

# EXPLICIT CONSTRUCTION OF DECOMPOSABLE JACOBIANS

MESUT BUĞDAY AND MOHAMMAD SADEK

**ABSTRACT.** In this note we give explicit constructions of decomposable hyperelliptic Jacobian varieties over fields of characteristic 0. These include hyperelliptic Jacobian varieties that are isogenous to a product of two absolutely simple hyperelliptic Jacobian varieties, a square of a hyperelliptic Jacobian variety, and a product of four hyperelliptic Jacobian varieties three of which are of the same dimension. As an application, we produce families of hyperelliptic curves with infinitely many quadratic twists having at least two rational non-Weierstrass points; and families of quadruples of hyperelliptic curves together with infinitely many square-free  $d$  such that the quadratic twists of each of the curves by  $d$  possess at least one rational non-Weierstrass point.

## 1. INTRODUCTION

An abelian variety is said to be *decomposable* over a field  $K$  if it is isogenous to a product of abelian varieties of lower dimension. The study of decomposable Jacobian varieties of genus two curves was initiated in [7], see also [11]. A family of hyperelliptic curves of arbitrary genus whose Jacobians decompose into two abelian varieties was given in [4], namely, for the Jacobian of the hyperelliptic curve defined by the equation

$$y^2 = (x^n - 1)(x^n - t), \quad n = 2k + 1, \quad k > 1, \quad t \in \mathbb{C} \setminus \{0, 1\},$$

there are two algebraic curves  $Y_1$  and  $Y_2$  of genus  $k$  such that  $\text{Jac}(X)$  is isomorphic to  $\text{Jac}(Y_1) \times \text{Jac}(Y_2)$ . Ekedahl and Serre constructed examples of curves whose Jacobians decompose completely into elliptic curves, [5]. The reader may also see [21] for such examples of curves over number fields. Jacobian varieties of algebraic curves with many automorphisms provide examples of abelian varieties that contain many factors in their decompositions. In [14, 15, 16], such curves whose Jacobians contain many elliptic factors were displayed. In [2], the existence of Jacobians that are isogenous to the product of arbitrary many Jacobians of the same genus, not necessarily equal to one, was established.

In this note, we consider the following question. Given a positive integer  $n$  together with a partition  $n_1 \leq n_2 \leq \dots \leq n_k$  of  $n$ , does there exist a Jacobian variety of dimension  $n$  that decomposes into a product of  $k$  Jacobian varieties of dimensions  $n_1, \dots, n_k$ ? When  $k = 2$  and  $n$  is even, we give explicit examples of families of hyperelliptic Jacobian varieties that decompose into the product of two absolutely simple Jacobian varieties of the same dimension  $n/2$ ; and families

---

**Mathematics Subject Classification 2020:** 14H40, 14H25, 11G30

**Keywords:** Hyperelliptic curves, Jacobians, decomposable abelian varieties, rational points

of hyperelliptic Jacobian varieties that decompose as the square of a Jacobian variety. When  $n$  is odd, we present examples of hyperelliptic Jacobian varieties that decompose into the product of two absolutely simple Jacobian varieties of dimensions  $(n-1)/2$  and  $(n+1)/2$ . We exhibit families of hyperelliptic Jacobians that decompose into the product of three Jacobians of dimensions  $k$ ,  $k+1$ ,  $2k$  when  $n = 4k+1$ ,  $k \geq 1$ ; and  $k+1$ ,  $k+1$ ,  $2k+1$  when  $n = 4k+3$ ,  $k \geq 0$ . Further, we prove the existence of hyperelliptic Jacobian varieties of odd dimension  $n$  that decompose as the product of four Jacobian varieties of dimensions  $k$ ,  $k$ ,  $k$ ,  $k+1$ , when  $n = 4k+1$ ,  $k \geq 1$ ; and  $k$ ,  $k+1$ ,  $k+1$ ,  $k+1$  when  $n = 4k+3$ ,  $k \geq 1$ . In particular, given any integer  $M$ , there is a decomposable Jacobian variety of dimension  $4M \pm 1$  whose decomposition contains three Jacobian factors each of dimension  $M$ .

Goldfeld Conjecture states that the average rank of elliptic curves over the rational field in families of quadratic twists is  $1/2$ . In other words, quadratic twists of an elliptic curve over the rational field with rank at least 2 are rare. In [17, 12], quadratic twists of elliptic curves with ranks at least 2 or 3 were given. A similar problem was posed to find tuples of elliptic curves whose quadratic twists by the same rationals are of positive rank infinitely often, [1, 3, 8]. As for hyperelliptic curves, one may construct families of these curves with infinitely many quadratic twists that possess no rational points, [18, 19, 13]. As a byproduct of our construction of decomposable Jacobian varieties, we produce examples of hyperelliptic curves with infinitely many quadratic twists possessing at least two rational non-Weierstrass points. In particular, we introduce examples of elliptic curves with infinitely many quadratic twists of rank at least 2. In addition, we give examples of families of quadruples of hyperelliptic curves, three of which are of the same genus, such that for infinitely many square-free rationals the quadratic twists of each of these hyperelliptic curves by these rationals possess at least one rational non-Weierstrass point.

**Acknowledgment.** The authors would like to thank the anonymous referee for many suggestions that improved the manuscript. These suggestions include the statement and proof of Theorem 3.3.

This work is supported by The Scientific and Technological Research Council of Turkey, TÜBİTAK, research grant ARDEB 1001/122F312. M. Sadek acknowledges the support of BAGEP Award of the Science Academy, Turkey.

## 2. PRELIMINARIES

Throughout this work  $K$  is a field with  $\text{char } K = 0$  whose algebraic closure is  $\overline{K}$ . The Jacobian variety of a smooth algebraic curve  $C$  will be denoted by  $\text{Jac}(C)$ . If two abelian varieties  $A$  and  $B$  over  $K$  are isogenous, we write  $A \sim B$ .

An abelian variety  $A$  defined over  $K$  is called *simple* if there are no lower dimensional abelian varieties  $B$  and  $C$  over  $K$  such that  $A$  is isogenous to the product  $B \times C$ , otherwise it is called *decomposable*. If  $A$  is simple over  $\overline{K}$ , then it is called *absolutely simple*.

In this note, abusing notation, elliptic curves will be called hyperelliptic curves (of genus 1). Two hyperelliptic curves of genus  $g \geq 2$  described by the following equations

$$y^2 = f(x) \in K[x] \quad \text{and} \quad y^2 = f'(x) \in K[x]$$

are *isomorphic* if and only if

$$x = \frac{ax + b}{cx + d}, \quad y = \frac{ey}{(cx + d)^{g+1}}, \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K), \quad e \in K^*.$$

Given a hyperelliptic curve, one would like to know whether its Jacobian is simple or not.

If  $A$  is an abelian variety defined over  $K$ , we write  $\text{End}(A)$  for the ring of  $\overline{K}$ -endomorphisms of  $A$ . The following results of Zarhin introduce simplicity criteria for certain hyperelliptic Jacobian varieties based on the Galois group of the defining polynomial.

**Theorem 2.1.** *Let  $C$  be a hyperelliptic curve defined by the equation  $y^2 = f(x)$ , where  $f(x)$  is polynomial of degree  $n$  without multiple roots in  $K[x]$ .*

- i) *Assume  $n \geq 5$ . If  $\text{Gal}(f)$  is either the full symmetric group  $S_n$  or the alternating group  $A_n$ , then  $\text{End}(\text{Jac}(C)) = \mathbb{Z}$ . In particular,  $\text{Jac}(C)$  is an absolutely simple abelian variety, see [22].*
- ii) *Assume  $n \geq 6$  is even. If  $f(x) = (x - t)h(x)$  with  $t \in K$  and  $h(x) \in K[x]$ , is such that  $\text{Gal}(h)$  is either  $S_{n-1}$  or  $A_{n-1}$ , then  $\text{End}(\text{Jac}(C)) = \mathbb{Z}$ . In particular,  $\text{Jac}(C)$  is an absolutely simple abelian variety, see [23].*
- iii) *Assume  $n \geq 9$  is odd. If  $f(x) = (x - t)h(x)$  with  $t \in K$  and  $h(x) \in K[x]$ , is such that  $\text{Gal}(h)$  is either  $S_{n-1}$  or  $A_{n-1}$ , then  $\text{Jac}(C)$  is an absolutely simple abelian variety, see [23].*

The following result, [6, Theorem 8] introduces a method to construct absolutely simple varieties over number fields.

**Proposition 2.2.** *Let  $K$  be a number field. Let  $g \geq 1$  be an integer, and let  $f \in K[x]$  be a polynomial of degree  $2g$  with no multiple roots. Consider the hyperelliptic curve of genus  $g$  over  $K(T)$  defined by  $C_T : y^2 = f(x)(x - T)$ . Then there are only finitely many  $t \in K$  such that the Jacobian of  $C_t$  is not absolutely simple.*

### 3. DECOMPOSITION INTO TWO ABELIAN SUBVARIETIES

Let  $C$  be a hyperelliptic curve over  $K$  with hyperelliptic involution  $\iota$  giving rise to the morphism  $C \rightarrow C/\langle \iota \rangle \cong \mathbb{P}^1$ . We assume that  $C$  possesses an automorphism  $\sigma$  of order 2 such that  $\sigma \neq \iota$ . We set  $\tau = \sigma \circ \iota$ . Writing  $C_\sigma$  and  $C_\tau$  for  $C/\langle \sigma \rangle$  and  $C/\langle \tau \rangle$  respectively, we obtain the quotient morphisms  $\phi_\sigma : C \rightarrow C_\sigma$  and  $\phi_\tau : C \rightarrow C_\tau$  respectively. This yields a morphism  $\phi = (\phi_\sigma, \phi_\tau) : C \rightarrow C_\sigma \times C_\tau$ , hence a morphism  $\text{Jac}(C) \rightarrow \text{Jac}(C_\sigma) \times \text{Jac}(C_\tau)$ . This morphism is an isogeny, [9], in fact, it is a decomposed Richelot isogeny.

**Lemma 3.1.** [10, Theorem 1] *Let  $C$  be a hyperelliptic curve with an automorphism  $\sigma$  of order 2, which is not the hyperelliptic involution. We set  $\tau = \sigma \circ \iota$  where  $\iota$  is the hyperelliptic involution on  $C$ . Then, the isogeny  $\text{Jac}(C) \rightarrow \text{Jac}(C_\sigma) \times \text{Jac}(C_\tau)$  is a decomposed Richelot isogeny.*

In this work, we give special attention to the hyperelliptic curve defined by  $y^2 = f(x^2)$  where  $f(x) \in K[x]$  has no multiple roots.

**Proposition 3.2.** *Let  $f(x) \in K[x] \setminus xK[x]$  have no multiple roots. Define the following hyperelliptic curves over  $K$*

$$C_f : y^2 = f(x^2), \quad E_f : y^2 = f(x), \quad H_f : y^2 = xf(x).$$

*Then  $\text{Jac}(C_f) \sim \text{Jac}(E_f) \times \text{Jac}(H_f)$ .*

PROOF: We write  $\sigma$  for the automorphism  $(x, y) \mapsto (-x, y)$  on  $C_f$ . The automorphism  $\sigma$  is of order 2. The map  $\phi_\sigma : C_f \rightarrow E_f$  defined by  $\phi_\sigma : (x, y) \mapsto (x^2, y)$  is the quotient map  $C_f \rightarrow C_f/\langle\sigma\rangle \cong E_f$ . Similarly, if we set  $\tau = \sigma \circ \iota$ , then  $\phi_\tau : C_f \rightarrow H_f$  defined by  $\phi_\tau : (x, y) \mapsto (x^2, xy)$  is the quotient map  $C_f \rightarrow C_f/\langle\tau\rangle \cong H_f$ .  $\square$

For an abelian variety  $A$  defined over  $K$ , we set

$$\text{End}^0(A) := \text{End}(A) \otimes \mathbb{Q}$$

to be the corresponding endomorphism algebra of  $A$ , which is a semisimple algebra over the field of rational numbers  $\mathbb{Q}$ .

**Theorem 3.3.** *Let  $K$  be a field of characteristic 0 with algebraic closure  $\overline{K}$ . Let  $f(x) \in K[x]$  be an irreducible polynomial of even degree  $n \geq 8$  such that its Galois group is either the full symmetric group  $S_n$  or the alternating group  $A_n$ . Consider the hyperelliptic curve of genus  $n - 1$  defined by the equation  $y^2 = f(x^2)$  over  $K$ .*

*Then  $\text{Jac}(C_f)$  is isogenous to a product of absolutely simple Jacobian varieties,  $A$  and  $B$ , of hyperelliptic curves of genus  $(n/2 - 1)$  and  $n/2$  respectively. In addition,  $\text{End}(A) = \mathbb{Z}$  and  $\text{End}(B) = \mathbb{Z}$ . In particular,  $\text{End}^0(\text{Jac}(C_f))$  is isomorphic to  $\mathbb{Q} \oplus \mathbb{Q}$ .*

PROOF: Since  $f(x)$  is irreducible and  $\deg(f) > 1$ , one has  $f(0) \neq 0$ . By Proposition 3.2, there is an isogeny of abelian varieties  $\text{Jac}(C_f) \sim \text{Jac}(E_f) \times \text{Jac}(H_f)$  where  $E_f$  and  $H_f$  are defined as in Proposition 3.2. Moreover, the abelian varieties  $\text{Jac}(E_f)$  and  $\text{Jac}(H_f)$  are of (distinct) dimensions  $(n/2 - 1)$  and  $n/2$ , respectively. In particular,  $\text{Jac}(E_f)$  and  $\text{Jac}(H_f)$  are not isogenous. By Theorem 2.1,  $\text{Jac}(E_f)$  and  $\text{Jac}(H_f)$  are absolutely simple. In addition, both endomorphism rings  $\text{End}(\text{Jac}(E_f))$  and  $\text{End}(\text{Jac}(H_f))$  are the ring of integers  $\mathbb{Z}$ . Since  $\text{Jac}(E_f)$  and  $\text{Jac}(H_f)$  are not isogenous, it follows that the endomorphism algebra of the product  $\text{Jac}(E_f) \times \text{Jac}(H_f)$  is isomorphic to  $\mathbb{Q} \oplus \mathbb{Q}$ . Now, since the abelian varieties  $\text{Jac}(C_f)$  and  $\text{Jac}(E_f) \times \text{Jac}(H_f)$  are isogenous, their endomorphism algebras are isomorphic. Therefore, the endomorphism algebra of  $\text{Jac}(C_f)$  is also isomorphic to  $\mathbb{Q} \oplus \mathbb{Q}$ .  $\square$

**Proposition 3.4.** *Let  $f(x) \in K[x]$  be of degree  $n$  such that  $\text{Gal}_K(f) = S_n$  or  $A_n$ . Let  $C_f, E_f$  and  $H_f$  be as in Proposition 3.2.*

*If  $n = 2g + 1 \geq 5$ , then  $\text{Jac}(C_f) \sim \text{Jac}(E_f) \times \text{Jac}(H_f)$ , where both  $\text{Jac}(E_f)$  and  $\text{Jac}(H_f)$  are absolutely simple of dimension  $g$ .*

*If  $n = 2g + 2 \geq 8$ , then  $\text{Jac}(C_f) \sim \text{Jac}(E_f) \times \text{Jac}(H_f)$ , where both  $\text{Jac}(E_f)$  and  $\text{Jac}(H_f)$  are absolutely simple of dimension  $g$  and  $g + 1$ , respectively.*

PROOF: The statement follows from Proposition 3.2 and Theorem 2.1.  $\square$

**Theorem 3.5.** *Let  $K$  be a number field. Given any integer  $n \geq 2$ , there exist infinitely many hyperelliptic curves of genus  $n$  with Jacobian varieties that are isogenous over  $K$  to the product of two absolutely simple Jacobian varieties of hyperelliptic curves of genus  $n/2$  and  $n/2$  if  $n$  is even; and  $(n-1)/2$  and  $(n+1)/2$  if  $n$  is odd.*

PROOF: The statement holds in view of Proposition 3.4 for any integer  $n$  except possibly 2, 3 and 5. A hyperelliptic curve with genus two whose Jacobian splits can be constructed easily using Proposition 3.2. For example, one may consider the curve  $y^2 = f(x^2)$  where  $f(x) \in K[x] \setminus xK[x]$  is a polynomial of degree 3 with no multiple roots.

Let  $f(x)$  be a polynomial of degree  $d = 4$ ; or of degree  $d = 6$  with Galois group either  $A_6$  or  $S_6$ . The Jacobian of the curve  $y^2 = f(x)$  is absolutely simple. This is justified by the fact that the Jacobian is an elliptic curve when  $d = 4$ ; or it is an absolutely simple Jacobian of a genus two curve when  $d = 6$ , see Theorem 2.1. Now, for all but finitely many  $t \in K$ , the Jacobian of the curve  $y^2 = (x-t)f(x)$  is absolutely simple, see Proposition 2.2. For each such value of  $t$  such that  $t$  is not a root of  $f$ , we consider the curves  $y^2 = g_t(x) = f(x+t)$  and  $y^2 = xg_t(x)$ . The latter curves are of genus 1 and 2, respectively, when  $d = 4$ ; or of genus 2 and 3, respectively, when  $d = 6$ , with absolutely simple Jacobians. In addition, the Jacobian of the curve  $y^2 = g_t(x^2) = f(x^2+t)$  is of dimension 3 when  $d = 4$ ; or of dimension 5 when  $d = 6$ , for any such  $K$ -rational value  $t$ ; and it enjoys the required splitting property, see Proposition 3.2.  $\square$

The following proposition indicates that given a polynomial in  $K[x]$  of degree  $n$  with no multiple roots, one may construct an infinite sequence of hyperelliptic curves of any genus  $\geq n-1$  whose Jacobian varieties decompose into two hyperelliptic Jacobian varieties whose dimensions differ by at most 1.

**Proposition 3.6.** *Let  $f(x) \in K[x] \setminus xK[x]$  be a polynomial with no multiple roots. Define the following sequence of polynomials*

$$\begin{aligned} f_0(x) &= f(x), \\ g_i(x) &= xf_i(x), \quad i \geq 0, \\ f_i(x) &= g_{i-1}(x + a_{i-1}), \quad a_{i-1} \text{ is not a root of } g_{i-1}(x), \quad i \geq 1. \end{aligned}$$

Setting  $H_{-1} : y^2 = f(x)$ ,  $H_i : y^2 = g_i(x)$  and  $C_i : y^2 = f_i(x^2)$ , one has  $\text{Jac}(C_i) \sim \text{Jac}(H_{i-1}) \times \text{Jac}(H_i)$ ,  $i \geq 0$ .

If  $\deg f = 2g + 1$ , then  $H_{i-1}$ ,  $H_i$  and  $C_i$  are of genus  $g + i/2$ ,  $g + i/2$  and  $2g + i$ , respectively, when  $i$  is even; and of genus  $g + r$ ,  $g + r + 1$ ,  $2g + i$ , respectively, when  $i = 2r + 1$  is odd.

If  $\deg f = 2g + 2$ , then  $H_{i-1}$ ,  $H_i$  and  $C_i$  are of genus  $g + i/2$ ,  $g + i/2 + 1$ ,  $2g + i + 1$ , respectively, when  $i$  is even; and of genus  $g + r + 1$ ,  $g + r + 1$ ,  $2g + i + 1$ , respectively, when  $i = 2r + 1$  is odd.

PROOF: Observing that  $E_i : y^2 = f_i(x)$  and  $H_{i-1}$ ,  $i \geq 1$ , are isomorphic hyperelliptic curves, the proof follows directly from Proposition 3.2.  $\square$

In a similar fashion, we note that the construction of the genus 3 and 5 curves using Proposition 2.2 in the proof of Theorem 3.5 can be used to provide an alternative way of constructing families

of hyperelliptic curves of genus  $2n + 1 \geq 5$  whose Jacobians decompose into the product of two absolutely simple abelian varieties of dimensions  $n$  and  $n + 1$ . In addition, the defining polynomials of these curves are essentially multiples of a fixed polynomial of even degree with no multiple roots.

Given a polynomial  $f \in K[x]$  of even degree with no multiple roots, we set

$$S(f) = \{t \in K : \text{the Jacobian of } y^2 = (x - t)f(x) \text{ is not absolutely simple; or } t \text{ is a root of } f(x)\}.$$

By Proposition 2.2,  $S(f)$  is finite.

**Corollary 3.7.** *Let  $K$  be a number field. Let  $f(x) \in K[x] \setminus xK[x]$  be a polynomial of degree  $2g$ ,  $g \geq 1$ , with no multiple roots. Define the following sequence of polynomials*

$$\begin{aligned} f_0(x) &:= f(x), & g_{0,t_0}(x) &:= xf_0(x + t_0), \quad t_0 \notin S(f_0), \\ f_{i,t_{i-1}}(x) &:= (x + r'_{i,t_{i-1}})^{2g+2} g_{i-1,t_{i-1}} \left( \frac{x + r_{i,t_{i-1}}}{x + r'_{i,t_{i-1}}} \right), \quad r_{i,t_{i-1}} \neq r'_{i,t_{i-1}}, & g_{i,t_i}(x) &:= xf_{i,t_{i-1}}(x + t_i), \quad t_i \notin S(f_{i,t_{i-1}}), \quad i \geq 1, \end{aligned}$$

where  $r_{i,t_{i-1}}$  and  $r'_{i,t_{i-1}}$  are chosen so that  $f_{i,t_{i-1}}(x) \in K[x] \setminus xK[x]$ .

Setting  $H_{i,t_i} : y^2 = g_{i,t_i}(x)$ , and  $C_{i,t_{i-1}} : y^2 = f_{i,t_{i-1}}(x^2 + t_i)$ , then  $\text{Jac}(C_{i,t_{i-1}}) \sim \text{Jac}(H_{i-1,t_{i-1}}) \times \text{Jac}(H_{i,t_i})$ , where  $\text{Jac}(H_{i-1,t_{i-1}})$  is absolutely simple for  $i \geq 1$ . The genus of the curves  $H_{i,t_i}$  and  $C_{i,t_{i-1}}$  are  $g + i$  and  $2g + 2i - 1$ , respectively.

PROOF: We remark that the polynomial  $f_{i,t_{i-1}}$  is of even degree. The statement holds in view of Proposition 2.2 and Proposition 3.2 as the curves  $H_{i-1,t_{i-1}}$  and  $E_{i,t_{i-1}} : y^2 = f_{i,t_{i-1}}(x)$  are isomorphic hyperelliptic curves.  $\square$

#### 4. FAMILIES OF DECOMPOSABLE HYPERELLIPTIC JACOBIAN VARIETIES

We recall that  $K$  is a field with  $\text{char } K = 0$ . We start this section with the following definition.

**Definition 4.1.** A polynomial  $f(x) \in K[x]$  is said to be *palindromic* if  $f(x) = x^d f(1/x)$  where  $d = \deg f$ , i.e., if  $f(x) = \sum_{i=0}^d a_i x^i$ , then  $a_i = a_{d-i}$  for  $0 \leq i \leq d$ .

We write  $C_2$ ,  $V_4$  and  $D_4$  for the cyclic group with 2 elements, the Klein-4 group, and the dihedral group with 8 elements, respectively.

**Proposition 4.2.** *Let  $f(x) \in K[x]$  be an even palindromic polynomial of degree  $2g + 2$  with no multiple roots.*

- i) *If  $C : y^2 = f(x)$ , then  $D_4 \hookrightarrow \text{Aut}(C)$ , when  $g$  is even.*
- ii) *If  $C : y^2 = f(x)$ , then  $C_2 \times C_2 \times C_2 \hookrightarrow \text{Aut}(C)$ , when  $g$  is odd.*
- iii) *If  $C' : y^2 = xf(x)$ , then  $V_4 \hookrightarrow \text{Aut}(C')$ .*

PROOF: We write  $f(x) = a_{2g+2}x^{2g+2} + a_{2g}x^{2g} + \cdots + a_2x^2 + a_0$ , where  $a_{2i} = a_{2g+2-2i}$ ,  $0 \leq i \leq g+1$ . For i) and ii) apart from the hyperelliptic involution, the curve  $C$  has the following automorphisms of order 2

$$\sigma : (x, y) \mapsto (-x, y) \quad \text{and} \quad \tau : (x, y) \mapsto \left( \frac{1}{x}, \frac{y}{x^{g+1}} \right).$$

We note that  $\sigma^2 = \tau^2$ . Moreover,  $(\sigma \circ \tau)^2 = \iota$  when  $g$  is even. It follows that the group generated by  $\sigma$  and  $\tau$  is isomorphic to the dihedral group  $D_4$ . Specifically, if we fix a representation  $D_4 := \langle a, b \mid a^2 = b^2 = (ab)^4 = 1 \rangle$ , then we have the following inclusion

$$D_4 \hookrightarrow \text{Aut}(C); \quad a \mapsto \sigma, \quad b \mapsto \tau.$$

ii) follows in a similar fashion by observing that  $\sigma \circ \tau$  is an automorphism of order 2 when  $g$  is odd.

For iii) one may check that the map

$$\sigma : C' \rightarrow C' : \quad (x, y) \mapsto \left( \frac{1}{x}, \frac{y}{x^{g+2}} \right)$$

is an automorphism of  $C'$ , see §2, of order 2. The automorphisms  $\iota, \sigma, \sigma \circ \iota, 1$  form a subgroup of  $\text{Aut}(C')$  isomorphic to the Klein 4-group,  $V_4$ .  $\square$

If  $f(x) = a_{2g+2}x^{2g+2} + a_{2g}x^{2g} + \cdots + a_2x^2 + a_0 \in K[x]$  is an even palindromic polynomial with no multiple roots, we write  $f_h(x) = a_{2g+2}x^{g+1} + a_{2g}x^g + \cdots + a_2x + a_0$ . We notice that  $f_h(x)$  is a palindromic polynomial itself. We, moreover, set  $F_h(x, y) = a_{2g+2}x^{g+1} + a_{2g}x^g y + \cdots + a_2x y^g + a_0 y^{g+1}$ .

**Theorem 4.3.** *Let  $f(x) = a_{2g+2}x^{2g+2} + a_{2g}x^{2g} + \cdots + a_2x^2 + a_0 \in K[x]$  be an even palindromic polynomial with no multiple roots. Let  $f_h(x) = a_{2g+2}x^{g+1} + a_{2g}x^g + \cdots + a_2x + a_0$ . Assume, moreover, that  $C : y^2 = f(x)$  and  $E : y^2 = f_h(x)$ .*

- i) *If  $g \geq 2$  is even, then  $\text{Jac}(C) \sim (\text{Jac}(E))^2$ .*
- ii) *If  $g \geq 3$  is odd, then  $\text{Jac}(C) \sim \text{Jac}(E) \times \text{Jac}(G_1) \times \text{Jac}(G_2)$  where  $G_1 : y^2 = p(x)$  and  $G_2 : y^2 = xp(x)$ , and  $p(x) \in K[x]$  is such that  $p(x^2) = (x^2 - 1)F_h(x + 1, x - 1)$ .*

PROOF: One observes that  $\text{Jac}(C) \sim \text{Jac}(E) \times \text{Jac}(H)$ , where  $H$  is defined by  $y^2 = x f_h(x)$ , see Proposition 3.2.

If  $g = 2k$ , then  $E$  and  $H$  are isomorphic hyperelliptic curves via the transformation

$$H \longrightarrow E, \quad (x, y) \mapsto \left( \frac{1}{x}, \frac{y}{x^{k+1}} \right),$$

see §2, hence the result.

If  $g = 2k + 1$ , then we consider the map

$$H \longrightarrow G, \quad (x, y) \mapsto \left( \frac{x+1}{x-1}, \frac{y}{(x-1)^{k+2}} \right)$$

where  $G : y^2 = \ell(x)$ . One obtains that

$$\ell(x) = (x^2 - 1) \left( a_{2g+2}(x+1)^{2k+2} + a_{2g}(x+1)^{2k+1}(x-1) + \cdots + a_2(x+1)(x-1)^{2k+1} + a_0(x-1)^{2k+2} \right),$$

hence  $\ell(-x) = \ell(x)$ , and  $\ell$  is an even polynomial of degree  $2k + 4$ . It follows that  $\ell(x) = p(x^2)$  for some  $p(x) \in K[x]$ . In view of Proposition 3.2,  $\text{Jac}(G) \sim \text{Jac}(G_1) \times \text{Jac}(G_2)$ , where  $G_1 : y^2 = p(x)$  and  $G_2 : y^2 = xp(x)$ .  $\square$

**Remark 4.4.** In Proposition 4.2, The curve  $C' : y^2 = xf(x)$  possesses the automorphisms  $\sigma$  and  $\sigma \circ \iota$  described by  $(x, y) \mapsto \left(\frac{1}{x}, \frac{\pm y}{x^{g+2}}\right)$ . In Theorem 4.3, the curve  $C'$  is described using a different equation, namely,  $y^2 = p(x^2)$  where the two aforementioned automorphisms are now  $(x, y) \mapsto (-x, \pm y)$ . Therefore,  $C'/\langle\sigma\rangle$  and  $C'/\langle\sigma \circ \iota\rangle$  are isomorphic to the hyperelliptic curves defined by  $y^2 = p(x)$  and  $y^2 = xp(x)$ .

**Corollary 4.5.** i) *For any integer  $n \geq 1$ , there exist hyperelliptic curves of genus  $2n$  whose Jacobian varieties are isogenous over  $K$  to the square of the Jacobian of a hyperelliptic curve of genus  $n$ .*  
ii) *For any integer  $n \geq 1$ , there exist hyperelliptic curves of genus  $2n + 1$  whose Jacobian varieties are isogenous over  $K$  to the product of three Jacobian varieties of hyperelliptic curves of genus  $n$ ,  $(n + 1)/2$ , and  $(n + 1)/2$  if  $n$  is odd; and  $n$ ,  $1 + n/2$ , and  $n/2$  if  $n$  is even.*

**Remark 4.6.** We remark that Proposition 3.2 may be used to construct hyperelliptic Jacobian varieties of dimension  $2n + 1$  that decompose into three Jacobian varieties of lower dimensions, namely,  $n + 1$ ,  $(n + 1)/2$ ,  $(n - 1)/2$  if  $n$  is odd; and  $n + 1$ ,  $n/2$ ,  $n/2$  if  $n$  is even; which differs from the partitions of the dimension given in Corollary 4.5. In addition, Proposition 3.2 does not provide a decomposable Jacobian variety whose dimension is 3.

**Example 4.7.** If we consider the curve

$$C : y^2 = ax^6 + bx^4 + bx^2 + a \in K[x],$$

then  $\text{Jac}(C) \sim E^2$  where  $E$  is the elliptic curve  $y^2 = ax^3 + bx^2 + bx + a$ .

**Example 4.8.** In Theorem 4.3, if one considers the curve

$$C : y^2 = ax^8 + bx^6 + cx^4 + bx^2 + a \in K[x]$$

of genus 3, then  $\text{Jac}(C)$  is isogenous to the product of three elliptic curves that are the Jacobians of the following genus 1 curves

$$\begin{aligned} E_1 : y^2 &= ax^4 + bx^3 + cx^2 + bx + a, \\ E_2 : y^2 &= (2a + 2b + c)x^3 + (10a - 2b - 3c)x^2 + (-10a - 2b + 3c)x + (-2a + 2b - c), \\ E_3 : y^2 &= x \left( (2a + 2b + c)x^3 + (10a - 2b - 3c)x^2 + (-10a - 2b + 3c)x + (-2a + 2b - c) \right). \end{aligned}$$

**Proposition 4.9.** *Let  $f(x) \in K[x]$  be a palindromic polynomial of degree at least 3. Consider the hyperelliptic curve  $C : y^2 = f(x^4)$ . Then  $\text{Jac}(C) \sim \text{Jac}(E_1) \times \text{Jac}(E_2) \times \text{Jac}(G_1) \times \text{Jac}(G_2)$ , where  $E_1 : y^2 = f(x)$ ,  $E_2 : y^2 = xf(x)$ , and  $G_1$  and  $G_2$  are as in Theorem 4.3.*

PROOF: In view of Theorem 4.3, one has  $\text{Jac}(C) \sim \text{Jac}(E) \times \text{Jac}(G_1) \times \text{Jac}(G_2)$  where  $E : y^2 = f(x^2)$ . Now due to Proposition 3.2, one obtains that  $\text{Jac}(E) \sim \text{Jac}(E_1) \times \text{Jac}(E_2)$ .  $\square$

**Corollary 4.10.** *Given any integer  $n \geq 2$ , there exist hyperelliptic curves of genus  $2n + 1$  whose Jacobian varieties are isogenous over  $K$  to the product of four Jacobian varieties of hyperelliptic*



curves of genus  $(n-1)/2$ ,  $(n+1)/2$ ,  $(n+1)/2$ , and  $(n+1)/2$  if  $n$  is odd; and  $n/2$ ,  $n/2$ ,  $n/2$ , and  $1+n/2$  if  $n$  is even.

**Example 4.11.** The Jacobian of the hyperelliptic curve  $y^2 = ax^{12} + bx^8 + bx^4 + a$  is isogenous to the product of the elliptic curves that are Jacobians of the genus one curves  $E_1$ ,  $E_2$ ,  $G_1$ ; and the Jacobian of the genus 2 curve  $G_2$

$$\begin{aligned} E_1 : y^2 &= ax^3 + bx^2 + bx + a, \\ E_2 : y^2 &= x(ax^3 + bx^2 + bx + a), \\ G_1 : y^2 &= 2(a+b)x^4 + 2(14a-2b)x^3 + 2(-14a+2b)x + 2(-a-b), \\ G_2 : y^2 &= x\left(2(a+b)x^4 + 2(14a-2b)x^3 + 2(-14a+2b)x + 2(-a-b)\right). \end{aligned}$$

## 5. RATIONAL POINTS ON QUADRATIC TWISTS

In this section, given any integer  $g \geq 1$ , we construct a hyperelliptic curve of genus  $g$  with infinitely many quadratic twists containing at least two  $K$ -rational non-Weierstrass points.

**Proposition 5.1.** *Let  $f(x) = a_{2g+2}x^{g+1} + a_{2g}x^g + \cdots + a_2x + a_0 \in K[x]$  be a palindromic polynomial with no multiple roots. Consider the curve  $C : y^2 = f(x)$ . If  $g$  is even, then there exists infinitely many quadratic twists of  $C$  with at least two  $K$ -rational non-Weierstrass points.*

PROOF: Consider the curve  $C_{f(t^2)}$  defined over  $K(t)$  by

$$f(t^2)y^2 = f(x).$$

The set of rational points of  $C_{f(t^2)}$  contains the  $K(t)$ -rational points  $(t^2, 1)$  and  $(\frac{1}{t^2}, \frac{1}{t^{2k+1}})$  where  $g = 2k$ . We remark that these points are obtained by considering the quotient maps in 4.3 i).  $\square$

In the previous proposition, if  $g = 2$ , then  $C$  is a genus 1 curve. Over a number field  $K$ , this implies the existence of infinitely many quadratic twists of  $C$  that are elliptic curves with Mordell-Weil rank at least 2. That the points are of infinite order follow from Silverman Specialization Theorem, [20, Theorem 20.3], whereas the independence of the points follow from the fact that the quotient maps in Theorem 4.3 are independent maps by construction.

In what follows, we concern ourselves with the construction of tuples of hyperelliptic curves  $C_1, \dots, C_n$  and infinitely many square-free  $K$ -rational  $d$  such that the quadratic twists of these curves by each  $d$  contain  $K$ -rational non-Weierstrass points.

**Proposition 5.2.** *Let  $f(x) \in K[x]$  be a palindromic polynomial of degree at least 3 with no multiple roots. Consider the curves  $E_1 : y^2 = f(x)$ ,  $E_2 : y^2 = xf(x)$ ,  $G_1 : y^2 = p(x)$  and  $G_2 : y^2 = xp(x)$ , where  $p(x)$  is defined as in Theorem 4.3. There exists infinitely many nonzero  $d \in K \setminus K^2$  such that the quadratic twists of  $E_1$ ,  $E_2$ ,  $G_1$  and  $G_2$  by  $d$  contain  $K$ -rational non-Weierstrass points.*

PROOF: We set  $n := \deg f$ . We will list down the quadratic twists together with the  $K$ -rational points on them

$$\begin{aligned} f(t^4)y^2 &= f(x), & (t^4, 1), \\ f(t^4)y^2 &= xf(x), & \left(\frac{1}{t^4}, \frac{1}{t^{2n+2}}\right), \\ f(t^4)y^2 &= p(x), & \left(\frac{(t^2+1)^2}{(t^2-1)^2}, \frac{2^{n+1}t}{(t^2-1)^{n+1}}\right), \\ f(t^4)y^2 &= xp(x), & \left(\frac{(t^2+1)^2}{(t^2-1)^2}, \frac{2^{n+1}t(t^2+1)}{(t^2-1)^{n+2}}\right). \end{aligned}$$

These  $K$ -rational points are obtained using the quotient maps in Proposition 4.9.  $\square$

In Proposition 5.2, if  $f$  is chosen to be of degree 3, then the proposition presents an example of three elliptic curves together with a genus 2 curve such that there are infinitely many  $d$  for which the quadratic twists of these curves by such a  $d$  has at least one  $K$ -rational point. Moreover, if  $K$  is a number field, these rational points are of infinite order on the quadratic twists of the elliptic curves, and it is a  $K$ -rational non-Weierstrass point on the genus two curve.

#### REFERENCES

- [1] M. Alaa and M. Sadek, High rank quadratic twists of pairs of elliptic curves, *Journal of Number Theory*, **174** (2017), 436–444.
- [2] A. Carocca, H. Lange and R. E. Rodríguez, Decomposable Jacobians, *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)* **XXII** (2021), 1673–1690.
- [3] G. Coogan and J. Jimenez-Urroz, Mordell–Weil ranks of quadratic twists of pairs of elliptic curves, *J. Number Theory*, **96** (2002), 388–399.
- [4] C. J. Earle, Some Jacobian varieties which split, *Lecture Notes in Mathematics*, **747** (1978), 101–107.
- [5] T. Ekedahl, J.-P. Serre, Exemples de courbes algébriques à jacobienne complètement décomposable. *C. R. Acad. Sci.* **317** (1993), Sér. I, 509–513.
- [6] J. S. Ellenberg, C. Elsholtz, C. Hall, and E. Kowalski, Non-simple abelian varieties in a family: geometric and analytic approaches, *Journal of the London Mathematical Society*, **80.1** (2009): 135–154.
- [7] T. Hayashida and M. Nishi, Existence of curves of genus two on a product of two elliptic curves, *J. Math. Soc. Japan*, **17** (1965), 1–16.
- [8] B.-H. Im, Positive rank quadratic twists of four elliptic curves, *J. Number Theory*, **133** (2013), 492–500.
- [9] E. Kani and M. Rosen, Idempotent relations and factors of Jacobians, *Math. Ann.*, **284** (1989), 307–327.
- [10] T. Katsura and K. Takashima, Decomposed Richelot isogenies of Jacobian varieties of hyperelliptic curves and generalized Howe curves, preprint, <https://arxiv.org/pdf/2108.06936>.
- [11] R. M. Kuhn, Curves of genus 2 with split Jacobian, *Transactions of the American Mathematical Society*, **307** (1988), 41–49.
- [12] M. Kuwata, Quadratic twists of an elliptic curve and maps from a hyperelliptic curve, *Mathematical Journal of Okayama University*, **47.1** (2005), 85–98.
- [13] F. Legrand, Twists of superelliptic curves without rational points, *Int. Math. Res. Not.*, (2018), 1153–1176.
- [14] J. Paulhos, *Decomposing Jacobians of curves with extra automorphisms*, *Acta Arith.*, **132** (2008), 231–244.
- [15] J. Paulhus, Elliptic factors in Jacobians of hyperelliptic curves with certain automorphism groups, *The Open Book Series* **1.1** (2013), 487–505.

- [16] J. Paulhus and A. M. Rojas, Completely decomposable Jacobian varieties in new genera, *Experimental Mathematics*, **26** (2017), 430–445.
- [17] K. Rubin and A. Silverberg, Rank frequencies for quadratic twists of elliptic curves, *Exp. Math.*, **10** (2001), 559–569.
- [18] M. Sadek, On Quadratic Twists of Hyperelliptic Curves, *Rocky Mountain Journal of Mathematics*, **44** (2014), 1015–1026.
- [19] M. Sadek, Minimal Regular Models of Quadratic Twists of Genus Two Curves, *Acta Arithmetica*, **183** (2018), 317–337.
- [20] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, GTM 106, 2nd Edition, Springer, 2009.
- [21] T. Yamauchi, On curves with split Jacobians, *Communications in Algebra*, **36** (2008), 1419–1425.
- [22] Y. G. Zarhin, Hyperelliptic jacobians without complex multiplication, *Mathematical Research Letters*, **7** (2000), 123–132.
- [23] Y. G. Zarhin, Families of absolutely simple hyperelliptic Jacobians, *Proceedings of the London Mathematical Society*, **100.1** (2010), 24–54.

FACULTY OF ENGINEERING AND NATURAL SCIENCES, SABANCI UNIVERSITY, TUZLA, İSTANBUL, 34956 TURKEY  
*Email address:* mesut.bugday@sabanciuniv.edu

*Email address:* mohammad.sadek@sabanciuniv.edu