Generically, the only involution fixing B_2 is $x \mapsto -x$; it follows that $h^{-1}uh(x_i) = u(x_i)$ for $1 \leq i \leq 3$; hence $h^{-1}uh = u$, and h is a homography commuting with u, and therefore of the form $x \mapsto ax$ or $x \mapsto a/x$. Since h maps $\{v, 1/v\}$ onto $\{w, 1/w\}$ we have $a^2 = 1$, and the result follows.

2.4 Simplicity of J_C

For $g = 2$, the curve C is the generic curve of genus 2, so its Jacobian is absolutely simple.

For $g = 3$ we specialize the indeterminates, taking for example $v = 2$, $a_1 = 1$, $a_2 = 3$, $a_3 = 4$; the characteristic polynomial of Frobenius for the reduction modulo 13 is

$$y^6 + 2y^5 + 3y^4 + 44y^3 + 39y^2 + 228y + 2197.$$

Its roots are $-(1+2i\cos\frac{5\pi}{7})(1+2i\cos\frac{3\pi}{7})(1+2i\cos\frac{\pi}{7})$ and its conjugates, with $i = \sqrt{-1}$; they generate the field $\mathbb{Q}(i, 2\cos\frac{2\pi}{7})$, whose roots of unity are those of the field $L = \mathbb{Q}(i)$. If the Jacobian were not absolutely simple then there would exist an integer n such that y^n is in L, and then y^n would be equal (up to a root of unity) to $(3 \pm 2i)^n$; therefore, up to a root of unity, y would be an element of L.

For $g \geq 4$, we work recursively on g: Specializing $x_g \to 0$, we find the curve of genus $g-1$ associated with $v, x_1, \ldots, x_{g-1}$; so if J_C is not simple then it must be isogenous to $D \times E$, where D is absolutely simple of dimension $g-1$.

If we specialize v at $\sqrt{-1}$, the curve C admits an automorphism $(x, y) \mapsto (-x, y)$, and is a double covering of the two curves defined by $y^2 = (x+1)(x-x_1^2)\cdots(x-x_g^2)$ and $y^2 = x(x+1)(x-x_1^2)\cdots(x-x_g^2)$, which have genus $g/2$ if g is even and genus $(g-1)/2$ and $(g+1)/2$ otherwise; so J_C is isogenous to the product of their Jacobians, which are generically absolutely simple. This contradicts the fact that J_C is isogenous to $D \times E$; it follows that, when $g \geq 4$, the Jacobian J_C is absolutely simple.

References

[1] J.-B. Bost and J. F. Mestre. *Moyenne arithmético-géometrique et périodes de courbes de genre 1 et 2.* Gaz. Math. Soc. France **38** (1988), 36–64

[2] F. Richelot. *Essai sur une méthode générale pour déterminer la valeur des intégrales ultra-elliptiques, fondée sur des transformations remarquables de ces transcendantes.* C. R. Acad. Sci. Paris **2** (1836), 622–627

[3] F. Richelot. *De transformatione integralium Abelianorum primiordinis commentatio.* J. Reine Angew. Math. **16** (1837), 221–341.