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, the following theorem holds:

**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 $C$, the image of the curves $C$ in the moduli space of hyperelliptic curves of genus $g$ over $C$ 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 \( 1 \leq i \leq g \); 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

\[
p_2(v)p_1(x)q_2(z) - p_1(v)p_2(x)q_1(z) + (a_1p
\]
2.2 The case where \( g \) is odd

To prove the theorem for odd \( g \) it is enough to specialize \( a_0 \to 0 \) 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 \( w(P_2) = P_6 \). Choosing coordinates such that \( u \) maps \( x \to -x \), the involution \( w \) has the form \( x \to f(x) \), which we can bring into the form \( x \to 1/x \) 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 \( h : x \to (ax + b)/(cx + d) \) is a homography such that the set \( A = \{h(v), h(x_1), \ldots, h(x_g), h(-x_1), \ldots, h(-x_g)\} \) is in the form \( \{v, y_1, y_2, \ldots, y_6 \} \), then \( h \) is of the form \( x \to \pm x \) or \( x \to \pm 1/x \).

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 \( x_i, -x_i \) \( \in B \), and if \( b \) is equal to \( v \) or \( 1/v \) then \( \{v, 1/v\} \subseteq B \). 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 \( h(\{v, 1/v\}) = \{v, 1/v, u\} \). But the generic genus 2 curve with automorphism group \( \mathbb{Z}/2\mathbb{Z} \) is in the form \( y^2 = (x^2 - x_1^2)(x^2 - x_2^2)(x^2 - x_3^2) \); its automorphism group formed by the four elements \( (x, y) \to (\pm x, \pm y) \).

Generically, the only involution fixing \( B_2 \) is \( x \to -x \); 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 \( x \to ax \) or \( x \to a/x \).

Since \( u \) maps \( \{v, 1/v\} \) onto \( \{v, 1/v\} \) 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

\[ y^6 + 2y^5 + 3y^4 + 4y^3 + 3y^2 + 28y + 2197. \]

Its roots are \((-1 + 2i \cos \frac{\pi}{6})(1 + 2i \cos \frac{\pi}{6})\) and its conjugates, with \( i = \sqrt{-1} \); they generate the field \( \mathbb{Q}(i, 2\cos \frac{\pi}{6}) \), whose roots of unity are those of the field \( L = \mathbb{Q}(i) \). If the Jacobian were not absolutely simple if and only if 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 \( x_0 \to 0 \), we find the curve of genus \( g - 1 \) associated with \( u, x_1, \ldots, x_{g-1} \); 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 \( (x, y) \to (-x, y) \), and is a double covering of the two curves defined by \( y^2 = (x + 1)(x - x_1^2)(x - x_2^2)(x - x_3^2) \) and \( y^2 = x(x + 1)(x - x_1^2)(x - x_2^2)(x - x_3^2) \), 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

